Vergunningverlening en digitale veiligheid van bedrijven

Een verkenning van lokale handelingsperspectieven

08-03-2024

Mr. Suzanna Twickler, mr. Denise de Boer & dr. Willem Bantema

THORBECKE ACADEMIE

NHL STENDEN

Inhoudsopgave

Samenvatting

Digitale onveiligheid van bedrijven en evenementen krijgt steeds meer aandacht, mede vanwege de mogelijke maatschappelijke gevolgen die verwezenlijking van die risico's met zich meebrengt. Tot op heden ontbreekt het burgemeesters en voorzitters van veiligheidsregio's aan bestuursrechtelijke mogelijkeden om digitale risico's bij bedrijven en evenementen te voorkomen of te beperken. In dit rapport wordt onderzocht in hoeverre burgemeesters, of andere gemeentelijke bestuursorganen, de digitale veiligheid van bedrijven kunnen regelen middels vergunningen. Daartoe staat de volgende hoofdvraag centraal:

> Hoe kunnen gemeenten en medeoverheden de digitale veiligheid binnen gemeenten vergroten door aandacht te besteden aan digitale veiligheid bij vergunningverlening bij bedrijven die binnen de gemeente gevestigd zijn of zich willen vestigen?

Het onderzoek is uitgevoerd middels juridische analyse- en bronnenonderzoek en een empirisch deel waarbij interviews en een focusgroep zijn gehouden.

Digitale risico's kunnen worden onderscheiden in vier typen: kwetsbaarheid van informatie, kwetsbaarheid van systemen, gedigitaliseerde criminaliteit en online aangejaagde ordeverstoringen. Vooral de eerste twee typen zijn van belang voor dit onderzoek. Deze risico's kunnen op verschillende manieren leiden tot verstoringen van de openbare orde, digitale ontwrichting of gevolgen voor de fysieke leefomgeving. De mate van die verstoring is niet inherent verbonden aan de aard of omvang van een organisatie of evenement, al kan de aard en omvang wel bijdragen aan het risicobeeld (denk daarbij aan vitale processen of Seveso-inrichtingen). Bedrijven handelen veelal in ketens, waarbij organisaties binnen die ketens vatbaar kunnen zijn voor aanvallen die gevolgen hebben voor de rest van de keten. Dit maakt dat het risicobeeld van één bedrijf in een keten directe impact kan hebben op andere bedrijven in de keten.

De vraagstukken rond digitale veiligheid staan hoog op de agenda bij overheden. Door de Europese Unie zijn wetgevingsinstrumenten ontwikkeld die zien op beveiliging van netwerk- en informatiesystemen, de bescherming van persoonsgegevens en meer recent de digitale beveiliging van bepaalde (vitale) sectoren en bedrijven die daaraan leveren (NIS2-richtlijn). Deze wetgevingsinstrumenten bieden, voor zover al geïmplementeerd, geen gemeentelijke bevoegdheden. De oogmerken van de Omgevingswet, Gemeentewet en de reikwijdte van de Algemene Plaatselijke Verordening zouden mogelijkheden kunnen bieden voor gemeentelijke invulling.

Daartoe is van belang dat gemeenten een regelgevende bevoegdheid hebben ten aanzien van zaken die binnen hun huishouding vallen, die niet mag indruisen tegen hogere regelgeving. Binnen het gemeentelijke vergunningstelsel zijn in veel gevallen mogelijkheden geboden voor het stellen van maatwerkregels of -voorschriften. De reikwijdte van die bevoegdheid wordt beperkt door de oogmerken waar die wet- en regelgeving op is gebaseerd. De bevoegheid tot het stellen van dergelijke regels of voorschriften mag niet worden ingezet voor een ander doel dan waarvoor deze is verleend. In veel gevallen zien die oogmerken op veiligheid en/of gevolgen voor de fysieke leefomgeving. Indien verwezenlijking van digitale risico's gevolgen heeft voor die veiligheid en/of de fysieke leefomgeving, zou het huidig vergunningstelsel een mogelijkheid kunnen bieden. Daarbij is van belang dat er voldoende kennis, financiële middelen en juridische grondslag moet zijn voor de handhaving van die voorschriften, alsmede dat de gestelde voorschriften in overeenstemming zijn met Europees en nationaal recht.

Een belangrijke constatering binnen het onderzoek is dat de wenselijkheid van dergelijke lokale invulling ter discussie wordt gesteld door respondenten. Er bestaat al veel onduidelijkheid over de geldende wettelijke kaders, en lokale verschillen zouden daarop een negatieve invloed kunnen hebben. Regulering op nationaal of Europees niveau zou volgens de respondenten wenselijker kunnen zijn. Op lokaal niveau zouden andere interventies kunnen worden ingezet, zoals communicatiestrategieën of het eisen van bepaalde certificaten bij eigen aanbestedingen.

Geconcludeerd wordt dat het stellen van vergunningvoorschriften of maatwerkregels, onder omstandigheden, juridisch mogelijk is. Het is nu nog onbekend of de implementatie van de NIS 2-Richtlijn zich daartegen verzet of dat er rumte ontstaat voor gemeenten tot het stellen van aanvullende regels. De consultatieronde over deze richtlijn en implementatiewet kan ieder moment plaatsvinden.
Geadviseerd wordt om in ieder geval nu al de bestaande digitale risico's binnen de gemeente in kaart te brengen. Zo kan worden voorbereid op mogelijke risico's, en worden organisaties bewust van de risico's die hun bedrijfsvoering met zich mee brengt.

1 Inleiding en aanleiding

Dit onderzoek gaat over de mogelijkheden die vergunningverlening en vergunningen kunnen bieden voor het stellen van eisen of verplichtingen voor de digitale veiligheid voor bedrijven die gevestigd zijn of zich willen vestigen binnen gemeenten. In het geval van evenementen is de gemeente vergunningverlener maar er zijn ook andere partijen/medeoverheden betrokken (zoals de provincie). Dit vraagstuk is verkennend omdat onder andere onduidelijk is welke vergunningen er zijn en welke mogelijkheden zij bieden voor het reguleren van digitale veiligheid en ook is de vraag hoe groot het veiligheidsrisico is wanneer de gemeente of een andere partij geen eisen stelt en toezicht houdt op de digitale veiligheid van bedrijven.

We observeren vooraf dat in veel gevallen het fysieke domein of fysieke risico's het vertrekpunt zijn voor de inrichting van de regelgeving en waarschijnlijk ook voor de vergunningverlening. Dat blijkt onder andere uit onderzoeken naar bevoegdheden van burgemeesters om online aangejaagde ordeverstoringen aan te pakken.[1] Zo worden bijvoorbeeld bedrijven die werken met gevaarlijke stoffen (de zogenaamde Seveso-inrichtingen, voorheen BRZO-bedrijven)[2] vaak gezien als bedrijven met specifieke risico's voor het fysieke domein, maar allicht zijn er andere bedrijven waar men niet direct aan denkt, als er wordt gekeken naar digitale veiligheid. Te denken valt bijvoorbeeld een aan verzekeringsmaatschappij die zich in de gemeente vestigt. De gevolgen zijn niet te overzien als bergen persoonsgegevens op straat komen te liggen als gevolg van een hack. De vraag is dan onder andere of een dergelijke digitale onveiligheid een probleem is voor de openbare orde en veiligheid. Vanwege het pionierende karakter van dit onderzoek is ervoor gekozen om informatie te verzamelen door middel van interviews onder experts en bestuurders alsmede een focusgroep.

De kern van dit onderzoek omvat het in kaart brengen van digitale risico's bij bedrijven in brede zin – waaronder bedrijven die evenementen organiseren. Vervolgens wordt onderzocht welke gemeentelijke vergunningen van toepassing kunnen zijn op bedrijven. Er wordt inzichtelijk gemaakt welke juridische mogelijkheden er zijn om partijen te motiveren om zich aan bepaalde eisen te voldoen en welke normenkaders zich eventueel goed lenen voor het mitigeren van

[1] Zie daarvoor Bantema et.al., *'Burgemeester in Cyberspace'*, Den Haag 2018, Bantema, Westers, Munneke, *'Niet bevoegd, wel verantwoordelijk'*, Den Haag 2020, Bantema et.al., *'Black box monitoring'*, Den Haag, 2021, en Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022.
[2] BRZO-bedrijven zijn bedrijven waar met een grote hoeveelheid gevaarlijke stoffen wordt gewerkt. Een en ander is geregeld in de Omgevingswet per 1 januari 224.

de grootste digitale risico's. Daarnaast is ook de vraag of het nodig en wenselijk is om lokaal of regionaal te sturen op digitale veiligheid bij bedrijven en ook de vraag in hoeverre gemeenten en of medeoverheden het toezicht hierop waar kunnen maken. Samengevat heeft dit onderzoek tot doel om het lokale handelingsperspectief voor gemeenten te verkennen om via vergunningverlening eisen te stellen aan digitale veiligheid van bedrijven die in de gemeente gevestigd zijn of bedrijven die binnen de gemeentegrenzen evenementen organiseren in het publieke domein.

1.1 Aanleiding

In het begin van 2022 werd het onderzoek 'Bestuurlijke bevoegdheden cyber' van het Nederlands Instituut Publieke Veiligheid (NIPV) gepubliceerd.[3] Dat onderzoek betrof een verkenning naar bevoegdheden en interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's bij (dreigende) digitale incidenten. Eén van de conclusies van het NIPV-rapport is dat het ontbreekt aan interventie-mogelijkheden en bevoegdheden om vroegtijdig een digitaal incident of crisis met of zonder maatschappelijke gevolgen te beperken of zelfs te vermijden. Voorkomen is immers nog altijd beter dan genezen. Pas als er maatschappelijke gevolgen ontstaan die van invloed kunnen zijn op de openbare orde en veiligheid, zijn er vanuit de klassieke bevoegdheden mogelijkheden om in te grijpen en de (cascade)effecten te bestrijden.

Uit het onderzoek kwamen ook een aantal concrete interventies naar voren die mogelijk kunnen bijdragen aan het aan de voorkant beter kunnen regelen van de digitale veiligheid van bedrijven. Concreet wordt in het NIPV-rapport onder andere verwezen naar mogelijkheden bij het gemeentelijke vergunningverleningstraject van de in gemeente gevestigde (of te vestigen) bedrijven en daarnaast ook de digitale veiligheid van evenementen als onderdeel daarvan. In dat laatste geval kunnen gemeenten bijvoorbeeld organisaties en bedrijven bij de verlening van evenementenvergunningen vragen om aantoonbaar aandacht te hebben voor de Algemene Verordening Gegevensbescherming (AVG) en voor andere aspecten van digitale veiligheid. Voor wat betreft de bedrijven die in de gemeente gevestigd zijn wordt in het NIPV-rapport wordt aangegeven dat het in het bijzonder gaat om bedrijven die niet direct onder de vitale infrastructuur vallen, aangezien voor vitale bedrijven al minimale vereisten gelden.[4]

Eén van de vragen die de VNG (Commissie Bestuur en Veiligheid) stelt is of vergunningsverleners bij gemeenten de kennis en expertise in huis

[3] Van der Varst e.a., *Bestuurlijke bevoegdheden cyber*, Arnhem: Nederlands Instituut Publieke Veiligheid, 2022.
[4] Dit nemen wij niet over als gegeven en maakt deel uit van het onderzoek.

hebben om digitale risico's van bedrijven en organisatoren van evenementen te beoordelen. Deze vraag gaat verder dan alleen de rol van gemeenten. Het gaat daarbij onder andere ook om de adviserende rol die politie en veiligheidsregio's vervullen bij de vergunningverlening. De VNG wil vervolgonderzoek naar de mogelijk ontbrekende bevoegdheden en interventiemogelijkheden op het gebied van vergunningverlening in relatie tot digitale veiligheid. Door het uitvoeren van vervolgonderzoek verwacht de VNG te voorzien in de behoefte en wens van gemeenten om proactief digitale incidenten en crises te kunnen voorkomen of de (cascade)effecten te beperken. Dit sluit eveneens aan bij het programmaplan ADV in het kader van voorbereiding op digitale ontwrichting, incidenten en crises. Daarnaast beoogt dat verkennende onderzoek bij te dragen aan de digitale weerbaarheid van overheid, bedrijven en maatschappelijke organisaties, wat eveneens een pijler is in de Nederlandse Cybersecuritystrategie 2022-2028.[5]

1.2 Hoofd- en deelvragen

In deze rapportage staat de volgende hoofdvraag centraal:

> Hoe kunnen gemeenten en medeoverheden de digitale veiligheid binnen gemeenten vergroten door aandacht te besteden aan digitale veiligheid bij vergunningverlening bij bedrijven die zich binnen de gemeente gevestigd zijn of zich willen vestigen?

De hoofdvraag wordt beantwoord aan de hand van de volgende deelvragen:

1. Wat zijn de digitale risico's bij bedrijven en de mogelijke (maatschappelijke) gevolgen van die risico's of bedreigingen voor de openbare orde en veiligheid en of digitale ontwrichting en welke bedrijven hebben een verhoogd maatschappelijk risico?
2. Welke juridische (normenkaders) lenen zich goed voor het reguleren van digitale risico's bij bedrijven in de vergunningverlening door gemeenten en medeoverheden (bijvoorbeeld BIO of ISO 27001)?[6]
3. Welke soorten vergunningen en vergunningverleners zijn te onderscheiden en wordt er al aandacht besteed aan digitale veiligheid binnen de vergunningverlening aan bedrijven door gemeenten en medeoverheden?
4. Welke juridische mogelijkheden hebben gemeenten en medeoverheden om bedrijven te verplichten aan bepaalde eisen te voldoen?

---

[5] NCSC, *Nederlandse Cyber Security Strategie 2022-2028*, Nationaal Cyber Security Centrum: 2022, p.20.

[6] Dit is ook relevant als het nu juridisch nog niet zou kunnen.

5. Wat zijn eventuele randvoorwaarden/knelpunten bij die wijze van regulering (bijvoorbeeld kennis, bewustzijn, gevoelde verantwoordelijkheid, capaciteit, zicht op het vraagstuk).

1.3 Methoden

Het onderzoek bestaat uit een juridische analyse- en bronnenonderzoek en een empirisch deel waarbij interviews en een focusgroep zijn gehouden. Tevens is in de onderzoeksperiode een *webinar* gevolgd over de invoering van de NIS2 (7 december 2023) om de NIS2 en gevolgen daarvan optimaal te kunnen betrekken in het onderzoek.

Het juridisch bronnenonderzoek is gebaseerd op wetgeving, jurisprudentie, annotaties en literatuur. De dataverzameling heeft plaatsgevonden tussen 1 oktober 2023 en 10 januari 2024. De actualiteit is zoveel mogelijk meegenomen in het onderzoek en is bijgewerkt tot 10 januari 2024. Daarnaast is een beknopt literatuuronderzoek verricht naar digitale veiligheid en risico's in relatie tot bedrijven en evenementen.

Voor het empirische deel/de praktijkverkenning is een focusgroep afgenomen (5 december 2023) en zijn 15 interviews met 16 respondenten gehouden tussen 28 november en 22 december 2023 met zowel experts op het gebied digitale veiligheid alsook met meerdere burgemeesters die binnen de regio digitale veiligheid in hun portefeuille hebben. De gesprekken zijn opgenomen en verwerkt in gespreksverslagen die ter goedkeuring aan de respondenten zijn voorgelegd. Het protocol van de interviews staat in bijlage 1. Tevens is er een focusgroep gehouden bij aanvang van het onderzoek. De focusgroep omvatte 9 deelnemers met brede expertise op dit vraagstuk. Tijdens de focusgroep is onder andere ingegaan op de effecten van digitale incidenten op de openbare orde, de wenselijkheid van regels op lokaal niveau en het juridische normenkader omtrent dit onderwerp (de volledige opzet is te vinden in bijlage 3). De volledige lijst van de respondenten van de interviews zijn te vinden in bijlage 2, van de focusgroep in bijlage 4.

1.4. Leeswijzer

Dit onderzoek vangt in hoofdstuk 2 aan met het schetsen van de digitale risico's en de gevolgen van de verwezenlijking van die risico's bij bedrijven en evenementen. In hoofdstuk 3 worden de juridische normenkaders voor het reguleren van die risico's uitgewerkt, waarna in hoofdstuk 4 een overzicht wordt gegeven van het huidige vergunningstelsel en het toetsingskader daarop. Deze informatie wordt in hoofdstuk 5 samengebracht tot mogelijke beleidsmaatregelen. Vervolgens wordt in hoofdstuk 6 de wenselijkheid van gemeentelijke regulatie behandeld, waarbij ook randvoorwaarden en knelpunten worden uitgewerkt. In hoofdstuk 7

wordt ten aanzien van de hoofdvraag geconcludeerd, waarna aanbevelingen volgen.

2 Digitale risico's bij bedrijven en evenementen en hun invloed op de maatschappij

In dit hoofdstuk staat de volgende deelvraag centraal:

> Wat zijn de digitale risico's bij bedrijven en de mogelijke (maatschappelijke) gevolgen van die risico's of bedreigingen voor de openbare orde en veiligheid en of digitale ontwrichting en welke bedrijven hebben een verhoogd maatschappelijk risico?

Ter beantwoording van deze deelvraag wordt allereerst inzage gegeven op digitale risico's voor organisaties en bij evenementen, waarna verschillende typen risico's worden uitgewerkt en wordt geschetst in hoeverre de aard van een organisatie impact heeft op de mogelijke (maatschappelijke) gevolgen.

2.1 Digitale risico's en de invloed op organisaties en evenementen

In het najaar van 2023 is de meest recente Risico- en crisisbarometer uitgebracht in opdracht van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Daarin is in kaart gebracht waar Nederlanders zich het meeste zorgen over maken. In de top 3 staan zowel digitale dreigingen als het stoppen van vitale processen, respectievelijk 46% en 43% van de Nederlanders maakt zich daar de meeste zorgen over).[7] Daarbij scoren digitale dreigingen bij Nederlanders ook hoog als het gaat om de ernst van de verwezenlijking van zo'n dreiging voor de Nederlandse samenleving.[8]

In en buiten Nederland zijn er talloze voorbeelden van digitale incidenten die leidden tot maatschappelijke onrust, denk aan hacks of computerstoringen in ziekenhuizen (respectievelijk UMCG en Ikazia Ziekenhuis), digitale aanvallen op de Rotterdamse haven en (ver)storingen in telefoniesystemen. Voorkomen is beter dan genezen, met name waar het digitale risico's en crises betreft. In het Landelijk Crisisplan Digitaal is beschreven op welke wijze digitale crises

[7] I&O Research Enschede en Amsterdam. *Risico- en crisisbarometer najaar 2023.* NCTV: 2023; onder cyberdreigingen, p. 26.
[8] I&O Research Enschede en Amsterdam. *Risico- en crisisbarometer najaar 2023.* NCTV: 2023; onder cyberdreigingen, p. 20.

verschillen van andere type crises.[9] Daarbij kan gedacht worden aan de snelheid van manifestatie, de impact op ketenpartners, het achterhalen van de bron van de crisis, grensoverschrijdendheid en de mogelijke impact op de verantwoordelijke (crisis)organisatie. Zo kan door de verwezenlijking van een dergelijk risico van het ene op het andere moment sprake zijn van ontregeling van één of meerdere (vitale) processen gelijktijdig, waardoor maatschappelijke ontwrichting kan ontstaan. Digitale risico's kunnen op verschillende manieren ontstaan, zowel door middel van digitale dreigingen als door middel van fysieke dreigingen. In onderzoek van het *Centre of Expertise Cyber Security* wordt beschreven dat deze dreigingen mede gezondheidsschade bij burgers als risico kunnen hebben.[10]

Het feit dat de verwezenlijking van digitale risico's maatschappelijke impact kan hebben wordt onderschreven in de literatuur. In de Handreiking Cybergevolgbestrijding G4-gemeenten worden een viertal scenario's onderscheiden aan de hand van de impact van een (digitale) crisis.[11] Daarbij wordt onder andere de geografische reikwijdte van de impact meegewogen, alsmede het type domein dat wordt verstoord en de duur van de maatschappelijke impact. De maatschappelijke impact wordt geduid op drie niveaus:

1. **Klein**: mensen merken er niet gelijk veel van, back-up van systemen aanwezig;
2. **Middel**: mensen hebben er last van, dagelijks leven geraakt, hebben niet gelijk alternatief;
3. **Groot**: vitale systemen, dagelijkse levensbehoeften geraakt, mensenlevens op het spel.

Waar in de literatuur vooral wordt geraakt aan het dagelijks leven en het niet hebben van een alternatief, kan uit de interviews en focusgroep worden afgeleid dat er ook een belang schuilt in het hebben voor oog voor situaties die maatschappelijke verontwaardiging kunnen opleveren. Daarbij valt te denken aan ongelukken die in de ogen van de samenleving voorkomen hadden kunnen worden. Het is daarom van belang om oog te houden voor de verschillende typen risico's, die elk hun eigen eigenschappen en mogelijke gevolgen voor de leefomgeving, openbare orde of de maatschappij als geheel kennen.

---

[9] Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Landelijk Crisisplan Digitaal*. NCTV: 2022, p.7-8.
[10] Bekkers, Van der Kleij en Leukfeldt. *Cyber-ketenweerbaarheid. Een verkennend onderzoek naar dreigingen, wetsbaarheden en geleerde lessen*. Centre of Expertise Cyber Security, Lectoraat Cyber Security in het mkb: 2021, paragraaf 2.4.
[11] Berenschot. *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten*. Berenschot Groep B.V: 2020, p.5.

2.2 Verschillende typen risico's

In het Focusblad Digitale Veiligheid van de VNG wordt een indeling van digitale risico's gehanteerd, waarbij gewerkt wordt met een viertal risicoclusters.[12] Deze risicoclusters bestaan uit:

1. **Kwetsbaarheid van informatie** (diefstal, verlies, aantasting van informatie);
2. **Kwetsbaarheid van systemen** (digitale ontregeling, ontwrichting, blokkades van systemen);
3. **Gedigitaliseerde criminaliteit** (voornamelijk vermogens- en geweldscriminaliteit ondersteund door internet);
4. **Online aangejaagde ordeverstoring** (polarisatie, maatschappelijke onrust ondersteund door internet).

Analyse van deze risicoclusters en de bijbehorende voorbeelden, modaliteit en modus operandi gerelateerd aan de risico's voor gemeenten brengt met zich mee dat digitale risico's in de zin van dit onderzoek met name te relateren zijn aan Risicocluster 1 (Kwetsbaarheid van informatie), Risicocluster 2 (Kwetsbaarheid van systemen) en Risicocluster 4 (Online aangejaagde ordeverstoring).
Dit laatste risico valt buiten de reikwijdte van dit onderzoek en is uitgebreid beschreven in eerdere onderzoeken.[13] De classificatie en verdere duiding van de digitale risico's en de invloed op de openbare orde zal worden beschreven op basis van de eerste twee clusters.

2.3 Risicocluster 1: Kwetsbaarheid van informatie

Organisaties beheren tal van informatie, zoals (bijzondere) persoonsgegevens, productiegegevens, informatie over gepatenteerde technologie, informatie over beveiliging(sbeleid) en andere bedrijfsgeheimen. De kwetsbaarheid van informatie ziet op de diefstal, het verlies of de aantasting van deze informatie. Dat kan van opzettelijke (bijv. *ransomware)* of niet-opzettelijke (bijv. *systemcrashes* of *user error*) aard zijn. In beide gevallen kunnen de gevolgen van die aantasting van informatie leiden tot maatschappelijke onrust of een verstoring van de openbare orde. Hersteloperaties kunnen tijdelijke uitval van dienstverlening of bedrijfsvoering betekenen, maar ook het lekken van vertrouwelijke, privacygevoelige of gemanipuleerde gegevens kan leiden tot maatschappelijke onrust.[14] Informatie binnen een organisatie kan ook ten grondslag liggen aan de aansturing van systemen binnen een organisatie (*Cyber-Physical Systems*). Aantasting van die informatie

---

[12] VNG. *Focusblad digitale veiligheid*. Vereniging Nederlandse Gemeenten: 2022, p.5.
[13] Zie daarvoor Bantema et.al., *'Burgemeester in Cyberspace'*, Den Haag 2018, Bantema, Westers, Munneke, *'Niet bevoegd, wel verantwoordelijk'*, Den Haag 2020, Bantema et.al., *'Black box monitoring',* Den Haag, 2021, en Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022.
[14] VNG. *Focusblad digitale veiligheid*. Vereniging Nederlandse Gemeenten, 2022, p.6.

kan daarmee direct invloed hebben op die fysieke systemen, waarbij bijvoorbeeld gedacht kan worden aan waterkeringen of verkeersknooppunten die worden ontregeld.

Eén van de voorbeelden die wordt meegewogen in de Handreiking Cybergevolgbestrijding G4-gemeenten is een digitale aanval op scholengemeenschappen in de vorm van *ransomware,* waarbij de getroffen informatie persoonsgegevens en cijfers van studenten en functioneringsgegevens van medewerkers bevat. Er wordt gedreigd met publicatie van deze gegevens als niet wordt voldaan aan de financiële eisen van de *hacker*. De situatie doet de ronde via sociale media en leidt tot maatschappelijke verontwaardiging en onrust binnen de gemeente, waarna ook Kamervragen worden gesteld aan de Minister van Onderwijs, Cultuur en Wetenschap.[15] Het gaat hier nadrukkelijk om een voorbeeld van opzettelijke aard, waarbij de maatschappelijke impact ook een bijdrage kan leveren aan de bereidwilligheid van organisaties om de eisen van de *hacker* in te willigen.

Een analyse van de verzamelde informatie via focusgroep en interviews over het bovenstaande laat zien dat respondenten over het algemeen van mening zijn dat gemeenten geen rol hebben bij informatiebeveiliging dan wel datalekken, dan alleen als dit plaatsvindt binnen de eigen organisatie van de gemeente. Een datalek leidt volgens respondenten niet direct tot een openbare- ordeprobleem. Organisaties en bedrijven, al dan niet in een keten, blijven daarvoor verantwoordelijk volgens respondenten. Wel zijn twee respondenten, bestuurders, desgevraagd van mening dat ze het belangrijk vinden te weten welke bedrijven er in hun gemeente zijn gevestigd en welke digitale impact ze kunnen hebben **(R12)** al dan niet via de koepelorganisaties voor bedrijven **(R7)**.

2.4 Risicocluster 2: Kwetsbaarheid van systemen

Naast informatiekwetsbaarheid kan ook de kwetsbaarheid van systemen leiden tot digitale incidenten. Hierbij kan gedacht worden aan de uitval, ontregeling of ontwrichting van systemen, zoals websites, portalen, voorzieningen, dienstverlening of slimme apparatuur.[16] Steeds meer fysieke systemen worden, al dan niet *real-time*, digitaal aangestuurd – zoals ook in de vorige paragraaf is benoemd. Deze systemen kunnen kwetsbaar zijn indien de informatie op basis waarvan zij worden aangestuurd wordt aangetast, maar dragen ook het risico dat de systemen zelf kunnen worden ontwricht.

[15] Berenschot. *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten*. Berenschot Groep B.V.: 2020, p.16.
[16] VNG. *Focusblad digitale veiligheid*. Vereniging Nederlandse Gemeenten: 2022, p.6.

Kwetsbaarheid van systemen kan volgens de meeste respondenten (**R1, R4, R6, focusgroep**) leiden tot openbare ordeverstoringen. De mate waarin verschilt per respondent. Met name in de focusgroep werd aangegeven dat ieder systeem dat digitaal ontregeld wordt, openbare orde-effecten kan hebben. Als voorbeeld werd genoemd milieuverontreiniging bij ontregelde bedrijfssystemen. Openbare ordeproblemen worden met name gekoppeld aan verstoring van systemen bij vitale infrastructuur zoals betalingssystemen bij banken maar ook bij gemeenten daar waar uitkeringen moeten worden verstrekt, **(R4)** het ontregelen van elektriciteit, waterleiding en datacenters.

2.5 Verhoogde maatschappelijke (digitale) risico's bij bedrijven

De mate van impact van de verwezenlijking van digitale risico's kan afhankelijk zijn van diverse factoren. Naast de verschillende typen risico's kan ook de aard, doelgroep of de wijze van uitvoering van werkzaamheden binnen een bedrijf een rol spelen. Vanuit de respondenten wordt benadrukt dat hierbij oog moet worden gehouden voor de keten waarin een bedrijf opereert: in een keten van een bedrijf in de vitale infrastructuur zitten ook vaak bedrijven die buiten die infrastructuur vallen. Als voorbeeld wordt verwezen naar een (relatief klein) onderhoudsbedrijf, dat sluizen, bruggen en andere natte en droge infrastructuur onderhoudt. Als die de digitale veiligheid niet op orde heeft, dan kan dat de rest in die keten schaden. Deze ketenafhankelijkheid wordt onderschreven in onderzoek van het Centre of Expertise Cyber Security (2021).[17]

De activiteiten van het ene bedrijf kunnen daarmee impact hebben op activiteiten van een ander bedrijf. Deze verbondenheid brengt met zich mee dat respondenten een onderscheid tussen bijvoorbeeld vitale bedrijven en niet-vitale bedrijven niet zien als een onderscheid dat als een heilige graal moet worden beschouwd. Ook niet-vitale bedrijven kunnen impact hebben op vitale sectoren. Indien een dergelijk bedrijf getroffen wordt, zou dat direct een bredere impact kunnen hebben dan alleen binnen dat bedrijf. De NIS2 houdt tevens rekening met deze ketenweerbaarheid en zal verder in dit onderzoek aan de orde komen. In het eerdergenoemde onderzoek naar ketenweerbaarheid worden voorbeelden genoemd in de onderzochte sectoren. Organisaties binnen de keten kunnen dienen als ingang voor *stepping stone-aanvallen*, waardoor bijvoorbeeld via kleinere organisaties grotere

[17] Bekkers, Van der Kleij en Leukfeldt. *Cyber-ketenweerbaarheid. Een verkennend onderzoek naar dreigingen, wetsbaarheden en geleerde lessen*. Centre of Expertise Cyber Security, Lectoraat Cyber Security in het mkb: 2021

organisaties geraakt kunnen worden.[18] Het is daarmee niet alleen van belang dat de bedrijven waar een groter direct risico op maatschappelijke ontwrichting bestaat, worden gereguleerd, maar ook alle bedrijven in die keten om zwakke plekken zoveel mogelijk te voorkomen.[19] Het verdient, volgens de respondenten, de voorkeur om niet slechts te kijken naar de risico's van het bedrijf zelf, gelet op grootte, aard van de werkzaamheden of branche. Mede van belang is in welke keten zij opereren en aan welke risico's zij andere bedrijven of organisaties kunnen blootstellen door hun eigen digitale onveiligheid.

"Alle digitale processen, organisaties en sectoren zijn potentieel kwetsbaar voor cyberincidenten.", zo schrijft ook het NCTV in het Cybersecuritybeeld 2023. Hoewel de sector waarin een bedrijf opereert niet als uitgangspunt voor een risicoclassificatie kan dienen, kunnen op basis van de ervaringen en scenario's van respondenten en uit de literatuur wel indicatoren worden gedestilleerd die kunnen helpen bij een risicoclassificatie. Allereerst worden door de NCTV ten aanzien van vitale processen twee categorieën onderscheiden, waarbij processen in categorie A (bijvoorbeeld drinkwatervoorziening) bij uitval of aantasting grotere gevolgen hebben dan de processen in categorie B (bijvoorbeeld internettoegang en dataverkeer).[20] Deze vitale processen zijn in het onderzoek gekoppeld aan de standaard bedrijfsindeling (SBI) van de Kamer van Koophandel (KvK), waardoor in hoofdlijnen categorieën van bedrijven kunnen worden aangewezen waar sprake kan zijn van vitale processen waarbij de verwezenlijking van digitale risico's leidt tot een grotere mate van digitale ontwrichting. Dit overzicht is hieronder opgenomen in tabel 1.

Tabel 1 - Overzicht vitale processen in relatie tot SBI

Vitale processen in relatie tot SBI	
Vitale processen categorie A	- SBI B: Winning van delfstoffen - SBI D: Productie en distributie van en handel in elektriciteit, aardgas, stoom en gekoelde lucht - SBI E: Winning en distributie van water; afval- en afvalwaterbeheer en sanering
Vitale processen categorie B	- SBI C: Industrie

[18] Bekkers, Van der Kleij en Leukfeldt. *Cyber-ketenweerbaarheid. Een verkennend onderzoek naar dreigingen, wetsbaarheden en geleerde lessen*. Centre of Expertise Cyber Security, Lectoraat Cyber Security in het mkb: 2021.
[19] Van Ruijven & Keijser. *Ketenweerbaarheid tegen cyberdreigingen. Uitgangspunten, good practices en een stappenplan voor het vergroten van cyber-ketenweerbaarheid*. TNO: 2017, p.5.
[20] Nederlands Instituut Publieke Veiligheid, *Vitale processen*, z.d.

	- SBI D: Productie en distributie van en handel in elektriciteit, aardgas, stoom en gekoelde lucht
	  o *Ten aanzien van regionale distributie van elektriciteit en gas*
	- SBI E: Winning en distributie van water; afval- en afvalwaterbeheer en sanering
	  o *Ten aanzien van het keren en beheren van waterkwantiteit*
	- SBI H: Vervoer en opslag
	- SBI J: Informatie en communicatie
	- SBI K: Financiële instellingen
	- SBI O: Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen

Daarnaast speelt de afhankelijkheid van digitale processen een rol: in bedrijven met een lage mate van afhankelijkheid van digitale systemen spelen minder digitale risico's dan in bedrijven waar deze mate hoger is. Vanuit de respondenten wordt verwezen naar BRZO-bedrijven[21] met procesautomatisering of industriële automatisering, waarbij het risico bijvoorbeeld bestaat dat digitale onveiligheid leidt tot ontploffingen of milieuverontreiniging. Daar wordt ook naar verwezen door het NCTV, die stelt dat het zaak is operationele technologie of toepassing van industriële toepassing van Internet of Things (IoT) onder de aandacht te houden om weerbaarheid te vergroten.[22] Daarbij wordt benadrukt dat systemen die afhankelijk zijn van operationele technologieën (hierna: OT) een ander risicobeeld kennen dan zuivere IT-systemen: in het geval van OT-systemen beperken de risico's zich in de meeste gevallen niet tot financiële of reputatieschade, maar kan verwezenlijking van die risico's leiden tot schade aan industriële apparatuur en de nabije omgeving. De mogelijkheid dat er slachtoffers vallen wordt daarbij niet uitgesloten.[23] In rapportages van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) wordt verwezen naar de aanwezigheid van analoge terugvalopties als mogelijke bepalende factor voor de omvang van de schade of het aantal slachtoffers.[24]

De verschillende factoren die zien op het aanwijzen van (categorieën van) bedrijven met een verhoogd maatschappelijk risico zijn beknopt

[21] Na inwerkingtreding van de Omgevingswet worden BRZO-bedrijven als Seveso-inrichtingen aangeduid, zie in dat kader art. 4.2 e.v. Omgevingswet.

[22] Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2023*, NCTV: 2023, p. 34.

[23] Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2023*, NCTV: 2023, p. 34.

[24] Wetenschappelijke Raad voor het Regeringsbeleid (2019) *Voorbereiden op digitale ontwrichting, WRR-Rapport 101*, Den Haag: WRR, p. 54.

samengevat in een indicatorenlijst, waar onderscheid is gemaakt tussen een hoog-risicovolle factoren en middelhoog-risicovolle factoren, hieronder te vinden in tabel 2.

Tabel 2 - Indicatorenlijst verhoogd maatschappelijk risico

Indicatorenlijst - risicoverhogende factoren ten aanzien van de aard van organisatie en de keten waarin de organisatie zich bevindt	
Hoog-risicofactor	- Bedrijf maakt onderdeel uit van de vitale processen, categorie A - Bedrijf kent een SBI-classificatie in SBI-B, SBI-D, of SBI-E - Organisatie staat in (in)directe verbinding met de vitale processen, categorie A - Bedrijf staat in (in)directe verbinding met bedrijven met bovengenoemde SBI-classificaties - Aanwezigheid van operationele technologie in Seveso-inrichtingen (voorheen BRZO) - Afhankelijkheid van operationele technologie - Afwezigheid van analoge terugvaloptie
Middelhoog risicofactor	- Organisatie maakt onderdeel uit van de vitale processen, categorie B - Organisatie staat in (in)directe verbinding met de vitale processen, categorie B - Bedrijf kent een SBI-classificatie in SBI-C, SBI-D, SBI-E, SBI-H, SBI-J, SBI-K of SBI-O - Bedrijf staat in (in)directe verbinding met bedrijven met bovengenoemde SBI-classificaties - Aanwezigheid van operationele technologie

2.6 Verhoogde maatschappelijke (digitale) risico's bij evenementen

Evenementen bestaan er in vele vormen: van kleine buurtbarbecues tot grote meerdaagse festivals. Evenementen worden in de praktijk onderscheiden in verschillende categorieën, rekening houdend met de risico's van een evenement. In veel gevallen wordt onderscheid gemaakt tussen reguliere evenementen (categorie A), aandachtevenementen (categorie B) en risicovolle evenementen

(categorie C).[25] Uit onderzoek van de Rijksuniversiteit Groningen in 2018 kwamen een tweetal potentiële risico's naar voren bij evenementen: aanvallen op systemen (zoals de informatieschermen of de geluidsinstallatie) en het omgaan met vertrouwelijke informatie.[26] In paragraaf 2.3 kwam reeds naar voren dat respondenten weinig maatschappelijke risico's zien ten aanzien van de kwetsbaarheid van informatie. Bij de meeste evenementen wordt ook geen (grote mate van) aanwezigheid van bijzondere persoonsgegevens verwacht, wat zou kunnen leiden tot grootschalige maatschappelijke verontwaardiging. Veiligheid van evenementen komt niet naar voren in het Cybersecuritybeeld 2023 van het NCTV. Toch zijn er diverse scenario's te bedenken, zo blijkt uit een rapportage van Scherp in Veiligheid (2023). "Van gehackte toegangspoortjes tot gesaboteerde led-schermen die het publiek de verkeerde kant opsturen;" er worden scenario's geschetst die kunnen leiden tot grote verstoringen en mogelijk dodelijke slachtoffers (denk aan verdrukking).[27] Cyberincidenten bij evenementen hebben ook al plaatsgevonden. Zo wordt in de interviews een situatie beschreven van een weigerend betaalsysteem bij de horecabedrijven op Lowlands. Er werd toen gratis drank weggegeven omdat gevreesd werd voor rellen indien als gevolg van deze storing de horeca zou moeten sluiten tijdens de optredens. De respondent benoemt dat het goed is als dienstverlenende bedrijven preventieve maatregelen nemen en een *back-up plan* hebben voor als een systeem uitvalt (**R5, R13**). In de interviews worden ook scenario's geschetst ten aanzien van het uitvallen of hacken van communicatiesystemen van de beveiliging van een evenement. Vanuit de respondenten worden vooral risico's gezien ten aanzien van evenementen met risicoclassificatie C en evenementen met een groot aantal deelnemers.

2.7 Conclusie

In dit hoofdstuk is besproken welke digitale risico's er bestaan bij bedrijven, welke maatschappelijke gevolgen die risico's kunnen hebben en welke bedrijven of evenementen een verhoogd maatschappelijk risico hebben. Digitale onveiligheid kan leiden tot diverse digitale risico's binnen bedrijven en bij de organisatie en uitoefening van evenementen. Ter bepaling van de mate van (maatschappelijke) risico's kan gebruik worden gemaakt van bestaande risicomodellen, maar dient rekening gehouden te worden met het feit dat organisaties niet op zichzelf staan. Bij het bepalen van risico's is daarom ook van belang in welke keten een organisatie

[25] Vereniging van Evenementen Makers, *Nationaal Handboek Evenementen Veiligheid 1.0. Een gemeenschappelijk denkkader omtrent veiligheid*. NHEV: 2019, tevens genoemd door respondenten R5, R6 en R7.
[26] Asslani, van den Berg, Hofman & Xue, *Rapport digitale veiligheid evenementen*. RUG: 2018
[27] 'Afgehackt', scherpinveiligheid.nl, 14 november 2023.

optreedt, en welke impact digitale onveiligheid binnen die keten kan hebben. Een klein bedrijf dat op het oog weinig impact lijkt te hebben, kan een ingang bieden bij grotere bedrijven waar het risico op maatschappelijke of fysieke gevolgen bij digitale incidenten groter is. Bij het bepalen van de risico's zijn daarom niet alleen directe, maar ook indirecte risico's van belang. Een aantal sectoren kent grotere risico's, zoals sectoren waarbij de processen deel uitmaken van vitale processen of indien sprake is van Seveso-inrichtingen (voorheen BRZO-bedrijven). Bedrijven die in ketenverbinding staan met dergelijke sectoren hebben een afgeleid verhoogd risico. Een andere indicator ziet op de afhankelijkheid van technologieën, en de aan- of afwezigheid van analoge terugvalopties.

3 Juridische normenkaders voor het reguleren van digitale veiligheid voor private en publieke organisaties.

In dit hoofdstuk staat de volgende deelvraag centraal:

> Welke juridische (normenkaders) lenen zich goed voor het reguleren van digitale risico's bij bedrijven in de vergunningverlening door gemeenten en medeoverheden?

De basis voor het reguleren van digitale veiligheid is te vinden in de internationale certificeringssystematiek, de ISO-standaard. Binnen Nederland is deze vertaald naar de NEN-ISO, speciaal gericht op informatiebeveiliging. De EU is actief bezig met het uitvoeren van een digitale agenda en de informatieveiligheid heeft daarin een hoge prioriteit. Alle lidstaten zijn verplicht om de EU-richtlijnen op dit gebied binnen een korte periode te implementeren in nationale wetgeving.
Naast de wetgeving op het gebied van digitale veiligheid, worden in dit hoofdstuk nationale wetten genoemd, die in zijn algemeenheid van invloed kunnen zijn op het regelen van digitale veiligheid in gemeentelijke vergunningen. Daarbij wordt onderscheid gemaakt tussen wet- en regelgeving die specifiek gericht is op digitaliseringsthema's, en wet- en regelgeving waaruit mogelijke bevoegdheden voortvloeien gelet op doelstelling. Ook in de interviews en focusgroep is aandacht besteed aan het juridische normenkader. In dit hoofdstuk komt daarmee ook naar voren hoe vanuit de praktijk wordt aangekeken tegen het vraagstuk.

3.1 Specifiek gericht op digitaliseringsthema's

Voor de wet- en regelgeving die in deze paragraaf wordt behandeld is reeds duidelijk dat deze (al dan niet mede) van toepassing is op digitaliseringsvraagstukken, gelet op de doelen waarmee de regelgeving is opgesteld. In deze paragraaf komen de Wet beveiliging netwerk- en informatiesystemen, de Algemene verordening gegevensbescherming, NEN- en ISO-normen alsmede de NIS 2-richtlijn aan de orde.

3.1.1 Wet beveiliging netwerk- en informatiesystemen

De Wet beveiliging netwerk- en informatiesystemen is de Nederlandse implementatie van de Europese richtlijn 2016/1148 (NIB-richtlijn), die gericht is op het creëren van een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Europese Unie. De wet wordt ook wel de Cybersecuritywet genoemd.[28] Deze wet is gericht op aanbieders van essentiële diensten (bijvoorbeeld nutsbedrijven,

[28] *Kamerstukken II*, 2017-18, 34 883, nr. 3 (MvT), p. 1.

vervoersbedrijven en banken) en digitale dienstverleners (zoals Cloud aanbieders en online zoekmachines).[29]
Voor deze aanbieders geldt dat zij passende en evenredige technische en organisatorische maatregelen dienen te nemen om risico's ten aanzien van de beveiliging van netwerk- en informatiesystemen te beheersen.[30] Naast de beheersing van risico's dienen maatregelen getroffen te worden om incidenten te voorkomen én de gevolgen van die incidenten te beperken.[31]

3.1.2 Algemene verordening gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) beoogt de rechten van gegevensbescherming te versterken, de regelgeving te harmoniseren en toekomstbestendig te maken.[32] De AVG is, voor zover van belang voor dit onderzoek, van toepassing op organisaties die persoonsgegevens verwerken. In de basisbeginselen van de AVG is een verplichting opgenomen tot het treffen van technische en organisatorische maatregelen om een passende mate van beveiliging te borgen, zodat gegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en verlies, vernietiging of beschadiging.[33]

3.1.3 NEN- ISO normen

De ISO 27001 en de ISO 27002 zijn standaardnormeringen voor de informatiebeveiliging. Het betreft een internationale norm die van toepassing is op alle typen organisaties, publiek en privaat. De Nederlandse toepassing ervan, de NEN-ISO 27001 en NEN-ISO 27002, noemen eisen voor het binnen de context van de organisatie vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging.[34] Voor overheden geldt nog een speciaal normenkader, te weten de Baseline Informatiebeveiliging Overheid (BIO), die in 2018 door de ministerraad is vastgesteld en geldt voor alle Nederlandse overheden.[35]

De BIO is gebaseerd op de NEN-ISO 27001:2017 en NEN-ISO 27002:2017 en kent een concretisering van het algemene ISO-normenkader voor overheden. Volgens de website digitaleoverheid.nl wordt op dit moment gewerkt aan de BIO 2.0.

---

[29] Art. 1. Wet beveiliging netwerk- en informatiesystemen; *Kamerstukken II*, 2017-18, 34 883, nr. 3 (MvT), p. 1; art. 2 Besluit beveiliging netwerk- en informatiesystemen.
[30] Art. 7 Wet beveiliging netwerk- en informatiesystemen.
[31] Art. 8 Wet beveiliging netwerk- en informatiesystemen.
[32] Verordening (EU) 2016/679, zie overweging 1, 3 en 6.
[33] Art. 5, eerste lid onder f, Algemene verordening gegevensbescherming.
[34] nen.nl, ISO 27001, ISO 27002.
[35] 'Baseline informatiebeveiliging overheid', digitaleoverheid.nl, z.d. Staatscourant 2020, 7857.

3.1.4 NIS2-richtlijn

Op 14 december 2022 is richtlijn 2022/2555 aangenomen, ook wel de NIS2-richtlijn genoemd.[36] Met deze richtlijn wordt onder andere beoogd capaciteiten op het gebied van digitale beveiliging in de hele EU op te bouwen, teneinde bij te dragen aan de veiligheid van de EU en tot de doeltreffende werking van haar economie en samenleving.[37]

In deze richtlijn wordt expliciet niet alleen aandacht besteed aan het op digitaal niveau beheren van risico's, maar ook aan fysieke componenten die een gevolg kunnen hebben voor de digitale infrastructuur binnen een bedrijf. Dat vereist een benadering waarin zowel het netwerk- en informatiesysteem, als de fysieke omgeving waarin die systemen zich bevinden, worden beschermd – ten aanzien van fysieke risico's behelst dat bijvoorbeeld brand, diefstal, telecommunicatiestoringen en ongeoorloofde fysieke toegang.[38]

Deze richtlijn regelt voor de organisaties, die hieronder vallen, een zorgplicht, inhoudende het regelmatig doen van risicobeoordeling binnen de organisatie, een meldplicht bij digitale incidenten en het toezicht, dat wordt belegd bij een onafhankelijke autoriteit.[39]

De NIS2-richtlijn dient nog te worden vertaald naar nationale wetgeving. Op dit moment is men daarmee bezig en op genoemde website wordt vermeld dat er binnenkort (januari 2024) een consultatieronde komt.[40] In paragraaf 5.1.3 wordt nader ingegaan op de NIS2 in relatie tot de aanvullende regelgevende bevoegdheid van een gemeente op dit punt.

3.2 Niet specifiek gericht op digitaliseringsthema's

Voor een deel van de onderzochte wet- en regelgeving geldt dat deze niet specifiek gericht zijn op digitaliseringsthema's, maar waarbij de aard van de wet- en regelgeving wel annex is aan deze thema's. Het gaat daarbij ook specifiek om wet- en regelgeving die ten grondslag

---

[36] NIS = Network and Information Systems; Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad, 14 december 2022, betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de gehele Unie, tot wijziging van de richtlijn (EU) 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148, (NIS2 Richtlijn), digitaleoverheid.nl, zoeken op 'NIS2'.

[37] Richtlijn (EU) 2022/2555 betreffende maatregelen een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn), aanhef onder 1.

[38] Richtlijn (EU) 2022/2555, aanhef onder 79.

[39] digitaleoverheid.nl, zoeken op NIS2.

[40] zie daarvoor ook de website van het NCSC, 'wat gaat de NIS2 richtlijn betekenen voor uw organisatie?'. Daarin wordt vermeld dat de consultatieronde nog moet starten.

ligt aan de vergunningen die gebruikelijk zijn in gemeenten, die verder worden behandeld in hoofdstuk 4.

3.2.1 Omgevingswet

Omgevingsvergunningen vormen een groot deel van de vergunningen die worden verleend binnen decentrale overheden. De bevoegdheidsgrondslag van deze vergunningen vloeit voort uit de Omgevingswet. Het toepassingsbereik van de Omgevingswet ziet, in hoofdlijnen, op twee zaken: de fysieke leefomgeving en activiteiten die gevolgen hebben of kunnen hebben voor de fysieke leefomgeving.[41] Voor de toetsing van die wet aan de toepasbaarheid ervan op digitale aspecten, is het van belang te duiden wat onder deze fysieke leefomgeving wordt verstaan. De Omgevingswet bevat een niet-limitatieve opsomming: bouwwerken, infrastructuur, watersystemen, water, bodem, lucht, landschappen, natuur, cultureel erfgoed en werelderfgoed.[42] Ten aanzien van gevolgen voor de fysieke omgeving ziet de Omgevingswet op gevolgen die kunnen voortvloeien uit het wijzigen van onderdelen van de fysieke leefomgeving of het gebruik daarvan, het gebruik van natuurlijke hulpbronnen, activiteiten waardoor emissies, hinder of risico's worden veroorzaakt en het nalaten van activiteiten.[43] Zo wordt in de Omgevingswet ook expliciet aandacht besteed aan 'ongewone voorvallen', waarmee gebeurtenissen die afwijken van normale omstandigheden waaronder een activiteit plaatsvindt en waardoor significante nadelige gevolgen voor de fysieke leefomgeving zijn of worden veroorzaakt of te worden dreigen veroorzaakt.[44] Onder ongewone voorvallen worden bijvoorbeeld storingen in het productieproces of in de voorzieningen verstaan, ongeacht de oorzaak van een dergelijke storing.[45] Uit de memorie van toelichting van de Omgevingswet volgt dat het parlement oog heeft voor de mogelijkheid dat 'ongewone voorvallen' leiden tot rampen of crises.[46]

Belangrijk in het kader van digitale risico's is de specifieke duiding dat gevolgen voor de mens ook worden beschouwd als gevolgen voor de fysieke leefomgeving, voor zover dat wordt óf kan worden beïnvloed door of via onderdelen van de fysieke leefomgeving.[47] Eén van de voorbeelden die in de memorie van toelichting wordt genoemd betreft het niet onderhouden van bouwwerken of installaties.[48] Hoewel digitaliseringsaspecten daarin niet expliciet zijn opgenomen, zou tegenwoordig onder onderhoud tevens het digitale onderhoud – zoals

---

[41] Art. 1.2, eerste lid, Omgevingswet.
[42] Art. 1.2, tweede lid, Omgevingswet.
[43] Art. 1.2, derde lid, Omgevingswet.
[44] Art. 19.1 e.v. Omgevingswet, *Kamerstukken II 2013/14*, 33962, 3, p. 248-249.
[45] Zie in dat kader bijvoorbeeld ABRvS 10 juli 2019, ECLI:NL:RVS:2019:2335, r.o. 5.2.
[46] *Kamerstukken II 2013/14*, 33962, 3, p. 248-249.
[47] Art. 1.2, vierde lid, Omgevingswet.
[48] *Kamerstukken II 2013/14*, 33962, 3, p. 392.

het uitvoeren van tijdige updates ten behoeve van de veiligheid van het systeem – kunnen worden verstaan. Systemen hebben niet meer slechts fysieke kwetsbaarheden, maar ook digitale kwetsbaarheden die fysieke kwetsbaarheden kunnen veroorzaken. Het niet-limitatieve karakter van de opsomming brengt met zich mee dat van gemeentebesturen slechts wordt verwacht dat zij redelijkerwijs tot het standpunt hoeven te komen dat een situatie onderdeel is van de fysieke leefomgeving.[49]

Voor de beoordeling van de reikwijdte van de Omgevingswet, is het belangrijk in kaart te brengen welke doelstellingen de wet nastreeft. Binnen deze doelen valt expliciet het bereiken en in stand houden van een veilige en gezonde fysieke leefomgeving en goede omgevingskwaliteit, waaronder aspecten van fysieke veiligheid worden bedoeld.[50] Waar de Omgevingswet regels op hoofdlijnen schetst, biedt het ook de mogelijkheid voor het opstellen van regels door het rijk ten aanzien van de in artikel 4.3 Omgevingswet genoemde onderwerpen. Deze regels zijn onder andere vastgelegd in het Besluit activiteiten leefomgeving (Bal), en zijn gesteld met het oog op het waarborgen van veiligheid en het beschermen van gezondheid en milieu. Onder het beschermen van het milieu wordt mede verstaan het beperken van de kans op en het voorkomen van ongewone voorvallen en de nadelige gevolgen daarvan, alsmede het voorkomen van waterschaarste en het vervullen van de maatschappelijke functies door watersystemen.[51]

3.2.2 Gemeentewet

Enkele digitale risico's zijn van dusdanige aard dat ze kunnen leiden tot een verstoring van de openbare orde, zoals aanvallen op ziekenhuizen of scholen. De burgemeester is ingevolge art. 172 Gemeentewet belast met de handhaving van die openbare orde, en heeft bij verstoringen van de openbare orde of ernstige vrees daarvoor de bevoegdheid de bevelen te geven die noodzakelijk zijn voor de handhaving van die orde. Onder openbare orde wordt een verstoring van enige betekenis voor de normale gang van zaken in of aan de openbare ruimte.[52]

3.2.3 Algemene Plaatselijke Verordening

De Algemene Plaatselijke Verordening stelt regels die het publieke domein van een gemeente dienen te beschermen.[53] De bevoegdheid tot het vaststellen van de APV berust in beginsel bij de gemeenteraad,

---

[49] *Kamerstukken II 2013/14*, 33962, 3, p. 391.
[50] Art. 1.3, aanhef, Omgevingswet; *Kamerstukken II* 2013/14, 33962, 3, p. 62 e.v.
[51] Art. 2.2 Besluit activiteiten leefomgeving.
[52] Bantema et.al., *'Burgemeester in Cyberspace'*, Den Haag 2018, p.18. De definities in dit onderzoek zijn gebaseerd op het rapport van De Jong et.al., *'Orde in de Openbare Orde'*, 2016, p.10-13 met daarin een uitgebreide bronnenlijst.
[53] E.R. Muller, H.R.B.M. Kummeling & R. Nehmelman (red.), *Instituten van de staat*, Deventer: Wolters Kluwer 2020, paragraaf 6.4.

die ervoor kan kiezen de vaststelling van (delen) van de APV te mandateren aan het college van burgemeester en wethouders of de burgemeester.[54]

3.3 Focusgroep en interviews over het juridische normenkader

3.3.1 Focusgroep

In de focusgroep is aandacht besteed aan de vraag wat relevante normenkaders zijn voor dit vraagstuk. Hieruit komen de NEN ISO-normen, de NIS2 maar mogelijk ook toekomstige AI-wetgeving naar voren als mogelijkheden. Volgens een van de focusgroep-respondenten komen er zoveel regels vanuit de EU op bedrijven af, dat volgens deze respondent niemand, ook niet in Brussel en in Den Haag, laat staan gemeenten, een goed overzicht hebben van welke normenkaders zich lenen of gaan lenen voor de regulering van de digitale veiligheid, omdat alles elkaar als het ware overlapt. Deze respondent pleit ervoor dat men er eerst zeker van moet zijn wat die regelgeving voor invloed heeft en hoe ze op elkaar inwerken, alvorens normenkaders voor vergunningen worden ontwikkeld.

3.3.2 Interviews met het werkveld

De rode lijn in de interviews is dat wordt verwezen naar het belang van gelijke regels voor alle gemeenten om te voorkomen dat er voor bedrijven ongelijkheid per gemeente ontstaat. Dit wordt niet wenselijk geacht door de respondenten. Die regels zouden georganiseerd kunnen worden door middel van certificering. Door respondenten wordt verwezen naar de voorwaarden van de NEN-ISO, de NIS2 en de BIO voor overheden, waarbij toepassing ervan ter discussie werd gesteld door respondenten om twee redenen. Allereerst moet voorkomen worden dat er hoge kosten voor bedrijven ontstaan. Ten tweede bestaat het risico dat digitale veiligheid een te hoog 'checklistgehalte' kan krijgen, waardoor de intrinsieke motivatie om digitaal veilig gedrag te vertonen bij bedrijven verdwijnt. Er komt in de interviews ook een indirect juridisch normenkader naar voren in de vorm van aanbestedingsregels die overheden hanteren in hun relatie met het bedrijfsleven. Ook dit is een mogelijkheid om digitale veiligheid bij bedrijven te verbeteren door in deze regels voorwaarden hierover op te nemen.

Eén van de respondenten geeft aan dat de gemeente kan bepalen met wie ze zakendoet en dus ook kan bepalen dat met bepaalde bedrijven, die niet voldoen aan bijvoorbeeld de NIS2 dan wel de NEN ISO-standaard, geen zaken wordt gedaan. In die zin kan de gemeente in ieder geval druk uitoefenen en als dit als vergunningvoorschrift is opgenomen in een evenementenvergunning, is er een direct toezicht

[54] Artt. 127 Grondwet en 147, eerste lid, Gemeentewet.

mogelijk volgens deze respondent. Artikel 21 NIS2 biedt dan weer een grond voor het nemen van de basismaatregelen voor de digitale veiligheid (**R1**).

Er is nog veel onduidelijk over de mogelijkheid om buiten de NIS2, waarbij extra eisen worden gesteld aan een groot aantal bedrijven, aanvullende eisen te stellen als gemeente of provincie. De respondenten denken hier wisselend over. Eén van de respondenten hoopt dat dit geregeld kan worden in de implementatiewetgeving van de NIS2 door het rijk (**R4**). Ook een andere respondent vindt dit ingewikkeld en zou vooral graag zien dat bij evenementen het risico op verstoringen vanuit het digitale domein verminderd kunnen worden (**R5**). Een andere respondent geeft aan dat er in vergelijking met de vorige NIS al veel bedrijven onder vallen (**R2**), behalve bedrijven met minder dan 50 medewerkers, maar uiteindelijk valt 70-80 procent van de bedrijven er onder vanwege de doorwerking van de richtlijn naar bedrijven die zakendoen met NIS2-plichtige bedrijven. In de ogen van deze respondent zijn de bedrijven die buiten de NIS2 vallen vaak niet vitaal of essentieel, maar de vraag is wat je die bedrijven wil verplichten, waarbij als randvoorwaarde geldt dat het niet te complex moet worden. In het laatste geval verwijst de respondent naar de ervaring die veel gemeenten hebben met de AVG. Een van de respondenten is van mening dat gemeenten een te beperkte kennis van zaken hebben op het terrein van de digitale veiligheid om hier een serieuze rol waar te maken. Op rijksniveau kan dat beter georganiseerd worden (**R12**).

Er worden ook alternatieven genoemd omdat men onder andere vindt dat het niet duidelijk is hoe de implementatiewet van de NIS2-richtlijn eruit komt te zien voor Nederland (**R14**). Deze respondent denkt dat gemeenten wellicht alleen via de inkoopvoorwaarden invloed op de digitale veiligheid van bedrijven kunnen uitoefenen, waarbij verwezen wordt naar de inkoopvoorwaarden van de VNG, waarin informatiebeveiliging is geregeld. Veilige producten en diensten maken daarvan onderdeel uit. Het is ook nog niet duidelijk hoe de NIS2-regelgeving gehandhaafd gaat worden en wie het toezicht gaat doen. Volgens deze respondent heeft de gemeente nog geen mogelijkheid om bedrijven te weren die niet voldoen aan de NIS2. Dat zou nog een mogelijkheid kunnen zijn.

Een andere respondent wijst het idee van aanvullende regelgeving door gemeenten af omdat het thema leent zich niet leent om in alle gemeenten iets anders af te spreken. Voor bedrijven dient er volgens deze respondent een lijn getrokken worden ten aanzien van de te stellen eisen, waarbij de NIS2 een uitgangspunt is (**R6**). De vraag is vervolgens of digitale veiligheid standaard een onderdeel moet zijn van het eisenpakket van een gemeente of alleen bij evenementen waarbij een digitaal risico speelt. Het bedrijf doorlichten heeft volgens deze respondent geen zin. De controle moet wel gekoppeld zijn aan

risico's op evenementen omdat de gemeente anders zijn bevoegdheden te buiten gaat.

3.4 Conclusie

In dit hoofdstuk werd besproken welke juridische (normen)kaders zich lenen voor het reguleren van digitale risico's bij bedrijven in vergunningverlening door gemeenten en medeoverheden. Het huidig juridisch kader van regels voor digitale veiligheid bij bedrijven wordt gevormd door de Wet beveiliging netwerk- en informatiesystemen, de AVG en de EU- richtlijn NIS2, die uiterlijk 17 oktober 2024 in nationale wetgeving dient te zijn omgezet. Decentrale overheden hebben op grond van deze wetten geen juridische invloed op de digitale veiligheid ervan. Daarvoor zijn andere instanties aangewezen.

Voor de Omgevingswet, Gemeentewet en APV geldt dat ze niet specifiek gericht zijn op digitalisering, maar ze bieden wel mogelijkheden voor decentrale overheden om voorschriften te stellen over digitale veiligheid. De Omgevingswet biedt een interessante mogelijkheid in artikel 1.2 eerste lid, daar waar staat dat de wet van toepassing is op activiteiten die gevolgen hebben of kunnen hebben voor de fysieke leefomgeving. Digitale onveiligheid zou gevolgen kunnen hebben voor de fysieke leefomgeving waardoor dit artikel een opening biedt voor nader onderzoek. De Gemeentewet en de APV gaan over de beveiliging van de publieke ruimte. Op basis van de daarin opgenomen algemene, klassieke bevoegdheden en regels over de bescherming van de openbare orde, kan de burgemeester optreden als er effecten op de openbare orde zijn vanuit het digitale domein. Vergunningen en vergunningvoorschriften die daarop toezien zijn hoofdzakelijk verleend voor (vormen van) evenementen.

Uit het onderzoek blijkt dat er ruimte is om zowel de Omgevingswet als de Gemeentewet en APV aan te grijpen voor het beheersen van digitale veiligheid, indien dat bijdraagt aan de doelen waarvoor deze regelingen zijn opgesteld.

Uit het veldonderzoek is gebleken dat gemeenten nu al indirect invloed kunnen uitoefenen op de digitale veiligheid van bedrijven door er aandacht aan te besteden in de aanbestedingsregels. In dat verband biedt de NIS2 aanvullende mogelijkheden omdat bedrijven, die zakendoen met NIS2-plichtige bedrijven/overheden ook aan de NIS2-eisen moeten voldoen.

4 Vergunningen en de huidige aandacht voor digitale aspecten in vergunningverlening

In dit hoofdstuk staat de volgende deelvraag centraal:

> Welke soorten vergunningen zijn te onderscheiden en wordt er al aandacht besteed aan digitale veiligheid binnen de vergunningverlening aan bedrijven door gemeenten en medeoverheden?

Ter beantwoording van deze deelvraag worden allereerst de vergunningen die voortvloeien uit de Omgevingswet behandeld, waarna de vergunningen op grond van de APV aan de orde komen. Dit is gedaan op basis van literatuuronderzoek en een wetsanalyse.

4.1 Omgevingsvergunningen

Met de inwerkingtreding van de Omgevingswet (verder uitgewerkt in par. 3.2.1) is er een wijziging in de grondslag van omgevingsrechtelijke regels ontstaan. Waar in de, inmiddels vervallen, Wet ruimtelijke ordening, toelatingsplanologie centraal stond – is de Omgevingswet gestoeld op het principe van uitnodigingsplanologie. Deze omwenteling brengt met zich mee dat de overgang van bestemmingsplan naar omgevingsplan ook een andere invulling van de regels vergt. Waar in het oude stelsel (*toelatingsplanologie*) nauwkeurige regels golden over wat er op welk gebied binnen de bestemmingsplangrenzen was toegestaan, voorzien omgevingsplannen in meer algemene regels en is de mogelijkheid voor gebiedende regels opengesteld (uitnodigingsplanologie). Deze wijziging brengt met zich mee dat het aantal vergunningplichtige activiteiten onder de Omgevingswet is afgenomen. Vergunningplichtige activiteiten kunnen voortvloeien uit rijksregels (Omgevingwet en de daarop gebaseerde Besluit activiteiten leefomgeving (Bal) en Besluit bouwwerken leefomgeving (Bbl) en uit decentrale regels: provinciaal in de omgevingsverordening, gemeentelijk in het omgevingsplan en voor de waterschappen in de waterschapsverordening.[55]

In de volgende paragrafen is een weergave op hoofdlijnen opgenomen van vergunningplichtige activiteiten ingevolge de Omgevingswet, waarbij het oogmerk van de regels wordt geschetst. Activiteiten waar geen decentrale overheid als bevoegd gezag is opgenomen zijn in dit overzicht weggelaten.

[55] iplo.nl, zoeken op vergunningplicht

4.1.1 Omgevingsplanactiviteit

Een omgevingsplanactiviteit is een activiteit die in het omgevingsplan vergunningplichtig is gesteld, of een activiteit die in strijd is met het omgevingsplan.[56] De hoofdregel daarbij is dat het college van burgemeester en wethouders het bevoegd gezag is, omdat het gaat om decentrale regels in het gemeentelijke omgevingsplan. Omgevingsplanactiviteiten worden gesteld met als oogmerk de doelen van de Omgevingswet: het met het oog op duurzame ontwikkeling, de bewoonbaarheid van het land en de bescherming en verbetering van het leefmilieu bereiken en in stand houden van een veilige en gezonde fysieke leefomgeving en omgevingskwaliteit, alsmede het doelmatig beheren, gebruiken en ontwikkelen van de fysieke leefomgeving ter vervulling van maatschappelijke behoeften.[57] Deze doelen zijn schematisch weergegeven in paragraaf 4.1.9.

4.1.2 Rijksmonumentactiviteit

Ingevolge art. 13.1 e.v. Bal is het college van burgemeester en wethouders in beginsel bevoegd gezag ten aanzien van rijksmonumentactiviteiten. Voor rijksmonumentactiviteiten die in hoofdzaak worden verricht in territoriale zeeën buiten de gemeente geldt een uitzondering, en is de Minister van Infrastructuur en Waterstaat bevoegd.[58] De regels ten aanzien van rijksmonumentactiviteiten zijn gesteld met het oogmerk op het behoud van cultureel erfgoed.[59] De hoofdregel is dat rijksmonumentactiviteiten vergunningplichtig zijn – behalve ten aanzien van activiteiten genoemd in art. 13.11 Bal. Er geldt te allen tijde een specifieke zorgplicht die ertoe strekt dat men alle redelijke maatregelen moet nemen om beschadiging of vernieling van het monument te voorkomen.[60] Ten aanzien van die specifieke zorgplicht kunnen maatwerkregels gesteld worden.[61]

4.1.3 Milieubelastende activiteiten en lozingsactiviteiten

Ingevolge art. 2.3 Bal is het college van burgemeester en wethouders in beginsel bevoegd gezag ten aanzien van milieuvergunningen, tenzij er sprake is van een uitzondering op die hoofdregel. In de tabel hieronder is een overzicht van deze uitzonderingen opgenomen:

Bevoegd gezag	Activiteiten
Waterschap (art. 2.4 Bal)	- Lozingsactiviteit op een oppervlaktewaterlichaam in beheer bij een waterschap

[56] Bijlage artikel 1.1 Omgevingswet
[57] Art. 5.21 Omgevingswet.
[58] Art. 13.4 Besluit activiteiten leefomgeving.
[59] Art. 13.2 Besluit activiteiten leefomgeving.
[60] Art. 13.7 Besluit activiteiten leefomgeving.
[61] Art. 13.8 Besluit activiteiten leefomgeving.

	- Lozingsactiviteit op een zuiveringstechnisch werk
Provincie (art. 2.5 Bal)	- Aanleggen en gebruiken van open bodemenergiesysteem
Minister van Infrastructuur en Waterstaat (art. 2.6 Bal)	- Lozingsactiviteit op een oppervlaktewaterlichaam in beheer bij het Rijk - Exploiteren van een buisleiding met gevaarlijke stoffen - Milieubelastende activiteiten die in hoofdzaak worden verricht in de gebieden genoemd in art. 2.6, tweede lid, Bal.
Minister van Economische Zaken en Klimaat (art. 2.7 Bal)	- Exploiteren van een mijnbouwwerk
Minister van Landbouw, Natuur en Voedselkwaliteit (art. 2.8 Bal)	- Op of in de bodem brengen van meststoffen

De regels ten aanzien van milieubelastende activiteiten zijn gesteld met het oogmerk op het waarborgen van veiligheid, het beschermen van gezondheid en het beschermen van het milieu.[62] Er geldt te allen tijde een specifieke zorgplicht die ertoe strekt dat men alle redelijke maatregelen moet nemen om nadelige gevolgen voor de veiligheid, gezondheid en milieu te voorkomen, beperken of achterwege te laten.[63] Onderdeel daarvan is het toepassen van de best beschikbare technieken en het treffen van passende maatregelen ten behoeve van het voorkomen van ongewone voorvallen.[64] Het bevoegd gezag kan maatwerkregels stellen ten aanzien van die specifieke zorgplicht, ongewone voorvallen en de algemene regels.[65] Daarnaast heeft het bevoegd gezag de bevoegdheid maatwerkvoorschriften te stellen aan vergunningen.[66]

4.1.4 Natura 2000-activiteiten

Ingevolge art. 11.3 Bal is het college van gedeputeerde staten bevoegd gezag ten aanzien van Natura 2000-activiteiten, tenzij sprake is van een Natura 2000-activiteit van nationaal belang of activiteiten genoemd in

[62] Art. 2.2 Besluit activiteiten leefomgeving.
[63] Art. 2.11 Besluit activiteiten leefomgeving.
[64] Art. 2.11, tweede lid onder c en e, Besluit activiteiten leefomgeving.
[65] Art. 2.12 Besluit activiteiten leefomgeving.
[66] Art. 2.13 Besluit activiteiten leefomgeving.

art. 4.12 Omgevingsbesluit die verslechterende of significant verstorende gevolgen voor een Natura 2000-gebied kunnen hebben. Die regels zijn gesteld met het oogmerk op natuurbescherming.[67] Er geldt te allen tijde een specifieke zorgplicht die ertoe strekt dat men alle redelijke maatregelen moet nemen om nadelige gevolgen voor de natuurbescherming te voorkomen, beperken of activiteiten om die reden achterwege te laten.[68] Het bevoegd gezag kan onder andere maatwerkregels stellen ten aanzien van die specifieke zorgplicht en ongewone voorvallen, alsmede met het oog op natuurbescherming.[69] Daarnaast heeft het bevoegd gezag de bevoegdheid maatwerkvoorschriften te stellen aan vergunningen.[70]

4.1.5 Flora- en fauna-activiteiten

Ingevolge art. 4.6 van het Omgevingsbesluit is het college van gedeputeerde staten bevoegd gezag ten aanzien van flora- en fauna-activiteiten, tenzij sprake is van een activiteit van nationaal belang of activiteiten genoemd in art. 4.12 Omgevingsbesluit.[71] Die regels zijn grotendeels gesteld met het oogmerk op natuurbescherming. Voor een aantal specifieke regels geldt een aantal aanvullende oogmerken.[72] Er geldt te allen tijde een specifieke zorgplicht die ertoe strekt dat men alle redelijke maatregelen moet nemen om nadelige gevolgen voor de natuurbescherming te voorkomen, beperken of activiteiten om die reden achterwege te laten.[73] Het bevoegd gezag kan onder andere maatwerkregels stellen ten aanzien van een aantal algemene regels.[74] Daarnaast heeft het bevoegd gezag de bevoegdheid maatwerkvoorschriften te stellen aan vergunningen.[75]

4.1.6 Wateronttrekkingsactiviteiten

Ingevolge art. 4.3 van het Omgevingsbesluit is het college van gedeputeerde staten bevoegd gezag ten aanzien van wateronttrekkingsactiviteiten.[76] Regels omtrent wateronttrekkingsactiviteiten zijn gesteld met de volgende oogmerken:[77]

- Het voorkomen en beperken van overstromingen, wateroverlast en waterschaarste;

---

[67] Art. 11.2 Besluit activiteiten leefomgeving.
[68] Art. 11.6 Besluit activiteiten leefomgeving.
[69] Art. 11.7 Besluit activiteiten leefomgeving.
[70] Art. 11.9 Besluit activiteiten leefomgeving.
[71] Art. 11.23, eerste lid, Besluit activiteiten leefomgeving.
[72] Art. 11.23 Besluit activiteiten leefomgeving.
[73] Art. 11.27, Besluit activiteiten leefomgeving.
[74] Art. 11.27 Besluit activiteiten leefomgeving.
[75] Art. 11.31 Besluit activiteiten leefomgeving.
[76] Artt. 4.3 Omgevingsbesluit jo. 16.4 Besluit activiteiten leefomgeving.
[77] Art. 16.2 Besluit activiteiten leefomgeving.

- Het beschermen en verbeteren van de chemische en ecologische kwaliteit van watersystemen; en,
- Het vervullen van maatschappelijke functies door watersystemen.

Er geldt geen specifieke zorgplicht. De wet voorziet niet in het stellen van maatwerkregels of maatwerkvoorschriften.

4.1.7 Ontgrondingsactiviteit

Ingevolge art. 4.6 van het Omgevingsbesluit is het college van gedeputeerde staten in beginsel bevoegd gezag ten aanzien van wateronttrekkingsactiviteiten in het winterbed van een tot de rijkswateren behorende rivier, of indien een meervoudige aanvraag een ontgrondingsactiviteit van meer dan 100.000 m^3 omvat.[78] Regels met betrekking tot ontgrondingsactiviteiten zijn gesteld met de volgende oogmerken: [79]

- Het voorkomen en beperken van overstromingen, wateroverlast en waterschaarste;
- Het beschermen en verbeteren van de chemische en ecologische kwaliteit van watersystemen; en,
- Het vervullen van maatschappelijke functies door watersystemen.

Er geldt geen specifieke zorgplicht. De wet voorziet niet in het stellen van maatwerkregels of maatwerkvoorschriften.

4.1.8 Bouwactiviteit

Ingevolge art. 2.2 Besluit bouwwerken leefomgeving (Bbl) is het college van burgemeester en wethouders bevoegd gezag ten aanzien van bouwactiviteiten, tenzij sprake is van een activiteit op dezelfde locatie als een vergunningplichtige lozing op een zuiveringstechnisch werk.[80] De oogmerken van die regels zijn afhankelijk van het type activiteit, in hoofdlijnen gelden dezelfde oogmerken als die van de Omgevingswet. Voor het in stand houden van bestaande bouw, nieuwbouw en voor verbouw zijn de regels gesteld met het oog op het waarborgen van veiligheid, het beschermen van de gezondheid en duurzaamheid en bruikbaarheid.[81] Voor gebruik van bouwwerken en bouw- en sloopwerkzaamheden gelden specifiekere oogmerken.[82] Er gelden specifieke zorgplichten ten aanzien van bouwwerkinstallaties, bestaande bouwwerken, brandveilig gebruik, bouw- en sloopwerkzaamheden en mobiele puinbrekers. Die specifieke zorgplicht houdt op hoofdlijnen in dat alle redelijke maatregelen moeten worden getroffen om negatieve gevolgen ten aanzien van die onderwerpen te voorkomen. [83]

---

[78] Artt. 4.3 Omgevingsbesluit jo. 16.4 Besluit activiteiten leefomgeving.
[79] Art. 16.2 Besluit activiteiten leefomgeving.
[80] Art. 3.3 Besluit activiteiten leefomgeving.
[81] Respectievelijk artt. 3.2, 4.2 en 5.2 Besluit activiteiten leefomgeving.
[82] Artt. 6.2, 7.2 en 7.28 Besluit activiteiten leefomgeving.
[83] Respectievelijk artt. 2.6, 3.5, 6.4, 7.4 en 7.31 Besluit bouwwerken leefomgeving.

Ten aanzien van bouwwerken geldt dat het college van burgemeester en wethouders maatwerkregels kan stellen in het omgevingsplan.[84] Die maatwerkregels kunnen – voor zover mogelijk relevant voor dit onderzoek — worden gesteld ten aanzien van de bruikbaarheid bij nieuwbouw,[85] die slechts een versoepelend karakter ten opzichte van het Bbl kunnen hebben.[86]

4.1.9 Beoordelingsregels omgevingsvergunningen in relatie tot digitalisering

De hoofdregels ten aanzien van toetsingscriteria bij aanvragen van omgevingsvergunningen zijn opgenomen in hoofdstuk 8 van het Besluit kwaliteit leefomgeving. Een toetsing van dit hoofdstuk, in samenhang met de regels in het Omgevingsbesluit, Besluit activiteiten leefomgeving en het Besluit bouwwerken leefomgeving brengt met zich mee dat digitalisering geen expliciet onderdeel uitmaakt van de beoordelingsregels. De vraag of wel van een impliciete doorwerking sprake kan zijn komt later in deze rapportage aan bod. In de onderstaande tabel zijn de oogmerken per vergunningplichtige activiteit schematisch uitgewerkt:

Vergunningplichtige activiteit	Oogmerk regels
Omgevingsplanactiviteit	Met het oog op duurzame ontwikkeling, de bewoonbaarheid van het land en de bescherming en verbetering van het leefmilieu bereiken en in stand houden van een veilige en gezonde fysieke leefomgeving en omgevingskwaliteit, alsmede het doelmatig beheren, gebruiken en ontwikkelen van de fysieke leefomgeving ter vervulling van maatschappelijke behoeften.
Rijksmonumentactiviteit	Behoud van cultureel erfgoed.
Ontgrondingsactiviteit	Voorkomen en beperken van overstromingen, wateroverlast en waterschaarste; beschermen en verbeteren van chemische

[84] Art. 2.3 Besluit bouwwerken leefomgeving.
[85] Art. 4.7 Besluit bouwwerken leefomgeving.
[86] Art. 4.161 Besluit bouwwerken leefomgeving.

	en ecologische kwaliteit van watersystemen; vervullen van maatschappelijke functies door watersystemen.
Natura 2000-activiteit (GS)	Natuurbescherming.
Bouwactiviteit	*Afhankelijk van type activiteit.*
Milieubelastende activiteit en lozingsactiviteiten	Waarborgen van veiligheid, beschermen van gezondheid en beschermen van het milieu.
Waterontrekkingsactiviteit (GS)	Voorkomen en beperken van overstromingen, wateroverlast en waterschaarste; beschermen en verbeteren van chemische en ecologische kwaliteit van watersystemen; vervullen van maatschappelijke functies door watersystemen.
Een flora- en fauna activiteit	Natuurbescherming *Aanvullende oogmerken afhankelijk van type activiteit.*

Tabel 3 Schematische weergave oogmerken vergunningen

4.2 Vergunningen op grond van de Algemene Plaatselijke Verordening

Op lokaal niveau kunnen vergunningplichten in het leven worden geroepen door middel van de Algemene Plaatselijke Verordening (APV). In deze paragraaf staan die vergunningen centraal, die een mogelijk verband met de digitale veiligheid kunnen hebben.

4.2.1 Standplaatsvergunning

De standplaatsvergunning kent geen grondslag in wetten in formele zin; het verbod op het innemen van een standplaats zonder standplaatsvergunning is opgenomen in de model-APV van de VNG.[87] Het oogmerk van regels met betrekking tot standplaatsen is gelegen in de bescherming van het milieu, de ordening van straathandel en het voorkomen van verstoring van de openbare orde.[88] De weigeringsgronden van een standplaatsvergunning zijn gelegen in de belangen van de openbare orde, openbare veiligheid, volksgezondheid en de bescherming van het milieu alsmede de redelijke eisen van welstand en het in gevaar brengen van een redelijk verzorgingsniveau van de consument.[89]

[87] Art. 5:18 model-APV VNG.
[88] Toelichting art. 5:18 model-APV VNG.
[89] VNG, *Standplaatsen*, z.d.

4.2.2 Evenementenvergunning

De burgemeester heeft een verantwoordelijkheid en bevoegdheid als het gaat om toezicht op evenementen.[90] Ter uitvoering daarvan is in gemeentelijke APV's in veel gevallen een verbod opgenomen voor het houden van evenementen zonder vergunning van de burgemeester.[91] Bij de toetsing van deze aanvraag wordt rekening gehouden met de algemene weigeringsgronden in de APV, die in de Model-APV zien op de openbare orde, openbare veiligheid, volksgezondheid en bescherming van het milieu.[92] In sommige APV's zijn bijzondere weigeringsgronden opgenomen ten aanzien van evenementenvergunningen. Zo heeft de gemeente Amsterdam een specifieke weigeringsgrond indien "de organisator onvoldoende waarborgen biedt voor een goed verloop van het evenement, gelet op de hiervoor genoemde belangen,"[93] Om te toetsen of de vergunning kan worden verleend met het oog op die weigeringsgronden, is het van belang de risico's van een evenement in kaart te brengen. In het Nationaal Handboek Evenementen Veiligheid is door een groep van gemeenten, tezamen met de Vereniging van Evenementen Makers getracht een uniform kader te ontwikkelen, waarbij ook handvaten met betrekking tot het bepalen van risico's zijn opgenomen.[94] Onderdeel daarvan is het nagaan van mogelijke scenario's aan de hand van feitelijke gegevens. Aan de hand van die risicoanalyse kunnen vergunningsvoorschriften worden gesteld, die eisen kunnen inhouden ten aanzien van de bescherming van de openbare orde, openbare veiligheid, volksgezondheid en/of bescherming van het milieu bij vergunningplichtige evenementen.[95]

4.2.3 Exploitatievergunning

Algemeen wordt aangenomen dat in de APV een vergunningplicht kan worden opgenomen voor de bedrijfsmatige activiteiten (exploitatie) in een bepaald gebied of een bepaalde branche, indien kan worden aangetoond dat op die locatie of in die branche (criminele) activiteiten plaatsvinden die een negatief effect met zich meebrengen op de openbare orde en veiligheid of de leefbaarheid.[96] Branches waarin deze exploitatievergunningen gebruikelijk zijn betreffen de horeca en prostitutie. Ook voor exploitatie van speelgelegenheden is een exploitatievergunning vaak noodzakelijk.[97] Uit de Handreiking APV en

---

[90] Art. 174 Gemeentewet.
[91] Deze vergunningsplicht is tevens opgenomen in artt. 2:24-2:25 Model-APV VNG.
[92] Art. 1:8 Model-APV VNG.
[93] Art. 2.43, onder h, APV Gemeente Amsterdam.
[94] Vereniging van Evenementen Makers, *Nationaal Handboek Evenementen Veiligheid 1.0. Een gemeenschappelijk denkkader omtrent veiligheid*. NHEV: 2019, p. 297.
[95] Art. 1.4 Model-APV VNG.
[96] Zie in dat kader ABRvS 3 maart 2021, ECLI:NL:RVS:2021:461 waar niet aan de motiveringsplicht is voldaan.
[97] Art. 3.28a e.v. Model-APV VNG.

Ondermijning van de VNG komen ook nog de autoverhuurders, glazenwassers, spyshops, woning- en kamerverhuur en recreatieparken naar voren als branches of activiteiten die in sommige gemeenten reeds vergunningplichtig zijn of worden gesteld bij APV.[98]

In het najaar van 2023 is de Model-APV van de VNG gewijzigd, met daarin als nieuwe toevoeging de mogelijkheid voor het creëren van een vergunningplicht voor aan te wijzen bedrijfsmatige activiteiten ter bestrijding van ondermijning.[99] Dit wordt ook wel een 'Ondermijningsvergunning' genoemd, een vorm van een exploitatievergunning. Deze ondermijningsvergunning was op eigen initiatief ook al opgenomen in APV's voorafgaand aan deze brief.[100] Deze vergunningplicht is ingericht met het oog op de openbare orde en veiligheid, en is gericht op het stimuleren van een gezond ondernemersklimaat en het weren van malafide ondernemers.

4.2.4 Alcoholvergunning

Voor horecabedrijven geldt voor het schenken van alcoholhoudende dranken dat er een vergunning op grond van de Alcoholwet aanwezig moet zijn. Die kan worden verleend door de burgmeester op grond van artikel 3 van deze wet. In artikel 25a van de Alcoholwet is bepaald dat bij gemeentelijke verordening het bedrijfsmatig of anders dan om niet verstrekken van alcoholhoudende drank in inrichtingen kan worden verboden of aan beperkingen kan worden onderworpen. In de model-APV van de VNG zijn hierover bepalingen opgenomen in het hoofdstuk over de openbare ordebepalingen. Deze wetgeving is in zijn geheel gericht op het fysieke domein. Echter laat een voorbeeld uit de interviews zien dat indien gedigitaliseerde betaalsystemen aanwezig zijn en deze haperen, er een risico bestaat voor de openbare orde (**R2**). Datzelfde kan verondersteld worden indien andere bedrijfssystemen al dan niet volledig digitaal zijn georganiseerd.

4.3 Focusgroep en interviews over vergunningen en de huidige aandacht voor digitale aspecten in vergunningverlening.

Uit de focusgroep blijkt dat er verschillend wordt gedacht over het stellen van regels, waarbij er drie lijnen zijn te ontdekken: voorstanders, tegenstanders en alternatieven voor regelgeving. Een deel van de respondenten ziet het vergunnen onder voorschriften van digitale veiligheid niet als gemeentelijke taak richting bedrijven. Los van de kennis en vaardigheden die vaak niet aanwezig zijn, kan eigen

[98] VNG, Handreiking APV en Ondermijning, Den Haag 2020, p. 29-39.
[99] Ledenbrief Vereniging Nederlandse Gemeenten, VNG, *7 november 2023*.
[100] Zie bijvoorbeeld art. 53a APV Tilburg, artt. 2:39-2:40d APV Maassluis en art. 2:47 APV Utrecht.

gemeentelijke regelgeving in hun ogen kostenverhogend werken voor bedrijven of maakt het de gemeente onaantrekkelijk als vestigingsklimaat voor bedrijven. Voorstanders vinden over het algemeen wel dat als er regels moeten komen, dit standaardregels moeten zijn die in alle gemeenten gelijk zijn. Ook hier wordt weer verwezen naar de certificeringsnormen (NEN ISO, NIS2, BIO). Als alternatief voor regels wordt door een aantal experts verwezen naar communicatie/ bewustwording als middel om digitale veiligheid bij bedrijven te bevorderen.

In de interviews is eenzelfde lijn van meningen te ontdekken voor het bedrijfsleven. Voorstanders van regels verwijzen als juridisch kader ook naar het Bouwbesluit, dat hiervoor kan dienen (**R4**) of de NEN ISO-/BIO-normen (**R4, R5, R6, R8, R10, R12, R14**).

Wat overduidelijk blijkt is dat van de geïnterviewde bestuurders niemand op dit moment regels stelt die de digitale veiligheid bij bedrijven regelt, omdat men vindt dat dit juridisch gezien niet kan. De bestuurders investeren in communicatie/ bewustwording, al dan niet met bedrijvenkoepels (**R7**). Een aantal respondenten zegt toezicht en handhaving op regionaal of landelijk niveau te prefereren (**R3, R8, R12**). De respondenten geven aan dat zij zich kunnen voorstellen dat gemeenten voor evenementen regels stellen op het gebied van de digitale veiligheid, maar dan bij de zogenaamde C-evenementen (de grote met landelijke uitstraling, zoals Lowlands, Zwarte Cross e.d.).

4.4 Conclusie

In dit hoofdstuk is besproken welke soorten vergunningen en vergunningverleners zijn te onderscheiden en of er al aandacht wordt besteed aan digitale veiligheid binnen vergunningverlening. Decentrale overheden kennen verschillende bevoegdheden tot vergunningverlening, zowel op nationaal als regionaal niveau. Voor decentrale overheden bestaat een op nationaal niveau in de Omgevingswet geregeld vergunningenstelsel. Daarnaast bestaat er lokaal ruimte voor het regelen van vergunningplichten, zoals het geval is bij de vergunningen op grond van de APV en de Alcoholwet.

Eén van de meest voorkomende typen vergunningen betreft vergunningen in het ruimtelijk domein, die sinds 1 januari 2024 gestoeld zijn op de Omgevingswet. De Omgevingswet kent een vergunningstelsel dat verschillende decentrale overheden belast met verschillende verantwoordelijkheden. Het overkoepelende doel van de Omgevingswet is gericht op het beschermen en benutten van de fysieke leefomgeving, wat een breed toepassingsbereik kent. Bij of ingevolge de Omgevingswet zijn of kunnen vergunningplichten in het leven worden geroepen die zien op bepaalde activiteiten. Vergunningplichten kunnen daarmee zowel op centraal als op decentraal niveau worden geregeld. Digitale veiligheid wordt niet als

zodanig genoemd binnen de Omgevingswet, maar verwezenlijking van risico's ten gevolge van digitale onveiligheid kan gevolgen met zich meebrengen voor de fysieke leefomgeving. Dat brengt met zich mee dat ook de beperking van digitale risico's ten behoeve van de bescherming van de fysieke leefomgeving binnen de reikwijdte van de Omgevingswet valt.

Die enkele constatering is onvoldoende om te kunnen stellen dat digitale risico's te allen tijde kunnen worden meegewogen in (omgevings)vergunningverlening. Vergunningen dienen te worden getoetst aan de hand van de beoordelingsregels die voortvloeien uit de regeling waarop deze gebaseerd zijn. Deze beoordelingsregels zijn vaak ruim geformuleerd, en bevatten geen specifieke eisen of beoordelingsnormen ten aanzien van digitalisering. Die ruime formulering brengt met zich mee dat digitale veiligheid een onderdeel van vergunningvoorschriften zou kunnen zijn. In hoeverre dat mogelijk is, hangt af van de oogmerken waarvoor de vergunningplicht in het leven is geroepen. Waar het gaat om de Omgevingswet kan worden geconcludeerd dat regulering allereerst slechts mag zien op de fysieke leefomgeving, of ten aanzien van gevolgen voor de fysieke leefomgeving. Slechts digitale risico's waarbij redelijkerwijs effecten op het fysieke domein kunnen worden verwacht zouden daarmee onderhavig kunnen zijn aan regulering op grond van de Omgevingswet. Vervolgens dient op basis van de specifieke vergunningsplicht te worden nagegaan of, en in hoeverre, regulering aansluit op de doelen die het instellen van die vergunningplicht nastreeft. Het stellen van voorschriften of regels ten behoeve van digitale veiligheid mag niet als uitgangspunt dienen, datzelfde geldt voor het oogmerk om de digitale veiligheid binnen bedrijven te vergroten. Er dient onderbouwd te kunnen worden dat voor de specifieke activiteit, aanvrager of locatie sprake is van digitale risico's die gevolgen voor de fysieke leefomgeving met zich mee kunnen brengen – waarbij de beperking van de risico's voor de fysieke leefomgeving het oogmerk dient te zijn.

Uit de focusgroep en de interviews kan worden geconcludeerd dat men wat afstand houdt tot het stellen van regels over digitale veiligheid bij bedrijven en verwijst naar certificering omdat men gelijke regels in alle gemeenten belangrijk vindt. Vanuit de praktijk komt naar voren dat voor zover de respondenten weten er op dit moment geen gemeenten zijn die voorschriften stellen aan evenementenvergunningen die de digitale veiligheid van evenementen regelen.

5 Juridische mogelijkheden van de gemeente voor het opleggen van verplichtingen ten aanzien van digitale risico's

In dit hoofdstuk staat de volgende deelvraag centraal:

> Welke juridische mogelijkheden hebben gemeenten en medeoverheden om bedrijven te verplichten aan bepaalde eisen te voldoen?

Ter beantwoording van deze deelvraag is onderzocht in hoeverre binnen het in hoofdstuk 3 aangegeven juridische kader, er juridische mogelijkheden voor gemeenten zijn om de digitale veiligheid te kunnen regelen voor bedrijven binnen de gemeente. De basis voor het handelen van een gemeente vormen de Grondwet en de Gemeentewet, maar ook het Europese recht geeft een vrij strak kader omdat in de gehele Europese Unie (EU) er sprake is van een vrije handel. Binnen de EU is sprake van een interne markt en een gemeenschappelijke ruimte waarbinnen goederen, diensten, kapitaal en personen vrij kunnen circuleren en bewegen. Met name de vrijheid voor bedrijven om zich binnen de gehele Europese unie te kunnen vestigen en handel te drijven vormt een belangrijke pijler van het unierecht. Overheden mogen daar niet zonder meer belemmeringen voor opwerpen. Gemeentelijke regels over de digitale veiligheid bij bedrijven vormen een potentiële belemmering. In deze paragraaf wordt de ruimte van de regelgevende bevoegdheid van de gemeente verkend in het licht van dit EU-recht. Bij de beantwoording van deze vraag is een literatuuronderzoek gedaan alsmede een wetsanalyse en zijn vragen gesteld aan de focusgroep van experts en aan de geïnterviewden.

5.1 Regelgevende bevoegdheid voor gemeenten

De regelgevende bevoegdheid voor gemeenten alsmede de reikwijdte ervan is vastgelegd in de Grondwet en de Gemeentewet. De regels dienen betrekking te hebben op 'de huishouding' van de gemeente.[101] Dat de openbare orde en de handhaving ervan tot het domein van deze huishouding behoren is o.a. te lezen in artikel 172 Gemeentewet, waarin de burgemeester het aangewezen bestuursorgaan is om deze openbare orde te handhaven. In het onderzoek 'Burgemeesters in cyberspace' is uitgewerkt wat onder het open begrip 'openbare orde' juridisch wordt verstaan. Dat is 'het niveau van rust' in de zin van 'normale gang van zaken' in het voor het publiek toegankelijke domein, ofwel het openbare

[101] Artt. 124 Grondwet jo. 108 Gemeentewet.

gemeenschapsleven. Maar ook 'een bepaalde toestand in de publieke ruimte, en wel een normale situatie van orde en rust.[102]

Dat de openbare orde valt onder het algemeen belang, dat de overheid geacht wordt te behartigen mag evident zijn. Zonder een handhaving van de openbare orde zou er chaos kunnen zijn.[103] Dat is precies wat speelt in de virtuele wereld. De ruime vrijheid door afwezigheid van regels zorgt voor misstanden, waardoor ook hier de overheid met regelgeving probeert een orde aan te brengen en deze te handhaven door middel van regels en beleid. Het meest recente vraagstuk is dat van de regeling rond Artificiële Intelligentie.[104] Dat er een openbare orde is in het virtuele domein is niet vanzelfsprekend, maar wordt zo langzamerhand wel verondersteld door de wetgever.[105]

Daar waar handhaving van de openbare orde in het virtuele domein nog lastig is voor gemeenten, is de handhaving bij het bestrijden van verstorende effecten in de fysieke openbare orde vanuit het virtuele domein duidelijk aan het worden, waarbij gemeenten optreden als deze ordeverstorende effecten zich voordoen in de betreffende gemeente, ook al staat de computer of server elders.[106]

5.1.1 De EU en de vrije handel van bedrijven

Gemeenten dienen te voldoen aan het EU-recht. De lidstaten zijn er verantwoordelijk voor dat hun decentrale overheden zich hieraan houden. Het is aan de lidstaten zelf hoe dit te regelen. In Nederland is dit geregeld in de Wet houdbare overheidsfinanciën (Whof) en de Wet naleving Europese regelgeving publieke entiteiten, waar in artikel 2, lid 4 een verwijzing is gemaakt naar de toezichtbepalingen in de Gemeentewet.[107]

Voor bedrijven, die zich vestigen in een gemeente geldt op basis van het unierecht in principe een vrije vestiging en een vrije handel in de gehele Europese Unie (EU).[108] Er mogen geen regels worden gesteld die deze vrijheden belemmeren en als er regels zijn, dan dienen deze te gelden voor alle bedrijven in de EU om discriminatie te voorkomen.[109] Ook dienen deze regels de overige principes van de EU-

---

[102] Bantema et.al., *'Burgemeester in Cyberspace'*, Den Haag 2018, p.18. De definities in dit onderzoek zijn gebaseerd op het rapport van De Jong et.al., *'Orde in de Openbare Orde'*, 2016, p.10-13 met daarin een uitgebreide bronnenlijst.
[103] Zie hierover o.a. Brouwer, 'Wat is openbare orde', in NJB 9 september 2016, nr. 1561.
[104] 'AI- regels: wat het Europees Parlement wil', europarl.europa.eu, 20 februari 2023.
[105] Bantema et. al., '*Burgemeesters in Cyberspace'*, Den Haag 2018, p.127-131.
[106] Bantema, Westers, Munneke, '*Niet bevoegd, wel verantwoordelijk'*, Den Haag 2020 en Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022, p. 32.
[107] Hirsch Ballin, Janse de Jonge & Leenknegt, *Uitleg van de Grondwet*, Den Haag: Boom Juridisch 2020, p. 553.
[108] Art. 26 Verdrag betreffende de Werking van de Europese Unie.
[109] Art. 3 Verdrag betreffende de Europese Unie.

regelgeving te respecteren en mogen zij geen ongerechtvaardigde belemmering vormen hiervoor, te weten:

- Transparantie. Regels dienen transparant te zijn en evenredig met het doel dat met de regel is gediend.[110]
- Het verbod van ontoelaatbare economische ordening, verwoord in een verbod op kwantitatieve beperkingen of maatregelen van gelijke werking. [111] Een maatregel van gelijke werking wordt aangemerkt als 'iedere (handels)regeling van EU-lidstaten, die de intracommunautaire handel al dan niet rechtstreeks, daadwerkelijk of potentieel, kan belemmeren (Dassonville-formule).[112] Dit betekent concreet dat een overheidsmaatregel, die het handelsverkeer kan belemmeren, een inbreuk kan vormen op artikel 34 VWEU. Dit kunnen gemeentelijke voorschriften voor bedrijven zijn.
- Voldoen aan richtlijn (EU) 2015/1535 (notificatierichtlijn), waarin is bepaald dat lidstaten technische voorschriften voor bedrijven dienen te melden aan de EC om ervoor te zorgen dat voldaan wordt aan het uitgangspunt van de vrijheid van goederen, personen, diensten en kapitaal.[113]
- Voldoen aan de EU Dienstenrichtlijn, die de vrijheid van diensten binnen de EU nader regelt. In Nederland is deze richtlijn vertaald in de Dienstenwet.[114] Deze wet zorgt ervoor dat verleners van diensten, die zich vestigen in een gemeente, op een eenduidige en eenvoudige wijze kunnen achterhalen aan welke regels ze moeten voldoen. Er dienen in dat verband zo weinig mogelijk administratieve en financiële lasten, waaronder vergunningverlening, te zijn voor deze bedrijven/ diensten.

Als gemeenten regels kunnen en willen stellen om de digitale veiligheid bij bedrijven te kunnen garanderen, dan mogen deze regels de vrije handel niet belemmeren en geen ontoelaatbare economische ordening omvatten.

De vraag is of vergunningsregels van gemeenten over de digitale veiligheid bij bedrijven een vorm van ontoelaatbare economische ordening is. Er zou kunnen worden gesteld dat een dergelijke regel een vorm van een (verborgen) kwantitatieve beperking of maatregel van gelijke werking is omdat het een beperking oplegt aan het bedrijf: het bedrijf kan nl. geen zakendoen indien de digitale veiligheid niet is

---

[110] Zie daarvoor o.a. ABRvS 20 juni 2018, ECLI_NL:RVS:2018:2062 (Appingedam), en ABRvS 27 maart 2019, ECLI:NL:RVS:2019:965.

[111] Artt. 34 en 35 VWEU.

[112] HvJEU, 11 juli 1974, ECLI:EU:C:1974:82, Dassonville.

[113] Richtlijn (EU) 2015/1535 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (codificatieregeling).

[114] Artt. 56-62 verdrag betreffende de werking van de Europese Unie, geïmplementeerd in de Dienstenwet, *Stbl.* 2009-505.

geregeld. Artikel 36 van het VWEU kent echter een uitzondering voor beperkende regels als ze dienen o.a. ter bescherming van de openbare orde mits ze geen discriminatie of een verkapte beperking van de vrije handel tussen lidstaten vormen. Als er dus een gemeentelijke regel is voor bedrijven ter bescherming van de digitale veiligheid met als oogmerk de bescherming van de openbare orde, dan zou die in principe toelaatbaar kunnen zijn, mits deze regel voldoet aan de overige vereisten van het EU-recht.

5.1.2 Doel van wetgeving bepalend voor nadere regelgeving

Bij het stellen van regels aan bedrijven, die zich vestigen in de gemeente, dient de gemeente zich aan bovenstaande EU-wetgeving te houden. Het doel van regels is vastgelegd in de betreffende wet en is bepalend voor de vraag of er nadere regels mogen worden gesteld door de gemeente via een vergunning en die doelen verschillen. In hoofdstuk 4 is nader ingegaan op de doelen/ oogmerken van de wetgeving, die van toepassing is bij de vestiging van bedrijven in een gemeente. Samenvattend zijn dat:

- Omgevingswet: regels in een bestemmingsplan (per 1.1.2024 het Omgevingsplan), waarin staat waar bedrijven zich mogen vestigen en aan welke regels met betrekking tot de fysieke leefomgeving ze moeten voldoen.[115]
- Milieuregels op basis van de Omgevingswet.
- Regels over natuurbescherming en bescherming van de flora en fauna op basis van de Omgevingswet.
- Regels ter bescherming van monumenten op basis van de Omgevingswet.
- Regels voor horecabedrijven over het schenken van alcoholhoudende dranken.
- Regels in de APV over reclame-uitingen, sluitingstijden van horeca en winkels, het plaatsen van objecten in de openbare ruimte.[116]

5.1.3 Aanvullende regelgevende bevoegdheid van gemeenten in het kader van NIS2

In paragraaf 3.1.4 werd de NIS2-richtlijn geïntroduceerd. Op dit moment werkt de regering aan een wetsvoorstel dat de zogenaamde NIS2-richtlijn, vastgesteld door de EU, moet implementeren.[117] De NIS2-

[115] Art. 4.1, eerste lid, Omgevingswet.
[116] E.R. Muller, H.R.B.M. Kummeling & R. Nehmelman (red.), *Instituten van de staat*, Deventer: Wolters Kluwer 2020, paragraaf 6.3.
[117] NIS = Network and Information Systems; Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad, 14 december 2022, betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de gehele Unie, tot wijziging van de richtlijn (EU) 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148, (NIS2 Richtlijn), digitaleoverheid.nl, zoeken op 'NIS2'.

richtlijn stelt eisen aan de digitale beveiliging van bepaalde (vitale) sectoren door te werken met (strenge) beveiligingsnormen en meldings- en rapportagevereisten voor incidenten.[118] Het is de opvolger van de NIS-richtlijn,[119] die in Nederland is geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen, de Wbni.[120] Het doel van de NIS2-richtlijn is het niveau van informatiebeveiliging en digitale veiligheid bij zowel publieke als private organisaties te verhogen. Deze organisaties zijn onderverdeeld in vier categorieën:

Tabel 4 — Categorieën organisaties en entiteiten op grond van de NIS2-richtlijn

Type organisatie op basis van sector	
Zeer kritieke sectoren	**Andere kritieke sectoren**
Energie, transport, Infrastructuur financiële markt, gezondheidszorg, drinkwater, digitale infrastructuur, afvalwater, overheidsdiensten, ruimtevaart, beheer ICT-diensten, bankwezen.	Digitale aanbieders, post- en koeriersdiensten, afvalstoffenbeheer, levensmiddelen, chemische stoffen, onderzoek, vervaardiging/ manufacturing.
Type entiteit op basis van organisatie	
Essentiele entiteiten	**Belangrijke entiteiten**
Organisaties met meer dan 250 werknemers of een netto-omzet van meer dan €50 miljoen en een balanstotaal van meer dan €43 miljoen.	Organisaties met minimaal 50 werknemers of een jaaromzet of balanstotaal van meer dan €10 miljoen.

Bovenstaande indeling is o.a. van belang voor de mate van toezicht op het bedrijf. Kleine ondernemingen vallen in principe niet onder de NIS2 tenzij hun product of dienst van cruciaal belang is en het bedrijf daardoor aangewezen wordt door een ministerie, waardoor het alsnog onder de NIS2-richtlijn gaat vallen.[121] Ook bedrijven die leveren aan NIS2-bedrijven en organisatie, dienen aan de eisen in de NIS2-richtlijn te voldoen,[122] waardoor gesteld kan worden dat zeer veel bedrijven eronder (gaan) vallen en slechts een beperkt aantal bedrijven niet.

De vraag die hierbij gesteld kan worden is, in hoeverre gemeenten aan deze laatste categorie bedrijven, die dus buiten de NIS2 vallen, regels

[118] digital-strategy.ec.europa.eu, zoeken op 'NIS2'.
[119] Richtlijn (EU) 2016/1148.
[120] *Stbl.* 2018, 389.
[121] Europadecentraal.nl, zoeken op NIS2.
[122] Richtlijn (EU) 2022/2555, overweging 85.

mogen stellen om de digitale veiligheid te garanderen in het kader van de handhaving van de openbare orde.
De handhaving van de openbare orde is een dwingende reden van algemeen belang, zoals genoemd in artikel 36 van het VWEU en artikel 15, lid 3 onder b van de Dienstenrichtlijn. Het is nog niet duidelijk in hoeverre een gemeente een expliciete aanvullende verordenende bevoegdheid heeft in de implementatiewetgeving van de NIS2-richtlijn, aangezien Nederland momenteel werkt aan deze wetgeving. Volgens de website van de overheid volgt op de concept-uitwerking een consultatieronde.[123]

Voor het vraagstuk van dit onderzoek is het van belang dat er duidelijkheid komt in de implementatiewet of een gemeente het instrument van de vergunning onder voorschriften kan en mag toepassen bij zogenaamde niet-vitale bedrijven, die wel degelijk digitaal ontwrichtende en openbare- ordeverstorende incidenten kunnen veroorzaken, wanneer de digitale veiligheid niet op orde is.

Een voorbeeld zou kunnen zijn een digitale storing bij de software van een (grote) kermisattractie, waardoor er ongelukken gebeuren en er paniek uitbreekt. Dit voorbeeld werd ook genoemd in de focusgroep. Ervan uitgaande dat een kermisattractie geen essentiële dienst in het kader van de NIS2-richtlijn is, zou een aanvullende regeling mogelijk moeten kunnen zijn.

Indien de implementatiewet van de NIS2-richtlijn deze aanvullende bevoegdheid regelt of nadrukkelijk uitsluit, dan is het duidelijk voor gemeenten. Als deze wet hier niet in voorziet, is het de vraag om gemeenten een aanvullende regelgevende bevoegdheid hebben. Daarbij geldt dan de leer van de aanvullende regelgevende bevoegdheid en de al eerdergenoemde uitgangspunten van het EU-recht.

De aanvullende regelgevende bevoegdheid voor gemeentelijke APV's op het gebied van digitale veiligheid is uitgewerkt in een eerder onderzoek.[124] In dit onderzoek is uitgelegd dat artikel 121 van de Gemeentewet bepaalt dat "De bevoegdheid tot het maken van gemeentelijke verordeningen blijft ten aanzien van het onderwerp waarin door wetten, algemene maatregelen van bestuur of provinciale verordeningen is voorzien, gehandhaafd, voor zover de verordeningen met die wetten, algemene maatregelen van bestuur en provinciale verordeningen niet in strijd zijn". Bepalend is of zowel het onderwerp als het motief van de regeling aan elkaar gelijk zijn. Zo ja, dan houdt de

[123] 'Begin 2024 meer inzicht in wat organisaties te wachten staat', nctv.nl, z.d.
[124] Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022.

gemeentelijke regeling van rechtswege op te gelden omdat een hogere regeling, die hetzelfde regelt, voorgaat in ons hiërarchisch ingerichte stelsel van wetgeving. APV-regelingen die hetzelfde onderwerp regelen, maar een ander motief/belang hebben, kunnen standhouden.
In het vraagstuk dat in dit voorliggende onderzoek centraal staat, moet afgewacht worden welk motief/ oogmerk de landelijke implementatiewet zal krijgen en of op basis daarvan er een aanvullende regelende bevoegdheid aanwezig is voor gemeenten. Dit is een aandachtpunt.

5.1.4 Interviews over de regelgevende bevoegdheid van gemeenten op het gebied van digitale veiligheid.

De meeste geïnterviewde respondenten zien geen mogelijkheden binnen de huidige wetgeving voor een aanvullende regelgevende bevoegdheid. Zo geeft een van hen letterlijk aan dat er geen tot weinig instrumenten beschikbaar zijn (**R4**). Eén van de respondenten geeft aan dat er idealiter wel juridische mogelijkheden zouden moeten zijn en dat het vreemd is dat dit nog niet is gebeurd, met name voor de vitale infrastructuur, waarbij verwezen wordt een chemiebedrijf dat door middel van een digitaal probleem of een hack voor een grote milieuverontreiniging zou kunnen zorgen (**R5**). Een andere respondent weet niet hoe het juridisch zit maar hij kan zich voorstellen dat er eisen komen op het moment dat bedrijven van cruciaal belang zijn voor de maatschappij **(R15)**. Een andere respondent geeft aan dat je nagenoeg geen regels kan opleggen op dit gebied, in tegenstelling tot de fysieke omgeving zoals bouwregels, maar voor de digitale veiligheid is dit lastig. Verwezen wordt daarbij naar De Nederlandsche Bank, die actief stuurt op de digitale veiligheid van banken maar bij bedrijven en met name het mkb lijkt dit lastig. Gezegd wordt nog dat in de zorg er op dit moment een inhaalslag gaande is omdat de digitale veiligheid nog niet zo goed voor elkaar is (**R1**). Eén van de respondenten zou graag zien dat gemeenten moeten kunnen experimenteren met soortgelijke bepalingen voor bedrijven als de openbare orde in het geding is. Bij evenementen wordt één en ander geregeld waarbij de organisator verantwoordelijk is en wordt gehouden voor een ordentelijk verloop van het evenement. De gemeente is niet aansprakelijk (**R15**). Een andere respondent ziet absoluut geen rol van gemeenten weggelegd bij vergunningverlening en noemt voorbeelden waarbij aangegeven wordt dat zelfs basale kennis op het gebied van privacyregels in vergunningen vaak al niet eens aanwezig is en hierdoor fouten worden gemaakt bij vergunningverlening (**R12**).

5.2 Toekomstige mogelijkheden voor vergunningverlening

Omdat de digitale ontwikkelingen zeer snel gaan en veel regelgeving wordt gemaakt om deze ontwikkelingen te beheersen, ook voor gemeenten, is geïnterviewden gevraagd naar hun visie op deze (nabije) toekomstige ontwikkelingen. Rode lijn daarin is dat men nog

wat huiverig is om regels te stellen vooral ook omdat de capaciteit en kunde ontbreekt op gemeentelijke niveau om toezicht uit te oefenen en te kunnen handhaven. Het regionale dan wel landelijke niveau wordt passender gevonden. Mochten er regels gesteld kunnen worden (men denkt dan met name voor evenementen in de evenementenvergunning) dan gaat de voorkeur uit naar gelijkluidende voor alle gemeenten en het principe van certificering wordt daarbij als voorbeeld genoemd.

5.2.1 Interviews over toekomstige mogelijkheden voor vergunningverlening.

Vanuit de interviews blijkt bij sommige respondenten een wens te bestaan naar het kunnen invoeren van vergunningsvereisten. Gemeenten zouden volgens hen moeten kunnen eisen dat de digitale infrastructuur veilig en beveiligd is als de mogelijkheid er zou zijn. Wellicht in de APV (ook **R15**) of bij een omgevingsvergunning zou zoiets geregeld moeten worden (**R5**). Door deze respondent wordt aangegeven dat de dialoog met bedrijven belangrijk is, maar is een mate van afdwingbaarheid en ingrijpen door de overheid gewenst, mede door de risico's in het digitale domein naar het fysieke domein toe. Als voorbeeld worden genoemd cybercrime en de datalekken. Een andere respondent (**R4**) ziet mogelijkheden om aan te haken bij hoofdstuk 6 van het Bouwbesluit[125] dat zodanig zou kunnen worden aangepast dat daar regels in komen die bedrijven verplichten de digitale veiligheid te regelen, eventueel via een certificeringsstelsel, zoals bijvoorbeeld bij elektriciteit. Gemeenten hebben dan een mogelijkheid om dit te controleren en te handhaven en er gaat een preventieve werking van uit. Een al bestaand wettelijk kader op rijksniveau wordt dan gebruikt zodat het voor alle gemeenten gelijk is. Een andere respondent geeft aan geen mogelijkheden te zien en geen controle uit te kunnen voeren hierop (**R7**).

Eén van de respondenten geeft aan dat er in het kader van de NIS2-richtlijn al veel geregeld gaat worden op het gebied van de digitale veiligheid voor een grote schare aan bedrijven. Er geldt een soort van ketenverantwoordelijkheid in die zin dat bedrijven die handelen met NIS2-plichtige bedrijven, ook aan de NIS2-bepalingen moeten voldoen. Wettelijk gezien zijn er volgens deze respondent geen instrumenten te bedenken in het publiekrecht om digitale veiligheid bij bedrijven als gemeente af te dwingen, maar privaatrechtelijk wel. Men zou voor een wettelijke regeling bij een gemeente kunnen denken aan een eis van digitale veiligheid van een bedrijf analoog aan de brandveiligheid ervan. Een bedrijf moet hoe dan ook brandveilig zijn en zou ook digitaal veilig moeten zijn. Een ingang zou kunnen zijn dat deze regels gesteld gaan worden vanuit de bescherming van de inwoners, via wellicht de

[125] Het Bouwbesluit is met inwerkingtreding van de Omgevingswet vervallen en opgevolgd door het Besluit bouwwerken leefomgeving.

invalshoek van certificering (ISO-, BIO-normen) analoog aan brandveiligheid. Daarbij zou dan de stelling moeten zijn dat het in het algemeen belang is van een gemeente dat een bedrijf met zijn bedrijfsprocessen geen gevaar mag opleveren voor anderen, ook niet met de daarbij gebruikte digitale systemen. Bij de AVG is het de vraag of klantgegevens die via een datalek buit worden gemaakt, vallen onder het algemeen belang van een gemeente. Dit wordt door de respondent betwijfeld (**R14**).

Respondent **R3** geeft aan dat er gekeken moet worden naar het doel van de vergunning, als dit het middel is om in een gemeente de digitale veiligheid te regelen, nog los van of het kan en mag. Men moet zich dan afvragen of digitale veiligheid valt onder het begrip openbare orde. Zonder meer eronder vallen lijkt in dit geval lastig omdat het effect op de openbare orde niet altijd is aan te tonen. Het zou mogelijk kunnen zijn dat artikel 108 van de Gemeentewet, waarin de huishouding van gemeenten centraal staat, een aanknopingspunt biedt volgens respondent en dan het is de vraag of artikel 121 van de Gemeentewet een aanvullende bevoegdheid geeft aan gemeenten. Wellicht dat volgens respondent het mogelijk is om in de omgevingsvergunning voorschriften te stellen over de digitale veiligheid, als het niet op orde hebben ervan kan leiden tot bijvoorbeeld milieu-incidenten. Het doel van de wet is dan relevant. Met het oog op de NIS2-richtlijn en de implementatiewetgeving (die nog vastgesteld moet worden) geeft de respondent aan dat gemeenten er rekening mee dienen te houden dat er geen regels kunnen worden gesteld in een APV indien er hogere regels zijn die dit expliciet dan wel impliciet (waarbij verwezen wordt naar de onderwerp- en motieftheorie)[126] uitsluiten. Daar moet men rekening mee houden.

5.2.2 Certificering als sturingsmiddel bij vergunningen

Een van de suggesties van respondenten is dat gemeenten met certificering als voorschrift gaan werken. Op die manier wordt ervoor gezorgd dat voorschriften voor bedrijven in alle gemeenten gelijkluidend zijn. Er ontstaat dan geen verschil in voorschriften per gemeente voor bedrijven. Een respondent **(R2)** geeft aan dat een aantal certificeringen algemeen geaccepteerd zijn. Bedrijven zien de relevantie en investeren om eraan te voldoen, zelfs als het niet-ICT-bedrijven betreft. Verwezen wordt hierbij naar de NEN ISO- 27001, hetgeen een traject is dat tijd, geld en inzet vraagt maar het ook iets oplevert omdat commerciële partijen doorgaans willen dat hun onderleveranciers ook gecertificeerd zijn, aldus deze respondent. Ook in de NIS2-richtlijn speelt ketenafhankelijkheid een grote rol: onderleveranciers moeten aan dezelfde eisen voldoen als het bedrijf

[126] zie daarvoor o.a. Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022, p.33.

waarmee zaken wordt gedaan. Dit heeft gevolgen voor kleinere mkb-bedrijven die leveren aan grote organisaties. Zij moeten dan ook aan NIS2-richtlijn voldoen. In de praktijk betekent dit dat zeer veel bedrijven aan de eisen van de NIS2-richtlijn moeten gaan voldoen. Als dat zo is, dan zouden gemeenten daar volgens de respondent ondersteuning voor kunnen aanbieden bij het bedrijvenloket, zodat ook kleinere mkb'ers aan wet- en regelgeving kunnen voldoen. Ten aanzien van aparte certificering wordt hierbij gesteld dat dit gelijkgetrokken zou moeten worden voor heel Nederland en niet apart, per gemeente (**R2**).

Een andere respondent vult aan dat er een soort landelijk certificeringssysteem zou moeten zijn. Kermisbedrijven werken voor hun attracties met certificering. De certificaten hiervoor moeten ze inleveren bij de aanvraag voor de evenementenvergunning, anders krijgen ze die niet. Zo'n systeem is te bedenken voor de digitale veiligheid van bedrijven in een gemeente. Certificering kan dan zorgen voor een uniform kader bij alle gemeenten, maar alleen als vergunningverlening mogelijk is (**R6**). Een andere respondent geeft aan dat keurmerken een mogelijkheid kunnen zijn of opname ervan als voorwaarde door verzekeringsmaatschappijen (**R14)**.

5.2.3 Specifiek juridische mogelijkheden voor evenementen

Voor evenementen geldt dat respondenten zich meer kunnen voorstellen bij een handelingsperspectief voor gemeenten, omdat daar al de evenementenvergunning wordt vereist voor het houden van een evenement. Uit de interviews komt naar voren dat het vergunningenstelsel voor evenementen zijn verdeeld over drie categorieën: A, B en C en dat digitale veiligheid vooral gekoppeld dient te worden aan type C, de grote evenementen met landelijke uitstaling. Respondent **R13** die zegt veel ervaring te hebben met de organisatie van dit type evenementen, lijkt het een goed idee om een experiment hierin te doen en te kijken wat er mogelijk is om de digitale veiligheid bij deze evenementen te regelen. De veiligheidsregio met zijn expertise zou hierin meegenomen kunnen worden omdat evenementen vaak een veiligheidsplan moeten hebben als onderdeel van de vergunning. De digitale veiligheid zou opgenomen kunnen worden en men zou kunnen kijken of dit juridisch kan en mag door bij wijze van experiment een dergelijke vergunning te verlenen (**R14**). Een andere respondent maakt een vergelijking met duurzaamheid, dat de gemeenteraad recent als uitgangspunt heeft geaccepteerd om geregeld te worden in evenementenvergunningen. Dat zou dus ook voor digitale veiligheid kunnen gelden. Ook hier kunnen net als eerdergenoemd certificering, NEN ISO- of BIO-normen zorgen voor een gelijkluidend kader, zodat ondernemers weten waar ze aan toe zijn. Grote gemeenten zouden hiervoor weer een voortrekkersrol kunnen vervullen omdat die capaciteit en kennis hebben, evenals de

veiligheidsregio's en de politie en verwijst weer naar het systeem dat de gemeente Amsterdam op dit moment bouwt (**R4**). [127]

Eerder werd aangegeven dat het digitale netwerk een risico kan zijn bij evenementen. De respondent geeft aan dat in een evenementenvergunning of veiligheidsplan zou kunnen worden opgenomen dat er gewerkt moet worden met een *stand-alone network*. Echter wordt de organisator van het evenement hiermee geconfronteerd met hoge kosten. Hier geldt proportionaliteit. Indien het verstoren van het internet bij het evenement een reëel risico is, kan gedacht worden aan een dergelijk voorschrift, maar anders zou het disproportioneel zijn **(R13).** Respondent zegt dat hij niet goed op de hoogte is van evenementvergunningen die aandacht besteden aan digitale veiligheid bij evenementen. Er wordt volgens hem nog niet actief aandacht aan besteed. Ook de NIS2-richtlijn wordt genoemd in relatie tot evenementenveiligheid. Volgens een van de respondenten biedt artikel 21 van de NIS2-richtlijn, waarin een aantal basismaatregelen worden genoemd, die ook voor evenementen toepasbaar zijn, een mogelijkheid. Voorts zijn de NEN ISO- en BIO-normen vrij uitgebreid en zijn die ook te vertalen naar de digitale risico's voor een evenement. Respondent attendeert erop dat in het Verenigd Koninkrijk er veel ervaring is met (cyber)safetymanagement (**R13**).

5.3 Alternatieve mogelijkheden voor het regelen van de digitale veiligheid bij bedrijven door gemeenten

Tijdens de focusgroep en de interviews werden door respondenten ook alternatieve wijzen naar voren gebracht die decentrale overheden zouden kunnen inzetten ten behoeve van het vergroten van de digitale veiligheid binnen diens grondgebied. Hoewel deze alternatieve beleidsmogelijkheden buiten de omvang van dit onderzoek vallen zijn het bruikbare niet-juridische suggesties die kunnen bijdragen aan meer digitale veiligheid bij bedrijven en daarom een plek krijgen binnen dit onderzoeksrapport.

5.3.1 Invloed door de gemeente op digitale veiligheid via aanbestedingsregels

Buiten vergunningverlening om kan de gemeente als aanbesteder ook invloed uitoefenen op de digitale veiligheid van bedrijven waar ze zaken mee doen. Zo geeft een respondent aan dat de gemeente kan bepalen dat er geen zaken worden gedaan indien een bedrijf niet voldoet aan de NIS2. In die zin kan de gemeente in ieder geval druk

[127] Zie daarvoor ook paragraaf 6.1.5.

uitoefenen. Mocht de digitale veiligheid als vergunningvoorschrift zijn opgenomen in een evenementenvergunning, dan is er een direct toezicht mogelijk volgens deze respondent. Artikel 21 van de NIS2-richtlijn biedt een grond voor het nemen van de basismaatregelen voor de digitale veiligheid (**R1**). Deze visie wordt ondersteund door anderen respondenten. Een geeft aan dat de gemeente hierop kan letten wanneer zij goederen en diensten afneemt van bedrijven (**R14**). Een andere respondent laat weten de digitale veiligheid gegarandeerd te willen zien bij de partner waar hij zaken mee doet. Een vergelijking wordt gemaakt met de AVG. Bij privacy-aangelegenheden wordt tegenwoordig gevraagd naar een verwerkingsovereenkomst. Dat zou hier ook kunnen. De vraag is wel of gemeenten de kennis in huis hebben (IT'ers) om dat te kunnen controleren (**R6**).

5.3.2 Gemeente als partner en rol van dialoog en bewustwording

Een analyse van de vraag, of er apart binnen gemeente aandacht moet komen voor de bewustwording binnen bedrijven die binnen het gemeentelijke grondgebied gevestigd zijn voor digitale veiligheid, laat zien dat de respondenten over het algemeen eenduidig zijn en dit bevestigen maar er wel kanttekeningen bij plaatsen. Zo wordt gewezen op een tekort aan mensen met een ICT-achtergrond en met verstand van zaken, waardoor het voor gemeenten lastig is om een gesprekspartner op niveau te zijn (focusgroep en **R1, R5, R6, R7, R12**), waarbij een respondent (**R12**) geeft aan dat het vrij normaal is om te weten welke bedrijven er gevestigd zijn in de gemeente en welke risico's/ impact deze bedrijven kunnen hebben binnen en buiten de gemeente. Contact met deze bedrijven vindt deze respondent behoren tot het takenpakket van de gemeente omdat het belangrijk wordt geacht om op de hoogte te zijn van de risico's. Een belangrijk vraagstuk vindt deze respondent hoe de eigen verantwoordelijkheid van bedrijven maar ook van inwoners op allerlei facetten in veiligheidsdomein te stimuleren, dus ook de digitale veiligheid.

Het is dus onduidelijk wat er van gemeenten verwachten kan worden op dit punt en of het haalbaar is om daar veel van te verwachten. De veiligheidsregio of het landelijke niveau wordt als passender gezien hiervoor (**R5, R8**) maar ook worden voorbeelden genoemd van onderop georganiseerde zelfcontrole door bedrijven op een bedrijventerrein en de inrichting van een groep bedrijven en instanties, waaronder een gemeente, die met elkaar proberen de digitale veiligheid te organiseren (resp. **R1, R4, R9** en **R12)**.

5.4 Conclusie

In dit hoofdstuk is besproken welke juridische mogelijkheden gemeente en andere medeoverheden hebben om bedrijven te verplichten aan bepaalde eisen te voldoen. De Gemeentewet kent gemeenten een autonome regelgevende bevoegdheid toe om zaken te regelen die vallen binnen de huishouding van de gemeente. Daarbij is van belang dat deze verordenende bevoegdheid niet indruist tegen

hogere regelgeving. In sommige gevallen is expliciet ruimte geboden aan decentrale overheden om aanvullende regels te stellen, bijvoorbeeld in de vorm van maatwerkvoorschriften. De reikwijdte van die bevoegdheid wordt beperkt door de oogmerken van de wet- en regelgeving waar dit op is gebaseerd.

Indien er een mogelijkheid is om als gemeente regels te stellen aan bedrijven over digitale veiligheid, dan hebben respondenten in dit onderzoek een voorkeur voor het aansluiten bij NEN ISO-standaarden voor informatiebeveiliging, omdat dan de regels voor alle gemeenten gelijk zijn. Verschillen tussen gemeenten worden niet wenselijk geacht omdat dit ondoorzichtig is en kostenverhogend werkt voor bedrijven. Voorts moet worden afgevraagd of in dat geval ook niet in strijd met de EU-beginselen voor een vrije markt wordt gehandeld omdat deze regels iedere vorm van vrije handel kunnen belemmeren en dat is niet toegestaan dan alleen in bepaalde gevallen als het gaat om o.a. de bescherming van de openbare orde.

De respondenten uit de focusgroep en de interviews lieten een gevarieerd beeld zien wat betreft de wenselijkheid van het hebben van een aanvullende regelgevende bevoegdheid door gemeenten op het gebied van digitale veiligheid. Waar de ene respondent totaal geen rol ziet weggelegd voor gemeenten, stelt een andere respondent dat digitale veiligheid hoe dan ook in het regelgebied van een gemeente opdoemt omdat er fysieke ongelukken kunnen gebeuren als gevolg van digitale onveiligheid. Tussen deze twee uitersten zijn nuances te bespeuren, waarbij niet alleen de bestuurders zicht willen hebben op het type bedrijf in de gemeente in relatie tot digitale veiligheid Een aantal respondenten voelen meer voor communicatie tussen met het bedrijfsleven en de gemeente om de digitale veiligheid blijvend onder de aandacht te brengen. ICT-deskundigen, maar ook bestuurders, betwijfelen of toezichtstaken op het gebied van digitale veiligheid bij de gemeenten moeten worden belegd omdat die de deskundigheid niet in huis hebben en er moeilijk aan deskundig personeel te komen is. Het regionale dan wel rijksniveau heeft daardoor hun voorkeur.

Het veldonderzoek laat zien dat de meeste respondenten voor evenementen, in tegenstelling tot bij bedrijven, wel mogelijkheden zien om regels te stellen om evenementen digitaal veiliger te maken. Hierbij kan aangehaakt worden bij de evenementenvergunning. Ook hier wordt de voorkeur uitgesproken voor het gebruik van certificering om zo geen verschillende regels te hebben tussen gemeenten. Dat geldt dan voor evenementen van de zogenaamde C-categorie. Voor de A- en B—categorie evenementen zijn voorschriften over digitale veiligheid volgens de respondenten niet nodig.

6 Randvoorwaarden en knelpunten bij regulering

In dit hoofdstuk staat de volgende deelvraag centraal:

> Wat zijn eventuele randvoorwaarden/knelpunten bij die wijze van regulering?

Hoewel dit onderzoek zich richt op de mogelijkheden binnen vergunningverlening, kwam tijdens de interviews en focusgroep naar voren dat verdere regelgeving en normregulatie knelpunten met zich meebrengen. Eerder is al naar voren gekomen dat er onduidelijkheid heerst binnen overheid en andere organisaties ten aanzien van de juridische normenkaders en de onderlinge werking daarvan. In het kader van het belang van digitale veiligheid van bedrijven en de nadelige effecten die onduidelijkheid van regelgeving met zich meebrengt, is tijdens de focusgroep ook de wenselijkheid van deze normregulatie besproken.

6.1 Knelpunt: het niveau van regelgeving: capaciteit en kennis bij gemeenten.

Vanuit de focusgroep is de algemene tendens dat de aanwezigen als knelpunt ervaren dat het schaalniveau van een gemeente voor het stellen van regels te klein en te kwetsbaar is. Specifiek voor digitale veiligheid vindt de focusgroep geen taak weggelegd voor decentrale overheden, maar wordt juist het EU-niveau, het nationale niveau dan wel het regionale niveau passend gevonden waarbij wordt verwezen naar de NIS2-richtlijn als voorbeeld. Niet alleen dat de al genoemde gelijkheid van regels belangrijk is voor de bedrijven, maar wat ook een belangrijke rol speelt is de benodigde capaciteit, kennis en kapitaal, die bij gemeenten niet of nauwelijks aanwezig wordt verondersteld.
Uit de interviews blijkt dat de meeste respondenten het hiermee eens zijn (**R1**).

Een andere respondent verwijst naar het hanteren van een uniforme set van normen en regels, vooral als een bedrijf internationaal werkt. Indien bedrijfsvestiging gekoppeld wordt aan een vergunning en de gemeente dit gaat handhaven, dan worden problemen in de kennis van gemeenten voorzien alsmede het ontstaan van de bureaucratie. De handhaving vanuit de gemeente, het al dan niet voldoen aan deze regels, wordt als een complex vraagstuk aangemerkt. Bij evenementen kunnen standaardregels (zoals certificering e.d.) een uitkomst bieden. In de interviews is hier nader op ingegaan (**R4, R5, R6, focusgroep**). In de focusgroep wordt gepleit voor een andere rol voor gemeenten, zij zien dat gemeenten het bewustwordingsproces best op kunnen pakken in hun werkgebied. Regelgeving door gemeenten wordt lastiger gevonden omdat dit negatief kan werken op de keuze van bedrijfsvestiging. Regelgeving kan in dat verband ook weer beter op

een ander schaalniveau liggen (provincie of rijk), aldus deze respondenten. Een van de respondenten noemt regelgeving door gemeenten een stap te ver, ook al vanwege praktische problemen, die zich voordoen bij regelgeving, zoals het inventariseren en oplossen van vraagstukken. Dit wordt ondersteund door een andere respondent die er niet aan moet denken dat een gemeente met regels komt op het gebied van digitale veiligheid omdat, analoog aan de energieregels, deze kostenverhogend zullen werken. Deze respondent ziet veel meer in het richten op de respons want daar zitten bedrijven meer op te wachten. Een andere respondent ziet de gemeentelijke rol meer als informatieloket voor bedrijven, waarbij doorverwezen wordt naar (inter)nationale standaarden en er vooral geen eigen regels moeten worden bedacht.
Een andere respondent is heel stellig in de mening dat er bij digitale risico's helemaal geen rol is weggelegd voor gemeenten. Het rijksniveau wordt passend geacht hiervoor, mede omdat veel regelgeving op dit gebied nu afkomstig is van de Europese Unie. Het rijk, maar niet de gemeente, kan dan stellen dat de digitale keten op orde moet zijn. Een gemeente kan zich hoogstens op het gebied van de openbare veiligheid voorbereiden op incidenten, maar volgens deze respondent is er geen rol weggelegd voor gemeenten bij het op orde hebben van de digitale veiligheid bij bedrijven. Er wordt een vergelijking gemaakt met het Bouwbesluit dat op nationaal niveau regels stelt voor bouwwerken. Kijkend naar het doel van deze wet maakt digitale veiligheid hier geen onderdeel van uit en moet men dit ook niet willen. De respondent geeft aan dat de kennis en kunde op het gebied van digitale veiligheid specialistisch is en samenhangt met de verschillende software die bedrijven gebruiken en dat juist specialistische bedrijven hier de *compliance* dienen uit te voeren. Een gemeente heeft die kennis niet in huis. Sowieso is de kennis bij gemeenten op het gebied van digitale veiligheid beperkt en heeft men binnenshuis al moeite met *compliance* in de ogen van deze respondent. Ook certificering wordt niet als mogelijkheid gezien vanwege de kosten en de complexe handhaving ervan door gemeenten (**R9**). Nog sterker in het afzien van een rol voor de gemeente is de volgende respondent, omdat bij gemeenten de kennis op dit gebied vaak niet aanwezig is en vakmensen moeilijk te werven zijn. Er worden voorbeelden genoemd en hierin wordt aangegeven dat zelfs basale kennis op het gebied van privacy vaak al niet eens aanwezig is en hierdoor fouten worden gemaakt bij vergunningverlening (**R12**). Deze respondent is dan ook van mening dat bedrijven zelf verantwoordelijk zijn voor het op orde hebben van hun digitale veiligheid, met regels die op landelijk niveau moeten worden vastgesteld. De rol die hier voor gemeenten is weggelegd is dat zij moeten nadenken over digitale veiligheid en hoe dit te organiseren in de gemeente, maar op rijksniveau dient dit geregeld te worden.

Tot slot is er ook nog een respondent die vindt dat de gemeente in de volle breedte een bijdrage kan leveren aan de digitale veiligheid van bedrijven. Zo geeft de respondent aan dat dat bedrijven hoe dan ook

weerbaar moeten zijn op digitaal gebied. Een gemeente kan daarop attenderen en dan is de handelswijze ervan niet anders dan dit bij inwoners van een gemeente te doen: erop attenderen hoe belangrijk het is, nog los van enige regel (**R14).**

6.2 Randvoorwaarde: Communicatie naast dan wel in de plaats van regelgeving

Vanuit de focusgroep is gediscussieerd over de vraag of dialoog en communicatie over digitale veiligheid belangrijker is dan het verplichten van bepaalde richtlijnen en eisen rondom digitale veiligheid. Een van de respondenten geeft aan dat bedrijven alleen het nodige doen als het in de regels staat – wetgeving is dus noodzakelijk. Tegelijkertijd wordt door respondenten communicatie als een belangrijke stok achter de deur gezien, naast regelgeving. Een mederespondent is het hiermee eens omdat wetgeving verplicht, maar ziet een woud aan wetgeving ontstaan, waarbij bedrijven wellicht geitenpaadjes kiezen om er onderuit te komen. Er wordt zo een papieren werkelijkheid gecreëerd. Deze respondent is voorstander van het geven van praktische hulp aan bedrijven om hun digitale veiligheid op orde te krijgen. Preventie- en communicatiebijeenkomsten laten zien dat praktische hulp nodig is bij bedrijven. Wat op basis van ervaring ook helpt is het regelen van digitale veiligheid binnen de ketenverantwoordelijkheid, waarbij als voorbeeld de aanbestedingsregels worden genoemd. Als bij een aanbesteding een regel is dat een deelnemend bedrijf de digitale veiligheid op orde moet hebben, dan draagt dat bij aan een actieve houding binnen het bedrijf om de digitale veiligheid te regelen.

Overige respondenten ondersteunen de gedachte van actieve hulp aan bedrijven, waarbij communicatie een rol speelt. Onder andere de complexiteit van regelgeving is daarbij een aandachtspunt. Met vindt dat het bedrijfsleven mede hierdoor achterblijft in de ontwikkeling. De AVG wordt als voorbeeld genoemd; niet ieder bedrijf is 'AVG-proof'.
Een van de respondenten geeft aan dat op basis van ervaring bedrijven de digitale veiligheid niet goed geregeld hebben omdat het kostenverhogend werkt en er niets aan verdiend wordt in hun beleving. Wel ontstaat er langzaam een kentering omdat meer bedrijven slachtoffer worden van cybercrime. Afgevraagd moet worden of wet- en regelgeving deze houding doet veranderen. Het kan helpen maar ook deze respondent is het eens met de tendens binnen de focusgroep, die inhoudt dat in dat geval er een praktisch handelingskader voor bedrijven moet komen. Communicatie alleen lijkt daarbij niet voldoende.
Een respondent wijst op het belang van bewustwording van digitale veiligheid bij gemeente en bedrijven en zegt in gesprek te zijn met VNO-NCW om bedrijven bewust te maken van de digitale veiligheid en dit een taak te vinden van de gemeente. Gemeenten hoeven daarbij niet op de hoogte te zijn van de digitale veiligheid van alle bedrijven

in de gemeente, maar kunnen wel in contact blijven met de koepelorganisaties (**R7**). In het verlengde daarvan kan de gemeente ook actief digitale veiligheid aanjagen of stimuleren. Zo wordt door een van de respondenten aangegeven dat wordt overlegd met het mkb en mkb-plus. In dat kader worden digitale weerbaarheidsinitiatieven ontwikkeld (**R11**).

6.3 Randvoorwaarde voor een beperkte rol voor gemeenten: regels via certificering, inkoopvoorwaarden en verzekering.

Waar sommige respondenten terughoudend zijn over de rol van een gemeente bij regulering van digitale veiligheid van bedrijven, zijn er ook respondenten die aandacht besteden aan de voorwaarden voor gemeenten om hier een rol te kunnen spelen.
Een van de respondenten geeft aan dat het stellen van regels door een gemeente voorstelbaar is, los van de wenselijkheid. Daarbij wordt verwezen naar een ISPS-code voor bedrijven in het Rotterdamse havengebied, die als gevolg van 11-9-2001 is ontwikkeld. In het verlengde daarvan vraagt respondent zich af of dit ook niet moet gelden voor digitale veiligheid bij de bedrijven, nog los van de overheidslaag die dit zou moeten regelen.

Een van de respondenten vindt het een goed idee dat gemeenten een rol spelen maar dan vanuit hun opdrachtgeverschap voor hard- en softwareproducten die ze inkopen en ze daarbij gebruik van standaarden en certificeringen die al beschikbaar zijn in de markt. Een andere respondent vindt het wenselijk dat digitale veiligheid lokaal dan wel regionaal geregeld wordt mits er geld, capaciteit en kennis ter beschikking wordt gesteld (**R8**). Anders werkt het niet, waarbij de vergelijking wordt getrokken met evenementen. Daar is kennis en capaciteit opgebouwd en kan in principe de gehele vergunning gecontroleerd worden. De discipline *cyber* zou toegevoegd kunnen worden, zodat dit onderdeel voldoende geborgd is. Het blijft echter lastig volgens deze respondent om te bepalen wie het regelt. De veiligheidsregio zou wellicht een goede plaats zijn om de digitale risico's bij bedrijven te monitoren omdat digitale crises vaak een bepaald schaalniveau hebben en veelal gemeentegrensoverschrijdend zijn. Ook zijn veel crises tegenwoordig sluimerend of duren steeds langer (pandemie) waardoor men meer aan de voorkant (preventie en beheersing) wil gaan zitten in plaats van de achterkant, die gericht is op de crisisgevolgbestrijding. Het acteren aan de voorkant vraagt extra investeringen in mensen en kennis, aldus deze respondent.

Een andere respondent geeft aan dat er gemeenten zijn die actief willen handelen richting bedrijven om de digitale veiligheid te stimuleren en te onderzoeken of een meer verplichtend karakter voor bedrijven vanuit de gemeente mogelijk is. Binnen de veiligheidsregio

maar ook binnen de politie is redelijk veel kennis op het gebied van digitale veiligheid aanwezig (**R11**).

Wat bedrijven betreft is professionalisering ervan belangrijk omdat nagenoeg alle bedrijfsprocessen tegenwoordig gedigitaliseerd zijn en in verbinding staan met elkaar via het internet. Daarom lijkt het deze respondent goed dat gemeenten instrumenten hebben om de digitale veiligheid ten behoeve van de maatschappelijke veiligheid van een gemeente te kunnen afdwingen bij bedrijven. Dat mag volgens hem ook gebeuren via eisen van verzekeringsbedrijven aan bedrijven, waarbij een bedrijf dat niet digitaal veilig is niet verzekerd kan zijn. Ook dat kan werken. Binnen de werkkring van deze respondent kan men zich niet permitteren dat de gegevens geraakt worden door een datalek of een *hack*, en dus moet alles op orde zijn.

Op de vraag of gemeenten aandacht moeten hebben voor digitale veiligheid bij bedrijven middels certificering, stelt een respondent dat er wel een rol voor gemeenten is weggelegd (**R2**). In de commerciële sector wordt in offertes vermeld aan welke certificering en NEN-normen de bedrijven voldoen. Doorgaans worden er alleen zakengedaan met partijen die over de juiste certificering beschikken. Gemeenten zouden deze handelswijze kunnen overnemen, voor zover dat al niet gebeurt. Een raamwerk gebaseerd op de BIO/ISO/NEN 7510 kan bijvoorbeeld helpen om dit op gemeentelijk niveau op te zetten. Gemeenten zouden voor bepaalde typen organisaties aan kunnen geven aan welke minimumeisen ze op het gebied van digitale veiligheid moeten voldoen.

6.4 Randvoorwaarde: vertrouwen en zelfregulering als route

Een van de respondenten **(R4)** geeft aan dat er momenteel discussie is over zelfregulering waarbij verwezen wordt naar de Belastingdienst, die veel op dit gebied naar hun klanten toe doet. De basis van handelen hierin is vertrouwen. Alleen als er bewust fout wordt gehandeld blijf het bedrijf onder controle. Op dit moment probeert de gemeente Amsterdam een dergelijke houding te regelen binnen de gemeentelijke organisatie. Daar wordt een systeem gebouwd tussen gemeente, bedrijfsleven, wetenschap en andere overheden in de regio op digitaal crisisgebied, wat als ecosysteem wordt aangeduid. Doel ervan is dat men in het geval van een digitale crisis met elkaar in verbinding staat. Ook dat is een vorm van *responsible regulations*, zoals zelfsturing. Dit wordt ook door respondent **R1** benadrukt, waarbij aangegeven wordt dat sectoren hun digitale veiligheid zelf dienen te regelen. De overheid is er dan voor het toezicht. De NIS2-richtlijn biedt een mogelijkheid voor dit toezicht.

6.5 Conclusie

In dit hoofdstuk is besproken welke randvoorwaarden en knelpunten kunnen spelen bij de regulering van digitale risico's. Uit het veldonderzoek blijkt dat er geen eenduidigheid is in het draagvlak voor een rol van gemeenten bij het stellen van eisen ter vergroting van de digitale veiligheid op lokaal niveau. Zo zijn niet alle respondenten overtuigd van het feit dat regulatie op gemeentelijk niveau thuishoort; voor hen geniet een Europese, nationale of regionale aanpak de voorkeur boven een lokale aanpak. Indien wel gekozen wordt voor een lokale aanpak geldt als randvoorwaarde dat er voldoende kennis bestaat binnen gemeenten om een heldere invulling van de regels of voorschriften te kunnen bieden. Daarnaast zijn kennis, financiële middelen en juridische grondslag als randvoorwaarde nodig voor het handhaven van de voorschriften. Zolang dat niet aanwezig is bij gemeenten, genieten voor respondenten andere middelen dan reguleren de voorkeur. Daarbij kan gedacht worden aan communicatiestrategieën, het verwijzen naar (inter-)nationale standaarden en het instellen van certificerings-, inkoop- en verzekeringseisen bij eigen afname van producten en diensten. Daarnaast wordt als randvoorwaarde waarde gehecht aan autonomie binnen organisaties, waar vertrouwen en zelfregulering aan de basis liggen.

7 Conclusie en aanbevelingen

In dit onderzoek stond de volgende hoofdvraag centraal:

> Hoe kunnen gemeenten en medeoverheden de digitale veiligheid binnen gemeenten vergroten door aandacht te besteden aan digitale veiligheid bij vergunningverlening bij bedrijven die zich binnen de gemeente gevestigd zijn of zich willen vestigen?

Deze vraag is beantwoord aan de hand van literatuuronderzoek, juridisch onderzoek en interviews/focusgroep. Daarin is aandacht besteed aan de consequenties van de verwezenlijking van digitale veiligheidsrisico's bij bedrijven en evenementen. Ook is een verkenning uitgevoerd naar soorten vergunningen en de relevante juridische normenkaders. Daarbij is de vertaling gemaakt naar juridische mogelijkheden voor gemeenten om vergunningvoorschriften te stellen over digitale veiligheid en is gekeken naar randvoorwaarden voor de uitvoering van het toezicht en controle op vergunningen door gemeenten of medeoverheden.

7.1 Conclusie

Digitale veiligheid is de basis van het beperken van digitale risico's om digitale incidenten te voorkomen. Digitale risico's bij bedrijven die van invloed kunnen zijn op de openbare orde en veiligheid zijn divers. Veel risico's hebben betrekking op de veiligheid als er een *hack* of een digitale storing plaatsvindt, die bedrijfsprocessen raakt maar er kan ook een gevaar voor de openbare orde ontstaan als de veiligheid van mensen in het geding is door de verstoring van bedrijfsprocessen, zoals milieuverontreiniging. In sommige gevallen zou die verstoring ook kunnen leiden tot verstoringen van de openbare orde, zoals bij milieuverontreiniging en aantasting van vitale infrastructuur. Deze risico's en digitale incidenten bestaan in verschillende vormen, die elk hun eigen toepassing hebben die al dan niet kunnen leiden tot gevolgen voor de fysieke leefomgeving of de openbare orde. Er zijn een aantal risicofactoren in kaart gebracht om de risico's binnen sectoren of bedrijven te kunnen duiden, zoals de mate waarin de organisatie of sector deel uitmaakt van de vitale processen of de keten daarin, de aanduiding als Seveso-inrichting, de aanwezigheid of afhankelijkheid van operationele technologieën en de afwezigheid van analoge terugvalopties. Uit dit onderzoek blijkt dat er op dit moment geen juridisch kader voor gemeenten bestaat dat specifiek gericht is op het creëren van verantwoordelijkheden, taken en/of bevoegdheden ten aanzien van digitale veiligheid van bedrijven. Toch worden er mogelijke openingen gevonden in de Omgevingswet en de APV.

Het wettelijk en regelgevend kader dat op dit moment door gemeenten wordt toegepast voor bedrijven bestaat, voor zover relevant, voor dit onderzoek uit de Omgevingswet, de Alcoholwet de Gemeentewet en de APV. Deze gaan in hoofdlijnen over de fysieke leefomgeving resp. de openbare orde. Uit het onderzoek blijkt dat het denkbaar is dat digitale incidenten gevolgen voor de fysieke leefomgeving of de openbare orde met zich meebrengen. Voor deze risico's kan daarom gelden dat ze vallen binnen de werkingssfeer van eerdergenoemde wet- en regelgeving. Voor de toepassing daarvan is van belang met welk oogmerk deze wet- en regelgeving is opgesteld, om te voorkomen dat bevoegdheden worden ingezet voor een ander doel dan waarvoor deze zijn verleend. Een algemene regel met als doel om de algehele digitale veiligheid te vergroten zal niet in overeenstemming zijn met de oogmerken. Dat is anders, indien sprake is van een regel die specifiek ziet op bedrijven of branches waarbij sprake is van een verhoogd risico op ontwrichtende gevolgen voor de fysieke leefomgeving of de openbare orde.

De APV biedt, gelet op het doel van de regeling om de openbare orde te beschermen, in ieder geval mogelijkheden om voor evenementen regels te stellen over de digitale veiligheid. De APV biedt voorts een mogelijkheid om voor openbare plaatsen en voor publiek toegankelijke plaatsen regels te stellen om de openbare orde te beschermen. Ten aanzien van bedrijven zou dezelfde lijn denkbaar zijn die wordt toegepast voor exploitatie van bedrijven met een verhoogd risico op ondermijning.

Ten aanzien van de Omgevingswet geldt dat daarmee activiteiten kunnen worden gereguleerd in de fysieke leefomgeving, alsmede activiteiten die gevolgen voor de fysieke leefomgeving met zich mee kunnen brengen. Uit de in kaart gebrachte digitale risico's blijkt dat de gevolgen van digitale incidenten tevens van invloed kunnen zijn op de fysieke leefomgeving. Gelet op het toepassingsbereik van de term fysieke leefomgeving, de doelstellingen van de Omgevingswet en de invulling van de specifieke eisen kan geredeneerd worden dat daaronder ook digitale activiteiten, die kunnen leiden tot een gevolg voor de fysieke leefomgeving, worden verstaan. Daarbij is analogie gevonden met de NIS2-richtlijn, waar ten aanzien van digitale risico's ook de fysieke component moet worden meegewogen.

Bij gebruik van het vergunningstelsel kunnen, indien de specifieke wet- en regelgeving dat toelaat, vergunningvoorschriften (in het geval van de Omgevingswet: maatwerkvoorschriften) worden gesteld bij een vergunning indien deze bijdragen aan de doelstelling van de vergunningplicht. Daarnaast moeten de verplichtingen die deze voorschriften met zich meebrengen in verhouding staan tot die doelen.

Gemeenten kunnen wel voorschriften verbinden aan evenementenvergunningen om ervoor te zorgen dat de digitale veiligheid bij een evenement is geregeld. De APV biedt hiervoor het

juridische kader, aangezien een digitale verstoring van een evenement kan leiden tot een openbare ordeverstoring. Dat is het aanknopingspunt om regels te stellen.

Gelet op artikel 108 Gemeentewet zou het mogelijk moeten zijn om via een vergunning of ontheffing voorschriften te stellen aan bedrijven om de digitale veiligheid te regelen, indien een digitale ontregeling van het bedrijf een verstoring van de gemeentelijke openbare orde of de fysieke leefomgeving betekent en mits de regels niet strijden met de EU- beginselen van het vrije verkeer van personen, goederen, diensten en kapitaal binnen de EU en de overige EU-regels, zoals hiervoor genoemd. De APV en de omgevingsvergunning zouden, gelet op hun doelstellingen, gebruikt kunnen worden om regels te stellen ten aanzien van die veiligheid indien dat bijdraagt aan de openbare orde en/of bescherming van de fysieke leefomgeving. Daarvoor zal eerst moeten worden vastgesteld welke gevolgen de verwezenlijking van digitale risico's met zich meebrengt binnen een bedrijf of branche. Dit zou door een gemeente in kaart kunnen worden gebracht door een inventarisatie te maken per bedrijfscategorie.

Randvoorwaarden waaraan gemeenten dienen te voldoen bij mogelijke regelgeving over de digitale veiligheid van bedrijven zijn hoe dan ook de eisen van het EU-recht:

- Een vrije vestiging zonder belemmerende regels;
- Geen discriminatie;
- Transparantie en evenredigheid van regels;
- Geen (verkapte) kwantitatieve beperkingen of maatregelen van gelijke werking;
- Voldoen aan de Dienstenrichtlijn en Dienstenwet;
- Voldoen aan de Notificatierichtlijn als er regels worden gesteld. Ze zullen moeten worden gemeld bij de EU omdat ze de vrijheid van goederen, diensten, personen en kapitaal kunnen belemmeren,

Daarnaast zal een goed toezicht- en handhaafplan moeten worden opgesteld en uitgevoerd. Voor het opstellen van regels of voorschriften, alsmede voor het toezicht en handhaving zijn kennis van zaken en voldoende menskracht ook een randvoorwaarde.

Deze randvoorwaarden zijn vaak aangedragen als argumenten tegen het stellen van voorwaarden ten aanzien van digitale veiligheid op gemeentelijk niveau. Die wenselijkheid staat ter discussie, waarbij ook stemmen opgaan om dit niet op gemeentelijk niveau te regelen vanwege de mate van expertise die nodig is om het opstellen van toegankelijke en passende voorschriften en de handhaving daarvan. Daarnaast brengt het regelen op lokaal niveau het risico van lokale verschillen met zich mee, waardoor het volgens respondenten nu al onduidelijke normenkader alsmaar onduidelijker wordt. Volgens hen komt dat niet ten goede aan het niveau van digitale veiligheid.

De komst van de NIS2-richtlijn brengt ook vraagtekens met zich mee. In die richtlijn staat dat bedrijven van een bepaalde categorie, te weten zeer kritieke en andere kritieke sectoren alsmede essentiële en belangrijke entiteiten, hun digitale veiligheid moeten hebben geregeld. Tevens dienen bedrijven, die een zakenrelatie aangaan met deze sectoren en entiteiten te voldoen aan de NIS2-eisen, waardoor het bereik van de NIS2-richtlijn veelomvattend zal zijn. De enkele categorie van bedrijven die buiten deze regeling valt, zullen (kleine) mkb-bedrijven zijn. Juist voor gemeenten kunnen deze bedrijven interessant zijn omdat hun werkingsgebied zich veelal tot de gemeente zal beperken. Het is nog niet duidelijk of de Implementatiewet van de NIS2-richtlijn gemeenten de ruimte biedt om nadere eisen te stellen op het gebied van de digitale veiligheid aan bedrijven, die niet onder de deze richtlijn vallen. Mocht de mogelijkheid niet in de wet worden opgenomen dan is het de vraag of gemeenten dit mogen op grond van hun aanvullende regelgevende bevoegdheid.[128]

Tenslotte kunnen gemeenten de digitale veiligheid bij bedrijven in hun gemeenten vergroten door in contact te treden met deze bedrijven en ze op het belang ervan de attenderen. Dat is mogelijk door met ze in gesprek te gaan waarbij dan ook de risico's voor de openbare orde in kaart kunnen worden gebracht. Er zou bij risicovolle bedrijven een afspraak kunnen worden gemaakt dat er bij digitale incidenten van een bepaalde omvang een melding wordt gedaan bij de burgemeester of de veiligheidsregio, zodat de risico's voor de openbare orde kunnen worden gebracht geïnventariseerd.

7.2 Aanbevelingen

Breng de digitale risico's binnen de gemeente aanhoudend in kaart
Op grond van het onderzoek adviseren wij allereerst de digitale risico's binnen het grondgebied in kaart te brengen, door te onderzoeken welke ondernemingen en evenementen voldoen aan één of meerdere indicatoren voor een hoog of middelhoog risico zoals omschreven in paragraaf 2.5 en 2.6. Daarbij kan aansluiting worden gevonden bij reeds verleende (omgevings-)vergunningen en KvK-inschrijvingen voor een globaal inzicht van digitale risico's. Overige informatie, zoals de aanwezigheid of afhankelijkheid van operationele technologie en de ketenverbinding met ondernemingen met hoge of middelhoge

[128] Zie voor een uitwerking daarvan het onderzoeksrapport Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022.

risicofactoren zijn lastiger specifiek in kaart te brengen binnen het grondgebied.

Hoewel daarmee, gelet op de risicofactoren, nog geen volledig beeld kan worden geschetst geldt een dergelijke globale inventarisatie als praktisch en uitvoerbaar uitgangspunt voor verdere stappen. Daarbij kan gedacht worden aan het uitzetten van vragenlijsten bij ondernemers, of het aangaan van gesprekken met ondernemingen waarvan reeds is vastgesteld dat zij een hoger risicobeeld genieten.

Door met ondernemers in gesprek te gaan over de organisatie van de digitale veiligheid binnen hun bedrijf geven decentrale overheden het signaal af dat het onderwerp niet meer van de politieke agenda verdwijnt, nu blijkt dat dit bij veel (kleinere) bedrijven nog niet helemaal op hun agenda staat. In algemene zin strekt het houden van een continue communicatielijn over digitale veiligheid met bedrijven die activiteiten ontplooien binnen de gemeente tot aanbeveling. Zo kan de gecreëerde risico-inventarisatie actueel blijven, met als mogelijk effect dat bij bedrijven ook meer bewustwording ontstaat ten aanzien van het belang van digitale veiligheid. Met het in kaart brengen van die risico's kan ook worden gecontroleerd of de bedrijven met een verhoogd risico reeds onderhevig zijn aan een vergunningstelsel dat zich leent voor regulatie. Indien dat in grote mate het geval is kan onderzocht worden welke vergunningvoorschriften of maatwerkregels wenselijk kunnen zijn, waarbij wordt aanbevolen aan te sluiten bij reeds bestaande normen.

Indien de hogere risico's zich bevinden bij organisaties of evenementen die niet onder een vergunningstelsel vallen kan de mogelijkheid voor het aanpassen van de APV om dit onderwerp te regelen een punt van overweging zijn, met name ten aanzien van horeca en evenementen. Het instrument van de het instellen van een vergunningplicht in het omgevingsplan lijkt ook een mogelijkheid en kan nader onderzocht te worden.

Ga de wenselijkheid van regulering op lokaal niveau na
De implementatiewet van de NIS2-richtlijn kan een grote invloed hebben op het handelingskader van gemeenten. Het is van belang deze ontwikkelingen te volgen en gebruik te maken van de consultatiefase. Deze richtlijn kan het bestaande handelingskader van decentrale overheden ofwel beperken, ofwel vergroten vanwege het vraagstuk rondom anterieure en posterieure regelgeving. Daarbij is van belang voor gemeenten om na te gaan of zij vinden dat lokale invulling van dergelijke regels wenselijk is, waarbij mede van belang is of binnen de organisatie voldoende kennis en kunde aanwezig is – of kan worden gecreëerd – om die invulling in goede banen te kunnen leiden.

Vervolgonderzoek
Er wordt geadviseerd vervolgonderzoek in te stellen ten aanzien van digitale veiligheid bij evenementen, waarbij ook een analyse van de

huidige beleidskaders binnen gemeenten wordt uitgevoerd en *best practices* binnen dat vergunningstelsel worden gezocht en toegepast richting digitalisering. Daarnaast zou vervolgonderzoek naar de mogelijkheden van het instellen van een vergunningplicht ten aanzien van (categorieën van) bedrijven met een verhoogd risico op digitale onveiligheid met maatschappelijke gevolgen wenselijk zijn.

8 Literatuurlijst

Asslani, Van den Berg, Hofman & Xue 2018
Asslani, van den Berg, Hofman & Xue, *Rapport digitale veiligheid evenementen*. RUG: 2018

Bantema 2018
W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.Ph. Stol, Burgemeesters in Cyberspace, *Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld,* Politie en Wetenschap, Centrum voor openbare orde en veiligheid, Apeldoorn 2018.

Bantema, 2021
W. Bantema e.a., *Black box van gemeentelijke online monitoring*, voor: Politie en Wetenschap, Centrum voor openbare orde en veiligheid, Apeldoorn, 2020.

Bantema, Westers & Munneke 2020
W. Bantema, S. Westers & S.A.J. Munneke, *Niet bevoegd, wel verantwoordelijk,* Den Haag: Boom Bestuurskunde 2020.

Bantema, Twickler & De Vries, 2022
W. Bantema, S.M.A. Twickler & S. de Vries, *Juridische grenzen en kansen bij openbare ordehandhaving*, Leeuwarden: NHLStenden University of Applied Sciences, 2022.

Berenschot 2020
Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten. Berenschot Groep B.V: 2020.

Bekkers, Van der Kleij & Leukfeldt 2021
L. Bekkers, R. van der Kleij & R. Leukfeldt, *Cyber-ketenweerbaarheid. Een verkennend onderzoek naar dreigingen, wetsbaarheden en geleerde lessen.* Centre of Expertise Cyber Security, Lectoraat Cyber Security in het mkb: 2021.

Brouwer, *NJB* 2016
J.G. Brouwer, 'Wat is openbare orde', *NJB* 2016/1561, (online via Kluwer Navigator).

Hisch Ballin, Janse de Jonge & Leenknegt, 2020
E. Hirsch Ballin, E. Janse De Jonge & G.J. Leenknegt, *Uitleg van de Grondwet*, Den Haag: Boom Juridisch 2020.

I&O Research 2023
Risico- en crisisbarometer najaar 2023. NCTV: 2023

De Jong 2016

M.A.D.W. de Jong e.a., *Orde in de openbare orde*, Utrecht/ Nijmegen, WODC Publications (online).

Muller, Kummeling & Nehmelman 2020
Instituten van de staat, Deventer: Wolters Kluwer 2020.

Nationaal Coördinator Terrorismebestrijding en Veiligheid 2022
Landelijk Crisisplan Digitaal. NCTV: 2022.

Nationaal Coördinator Terrorismebestrijding en Veiligheid 2023
Cybersecuritybeeld Nederland 2023, NCTV: 2023.

Nationaal Cyber Security Centrum 2022
Nederlandse Cyber Security Strategie 2022-2028, Nationaal Cyber Security Centrum: 2022.

Nederlands Instituut Publieke Veiligheid z.d.
Nederlands Instituut Publieke Veiligheid, *Vitale processen*, z.d.

Scherp in Veiligheid 2023
Scherp in Veiligheid, *Afgehackt*, 2023.

Van Ruijven & Keijser 2017
Th. van Ruijven & B. Keijser. *Ketenweerbaarheid tegen cyberdreigingen. Uitgangspunten, good practices en een stappenplan voor het vergroten van cyber-ketenweerbaarheid*. TNO: 2017.

Vereniging van Evenementen Makers 2019
Vereniging van Evenementen Makers, *Nationaal Handboek Evenementen Veiligheid 1.0. Een gemeenschappelijk denkkader omtrent veiligheid*. NHEV: 2019

Van der Varst e.a. 2022
L. van der Varst, J. Groenendaal, W. Bantema & F. Cools, *Bestuurlijke bevoegdheden cyber*, Arnhem: Nederlands Instituut Publieke Veiligheid, 2022.

VNG 2020
VNG, *Handreiking APV en ondermijning*. Vereniging Nederlandse Gemeenten: Den Haag 2020.

VNG 2022
VNG, *Focusblad digitale veiligheid*. Vereniging Nederlandse Gemeenten, 2022.

Wetenschappelijke raad voor het Regeringsbeleid 2019
WRR, *Voorbereiden op digitale ontwrichting, WRR Rapport 101*, Den Haag: 2019.

9 Jurisprudentieregister

- HvJEU, 11 juli 1974, ECLI:EU:C:1974:82, (Dassonville).
- HvJEU, 20 februari 1979, ECLI:EU:C:1979:42 (Cassis de Dijon-arrest).
- HvJEU, 24 november 1993, ECLI:EU:C:1993:905 (Keck et Mithouard).
- ABRvS 20 juni 2018, ECLI_NL:RVS:2018:2062 (Appingedam),
- ABRvS 27 maart 2019, ECLI:NL:RVS:2019:965.
- ABRvS 3 maart 2021, ECLI:NL:RVS:2021:461.

10 Parlementaire stukken

- Stbl. 2009-505.
- *Kamerstukken II 2013/14*, 33962, 3.
- *Kamerstukken II*, 2017-18, 34 883, nr. 3 (MvT).
- Stbl. 2018, 389.
- Stcrt. 2020, 7857.

11 Bijlagen

Bijlage 1	Interviewprotocols
Bijlage 2	Lijst van respondenten
Bijlage 2	Protocol van focusgroep
Bijlage 3	Lijst van deelnemers focusgroep

Bijlage 1 Interviewprotocol

Introductie.

Waarop is dit interview gebaseerd?
De Vereniging van Nederlandse Gemeenten (VNG) heeft voor haar leden een actielijn 'voorbereiding op digitale ontwrichting, incidenten en crisis' vastgesteld, als onderdeel van de Agenda Digitale Veiligheid. Ter uitvoering hiervan heeft de VNG gereageerd op het onderzoek 'Bestuurlijke bevoegdheden cyber' van het Nederlands Instituut Publieke Veiligheid (NIPV).[129] Het doel van dat onderzoek was een verkenning naar bevoegdheden en interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's bij (dreigende) digitale incidenten. De VNG wil hier verder onderzoek naar doen en heeft ons lectoraat gevraagd in hoeverre het instrument vergunning een mogelijkheid biedt voor burgemeesters om preventief de openbare orde te handhaven bij dreigende digitale incidenten.

Wie zijn wij en wat gaan we doen?
Allereerst bedankt dat u mee wilt werken aan ons onderzoek. Het lectoraat Bestuur en Veiligheid in een Digitaliserende Samenleving (verbonden aan de Thorbecke Academy, NHLStenden Hogeschool Leeuwarden) voert dit onderzoek uit in opdracht van de VNG om het handelingsperspectief voor burgemeesters inzake dreigende digitale incidenten verder te verkennen, na eerdere onderzoeken van ons op dit gebied.[130] De informatie die we verzamelen uit de focusgroep en interviews moet ons helpen om in kaart te brengen of er al vergunningen worden verleend met daarin regels opgenomen over cyberveiligheid en of er een handelingsruimte is bij gemeenten om regels te stellen voor bedrijven, die bij verstoring van hun processen de openbare orde kunnen bedreigen.

Wat doen we met de informatie uit de focusgroep/ het interview?
We schrijven een onderzoeksrapport en daarnaast wetenschappelijke artikelen. We zouden uw naam graag willen gebruiken in het eindrapport. Uiteraard kan uw bijdrage ook anoniem verwerkt worden. Gaat u ermee akkoord dat uw naam in het eindrapport opgenomen wordt? Verder zullen we het verslag van de focusgroep/ interview naar u opsturen, zodat u de mogelijkheid heeft om de inhoud van commentaar te voorzien.

---

[129] 'Bestuurlijke bevoegdheden cyber', nipv.nl, 30 september 2022.
[130] Bantema c.s., *Burgemeesters in cyberspace*, Den Haag, 2018, Bantema, Westers, Munneke, *'Niet bevoegd, wel verantwoordelijk'*, Den Haag 2020 en Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022.

Opname toegestaan?
Vindt u het goed dat het gesprek wordt opgenomen? De opnames worden alleen gebruikt voor het uittypen van het gesprek en worden daarna gewist. Het opnemen zorgt ervoor dat het interview zonder onderbrekingen kan worden afgenomen en uiteindelijk sneller kan worden afgerond. De opnames van het gesprek worden daarna gewist. Het opnemen zorgt ervoor dat het interview zonder onderbrekingen kan worden afgenomen en uiteindelijk sneller kan worden afgerond.

Introductievragen (optioneel)

1. Wat is uw functie?
2. Kunt u meer vertellen over uw werkzaamheden?

Inhoudelijke vragen

1. Welke juridische mogelijkheden hebben gemeenten en medeoverheden om bedrijven te verplichten aan bepaalde eisen te voldoen die de digitale veiligheid van het bedrijf te garanderen?

   Toelichting: Voor bedrijven, die zich vestigen in een gemeente geldt in principe op basis van het Unierecht een vrije vestiging in de gehele Europese Unie (EU). Er mogen geen regels worden gesteld die deze vrije vestiging belemmeren en als er regels zijn, dan dienen deze te gelden voor alle bedrijven in de EU om discriminatie te voorkomen. Ook dienen deze regels de overige principes van de EU-regelgeving te respecteren, te weten het vrije verkeer van goederen, diensten, kapitaal en personen en mogen zij geen ongerechtvaardigde belemmering vormen hiervoor. De regels dienen transparant te zijn en evenredig te zijn met het doel dat met de regel is gediend.[131]

2. Wat zijn eventuele randvoorwaarden/knelpunten bij die wijze van regulering (bijvoorbeeld kennis, bewustzijn, gevoelde verantwoordelijkheid, capaciteit, zicht op het vraagstuk).

3. Wat zijn mogelijke (maatschappelijke) gevolgen van die risico's of bedreigingen voor de openbare orde en veiligheid

[131] Zie daarvoor o.a. ABRvS 20-6-2018, ECLI_NL:RVS:2018:2062 (Appingedam), ABRvS 27-3-2019, ELI:NL:RVS:2019:965.

en of digitale ontwrichting en welke bedrijven hebben een verhoogd maatschappelijk risico?

4. Welke juridische (normenkaders) lenen zich goed voor het reguleren van dergelijke risico's in de gemeentelijke vergunningverlening? (bijvoorbeeld BIO of ISO 27001).

5. Wat zijn eventuele randvoorwaarden/knelpunten bij die wijze van regulering (bijvoorbeeld kennis)?

6. Op EU-niveau wordt binnenkort de NIS2 van kracht.[132] In hoeverre mag een gemeente aanvullende regels stellen bij bedrijven die buiten de NIS2 vallen, op het gebied van cyberveiligheid met als doel de bescherming van de openbare orde in die gemeente?

7. Bent u van mening dat in het bestuursrecht het virtuele domein onderdeel uitmaakt van het fysieke domein, waarbinnen de gemeente regels kan stellen? Of vindt u dat een regeling op gemeentelijk niveau in het virtuele domein alleen kan als de landelijk wetgever dit mogelijk heeft gemaakt overeenkomstig het legaliteitsbeginsel? Zo ja/ zo neen, hoe dan?

   Toelichting: dat de openbare orde valt onder het algemeen belang, dat de overheid geacht wordt te behartigen mag evident zijn. Zonder een handhaving van de openbare orde zou er chaos kunnen zijn.[133]
   Dat is precies wat speelt in de virtuele wereld. De complete vrijheid door afwezigheid van regels zorgde voor misstanden, waardoor ook hier de overheid met regelgeving probeert een orde aan te brengen en deze te handhaven door middel van regels en beleid. Het meest recente vraagstuk is dat van de regelingen rond Artificiële Intelligentie.[134]
   Dat er een openbare orde is in het virtuele domein is niet vanzelfsprekend, maar wordt zo langzamerhand wel verondersteld.[135]*Interessant in dit verband is het politiereglement van de 19 Brusselse gemeenten. Vanaf 1 september 2020 geldt een Gemeenschappelijk Algemeen Politiereglement voor alle negentien Brusselse gemeenten. Dit reglement is te vergelijken met de Nederlandse gemeentelijke*

[132] Richtlijn (EU) 2022/2555van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2). PbEU 2022, L333/80
[133] Zie hierover o.a. Brouwer, 'Wat is openbare orde', in *NJB* 9 september 2016, nr. 1561.
[134] 'AI- regels: wat het Europees Parlement wil', europarl.europa.eu, 20 februari 2023.
[135] Bantema et. al., '*Burgemeesters in Cyberspace*', Den Haag 2018, p.127-131.

APV. In Sectie 1, artikel 1, §5 is het volgende opgenomen: "Voor de toepassing van dit reglement omvat het begrip 'voor het publiek toegankelijke ruimte' naast de werkelijke ruimten ook de virtuele ruimten die toegankelijk zijn voor het publiek, zoals accounts op social media, forums en andere digitale platvormen die niet beperkt zijn tot een klein aantal personen die gemeenschappelijke interesses delen".[136]

Daar waar handhaving van de openbare orde in het virtuele domein nog lastig is voor gemeenten, is deze bij het bestrijden van openbare ordeverstorende effecten vanuit het virtuele domein in de fysieke domein redelijk duidelijk aan het worden.[137] *Preventie van de openbare ordeverstorende handelingen in het virtuele domein door het bestuursrecht blijft lastig door de werking van de grondrechten (artikelen 7 en 10 Grondwet, resp. uitingsvrijheid en privacybescherming). Maar wellicht is het mogelijk om andere bestuursrechtelijke instrumenten te gebruiken om als gemeente preventief invloed uit te oefenen op de bescherming van de openbare orde tegen verstoringen vanuit het virtuele domein. Onderzocht wordt hier het vergunningen- en ontheffingenstelsel.*

Heeft u nog iemand die we per se moeten interviewen of heeft u nog heeft u nog adviezen welke literatuur interessant is voor ons onderzoek?

[136] Politie.be, Algemene Politiereglementen.
[137] Bantema, Westers, Munneke, '*Niet bevoegd, wel verantwoordelijk*', Den Haag 2020 en Bantema, Twickler, De Vries, *'Juridische grenzen en kansen bij openbare ordehandhaving'*, Leeuwarden 2022.

Bijlage 2 Lijst van respondenten

Astrid de Jong
- Hoofd Veiligheidsalliantie regio Rotterdam

Astrid Nienhuis
- Burgemeester gemeente Heemstede
- Portefeuillehouder cyber

Daniel Rios Loogman
- Hoofd crisisbeheersing (specialiteit cyber) Veiligheidsregio Kennemerland

Erik Rutkens
- Praktor digitaal veilige apparatuur Noorderpoort
- Medeoprichter Hacksclusive

Henk Den Uijl
- Onderzoeker en docent NSOB

Ira Helsloot
- Hoogleraar Besturen en Veiligheid bij Radboud Universiteit

Iris Meerts
- Burgemeester gemeente Wijk bij Duurstede
- Portefeuillehouder Cyber

Jan Rijpstra
- Burgemeester gemeente Smallingerland
- Portefeuillehouder cyber

Jelle Groenendaal
- Adviseur risico- en crisismanagement
- Associate senior onderzoeker & trainer Crisislab

Jeroen Hamers
- Regionaal programmaleider Digitale Veiligheid en Cybercriminaliteit, Bureau Regionale Veiligheidsstrategie Midden-Nederland

Mariëtta Buitenhuis
- Advocaat bij AKD Advocaten

Niek Jan van den Hout
- Docent-onderzoeker Haagse Hogeschool
- Onderzoeksgroep Riskmanagement en Cybersecurity

Pieter Heiliegers
- Burgemeester gemeente Uithoorn
- Portefeuillehouder cyber

Raymond Slot
- Lector Cybersecurity Hogeschool Utrecht

Rian Van Dam
- Burgemeester gemeente Hollands Kroon
- Portefeuillehouder cyber

Syan Schaap
- Specialist evenementenveiligheidsbeleid

Bijlage 3 Protocol focusgroep

Focusgroep 5 december 2023 – 14.00-15.30
Vergunningverlening en cyberveiligheid

Achtergrond
Gemeenten kunnen organisaties en bedrijven bij de verlening van vergunningen vragen om aantoonbaar aandacht te hebben voor Algemene Verordening Gegevensbescherming (AVG) en voor andere aspecten van cyberveiligheid. In het bijzonder gaat het hier om bedrijven die weliswaar niet direct onder de vitale infrastructuur vallen, aangezien daarvoor al minimale vereisten gelden. Het gaat met name om niet-vitale bedrijven, maar die wel degelijk digitaal ontwrichtende en orde verstorende incidenten kunnen veroorzaken, wanneer de cybersecurity niet op orde is. De vraag is echter of de vergunningsverleners bij gemeenten de kennis en expertise in huis hebben om cyberrisico's van bedrijven en organisatoren te beoordelen. Niet alleen de gemeenten spelen immers een rol in de vergunningverlening, ook veiligheidsregio's beoordelen een apart katern voor bijvoorbeeld risico evenementen en brengen advies uit vanuit de hulpdiensten.
Als VNG willen we graag vervolgonderzoek laten uitvoeren om de ontbrekende lokale bevoegdheden en interventiemogelijkheden op het gebied van vergunningverlening in relatie tot cyberveiligheid te verkennen. Door het uitvoeren van vervolgonderzoek verwacht de VNG te voorzien in de behoefte en wens van gemeenten om proactief digitale incidenten en crisis te kunnen voorkomen of de (cascade)effecten te beperken. Dit sluit eveneens aan bij het programmaplan ADV in het kader van voorbereiding op digitale ontwrichting, incidenten en crisis. Daarnaast draagt dit vervolgonderzoek bij aan de digitale weerbaarheid van overheid, bedrijven en maatschappelijke organisaties, wat eveneens een pijler is in de Nederlandse Cybersecuritystrategie 2022-2028.[138]

Stellingen en vragen voor de discussie

1. Bij bedrijven die geen deel uitmaken van de vitale infrastructuur kunnen effecten op de openbare orde ontstaan bij digitale incidenten/onvoldoende cyberveiligheid.

[138] https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie/documenten/publicaties/2022/oktober/10/nlcs-2022

2. Communicatie is een sterker (sturings)instrument dan regelgeving om cyberveiligheid te vergroten.

3. Cyberincidenten binnen een bedrijf (mkb) zouden gemeld moeten worden bij de gemeente.

   Bijvoorbeeld: Bedrijven dienen in hun veiligheidsprotocollen de gemeente op te nemen als adressant *bij cyberincidenten, zodat beide partijen kunnen leren van ervaringen en de effecten ervan voor de openbare orde steeds duidelijker in kaart kunnen brengen*

4. Het is wenselijk dat gemeenten en mede-overheden regels stellen ten aanzien van cyberveiligheid bij bedrijven (mkb) binnen diens grondgebied.

5. Gemeenten en medeoverheden zijn in staat (los van de vraag of het juridisch kan) om voorschriften en eisen rondom cyberveiligheid te beoordelen (wat zijn eventuele knelpunten of randvoorwaarden).

6. Welke (juridische) normenkaders lenen zich goed voor de regulering van cyberveiligheid via vergunningen? Welke kaders en welke vergunningen?

Mogelijk worden na afloop van de focusgroep nog enkele specifieke vragen aan u nagestuurd. We kijken uit naar een boeiende sessie op 5 december!

Bijlage 4 Lijst van deelnemers focusgroep

Arjen Littooij
- Directeur veiligheidsregio Rotterdam-Rijnmond

Geert Jan Staal
- Lid Innovatieteam Amsterdam
- Lid Centrale Ondernemingsraad (portefeuillehouder cyber)

Henk van Ee
- Verbonden aan Saxion Hogeschool, centrum Veiligheid en digitalisering
- Communitymanager Cyberweerbaar NL

Jan Peter Soenveld
- Adviseur Veiligheid bij Scherpinveiligheid

Jurjen Jansen
- Lector Digitale weerbaarheid
- Verbonden aan Thorbecke Academie, NHL Stenden hogeschool
- Verbonden aan Politieacademie

Liesbeth Holterman
- Strategisch adviseur Cybersecurity
- Verbonden aan Cyberveilig Nederland

Thomas Kuil
- Beleidmedewerker cybercrime en digitaliserende criminaliteit, Openbaar Ministerie

Wouter Stol
- Lector Cybersafety
- Verbonden aan Thorbecke Academie, NHL Stenden hogeschool
- Verbonden aan Politieacademie

THORBECKE
ACADEMIE

NHL STENDEN