



Bestuurlijk koorddansen in een digitaliserende samenleving

Dr. Willem Bantema

THORBECKE
ACADEMIE
NHL STENDEN



Dr. Willem Bantema

Bestuurlijk koorddansen in een digitaliserende samenleving

Publicatie ter gelegenheid van lectorale rede (30 mei 2023)

De missie van het lectoraat Bestuur in een Digitaliserende Samenleving is om via goed en effectief bestuur bij te dragen aan (digitale) veiligheid in de Nederlandse samenleving. Door hoogwaardig praktijkgericht onderzoek draagt het lectoraat bij aan: kennisontwikkeling en het delen van kennis, oplossingen voor de beroepspraktijk en maatschappelijke vraagstukken, en de kwaliteit en toekomstbestendigheid van onderwijs en professionalisering. De onderzoekslijnen zijn:

1. Anticiperen op uitdagingen in digitalisering en maatschappij
2. Bijdragen aan effectief en goed bestuur en beleid in een digitaliserende samenleving
3. Betrekken van het maatschappelijke en burgerperspectief bij beleid en bestuur

Colofon



2023

Deze publicatie van NHL Stenden Hogeschool / Thorbecke Academie valt onder een Creative Commons Naamsvermelding 4.0 Internationaal-licentie. Dit betekent dat de kennis uit deze publicatie hergebruikt mag worden als basis voor de ontwikkeling van nieuwe kennis mits de naam van de auteur en NHL Stenden hierbij vermeld wordt. De volledige tekst van de licentie is te vinden op: <https://creativecommons.org/licenses/by/4.0/deed.nl>

Disclaimer

De auteur heeft er alles aan gedaan om alle bronnen en auteursrechthebbenden op te sporen en te vermelden.

Inhoud

Voorwoord	6	Hoofdstuk 3	33
Hoofdstuk 1	9	Kernvragen voor effectief en goed bestuur in een digitaliserende samenleving	
1.1 Inleiding op het lectoraat	10	3.1 Inleiding op de kernvragen	34
1.2 Een aanmoedigende recensie op een onderzoek dat achteraf een fundament bleek	10	3.2 Ethiek omarmen	34
1.3 Van agendering tot een nieuwe fase	12	3.3 Kennispositie versterken	35
		3.4 Bevoegdheden inzetten	37
		3.5 Monitoren van (on)veiligheid	39
		3.6 Samenwerken	42
		3.7 Conclusie	43
Hoofdstuk 2	23	Hoofdstuk 4	45
Complexiteit van bestuur en in een digitale samenleving		Het lectoraat Bestuur in een Digitaliserende Samenleving	
2.1 Inleiding	24	4.1 Inleiding	46
2.2 Inleiding op complexiteit	24	4.2 Missie en team	46
2.3 Technische complexiteit	24	4.3 Recent afgeronde en lopende projecten	51
2.4 Netwerkcomplexiteit	25	4.4 Valoriserende activiteiten	65
2.5 Echtheidscomplexiteit	25	4.5 Onderzoekslijnen en onderzoeks-thema's van het lectoraat	68
2.6 Cyborgcomplexiteit	26	4.6 Tot besluit	86
2.7 Ontwikkeling in complexiteit – een weging	27		
2.8 Organisatievermogen	27	Dankwoord	88
2.9 Informatievermogen	29		
2.10 Kenmerken van het internet en relevantie voor beleid	29		
2.11 Een opmaat naar vijf relevante hoofdlijnen	31		

Voorwoord

Dit boekwerk gaat over het verrichte werk en de eerste vervolgplannen van het NHL Stenden Thorbecke Academie lectoraat 'Bestuur in een Digitaliserende Samenleving'. Dit lectoraat werkt actief samen en vormt samen met het lectoraat 'digitale weerbaarheid van mens en organisatie' en de cross-over 'digital citizenship' de onderzoeksgroep Cybersafety.

Als lectoraat is het mogelijk om impact te hebben en de wereld of de manier we naar de wereld kijken iets te veranderen. Ook bij toekomstige professionals. Zo is de steeds meer ingeburgerde term 'online aangejaagde ordeverstoring' voor het eerst genoemd in ons onderzoek 'Niet bevoegd, wel verantwoordelijk'. In het onderzoek 'burgemeesters in cyberspace' zagen we dat de het heel moeilijk was om een strikt onderscheid te maken tussen ordeverstoringen met een offline en een online aanleiding, simpelweg omdat die sterk door elkaar lopen en sterk met elkaar verweven zijn. Dat zal de komende jaren nog verder toenemen. We hebben daarom gekozen voor de term 'online aangejaagde ordeverstoring' omdat online activiteiten in onze ogen een startpunt kunnen zijn voor een verstoring maar ook een tussentijdse katalysator die bestaande offline onrust kan versterken. Sinds het boek uit is gekomen zijn

er veel meer online aangejaagde ordeverstoringen geweest en is de term gemeengoed geworden in veiligheidsbeleid en agenda's van publieke partijen zoals gemeente en politie. Dat maakt het door Boom uitgegeven onderzoek een belangrijke mijlpaal in het denken over de invloed van het online domein op de openbare orde. Naast verschillende publicaties, lezingen voor uiteenlopende doelgroepen hebben we met het onderzoek meerdere keren het NOS-journaal gehaald, veel bijdragen in kranten en vakbladen verzorgd en ook een bijdrage geleverd in een Tweede Kamersessie over 'online gebiedsverboden'. Ook in het onderwijs hebben we mooie resultaten behaald. Studenten werken mee aan opdrachten en onderzoeken en kennis wordt gebruikt als tentamenstof.

Het doen van onderzoek op het grensvlak van recht, bestuur en veiligheid ligt ons team goed. We werken multidisciplinair. Het meest interessant vinden we het spanningsveld tussen het (verouderde) recht en snel veranderende technologische mogelijkheden waar burgers en natuurlijk ook criminelen gebruik van maken. Daarnaast is het lokale handhavingsaspect heel interessant in relatie tot het grenzeloze internet (is er een lokaal publiek online domein) en de territoriale begrenzing van de bevoegdheden van burgemeesters. Daarnaast komt ook privacy steeds vaker naar voren. Online kijken wat er speelt maakt dat je inbreuken kan maken op privacy van inwoners, door online in te grijpen kan je botsen met de vrijheid van meningsuiting. De technologische mogelijkheden zullen sneller toenemen dan de juridische waarborgen om technologie te reguleren. De komende jaren zal het lectoraat daarom meer aandacht vragen voor het maatschappelijke en burgerperspectief op digitale veiligheid en het gebruik van technologie door overheden om bij te dragen aan die veiligheid. Ethische vragen spelen daar een belangrijke rol. We werken actief samen met onze kenniskring, met collega's van de Thorbecke Academie en de onderzoeksgroep, met andere lectoren (intern en extern), met onze studenten en met de beroepspraktijk. We willen het aantal samenwerkingen de komende jaren nog verder uitbreiden. De gepresenteerde onderzoeksplannen zijn een eerste verkenning die de komende jaren nog verder uitgewerkt zullen worden.





Hoofdstuk 1

De wortels van het lectoraat 'Bestuur in een Digitaliserende Samenleving'

1.1 Inleiding op het lectoraat

De introductie op ons lectoraat 'Bestuur in een Digitaliserende Samenleving' beginnen we graag met een recensie die verscheen rond het uitkomen van het onderzoek 'burgemeesters in cyberspace', dit onderzoek, zo zal blijken, was het begin van een onderzoekslijn die uitmondde in het huidige lectoraat. De recensie laat zien op wat voor spannend terrein we onder andere onderzoek doen, dat we als lectoraat pionieren, dat we nieuwsgierig en een tikkeltje eigenwijs zijn en dat we in 2018 (en daarvoor) onze tijd wat vooruit waren. Het lectoraat, zo zal ik later ook nog betogen, heeft altijd een sterke rol in agendering gespeeld door te anticiperen op toekomstige ontwikkelingen. De recensie op ons eerste onderzoek was voor ons een aanmoediging om verder te gaan op dit onderzoeksthema en terrein. Voorts blijkt met terugwerkende kracht dat ons onderzoek een kenmerken van design-based-research (dbr) bevat. Dan nu terug naar de recensie die ik integraal heb overgenomen.¹

1.2 Een aanmoedigende recensie op een onderzoek dat achteraf een fundament bleek

In de sociaalwetenschappelijke methodologie wordt vaak betoogd dat het stellen van de juiste vragen zeker zo belangrijk is als het vinden van mooie antwoorden. Misschien klinkt dat inmiddels een beetje als een wat sleetse platitude. Dat het wel degelijk nog steeds een geldige stelling is, bewijst het onderzoek van Bantema cs. naar 'Burgemeesters in cyberspace'. Vertrekpunt van hun onderzoek was een niet bepaald alledaagse vraag. De vraag namelijk of er zoiets bestaat als openbare orde in de

digitale werkelijkheid, de virtuele wereld zoals die inmiddels bestaat naast en in verbinding met onze aloude fysieke werkelijkheid. En – zo luidt één van hun vervolgvragen – als er dan zoiets is als openbare orde in cyberspace, moet de orde daar dan ook gehandhaafd worden? Beschikken burgemeesters, die eerstverantwoordelijk zijn voor handhaving van de lokale openbare orde in de fysieke wereld, dan wel over instrumenten die geschikt zijn om ook in de virtuele wereld een vorm van openbare orde te handhaven? Intrigerende vragen, toch? Vragen ook die, bijna letterlijk, grensverleggend zijn.

Toen ik, alweer een tijdje geleden, door een van de onderzoekers werd benaderd voor een interview was mijn eerste reactie 'ik weet iets van burgemeesters en hun taken en bevoegdheden maar hier weet ik niets van af'. 'Dat zegt iedereen, die we benaderen', was het weerwoord van de onderzoeker en juist daarom vinden we het zo een interessant onderwerp. Wie daar wat verder over nadenkt, komt al snel tot de conclusie dat hij gelijk heeft. Sinds het uit de hand gelopen feestje in Haren – een tiener die een foutje maakte met haar Facebook uitnodiging voor een feestje triggerde ernstige wanordelijkheden – weten we dat (ook in Nederland) activiteiten in de zo abstract lijkende virtuele werkelijkheid hele reële consequenties in de alledaagse fysieke wereld kunnen hebben. Het lijkt welhaast een virtuele variant op het aloude Thomas Theorema: 'Als mensen situaties als reel definiëren dan hebben ze reële consequenties.'

De ontwikkelingen in de virtuele wereld, cyberspace, gaan zo snel dat kennis en reflectie, laat staan wetgeving, ver achter blijven. De eerste reactie van veel respondenten in dit onderzoek – 'daar weet ik niets van' – benadrukt hoezeer kennis en reflectie momenteel tekortschieten. Onbedoeld, maar zeker niet minder nuttig, krijgt het onderzoek daarmee iets van actie-onderzoek: het stimuleert de respondenten om over orde en ordehandhaving in cyberspace na te gaan denken. Noodgedwongen heeft het onderzoek van Bantema cs. dus vooral een verkennend karakter. Het brengt juridisch en empirisch in beeld wat openbare orde is, in hoeverre het begrip toepasbaar is in cyberspace en hoe het wordt ervaren en gehanteerd door burgemeesters, als de eerstverantwoordelijke bestuurders.

Gebrek aan ervaring met orde in cyberspace – maar vooral weinig reflectie tot nu toe – leiden tot zeer diverse beelden en opvattingen. Brede consensus is er eigenlijk alleen over het feit dat, als er zoiets als openbare orde in cyberspace bestaat, ook die orde gehandhaafd moet worden. Terecht, want er zijn vele voorbeelden te geven dat wat er gebeurt in cyberspace – denk bijvoorbeeld aan sociale media gebruik – een directe weerslag kan hebben op de traditionele openbare orde. De virtuele wereld wordt, anders dan traditionele media, gekenmerkt door weinig of geen inhoudelijke controle en door vaak sterke en snelle mobiliserende effecten. 'Haren' is daar een voorbeeld van. Radicalisering en jihadisme een ander.

Gaandeweg klinken bij de geïnterviewde experts en burgemeesters twijfels door of orde in cyberspace wel primair een lokaal probleem is, dat door burgemeesters met bestuursrechtelijke middelen gehandhaafd moet worden. Is het niet eerder iets dat niet

plaatsgebonden is – virtueel! – en dat dus landelijk door politie, OM en het strafrecht gehandhaafd dient te worden? Duidelijk meningsverschil is er ook over de vraag of je orde in cyberspace met beschikbaar (bestuursrechtelijk) instrumentarium kunt en moet handhaven of met speciaal voor de virtuele wereld ontwikkeld instrumentarium. Waarover we momenteel dus nog niet kunnen beschikken.

Wie gelijk heeft in discussies over strafrecht versus bestuursrecht of over bestaand versus nieuw instrumentarium is, zeker voorlopig, niet zo belangrijk. Veel belangrijker is dat dit onderzoek het denken op gang brengt en stimuleert. Dat is hard nodig. Ontwikkelingen in de virtuele wereld gaan momenteel heel snel. Ze hebben zelden of nooit uitsluitend positieve consequenties en ze hebben meestal ook duidelijk aantoonbare gevolgen voor de fysieke werkelijkheid. Of we een vorm van openbare orde moeten handhaven in cyberspace lijkt me inmiddels nauwelijks meer een vraag. We zullen wel moeten. Maar over wie dat dan gaat doen en met welke bestaande of nieuwe instrumenten, daarover wordt nog maar mondjesmaat nagedacht. Aan het verder op gang brengen van dat denken levert dit boek, ondanks een bescheiden omvang (150 pagina's), een belangrijke bijdrage.

Dit onderzoek was het begin van een onderzoekslijn die is uitgemond in het lectoraat 'Bestuur in een Digitaliserende Samenleving'. Al vanaf het begin heeft het onderzoek bijgedragen aan bewustzijn en steeds meer draagt het onderzoek bij aan effectief beleid en interventies en handelingsperspectief in de praktijk om digitale veiligheid te vergroten op een ethisch verantwoorde manier. Onder andere zullen we dit doen door de maatschappij en burgers nadrukkelijk te gaan betrekken bij die werkwijzen.

¹ <https://platformoverheid.nl/openbare-orde-online/>

1.3 Van agendering tot een nieuwe fase

In deze paragraaf komt de kern van het hoofdstuk aan bod. Ik wil de oorsprong en de kern van het huidige lectoraat laten zien. Later (hoofdstuk 4) zullen we ingaan op de onderzoekslijnen en beoogde activiteiten voor de komende jaren.

1.3.1 De onderzoeksgroep Cybersafety

De onderzoeksgroep Cybersafety verricht hoogwaardig praktijkgericht onderzoek om digitale veiligheid van te bevorderen in de digitaliserende samenleving, speciaal in de Nederlandse context. Het onderzoek werkt door in onderwijs, de beroepspraktijk en beleid en levert daarnaast een wezenlijke bijdrage aan de wetenschappelijke kennisvoorraad. De groep doet onder andere onderzoek naar hoe mensen, bedrijven en overheden zich beter kunnen beschermen tegen digitale aanvallen (onderzoek naar weerbaarheid²) en onderzoekt hoe de overheid kan bijdragen in veiligheidsbeleid en wat hun rollen en verantwoordelijkheden in het digitale domein zijn (destijds: bestuurlijke handhaving en digitalisering).

Er zal in deze bijdrage in meer detail worden ingegaan op een van de onderzoeken die in sterke mate bijdraagt aan een vitale regio en gestoeld is op een combinatie van sterke regionale binding (gemeente Leeuwarden) en landelijke samenwerking met het Nederlands Genootschap van Burgemeesters (in het vervolg NGB) en op die wijze ook

de gewenste doorwerking vindt op verschillende gebieden. Het kan gezien worden als een voorbeeld van de manier waarop de onderzoeksgroep haar voorstellersrol op het gebied van digitale veiligheid vervult. Het vervullen van een voortrekkersrol gaat niet zonder vallen of opstaan maar heeft het in dit geval geleid tot een grote maatschappelijke impact die regio-overtijgend is gebleken. In het vervolg van dit stuk zal aandacht zijn voor de eerste fase van het onderzoek naar bestuur in een digitaliserende samenleving (1), de fase waarin onderzoek start en wordt uitgevoerd (2), de resultaten van het onderzoek (3) en de maatschappelijke impact en doorwerking van het onderzoek (4). Er wordt afgesloten met een beschrijving van de veranderde tijdsgeschiedenis (5).

1.3.2 Het agenderen van bestuurlijke digitale veiligheidsvraagstukken

Lange tijd bleek gemeenten en burgemeesters buiten schot als een partij met een rol in het bevorderen van digitale veiligheid. Nederlandse burgemeesters hebben een bijzondere positie op het gebied van veiligheid doordat zij eigenaar zijn van de portefeuille openbare orde en veiligheid en een verregaand pakket aan bevoegdheden tot hun beschikking hebben om die te handhaven. Openbare orde is gericht op de 'normale gang van zaken in het publieke domein'.³ In 2010 stelt rechtenstudent (Vols) zich voor het eerst af of cyberspace of delen ervan tot de openbare orde gerekend moeten worden en of de burgemeester daar dan ook een

verantwoordelijkheid heeft.⁴ Het werk krijgt echter geen vervolg en het thema verdwijnt weer naar de achtergrond, totdat de onderzoeksgroep (toen nog lectoraat Cybersafety) het onderwerp omarmd. Project X in Haren (2012) speelde daarin een belangrijke rol. Bij Project X Haren was er een meisje uit Haren wiens uitnodiging voor een verjaardagsfeestje werd gekaapt door derden, vervolgens massaal via Facebook werd gedeeld en uiteindelijk leidde tot massale mensenmassa's in Haren met verscheidende vernielingen tot gevolg. Door toenmalig NHL werd samen met de Gemeente Leeuwarden (Ferd Crone) en het NGB (Wouter Jong) een kennisconferentie georganiseerd over de rol van burgemeesters in cyberspace. De teneur bij deze conferentie was dat burgemeesters voor zichzelf geen rol zagen weggelegd in de digitale wereld.⁵ Dat weerspiegelt heel goed de toenmalige tijdsgeschiedenis. Ook in het in 2010 gepubliceerde *Zakboek openbare orde en veiligheid* van het NGB komen te termijnen cyber, internet, digitaal en of digitale niet voor.⁶ Een eerste subsidieaanvraag in 2015 van NHL Hogeschool voor een onderzoek naar mogelijkheden voor virtuele ordehandhaving door burgemeesters werd niet gehonoreerd met een verwijzing naar een gebrek aan urgentie en te weinig vraagarticulatie vanuit de praktijk. Het jaar daarop, in 2016, werd een vergelijkbare aanvraag programma Politie en Wetenschap wel gehonoreerd.⁷ Dit laat zien een voortrekkersrol op een onderzoeksthema er een van de lange

adem is. In 2016 zijn de wortels gelegd voor een onderzoek met grote maatschappelijke impact, 'burgemeesters in cyberspace'. Dit is het onderzoek dat aan het begin van dit hoofdstuk in een recensie werd besproken.

1.3.3 De start van een onderzoekslijn

Vanaf 2017 deden onderzoekers van NHL samen met onderzoekers van de Rijksuniversiteit Groningen een multidisciplinair onderzoek naar de mogelijkheden voor burgemeesters om preventief op te treden in gevallen waarbij de openbare orde wordt verstoord of verstoord dreigt te raken door wat online gebeurt.⁸ De onderzoekers voeren een juridische analyse uit (wat kan en mag) maar kijken hoe vanuit de praktijk wordt gekeken naar de rol van gemeente en burgemeesters bij ordehandhaving en ook of burgemeesters voor zichzelf een rol zien weggelegd online. Dat praktijkonderzoek is uitgevoerd aan de hand van interviews met 33 experts (waaronder politie, veiligheidsregio's, CCV, wetenschappers, juristen, ambtenaren openbare orde en veiligheid en politiemensen) en 14 burgemeesters. Vanwege het verkennende karakter van het onderzoek is overwegend het sneeuwbalprincipe gebruikt om in kaart te brengen welke mensen uit de praktijk en welke burgemeesters ons input zouden kunnen geven voor het onderzoek. Tijdens de uitvoering van het onderzoek worden tussentijds uitkomsten gepresenteerd op verschillende thema-

² Jansen, J. (2018). Do you bend or break? Preventing online banking fraud victimization through online resilience. Dissertatie: Open Universiteit.

³ Jong, M.A.D.W. de e.a. (2017) *Orde in de openbare orde*. Wolters Kluwer: Alphen aan de Rijn

⁴ Vols, S. Virtuele handhaving van de openbare orde, masterscriptie Rijksuniversiteit Groningen.

⁵ Leeuwarder Courant, 11 september 2014, p. 28.

⁶ W. ph. Stol & L. Strikwerda, *Strafrechtspleging in een digitale samenleving*. Den Haag: Boom Juridisch, 2017, p. 55-56.

⁷ Sanne Boes (overleden op 05-04-2020) was penvoerder bij die aanvraag en heeft belangrijk werk verricht in de pionierende fase van dit onderzoek.

⁸ Bantema, W. e.a. (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*. Den Haag: Sdu (reeks Politie en Wetenschap)

dagen rondom gemeentelijke veiligheidsbeleid en treffen daarbij onder andere ook partijen zoals de Vereniging van Nederlandse Gemeenten (VNG), de G40 en de NGB. Dit maakte dat de praktijk al vroeg actief bij het onderzoek werd betrokken en dit zal zijn vruchten afwerpen bij de verdere valorisatie van het onderzoek en de doorwerking ervan, zo zal blijken.

1.3.4 Uitkomsten van het onderzoek

Het gedrag van mensen in een sterk gedigitaliseerde maatschappij laat zich echter steeds moeilijker scheiden in een 'online' en 'offline' deel. In werkelijkheid zijn die twee werkelijkheden daarvoor te sterk met elkaar verweven.' Enkele voorbeelden die het rapport worden genoemd zijn online oproepen tot illegale feesten en evenementen, oproepen tot demonstraties en tegendemonstraties, doelbewuste verspreiding van nepnieuws (en onrust op sociale media en offline) en treitervloggers die onder andere gezagsdragers filmen (ondermijnen, plagen) en vervolgens die beelden op Youtube zetten. Het gedrag is op het randje en de politieagenten hebben geen stok om mee te slaan. Als gevolg van de beelden, waarbij ook inwoners van Zaanstad worden lastiggevalen in de video's, komt er ook online een beweging op gang om de zogenaamde 'treitervlogger' te grazen te nemen. Het is duidelijk dat het niet gek is dat aan een online rol voor burgemeesters wordt gedacht.

Hebben burgemeesters dan ook mogelijkheden om met hun openbare-ordebevoegdheden in te grijpen in de online wereld. De belangrijkste conclusie van het onderzoek was dat burgemeesters, hun bevoegdheden niet kunnen inzetten. Er zijn meerdere problemen aan te wijzen bij een online toepassing van bevoegdheden. Voor een deel is dat

het gevolg van bevoegdheden die voor een groot gedeelte tot stand zijn gekomen aan het einde van de 19e eeuw. De eerste geslaagde vlucht van de gebroeders Wright moest nog volgen, televisie bestond nog niet en ook aan het internet was nog niet gedacht bij de ontwikkeling van die wetgeving. Zo bezien is het niet zo vreemd dat de bevoegdheden die toen zijn ontwikkeld, lastig toepasbaar zijn.

Eén van de drie grootste problemen is dat digitale bedreigingen zich niet aan fysieke gemeentegrenzen houden. Een burgemeester mag van oudsher alleen binnen zijn eigen gemeente optreden. Wanneer iemand uit een andere gemeente oproept tot een massale samenkomst, is de burgemeester van de ontvangende gemeente niet bevoegd om dat te voorkomen. Een ander probleem is dat ingrijpen al snel een ontoelaatbare inbreuk op grondrechten betekent, zoals de vrijheid van meningsuiting. Preventief ingrijpen via het internet betekent in veel gevallen het aanpassen of verwijderen van berichten van mensen, terwijl de burgemeester daartoe niet bevoegd is. Vrijwel alle gedragingen op het internet zijn uitingen. Uitingen die niet strafbaar zijn gesteld vallen ook buiten het bereik van de burgemeester, maar dat betekent niet in alle gevallen dat ze niet tot verstoringen kunnen leiden. Ook is het lastig om in te schatten wat de gevolgen op straat kunnen zijn van dreigende berichtgeving. Sommige oproepen via sociale media mondden uit in grote verstoringen, terwijl ze in andere gevallen weinig navolging krijgen. Dat maakt de verantwoording bij een eventueel ingrijpen lastig.

De voor het onderzoek benaderde burgemeesters denken wisselend over de mogelijkheid en wenselijkheid van het online toepassen van hun bevoegdheden in een online wereld. Sommige

burgemeesters willen geen bevoegdheden op het internet, omdat ze vinden dat burgemeesters zich verre van uitingen van burgers moeten houden en optreden door het Openbaar Ministerie en het strafrecht meer voor hand ligt. Anderen geven aan dat zij zich verantwoordelijk voelen voor de openbare orde binnen hun gemeente en dat online dreigingen binnen hun gemeente daar ook onder vallen. Enkele burgemeesters geven de voorkeur aan verandering van wetgeving, waardoor ook online ingrijpen door burgemeesters mogelijk wordt gemaakt. Sommigen pleiten voor de oprichting van een landelijke autoriteit die beter online kan handhaven. Het betreft vooral kwalitatieve gegevens, een enquête-onderzoek onder burgemeesters zal later plaatsvinden.

1.3.5 Doorwerking

Het is moeilijk om de valorisatie en de maatschappelijke impact van onderzoek vast te stellen. Toch is hier een poging gedaan door een onderscheid te maken tussen: doorwerking in vervolgstudies (1) kennisoverdracht voor een groter publiek in media (2) bijdrage aan wetenschappelijke kennis en discussies (3), doorwerking in de praktijk (4) en doorwerking in het onderwijs (5). Naar aanleiding van het onderzoek 'Burgemeesters in cyberspace' zijn twee vervolgstudies gehonoreerd die beide zijn gestart in 2019 en respectievelijk in 2020 en 2021 zijn afgerond. Deze zullen hier eerst kort worden beschreven omdat op andere punten de onderzoeken door elkaar lopen of in elkaars verlengde liggen ten aanzien van maatschappelijke impact en valorisatie. Het eerste onderzoek betreft een praktische studie naar interventiemogelijkheden van burgemeesters om openbare ordeverstoringen waarbij internet een rol speelt te kunnen voorkomen of handhaven. Zoals gezegd biedt de juridische

route, gebaseerd op de bevoegdheden van burgemeesters online, weinig mogelijkheden voor een online toepassing. Daarom is een vervolgonderzoek voor het Centrum Voor Criminaliteitspreventie en veiligheid (CCV) en het Ministerie van Justitie en Veiligheid (J en V) gestart naar de niet-juridische handhavingsmogelijkheden of interventies van burgemeesters. Die zijn overwegend gebaseerd op gezag van de burgemeester en geleerde lessen op dat gebied. Dat onderzoek is in september 2020 gepresenteerd (boekuitgave bij Boom Bestuurskunde) en is getiteld: 'Niet bevoegd, wel verantwoordelijk', handhavingsmogelijkheden bij online aangejaagde ordeverstoringen.

Een tweede vervolgonderzoek is in opdracht van het Programma Politie en Wetenschap en gaat over de wijze waarop gemeenten online monitoren en tegen welke knelpunten of juridische grenzen ze daarbij aanlopen. Uit het vooronderzoek bleek dat gemeenten op verschillende manieren proberen om op de hoogte te zijn wat er online speelt. Er lijken onder andere verschillen te zijn in de intensiteit waarmee ze dat doen en naar de gemeentelijke afdeling het uitvoert. Doel van het onderzoek is om in kaart te brengen wat gemeenten precies doen (en waarom) op het gebied van online monitoring ten behoeve van de openbare orde en veiligheid, met bijzondere aandacht voor juridische aspecten en de mate waarin daar in de praktijk rekening mee wordt gehouden. Het onderzoek heeft onder andere tot doel om gemeenten daarin te ondersteunen. Monitoring kan belangrijk zijn. Wanneer gemeenten niet weten wat er speelt kunnen ze zelf geen interventies inzetten. Tegelijkertijd heeft ook de politie een taak voor de openbare orde en veiligheid (uitvoering) en kan het zijn dat er dubbel werk wordt verricht.

Al snel bleek dat het onderzoekdomein zich goed leent voor communicatie richting een breder publiek, daarvan zullen enkele voorbeelden worden gegeven. Zo was er aandacht voor het onderzoek in regionale kranten zoals Leeuwarder courant⁹ en het Friesch Dagblad¹⁰, maar via reporter radio (radio 1)¹¹ en Binnenlands Bestuur.¹² Ook werd een van de onderzoekers bevraagd over de zedenzaak in Assen in het NOS-journaal van 20 uur op 24 augustus 2019. Ook de vervolgstudies naar bestuurlijke interventies¹³ en gemeentelijke monitoring van de openbare orde¹⁴ zijn onder andere via regionale kranten gepresenteerd aan een breder publiek. Het onderzoek beperkt zich niet tot bijdragen in de krant en andere media. Er is doorwerking in wetenschappelijke kennis en discussies met vakgenoten. Naast het onderzoeksrapport 'Burgemeesters in cyberspace' zijn er bijdragen voor wetenschappelijke tijdschriften zoals Bestuurswetenschappen¹⁵ en Cahier en is een bijdrage geleverd aan een boek over digitale veiligheid en de stad.¹⁶ Daarnaast is op een internationaal congres aandacht gevraagd voor het thema (International Conference on Public Policy 2019).¹⁷

Doorwerking in de praktijk is lastig te meten. Doch zijn er in dit geval duidelijk resultaten bereikt op dit gebied. Een van de resultaten betreft publicaties op relevante podia voor praktijkmensen op dit gebied, zoals in Ibestuur¹⁸, het Burgemeestersblad. Een heel concrete doorwerking van het onderzoek betrof de aanwezigheid van onderzoekers van de onderzoeksgroep Cybersafety bij de Lochemconferenties in 2019, een soort opleidingsdagen voor burgemeesters waarbij januari tot maart (6 bijeenkomsten, in totaal 200 burgemeesters) digitale veiligheid centraal stond en de een vertegenwoordiger van onderzoeksgroep als expert mocht optreden in een pandediscussie. In het verlengde daarvan verzorgde de onderzoeksgroep eind 2019 (en nu nog steeds) een hele dag onderwijs voor het door het NGB ingestelde vak 'de cyberburgemeester'.¹⁹ Later was er ook nog een speciale themadag rond digitalisering die georganiseerd werd door de NGB. Op die dag waren 60 burgemeesters aanwezig. Volgens de organisatie (Wouter Jong) was dat een ongekende opkomst voor het thema digitale veiligheid en zouden er enkele jaren eerder alleen maar technisch

geschoolde medewerkers naar de bijeenkomst zijn gestuurd om de burgemeesters te vertegenwoordigen. De meest concrete en tastbare doorwerking van het onderzoek was destijds zichtbaar in Digitale Agenda van de VNG, waar expliciet wordt verwezen naar het onderzoek 'burgemeesters in cyberspace' en een actielijn openbare orde bevoegdheden en rollen voor lokale bestuurders is opgenomen.²⁰

In het onderwijs heeft het onderzoek een doorwerking gekregen als tentamenstof (kennis) voor de minor Cybersafety (jaar 4), zijn er verschillende colleges verzorgd voor minoren cybersafety, de minor Recht, Bestuur en Veiligheid, HBO recht en in het eerste jaar van Integrale Veiligheid. Daarnaast speelt het onderzoek een belangrijke rol in de nieuwe minor (burge) meester in cyberspace die in september 2023 voor het eerst wordt aangeboden door de Thorbecke Academie. Ook zijn we opdrachtgever voor het Atelier recht en veiligheid en begeleiden we afstudeerders. Hierover later meer in hoofdstuk 4.

1.3.6 Een nieuwe fase tot de start van het lectoraat (tot maart 2022)

Waar deze bijdrage begon met het agenderen van digitale veiligheid en het geregeld voorkwam dat bestuurders verontwaardigd reageerden op vragen over hun rol in cyberspace is er inmiddels, nog geen 10 jaar later, een geheel andere situatie aan het ontstaan. Zo zijn er bestuurders die zelfs zeggenschap en verantwoordelijkheid claimen over

de virtuele openbare ruimte. In november 2019 schrijft burgemeester Halsema van Amsterdam in het voorwoord van de Amsterdamse 'Agenda Digitale Veiligheid': 'Als burgemeester van deze stad ben ik verantwoordelijk voor de openbare orde en veiligheid, waaronder ook de virtuele openbare ruimte.' Dat een burgemeester verantwoordelijkheid claimt voor de veiligheid in het digitale domein is een modern en tegelijk ook een juridisch interessant gegeven. Recent vraagt een andere burgemeester zich af of hij ook een digitaal gebiedsverbod kan opleggen en of hij naast het sluitingen van woningen ook internetverbindingen kan afsluiten.²¹ Daarnaast zijn er op verschillende plekken cyberburgemeesters benoemd. Samengevat breekt momenteel een fase aan waarin er vanuit de praktijk natuurlijke voortrekkers ontstaan om digitale veiligheid aan te jagen.

De eerder beschreven onderzoeken 'Niet bevoegd, wel verantwoordelijk' (2020) en 'Black box van online monitoring (2021) zijn inmiddels afgerond en hebben de nodige impact gehad. Rondom het uitkomen van het onderzoek 'Niet bevoegd, wel verantwoordelijk' zijn veel activiteiten georganiseerd. Het project is in Coronatijd door het CCV benut voor een heus online webinar dat op 200 live kijkers kon rekenen. Voorts hebben we bijgedragen aan een factsheet²² om de belangrijkste resultaten snel zichtbaar te maken en zijn er verschillende publicaties verschenen. De belangrijkste uitkomst van deze nieuwe fase is dat het concept en door

⁹ <https://www.lc.nl/friesland/Online-handhaven-De-burgemeester-is-tandeloos-23533193.html>

¹⁰ https://frieschdagblad.nl/2018/9/18/burgemeester-is-vaak-tandeloos-bij-online-handhaven?harvest_referrer=https%3A%2F%2Fwww.google.com%2F

¹¹ <https://www.nporadio1.nl/reporter-radio/onderwerpen/475057-burgemeesters-in-cyberspace>

¹² <https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/nieuws/onderzoek-burgemeesters-in-de-knel-met-online.9596420.lynkx>

¹³ <https://www.lc.nl/friesland/LC-Academie-Burgemeester-in-coronatijd-digitaal-koordansen-25585641.html>

¹⁴ <https://frieschdagblad.nl/2020/3/9/gemeente-kijkt-bij-inwoner-mee-op-facebook>

¹⁵ Bantema, W. (2020). Perspectief uit de praktijk – De lokale Facebookpagina als café: een discussie over het bestaan van publieke plaatsen op het internet en de regulering daarvan. *Bestuurswetenschappen*

¹⁶ Stol, W. ph. & Bantema, W. Stadbestuur en digitale veiligheid, een analyse van beleidsplannen. In M. Malsch en J. W. Sap (red.), *Orde en verwarring in de stad*. Boom Criminologie (te verschijnen).

¹⁷ Mayors in cyberspace: Lessons from the Netherlands regarding the role of local government in the event of digital disturbance of the public order (te raadplegen via Researchgate).

¹⁸ <https://ibestuur.nl/podium/de-rol-van-burgemeesters-in-cyberspace>

¹⁹ Ook dit jaar zal de onderzoeksgroep daar weer een deel van het onderwijs verzorgen.

²⁰ <https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024> (p. 12).

²¹ <https://www.destentor.nl/steenwijkerland/burgemeesters-regio-zwolle-en-deventer-willen-zelf-digitaal-ingrijpen-bij-cybercrime-a9808e70/?referrer=https://www.google.com/>

²² <https://hetccv.nl/onderwerpen/cybercrime/documenten/onderzoek-niet-bevoegd-wel-verantwoordelijk/>

onderzoek vastgestelde definitie van 'online aangejaagde ordeverstoringen' (zie Bantema e.a. 2020) werd overgenomen in de belangrijkste agenda's en landelijk beleid. In 2021 is zelfs besloten de cyberwegenkaart van het CCV uit te breiden met dit thema als vierde route.²³ Daarmee is het onderzoeksthema heel nadrukkelijk op de bestuurlijke agenda gekomen.

De grootste bekendheid van het onderzoek van Thorbecke Academie/NHL Stenden Hogeschool op dit specifieke terrein is toch wel gekomen van het onderzoek 'Black box van de gemeentelijke online monitoring'. Ook bij dit complexe onderzoek is samengewerkt met collega's van de Rijksuniversiteit Groningen. In dit onderzoek is de vragenlijst die is uitgezet onder ambtenaren OOV en gemeentelijke communicatiemedewerkers de belangrijkste bron van informatie. Uit het onderzoek, waar meer dan de helft van de gemeenten op een of andere manier in vertegenwoordigd waren kwam naar voren dat vrijwel alle gemeenten aan online monitoring doen (95%) en dat de kans op het verwerken van persoonsgegevens groot is bij de uitgevoerde werkzaamheden. Tegelijkertijd zagen we dat de juridische kennis en capaciteit binnen de organisatie (en kennis van monitoring het algemeen) laag was en dat de Functionaris Gegevensbescherming (FG) in de meeste gevallen niet werd betrokken.

Het onderzoek is vooral bekend geworden door één aspect. Zo blijkt dat gemeenten gebruikmaken van een omgevingsanalyse om meer informatie te verkrijgen over een fenomeen, groep of individu. Het komt voor dat gemeenten om die informatie te verkrijgen gebruik maken van nepaccounts of privéaccounts. Vooral dat eerste aspect, het gebruik van nepaccounts sloeg in als een bom en daar waren wij als onderzoeksgroep amper op voorbereid. De dag van het uitkomen van het onderzoek stond op de voorpagina van de Volkskrant – 'Gemeenten kijken op grote schaal in het geheim mee met burgers op sociale media'.²⁴ In navolging van nieuws over het NCTV, Defensie en zeker ook de toeslagenaffaire leek het land te klein op 18 mei 2021. Het onderzoek leidde tot Tweede Kamervragen en de hoofdonderzoeker, ikzelf dus, haalde het 20 uur journaal later dat jaar. Ook van dit onderzoek maakten we een webinar samen met CCV en produceerden we wederom een factsheet.

Deze onderzoeken leidden tot vervolgoopdrachten binnen Noord-Holland Samen Veilig (NHSV)²⁵, Regio IJsselland²⁶, de Vereniging van Nederlandse Gemeenten (VNG) en de Gemeente Amsterdam. Binnen NHSV leverden we een bijdrage aan de ontwikkeling van een (online) interventiekaart door de signalering en interventies die zijn ingezet op online aangejaagde ordeverstoringen in kaart te

brengen – een eerste regionale verkenning op dit thema. Dit was ook een pilotproject op 'online orde' binnen de citydeal 'Lokale weerbaarheid en cybercrime'. De uitkomst liet zien dat gemeenten preventiever moeten worden in de aanpak van online aangejaagde ordeverstoringen. De studie voor de VNG had tot doel om gemeenten en bestuur beter te laten antiperen op digitale veiligheidsuitdagingen en handelingsperspectief te bieden. De belangrijkste uitkomsten van onderzoek komen in het volgende twee hoofdstukken aan bod (hoofdstuk2 en 3). Ook van dit onderzoek werd een webinar en een factsheet gemaakt en het heeft een bijdrage geleverd aan agendering binnen de VNG en aan de agenda digitale veiligheid en ethiek.²⁷

In samenwerking met de Amsterdam zijn we het project Connect gestart – met subsidie vanuit de Citydeal 'Lokale weerbaarheid en cybercrime'. Doel van dat project is om de geweldspiraal te doorbreken door preventief online op te kunnen treden. De input hiervoor komt tot stand via een literatuurreview samen met sociaalpsychologen van de Rijksuniversiteit Groningen (evidence-based) in combinatie met best practices en input vanuit de praktijk (practice-based). Dit onderzoek is nog in uitvoering en wordt rond juni 2023 afgerond.

Tot slot en eerder werd al wel het onderzoek voor IJsselland afgerond naar de mogelijkheden die de Algemene Plaatselijke Verordening (APV) biedt om op te treden tegen online aangejaagde ordeverstoringen. Dat thema werd actueel in 2021 en 2022 en is dat nu nog steeds. De uitkomsten van dat onderzoek en de doorwerking daarvan zullen in hoofdstuk vier

aan bod komen. Het onderzoek werd gepubliceerd in oktober 2022. Het huidige lectoraat is niet los te zien van de ontwikkelingen die we hier hebben beschreven. Ter verbreding zijn ook onderzoeken gedaan naar smart cities en digitale veiligheid van smart cities (Kiem Subsidie) en onderzoek naar de rol en bewustzijn van gemeenten rond cybercrisis. We hebben de ambitie om de Kiem-aanvraag uit te breiden naar een Raak-publiek aanvraag later in 2023. Tevens is de onderzoeksgroep Cyber-safety, waar dit lectoraat onderdeel van uitmaakt, betrokken bij een Sprong-aanvraag samen met HHS en Saxion en zijn er gelden vrijgekomen voor de evaluatie van projecten binnen de genoemde City Deal 'lokale weerbaarheid en cybercrime' waar de Thorbecke Academie vertegenwoordigd is vanaf 2020.

1.3.7 De waarde van studentenproducten en mijlpalen

Tot slot wil ik nog speciale aandacht vragen voor studentonderzoek. Later, in hoofdstuk 4, zal blijken dat projecten van studenten in opdracht van het lectoraat bijdragen aan onderzoeksaanvragen. Deze projecten en opdrachten worden uitgevoerd binnen het atelier IVK, recht & veiligheid (jaar 4), binnen minoren (zoals cyber resilience en recht bestuur en veiligheid) en binnen het afstuderen. Een van die projecten wil ik hier kort benoemen als best practice. In 2019, voor de hele discussie over 'online gebiedsverboden' was een groepje studenten binnen de (voormalig) minor 'Cybersafety' enthousiast over een opdracht naar opvattingen en mogelijkheden van een digitaal gebiedsverbod. Ze deden interviews met burgemeesters, Tweede

²³ <https://hetccv.nl/onderwerpen/cybercrime/documenten/lokale-cyberwegenkaart/>

²⁴ <https://www.volkskrant.nl/nieuws-achtergrond/gemeenten-kijken-op-grote-schaal-en-in-het-geheim-mee-met-burgers-op-sociale-media~bb40d4c7/>

²⁵ De Vries, S. & Bantema, W. (2022). *Aanpak in kaart. Inzicht in een regionale aanpak van online aangejaagde ordeverstoringen*. Onderzoeksgroep Cybersafety.

²⁶ Bantema, W., Twickler, S. M. A. & De Vries, S. (2022). *Juridische grenzen en kansen bij openbare-ordehandhaving. Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen*. Leeuwarden: Onderzoeksgroep Cybersafety.

²⁷ <https://vng.nl/publicaties/agenda-digitale-grondrechten-en-ethiek-2022-2026>

Kamerleden, met ambtenaren openbare orde en veiligheid en ook met juristen. Hun onderzoek was erg goed uitgevoerd en vernieuwend, ze deden zelfs suggesties voor een definitie van een 'digitaal gebiedsverbod', omdat ze zagen dat er in de praktijk veel discussie over was (en dat is 2023 nog steeds zo). De titel van hun eindproduct was: 'Onderzoek naar het politieke discours rond een digitaal gebiedsverbod – de (on)mogelijkheden van een digitaal gebiedsverbod. Na het uitkomen van het onderzoek heb ik samen met een van de studenten een artikel geschreven voor *Bestuurswetenschappen* met als titel: Het digitaal gebiedsverbod als gemeentelijk wapen tegen online aanjaagde ordeverstoringen.²⁸ Dit hielp ons als lectoraat enorm om het thema te 'claimen' en onszelf op de kaart te zetten. Sterker nog, er werd vaker naar dit artikel verwezen in het nieuws dan naar ons nieuwe onderzoek dat door het lectoraat was uitgevoerd op dit thema. Zo heeft de NOS ook in 2023 meerdere malen verwezen naar dit artikel op basis van onderzoek dat door de onderzoeksgroep Cybersafety²⁹ is uitgevoerd, maar het betrof dus een studentenproject dat was omgeturnd tot een vakpublicatie. In de toekomst willen we dit vaker doen.

Ter afsluiting van dit hoofdstuk zal ik enkele mijnpalen benoemen in de ontwikkeling van de onderzoekslijn en het fundament van het lectoraat 'Bestuur in een Digitaliserende Samenleving' dat sinds maart 2022 bestaat. Enkele mijnpalen:

- Doorlopende lijn van onderzoeken sinds 2017.
- Onderzoek voor o.a. gemeenten (3x), maar ook voor Kiem (SIA) en Politie en Wetenschap (2x)
- Zichtbaar in publieke debat – krant en ook televisie (waaronder 20 uur journaal van de NOS)
- Invloed op beleid en discussie over beleid (zie cyberwegenkaart – vierde route)
- Tweede Kamervragen over onderzoek
- Doorwerking onderzoek naar bestuur/ burgemeesters - burgemeesterstraining
- Onderzoek voor de VNG op bestuur en digitalisering
- Multidisciplinair onderzoek, samenwerking universiteiten en binnen Thorbecke Academie.
- Veel lezingen, workshops en bijdragen aan congressen op het thema.
- Vakpublicatie samen met student over 'digitaal gebiedsverbod'

²⁸ Vuik, G. & Bantema, W. (2021). Vuik, G. & Bantema, W. (2021). *Het gebiedsverbod als gemeentelijk instrument tegen online aangejaagde ordeverstoringen*. Bestuurswetenschappen, 2021-3.

²⁹ Bijvoorbeeld: <https://nos.nl/artikel/2459792-gemeenten-pakken-jongeregeweld-aan-met-verbod-op-bezoek-websites>

Online opruien: macht aan burgemeester of burger?

Van de rellen dit weekeinde in Leeuwarden tot aangekondigde protesten bij de intocht van Sinterklaas: de openbare orde wordt steeds vaker op de proef gesteld door opruiende online-berichten.



De Mobiele Eenheid greep zaterdagavond in om de rust op het Zaailand en omliggende straten te herstellen. Vijftien personen werden door de politie aangehouden. FOTO ANTON KAPPERS

MAARTEN PENNEWAARD

Hulde aan de horecaondernemers in Leeuwarden', twitterde Tweede Kamerlid Wybren van Haga zaterdag. En Forum voor Democratie 'steunt alle horeca-ondernemers die gewoon open blijven'. Het zijn maar twee voorbeelden van uitingen op sociale media, die kunnen leiden tot verstoring van de openbare orde.

In Leeuwarden braken zaterdagavond rellen uit toen de cafés toch dichtgingen. Burgemeester Sybrand Buma kreeg 's middags van de politie al berichten doorgestuurd waaruit bleek dat op internet en sociale media oproepen rondgingen om naar Leeuwarden te gaan. Hogeschool NHL Stenden onderzoekt of de Algemene Plaatselijke Verordening, waarin elke gemeente regels omtrent openbare orde en veiligheid heeft vastgelegd, moet worden aangepast om 'online' te kunnen ingrijpen in zulke gevallen. Modernisering is absoluut nodig, vinden veel burgemeesters.

„Ze zijn nu niet bevoegd om preventief in te grijpen bij online oproepen tot ordeverstoring, maar wel verantwoordelijk als de openbare orde vervolgens ook echt wordt verstoord”, zeggen onderzoekers Willem Bantema en Sipke de Vries van de hogeschool.

Bantema houdt zich bij de onderzoeksgroep Cybersafety al enkele jaren bezig met dit thema. 'Digitaal koordanssen' noemde hij het eerder. Nu oproepen op podia als Facebook, Twitter en Telegram steeds frequenter worden is het tijd om te kijken wat er in de regelgeving zou moeten wijzigen. De coronacrisis zet de zaken extra op scherp, aldus Bantema: kijk maar naar de avond-

kliekrellen en verspreiding van desinformatie. NHL Stenden wil van gemeenten graag concrete voorvallen horen en is daarbij ook geïnteresseerd in wat er achter de schermen gebeurt om ongeregelde te voorkomen. „We lezen de berichten in de krant, maar we willen ook graag weten wat gemeenten doen als ze op internet een oproep zien die mogelijk kan leiden tot verstoring van de openbare orde.”

De voorbeelden worden gebruikt in een onderzoek dat wordt gedaan in opdracht van elf gemeenten in de regio IJsselland. Zij willen weten hoe burgemeesters online preventief kunnen ingrijpen bij dreigende verstoringen van de openbare orde. Rob Bats, burgemeester van Steenwijkerland (een van de opdrachtgevers) is ervan overtuigd dat hij en zijn collega's digitale bevoegdheden zullen krijgen. Hij is 'chef digitale veiligheid' in IJsselland en

kent de materie. Bats was in 2012 burgemeester in Haren, toen daar 'Project X' plaatsvond: duizenden jongeren uit het hele land trokken na een online oproep naar zijn gemeente wat leidde tot ernstige ongeregeldeheden.

Die nieuwe bevoegdheden zijn urgent, vindt Bats: „Anders is de andere partij aan tafel – Defensie noemt dat 'de vijand' – degene die met ons op de loop gaat”. Wat te doen als berichten anoniem worden geplaatst, of vanuit het buitenland? Een 'digitaal gebiedsverbod' – waarbij iemand tijdelijk de toegang tot een site of platform wordt ontzegd – wordt wel geopperd, maar wat zijn daarvan de juridische aspecten?

De wens om online preventief in te grijpen staat ook op gespannen voet met het recht op privacy van burgers en de vrijheid van meningsuiting. Ingewikkeld, weet ook Bantema. „Het belangrijkste punt is hier: proportionaliteit. Je kunt niet zomaar allerlei informatie over iemand verzamelen, er moet wel een gegronde reden zijn.”

Bantema en zijn medeonderzoekers verwachten over een half jaar resultaten te kunnen presenteren. Samen met studenten van de Thorbecke Academie, de Open Universiteit en bestuursrechtadvocaten kijken ze vooral naar juridische aspecten.

Het blijft koordanssen, aldus Bantema, met nog wel fundamentele vragen dan alleen over digitale bevoegdheden van burgemeesters. „Je kunt je op basis van alles wat er gebeurt afvragen: het internet zoals we dat ooit hebben bedacht, werkt dat op deze manier nog wel?”

Marga Waanders: 'Voorzichtig met extra bevoegdheden'

„Heel goed dat dit onderzoek plaatsvindt”, zegt Marga Waanders, burgemeester van Waadhoeke. „Maar ik vind wel dat je een beetje moet uitkijken met de roep om extra bevoegdheden.” Ook in haar gemeente leiden de sinterklaasintocht en coronamaatregelen tot uitingen op sociale media. „die we in de gaten houden. En de politie doet dat natuurlijk ook”. In 2017 greep Waanders, toen burgemeester in Dongeradeel, naar het wapen van een noodbevel uit vrees voor ongeregelde heden bij de landelijke intocht van Sinterklaas in Dokkum. Het beste is volgens haar bij online oproepen te proberen in contact te komen met diegene die zo'n oproep plaatst.

Sybrand Buma: 'Brede discussie over aanpak is nodig'

Moet online opruiing aangepakt worden via het bestuursrecht of het strafrecht? Burgemeester Sybrand Buma van Leeuwarden is hier nog niet uit. „Online uitingen kunnen leiden tot (offline) ordeverstoring gedrag. De wijze waarop dit aangepakt zou moeten worden is onderwerp van een brede discussie die niet alleen op

gemeentelijk niveau moet worden gevoerd”, geeft hij aan. Als de politie mogelijke opruiing signaleert kan de burgemeester een noodbevel of noodverordening uitvaardigen. Soms gaan politie en burgemeester ook het gesprek aan, waarbij degene die het bericht online heeft geplaatst een waarschuwing krijgt.

300 euro startbonus moet krantenbezorgers lokken

MELLE VELTMAN

LEEWARDEN Krantenwijkje doen? Steeds minder mensen komen daar nog vroeg hun bed voor uit. Een startbonus van 300 euro moet daar verandering in brengen.

Geen krant op de mat? Binnenkort krijg je dan een mailtje wanneer die wel komt. Dat zegt distributiemanager Ron Kwakman van Mediahuis, uitgever van onder meer de Leeuwarder Courant. Deze en andere maatregelen moeten de klanten over de bezorging terugdringen. Uiteindelijk hebben die vaak maar één oorzaak: er zijn simpelweg te weinig bezorgers.

Hoe nijpend is het probleem? „Alleen al in Friesland, Groningen en Drenthe hebben we in totaal zo'n 250 à 275 'open wijken'. Dat betekent niet dat de krant daar niet bezorgd wordt, maar wel dat er geen vaste bezorger is. Anderen moeten inspringen, waardoor de krant niet altijd voor 7 uur op de mat ligt.”

Verschilt het probleem per verspreidingsgebied? „Nee. Gelukkig niet, zou ik bijna zeggen. Kranten kampen overal met dezelfde problemen. Dat klokt mis-schijnlijk ook, maar stel je voor dat in Limburg wel genoeg bezorgers waren, en in Noord-Nederland niet. Dan doen we pas echt iets fout.”

Waarom is het zo moeilijk om aan bezorgers te komen? „Het is gewoon een moeilijke fase, juist omdat het economisch zo goed gaat. Ongeacht leeftijd, iedereen verdient bij ons hetzelfde: 10,60 euro per uur. Als je 16 bent, verdien je als vakkenvuller een stuk minder. En tóch werken jongeren liever bij de supermarkt.”

Hoe kan dat? „Misschien om het daar warm en droog is, terwijl het buiten sneeuwt en regent. Of misschien omdat ouders tegenwoordig liever wat geld toestoppen, dan dat ze hun kinderen vroeg de wakker laten zetten voor een krantenwijk. Ik kan het niet hard

Op reclames van Bezorgdekrant.nl, de distributiedienst van Mediahuis, zie ik altijd grijze mensen. Hebben jullie de jongeren al opgegeven? „Zeker niet. Maar de groep rond de 40 jaar, daar zit nou eenmaal de nieuwe aanwas. De meeste bezorgers zijn tegenwoordig tussen de 40 en 50 jaar.”

Nog even over de 300 euro. Wat als ik me aanmeld en ik het na twee weken voor gezien heb? „Daar is natuurlijk over nagedacht. De eerste 150 euro krijg je pas na drie maanden bezorgen, de tweede 150 euro pas na zes maanden. En ook

voor de bezorger die al aan de slag is komt er een bonus. Die krijgt 300 euro als hij een nieuwe bezorger weet te tippen.”

In andere regio's van Mediahuis krijgen mensen al bericht als bijvoorbeeld de bezorger ziek is. Welk probleem lost dit op? „Het een vicieuze cirkel. Gaat het slecht met de bezorging, dan staan ook de telefoons bij de klantenservice roodgloeiend. Met een geautomatiseerd systeem willen we de druk op de callcenters verminderen. En klanten hebben er natuurlijk ook de pest over in als ze helemaal niks horen wanneer er geen krant op de mat ligt.”



Hoofdstuk 2

Complexiteit van bestuur en in een digitale samenleving

2.1 Inleiding

In het najaar van 2020 vroeg de Vereniging van Nederlandse Gemeenten (VNG) ons om een verkenning te doen om bestuurlijke digitale veiligheidsuitdagingen in kaart te brengen voor de komende 5-10 jaar. Doel was om zowel bewustzijn alsook het handelingsperspectief van gemeenten te vergroten en bij te dragen aan effectief beleid om de bestuurlijke digitale veiligheidsuitdagingen met vertrouwen tegemoet te treden. In deze verkenning zijn Wouter Stol en ik niet alleen ingegaan op technologische ontwikkelingen maar ook op maatschappelijke ontwikkelingen en andere ontwikkelingen die van invloed zijn op de positie van gemeenten in een digitaliserende samenleving. Deze ontwikkelingen en soorten complexiteit zal ik in dit hoofdstuk beschrijven omdat ze inzicht geven in problemen rond digitalisering. Daarnaast zal ik ook met behulp van onderzoek van Rathenau Instituut ook globaal laten zien wat het internet en sociale media in potentie zo schadelijk maken. Het is goed om daar rekening mee te houden bij de ontwikkeling van beleid en interventies.³⁰

2.2 Inleiding op complexiteit

Enkele bijzondere kenmerken van onze gedigitaliseerde samenleving laten zich verenigen onder de noemer 'complexiteit'.³¹ Wat complex is en wat niet is voortdurend in ontwikkeling. Het is wel duidelijk dat digitalisering voor overheden, politie en ook het lokale bestuur tot ingewikkeldheden leiden waar men mee om moet zien te gaan. De relevantie van 'complexiteit' voor bestuurlijk handelen is dat een complexe omgeving het bestuurlijk handelen

lastiger maakt. Immers, complexiteit bemoeilijkt overzicht en inzicht, en maakt het dus ingewikkelder om doelgericht en effectief op te treden. Belangrijker nog is dat digitale complexiteit alle inwoners van een gemeente aangaat. Als zij hun leefwereld niet meer goed doorzien en overzien, ontstaan nieuwe veiligheidsproblemen, en die komen vroeg of laat op de bestuurlijke agenda.

Een ander aspect van de context waarin gemeenten hun werk verrichten, is dat de digitalisering nieuwe handelingsmogelijkheden biedt. Wat lokale overheden daar kunnen doen komt later aan bod. Voor nu gaat het eerst over de omgeving waarin de gemeente (en geldt ook voor politie) haar werk doet. Burgers en organisaties gebruiken de mogelijkheden die digitalisering biedt en dat vergroot hun handelingsrepertoire, waaronder hun vermogen tot sociale controle en tot sociale beïnvloeding. Dat burgers en organisaties meer mogelijkheden krijgen, is relevant voor de gemeente als bestuursorgaan. Immers, hoe bestuur je een omgeving waarin mensen steeds meer mogelijkheden tot handelen en beïnvloeden krijgen? Daarom wordt ook aandacht besteed aan twee potenties van digitalisering die burgers en organisaties benutten en die hun mogelijkheden vergroten: organisatie- en informatievermogen.

2.3 Technische complexiteit

De complexiteit vanwege digitalisering betreft om te beginnen een technische complexiteit. Mensen kunnen een digitale omgeving nu eenmaal minder eenvoudig doorzien dan bijvoorbeeld een mecha-

nische. Ze zien niet snel hoe digitale dingen werken, deels omdat dit niet fysiek zichtbaar is en deels omdat de software veel mogelijkheden kent. Mensen zien dus ook niet eenvoudig of hun omgeving wel of niet goed is beveiligd en wat daaraan valt te doen. Ze zijn wat beveiliging betreft dan ook eenvoudig om de tuin te leiden, of ze maken fouten. Dat mensen niet goed weten hoe digitaal aangestuurde gebruiksvoorwerpen precies werken, begint al bij het maken van de software, waarin stevast fouten zitten omdat ook programmeurs het geheel niet kunnen overzien. Kortom, door de digitalisering is de omgeving van mensen in technisch opzicht complexer geworden en dat maakt het voor hen moeilijker om veiligheidsproblemen op te merken en er wat aan te doen. Dit heeft invloed op de kennis die vereist is voor het uitvoeren voor bepaalde werkzaamheden maar gaat over het gedrag van medewerkers.

2.4 Netwerkcomplexiteit

Omdat digitale apparaten onderling zijn verbonden, ontstaan door de digitalisering omvangrijke netwerken, zowel tussen mensen (Internet of Men), tussen dingen (Internet of Things) als tussen mensen en dingen (Internet of Everything). Niet alleen onze klassieke desktopcomputers en telefoons zijn verbonden in een netwerk, maar ook kinderspeelgoed, auto's, grasmaaiers, horloges, implantaten en industriële machines. Niemand kan alle verbindingen nog overzien of vaststellen tot hoever ze reiken. Een zwakte op de ene plek kan resulteren in een beveiligingsprobleem op een andere plek. Communicatie, inclusief oproepen tot rellen en nepnieuws, loopt langs diverse en soms onnavolgbare digitale routes. Bovendien doorkruisen vraagstukken

van digitale veiligheid daardoor bestuurlijke jurisdicties, zodat niet altijd helder is wie waarvoor verantwoordelijkheid draagt of wie bevoegd is. Daarnaast zijn er, vanwege de netwerken, bij een veiligheidsvraagstuk direct veel publieke en private partijen betrokken waardoor het eenduidig toekennen van verantwoordelijkheid lastig is. Mensen leven dus vanwege de digitalisering in een wereld waarin zij niet weten hoe de dingen die zij gebruiken precies werken (technische complexiteit) en niet weten hoe en hoever die dingen met elkaar in verbinding staan (netwerkcomplexiteit). Daardoor weten ze niet hoe goed (of juist slecht) al die dingen en verbindingen zijn beveiligd. Omdat mensen hun gedigitaliseerde omgeving noch doorzien noch overzien, kunnen zij eenvoudig fouten maken die de beveiliging van dingen geweld aan doet, ook zonder dat zij dat merken. Mensen kunnen om dezelfde reden met een smoes tot dergelijke fouten worden verleid. Ook kunnen mensen die complexiteit bewust gebruiken om overheidstoezicht te bemoeilijken.

2.5 Echtheidscomplexiteit

In de onlinewereld kunnen we niet eenvoudig vaststellen wie is dan wel wat echt is of nep. 'Offline hebben we bijvoorbeeld identificatiepapieren met echtheidskenmerken, geld met echtheidskenmerken en gebouwen met echtheidskenmerken'.³² Online is dat niet op vergelijkbare wijze ontwikkeld. Offline kunnen we mensen herkennen, online kan je geregeld niet zien met wie je in contact staat. 'Het probleem is fundamenteel, want het gaat om de vraag hoe van twee identiek lijkende dingen kan worden bepaald welke echt is en welke niet.' (ibidem). Burgers hebben last van echtheidscomplexiteit bij bijvoorbeeld online

³⁰ Dit hoofdstuk is sterk gebaseerd op onderzoek van Stol & Bantema (Stol, W. & Bantema, W. (2021). *Lokaal bestuur in een digitaliserende samenleving. Essay over een stap in de ontwikkeling: een handelingskader*. Onderzoeksgroep Cybersafety).

³¹ Stol, W.Ph. (2020). Digitalisering en criminaliteit. Een beknopte inleiding op cybercrime. In C. de Poot, E. Lievens, W. Stol & L. De Kimpe (red.) (2020) *Cahier Politiestudies*, jaargang 2020/3, themanummer Politie en Cybercrime, pp. 13-22.

³² Jansen, J., S. Westers, S. Twickler en W. Stol (2019). *Aankoopfraude vanuit het buitenland. Alternatieven voor opsporing*. Den Haag: Sdu Uitgevers (reeks Politiekunde, nr. 99).

aankopen of online nieuwsberichten. De overheid moet omgaan met echtheidscomplexiteit bij opsporing en ordehandhaving. Door ontwikkelingen in kunstmatige intelligentie, denk aan Chat GPT, is het ook gemakkelijk om het behulp van technologie snel op informatie te zoeken en samen te vatten in nieuwe producten. Dit gaat niet alleen over de creatie van tekst maar ook nieuwe afbeeldingen kunnen ermee gemaakt worden. Ook hier geldt weer dat het moeilijk is vast te stellen of iets door een mens of door een computer is gemaakt en of het echt is of nep. Onderzoekers van de TU Tilburg verwachten dat tussen nu en 4-5 jaar ongeveer 90% van alle online content gemanipuleerd is.³³ Dit gegeven is weinig hoopvol en stelt ons voor veel uitdagingen op dit terrein.

2.6 Cyborgcomplexiteit

We wezen bij netwerkcomplexiteit al op de verbinding tussen apparaten en mensen. Dat gaat niet alleen om 'in verbinding staan' want ook is sprake van een fysieke vervlechting tussen technologie en menselijk lichaam ofwel cyborgcomplexiteit.³⁴ Zo'n 23 jaar geleden, op 24 augustus 1998, werd Kevin Warwick, wetenschapper op het gebied van mens-machine interactie van de University of Reading (UK), de eerste mens met een RFID-implantaat.³⁵ Hoorapparaten, geisha balls en pacemakers

zijn inmiddels digitaal aangestuurd. Vandaag de dag werken wetenschappers aan 'neuroprotheses': geïmplanteerde en aan de hersenen verbonden chips die het de drager mogelijk maken om met hersensignalen een computer³⁶ of een handprothese³⁷ aan te sturen. Er zijn inmiddels zelfs meerdere mensen die een chip onder hun huid hebben om contactloos te kunnen betalen.³⁸ Technologie dringt zo steeds vaker en verder het menselijk lichaam binnen.

Een andere variant van de verdergaande mens-computer integratie is de mens die zich als avatar³⁹ in de digitale wereld manifesteert. De Amerikaanse journalist Julian Dibbell beschreef in 1993, voor zover bekend voor het eerst, een virtuele aanranding.⁴⁰ Seksueel misbruik van avatars is nog steeds actueel. Op 3 juli 2018 bericht de BBC dat 'A US mum has written a Facebook post describing her shock at seeing her child's avatar being "gang raped" by others in the online game Roblox. Amber Petersen said her seven-year-old was playing the game, which is marketed at children, when she showed her the screen and asked what was happening. She also shared screenshots, which showed two male avatars attacking her daughter's female character.'⁴¹ Zoiets verhoudt zich moeizaam tot het huidige maatschappelijke klimaat inzake man-vrouw verhoudingen en

kan dus gemakkelijk aanleiding zijn tot maatschappelijke onrust en een roep om overheidsoptreden. Dit is minder vreemd dan het misschien lijkt: het Cybercrimeverdrag⁴² stelde al twintig jaar geleden virtuele kinderporno strafbaar om te voorkomen dat een sfeer ontstaat waarin seks met kinderen normaal is.⁴³ Als de Metaverse werkelijkheid wordt zullen ons nog veel meer van dit soort voorbeelden boven het hoofd hangen (meer hierover in hoofdstuk 4).

2.7 Ontwikkeling in complexiteit – een weging

Onze samenleving wordt nog immer complexer. De complexiteit van werktuigen en netwerken neemt al eeuwen toe.⁴⁴ Er is geen reden te veronderstellen dat deze ontwikkeling binnenkort stopt. Echtheidscomplexiteit neem voorlopig ook toe, getuige bijvoorbeeld ontwikkelingen in 'deepfake', een fenomeen waarbij getrukte video's van mensen en situaties dermate echt lijken dat we ze niet van echt kunnen onderscheiden. Cyborgcomplexiteit is een relatief nieuw fenomeen en te voorzien is dat ook dit de komende jaren zal toenemen, getuige de ontwikkelingen in neuroprotheses en toepassingen van virtual reality.

De vier dimensies van complexiteit staan uiteraard niet los van elkaar. Het zijn dimensies van één en dezelfde maatschappelijke ontwikkeling en als zodanig wel te onderscheiden maar niet te scheiden. Van deze vier dimensies mag echtheidscomplexiteit de meeste zorgen baren want zonder idee van wat echt of nep is, waar of onwaar, verliezen mensen hun oriëntatie en houvast. Politiek relevante en relatief nieuwe dimensies van echtheidscomplexiteit zijn verschijnselen als desinformatie, trollaccounts (en inzet algoritmes via social bots) en beïnvloeding van verkiezingen. Als we niet meer kunnen weten wat echt en waar is, hebben we ook niets meer in handen wat ons kan helpen omgaan met de andere complexiteitsdimensies. Daarom zal dit aspect aandacht genieten bij het onderzoek en onderwijs van de onderzoeksgroep cybersafety en specifiek binnen dit lectoraat.

2.8 Organisatievermogen

Digitale hulpmiddelen verschaffen burgers de mogelijkheid om zich eenvoudig te organiseren. Zij maken daarvan volop gebruik en dat heeft effect op openbare orde en veiligheid. Voor gemeenten is het bekendste voorbeeld vermoedelijk 'project X' in 2012, waarbij jongeren zich na oproepen op Facebook verzamelden in Haren voor een 'feest' dat eindigde in rellen met de Mobiele Eenheid en het aftreden van de burgemeester. Maar het verschijnsel is ouder. In 1997 organiseerden hooligans per SMS een vechtpartij in een weiland bij Beverwijk, waarbij een dode viel. Vandaag de dag speelt digitale

³³ <https://www.tilburguniversity.edu/nl/actueel/persberichten/deepfakes-kunnen-op-termijn-de-samenleving-ontwrichten>
³⁴ Stol, W.Ph. (2020). Digitalisering en criminaliteit. Een beknopte inleiding op cybercrime. In C. de Poot, E. Lievens, W. Stol & L. De Kimpe (red.) (2020) *Cahier Politiestudies*, jaargang 2020/3, themanummer Politie en Cybercrime, pp. 13-22.
³⁵ <http://edition.cnn.com/TECH/computing/9901/14/chipman.idg/>, geraadpleegd 30 april 2020.
³⁶ <https://www.umcutrecht.nl/nieuws/met-je-hersenen-een-apparaat-bedienen>, geraadpleegd 30 april 2020.
³⁷ NRC Next, 1 mei 2020, katern Wetenschap, p. E10.
³⁸ <https://techfi.nl/walletmor-contactloos-betalen-met-implantaat>
³⁹ Een digitaal verbeelde representatie van het menselijk lichaam.
⁴⁰ Zie ook Stol & Strikwerda (2017), paragraaf 2.4.2.
⁴¹ <https://www.bbc.com/news/technology-44697788>, 3 juli 2018, geraadpleegd 12 mei 2020.

⁴² Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001.
⁴³ Verbonden aan deze problematiek is de vraag of robots mensenrechten hebben.
⁴⁴ Bijvoorbeeld: Smith, A., (1987, oorspr. 1776). *The wealth of nations*. Harmondsworth: Penguin Books; Elias, N. (1984, oorspr. 1939). *Het civilisatieproces*. Utrecht/Antwerpen: Het Spectrum; Pieterse, M. (1981). *Het technisch labrynth*. Meppel: Boom.

communicatie een rol bij veel, zo niet alle openbare-ordevraagstukken. Als 'Beverwijk' wordt beschouwd als illustratie van digitaal organisatievermogen, is deze ontwikkeling dus al 26 jaar zichtbaar. Wie anno 2023 verrast is, heeft niet opgelet. Na de lange aanloop waarin het fenomeen is gegroeid, zijn online aangejaagde ordeverstoringen tegenwoordig geen bijzonderheid meer. Eerder lijken nu ordeverstoringen die niet online worden aangejaagd de uitzondering. Het is goed om te beseffen dat de fenomenen in Coronatijd een heel ander karakter hebben dan voorbeelden zoals Project X in Haren.

Eén van die verschillen is de toename van interactie tussen online en offline, zo wordt er ook tijdens rellen gefilmd (live) en opnieuw gedeeld waardoor er weer nieuwe spanningen ontstaan.⁴⁵

Mensen gebruiken de digitale mogelijkheden niet enkel om rellen te organiseren maar óók om bij te dragen aan openbare orde en veiligheid. Whatsapp-buurtpreventiegroepen zijn sinds de start van WhatsApp BuurtPreventie (WABP) op 1 juni 2015 een veelvoorkomend verschijnsel.⁴⁶ De familie van de vermiste Anne Faber organiseerden in 2019 zelf de zoektocht naar hun Anne. Dat was meer dan de politie deed en die heeft daar vervolgens haar voordeel mee kunnen doen.⁴⁷

Ook burgerinitiatieven hebben een grens in recht en ethiek. Online-pedojaagster Yvonne van H. ging met haar acties over de schreef en werd in 2009 veroordeeld wegens smaadschrift. Politiechef Oscar Dros meldt in 2020 dat de politie geen behoefte heeft aan de 'hulp' van pedojagers want zij "plegen strafbare feiten en er ontstaan gevaarlijke situaties".⁴⁸ In 2015 constateerde een journalist dat wat in Aalburg begon als Whatsapp-buurtpreventie, al snel was ontaard in een „heksenjacht op mensen met een Oost-Europees uiterlijk.”⁴⁹ In 2023 trok kinderboekenschrijver Pim Lammers zich terug als schrijver van het gedicht van de kinderboekenweek nadat hij op sociale media ervan werd beticht een pedofilieactivist te zijn. Hij kreeg als gevolg hiervan te maken met serieuze bedreigingen.⁵⁰ Onderzoeker Arnout de Vries ontwikkelde een handreiking voor burgerparticipatie die bijdraagt aan het schetsen van grenzen en mogelijkheden bij het betrekken van burgers.⁵¹

De essentie van bovenstaande is dat burgers zich door de digitale mogelijkheden eenvoudig kunnen organiseren, óók in relatie tot openbare orde en veiligheid. Ze dagen die uit of leveren daaraan naar eigen inzicht een bijdrage. In beide gevallen heeft de lokale overheid een rol. Ofwel ze moet reageren op de verstoringen die de digitaal georganiseerde

burgers teweegbrengen, ofwel ze moet toetsen hoe de digitaal georganiseerde en op rechtshandhaving gerichte activiteiten zich verhouden tot de grondbeginselen van de rechtsstaat. Stol pleit in dit verband voor de politie als 'autoriteit fatsoenlijke rechtshandhaving'.⁵² Daar kan aan toegevoegd worden dat de burgemeester het gezag voert over de ordehandhaving in een digitaliserende samenleving en is dus aan te spreken op het fatsoen ervan.

2.9 Informatievermogen

Losse individuen kunnen zich dus vanwege de digitalisering gemakkelijk en snel organiseren. Hun organisatiegraad is niettemin beperkt als we die vergelijken met bijvoorbeeld een fabriek, een overheidsorganisatie, een grootgrutter of een verzekeraar. Aan dergelijke gevestigde organisaties voegt de digitalisering ook nog wel organisatievermogen toe (werknemers gebruiken ook whatsapp) maar zij zijn daarvan geenszins afhankelijk. Aan gevestigde organisaties biedt de digitalisering vooral *informatie*-vermogen. Bijvoorbeeld banken, verzekeraars, autofabrikanten, grootgrutters en telecombedrijven hebben als nevenproduct een schat aan informatie over hun klanten, meer dan overheidsorganisaties. Van oudsher was de overheid de organisatie met informatie over burgers. De digitalisering heeft dat veranderd. Nu zijn dat vooral particuliere bedrijven. Bij uitstek denken we hier aan techreuzen die informatievermogen als verdienmodel hebben, zoals Google, Facebook, Microsoft, Apple en Amazon, en in Nederland ook Bol.com, maar daarnaast zijn er tal

van kleinere bedrijven die goede zaken doen dankzij hun nieuw verworven informatievermogen.

Individueen die zich eenmaal hebben georganiseerd kunnen zich daarna dankzij de digitalisering een informatievermogen verwerven. Er zijn gevallen waarin individuen zich met digitale middelen organiseren juist met het oog op informatievermogen. De met digitale middelen opgezette organisatie van de familie van Anne Faber was bijvoorbeeld gericht op het vergaren van informatie over Anne. Whatsapp preventiegroepen zijn ook gericht op informatievergaring. Zodra zo'n particulier initiatief een permanent karakter krijgt, gaat ze lijken op een gevestigde organisatie met informatievermogen als hoofdactiviteit, zoals het Meldpunt Kinderporno op internet. Maar ook valt te denken aan het internationale journalistieke onderzoeksplatform Bellingcat en het platform voor publicatie van gelekte informatie Wikileaks.⁵³

2.10 Kenmerken van het internet en relevantie voor beleid

Ondanks dat dit lectoraat zich niet alleen richt op digitale veiligheid en de rol van het internet kunnen we niet heen om de invloed van het internet en sociale media op de openbare orde en veiligheid. Er zijn verschillende soorten online onveiligheid te onderscheiden⁵⁴ en veel van de online onveiligheid bestonden ook al in het jaar nul. Anders gezegd, veel bronnen van onveiligheid zijn al zo oud als de mensheid maar door kenmerken van het internet zijn de effecten anders geworden en leidt het

⁴⁵ H. Moors e.a., *Avondklokrellen, lokale dynamiek in een mondiale crisis*. Emma 2022.

⁴⁶ <https://www.wabp.nl/wat-is-wabp-whatsapp-buurtpreventie/#:~:text=WABP%20staat%20voor%20WhatsApp%20BuurtPreventie,2017%20geregistreerd%20als%20Stichting%20WABP.&text=Een%20WABP%20groep%20is%20een,alarmerende%20situaties%20in%20de%20buurt,geraadpleegd%2017%20maart%202021>.

⁴⁷ Lam, J. en N.Kop (2020) *Schouder aan schouder: Burger- en politieparticipatie tijdens de vermissing van Anne Faber. Leerpunten uit de samenwerking tussen burgers en politie*. Apeldoorn: Politieacademie.

⁴⁸ <https://www.gelderlander.nl/binnenland/politie-over-pedojagers-dit-zijn-geen-helden-we-zijn-er-klaar-mee-a9664741/>, geraadpleegd 17 maart 2021.

⁴⁹ Reformatorisch Dagblad, 1 oktober 2015, op 17 maart 2021 geraadpleegd op <https://www.rd.nl/artikel/632741-aalburg-hoopt-op-doorstart-wakende-whatsapp-groepen>. Zie ook: <https://youtu.be/z31C8RhTadE>.

⁵⁰ <https://nos.nl/artikel/2463219-boekenwereld-steunt-pim-lammers-met-paginagrote-advertentie-in-kranten>

⁵¹ <https://www.tno.nl/nl/newsroom/2022/11/handboek-hulp-opsporing/>

⁵² Stol, W.Ph. (2021) Digitalisering en de rol van de politie. Naar een 'autoriteit fatsoenlijke rechtshandhaving'. *Panopticon*, vol. 42 nr. 2, pp. 161-168.

⁵³ Voor meer informatie en duiding over informatievermogen en organisatievermogen, zie Stol en Bantema, (2021).

⁵⁴ M, Huijstee, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen, *Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland*. Den Haag: Rathenau Instituut 2021.

tot nieuwe vraagstukken voor de veiligheid en in bredere zin ook voor bijvoorbeeld het functioneren van de democratie. Het Rathenau Instituut maakte een onderscheid in zes soorten kenmerken van het internet waar men kennis van kan nemen en die overwogen kunnen worden bij het nadenken over beleid en interventies die gericht zijn op gedrag op het internet en of sociale media. Dit zijn: alledaagsheid, verbindingen en netwerken, groeicapaciteit en bestendinging, escalatie, virtuele realiteit en wanorde. Ik zal ook laten zien dat deze categorieën deels overkomen met het onderscheid in complexiteit en de gevolgen van digitalisering voor de relatie tussen burgers en overheden (organisatievermogen en informatievermogen). Naar aanleiding van het onderzoek 'Online Ontspoord' noemen we enkele kenmerken van het internet die bijdragen aan de onveiligheid aldaar.

Alledaagsheid. Het internet is altijd en overal beschikbaar en informatie is gemakkelijk openbaar te maken. Dat geldt ook voor burgers of inwoners die overal smartphones bij zich hebben en binnen een hele korte tijd kunnen heel veel mensen kennis nemen van de informatie die wordt gedeeld. Er wordt ook gesproken van onmiddellijkheid, dat online interacties direct effect hebben. Wat lastig is voor autoriteiten is dat er geen pauze knop op het internet of sociale media zit, het internet gaat altijd door. Denk bijvoorbeeld aan jongerenwerk in een online omgeving – wie houdt er toezicht tussen bijvoorbeeld 18 uur en 8 uur in de ochtend? Het is moeilijk om het zo te organiseren dat er 24 uur toezicht is.

Verbindingen en netwerken. Dit is een interessant en overduidelijk kenmerken van het internet. Allereerst is het heel gemakkelijk om mensen rechtstreeks te bereiken. Dit kan gebruikt worden voor sociale contacten maar uiteraard ook gebruikt worden om

mensen te beschadigen. Interessanter is het concept 'syndicatie' waarbij het gemakkelijk is om via het internet gelijkgestemden te vinden. Waar in elk dorp wordt gesproken over 'dorpsgekken' kunnen deze inwoners met afwijkende meningen of gedrag zich online snel en gemakkelijk organiseren in relatief grote groepen, ze zijn niet langer geïsoleerd. Tot slot komt ook het concept 'echo chambers' naar voren in deze context. Dit concept gaat over de gedachte dat mensen vooral in contact komen met mensen met dezelfde gedachten en ideeën en dat dit hun wereldbeeld of gedachten nog verder bevestigd (conformation bias). Er is discussie over groot het effect van het internet is om deze 'echo chambers' maar de gedachte is dat met name door algoritmes mensen eenzijdig nieuws (filterbubbel) of informatie krijgen en dus in zeker zin zijn afscheiden van mensen met andere interesses en denkbeelden. Intussen zijn er ook onderzoeken die dit beeld enigszins nuanceren.

Groeicapaciteit en bestendinging. Het internet is zo ingericht dat het snel kan groeien en met name dat de verspreiding van informatie kan plaatsvinden zonder te veel barrières (viraliteit). Dit aspect speelt een belangrijke rol bij de zogenaamde 'online aangejaagde orderverstoringen' waar we later nog aandacht aan zullen besteden. Daarnaast is informatie makkelijk te kopiëren en moeilijk te verwijderen (persistentie en onbeheersbaarheid). Men zegt dan ook wel eens, het internet vergeet niet.

Escalatie. Een aspect dat hier onder valt betreft het filteren en uitvergrooten van informatie door zoekmachines (selectie en amplificatie). Dit hangt samen met het eerder beschreven aspect van filterbubbels en echokamers. Tot slot hangt de 'aandachtseconomie' hier ook nog mee samen, platformen zijn ontworpen met het oog op het maximaliseren van

aandacht. Dit aspect maakt ook een belangrijk onderdeel uit van de zogenaamde 'online aangejaagde ordeverstoringen'.

Virtuele realiteit. Zoals eerder al beschreven lijken veel dingen 'minder echt' online, dit kan het makkelijker maken om schadelijk gedrag te vertonen. Het internet heeft daarbij ook nog eens een entertainment functie, schadelijk gedrag kan ook vermaak zijn. Zoals eerder aangeven is het ook nog eens moeilijker om in te schatten wat echt is en wat nep.

Wanorde. Wat mij betreft de meest interessante categorie is wanorde. Dit gaat onder andere over onduidelijke normen, als samenleving zijn er geen duidelijke afspraken over wat wel en niet mag op internet (buiten het strafrecht). Dit kan verder verergerd worden door de wetteloosheid die er speelt, met name door internationalisering en het internationale karakter van het internet is het moeilijk om te achterhalen wie ergens achter zit. Naast dat 'daders' in het buitenland kunnen zitten is ook de anonimiteit van het internet een onderdeel van het probleem. Dit maakt dat mensen zich in een online omgeving vrij voelen en doen wat ze willen. De anonimiteit bemoeilijkt ook de handhaving van zogenaamde 'online gebiedsverboden'. In hoofdstuk 4 zullen we daar aandacht aan besteden.

2.11 Een opmaat naar vijf relevante hoofdlijnen
Op basis van de beschreven complexiteiten, maatschappelijke ontwikkelingen en kenmerken van het internet is duidelijk geworden dat technologie en digitalisering in potentie een grote invloed kunnen hebben op de maatschappij en op bestuur in een digitale samenleving. Op basis van deze kenmerken (en scenario's die zijn voorgelegd aan medewerkers uit het openbaar bestuur en wetenschappers zijn) globaal 5 kernvragen te onderscheiden die volgens ons lectoraat aandacht behoeven en relevant zijn voor een goed en effectief bestuur in een digitaliserende samenleving.⁵⁵ Daarover gaat het volgende hoofdstuk.

⁵⁵ Een bewerkte versie van - Stol, W. & Bantema, W. (2021). *Lokaal bestuur in een digitaliserende samenleving. Essay over een stap in de ontwikkeling: een handelingskader*. Onderzoeksgroep Cybersafety.



Hoofdstuk 3

Kernvragen voor effectief en goed bestuur in een digitali- serende samenleving

3.1 Inleiding op de kernvragen

Op basis van de vastgestelde complexiteit en maatschappelijke ontwikkelingen rondom bestuur en digitalisering (en na uitwerking van verschillende scenario's) zijn er vijf hoofdlijnen naar voren gekomen die gezien kunnen worden als globale kernvragen of kernaspecten die uitgedacht en uitgevoerd moeten worden om effectief en goed bestuur te realiseren op het gebied van digitale veiligheid en of veiligheid in het algemeen. Deze zijn oorspronkelijk uitgewerkt voor gemeenten maar zijn ook grotendeels toepasbaar op de overheid in bredere zin en bijvoorbeeld ook voor politiewerk of politiebeleid in een digitale samenleving. Er kwamen vraagstukken naar voren rond kennispositie, bevoegdheden, monitoren, samenwerken en ethiek.

Als gemeenten stappen willen zitten op het gebied van goed en effectief bestuur in een digitale samenleving kunnen zijn hun handelend vermogen vergroten door aan die vijf kernvragen aandacht te besteden. Uiteraard zijn er dwarsverbanden tussen deze vijf, maar we benoemen ze afzonderlijk omwille van de overzichtelijkheid. Eén dwarsverband verdient te worden benadrukt: ethiek speelt op elk van de andere vier aandachtsgebieden een richtinggevende rol en ethiek moeten we dan ook zien als een hoofdlijn die de andere vier doorsnijdt. In ons lectoraat zal ethiek de komende jaren een belangrijk rol spelen. De kernvragen die ik hier ga beschrijven zijn eerder gebruikt als startpunt voor een gemeentelijk handelingskader – om gemeenten te helpen bij het vergroten van hun vermogen om effectief te

handelen in een digitale samenleving.⁵⁶ Deze hoofdlijnen staan voor mij ook voor het op een thema-onafhankelijke manier naar relevante vraagstukken te kunnen kijken. Het geeft zich op essentiële randvoorwaarden waar ons lectoraat de komende met onderzoek en onderwijs kan ondersteunen om bij te dragen aan effectief en goed bestuur in een digitaliserende samenleving.

3.2 Ethiek omarmen

De overheid heeft wellicht als belangrijkste taak om, namens de samenleving als geheel, te waken over gemeenschappelijke waarden en normen. Dat is geen sluitpost maar een vertrekpunt, niet enkel wanneer het aardig uitkomt maar bij elk onderwerp. Het gaat dan om te beginnen om welke waarden en normen we als samenleving gehandhaafd willen zien. Direct daarmee verbonden zijn waarden en normen over de handhaving zelf. In het strafrecht spreken we van materieel en formeel strafrecht. Uiteindelijk zijn de waarden en normen aangaande de inhoud (wat mag wel en wat niet) minder belangrijk dan de waarden en normen aangaande het handhaven (hoe gaan we als samenleving om met schendingen van waarden en normen). 'De politie is er niet om boeven te vangen' stelde politiepsycholoog Frans Denkers al enkele decennia geleden, en liet dat direct volgen door 'de politie is er om *fatsoenlijk* boeven te vangen'. In het verlengde daarvan kunnen we de rol van de politie in een digitale samenleving omschrijven als 'autoriteit fatsoenlijke rechtshandhaving'.⁵⁷ Voor gemeenten ligt dat niet anders. Daarom zou de gemeente pleiten daarom

voor de gemeente gezien kunnen worden als een 'autoriteit fatsoenlijke bestuurlijke handhaving'. Dat is geen eenvoudige opgave, want een slager dient niet zijn eigen vlees te keuren. Een integere slager kan niettemin vooroplopen in het debat over kwaliteit en in maatregelen om die te verbeteren.

Allereerst dient het lokale bestuur te waken over de waarden en normen in haar eigen bestuurlijke handhaving. Er wordt in dit verband ook wel gesproken van publieke waarden – waarden die een afspiegeling van wat in de samenleving als belangrijke waarden voor beschouwd en die kunnen helpen op richting te geven aan beleid en besluitvorming door de overheid.

Samengevat is bij ethiek de centrale vraag 'wat voor een gemeente willen we zijn?'. Welk waarden en normen vertegenwoordigen wij en geven dus richting aan ons concrete handelen? Dit aspect van overheidshandelen zal de komende jaren veel aandacht krijgen van ons lectoraat. We zien dat het perspectief van de burger ontbreekt in veel discussies en denken dat door deze perspectieven te betrekken en via 'goed bestuur' in en digitale samenleving de zogenaamde kloof tussen bestuur en samenleving wat gedicht kan worden. Dit gaat zowel over het burgerperspectief alsook over het maatschappelijke perspectief.

3.3 Kennispositie versterken

Digitalisering vergroot het organisatie- en informatievermogen van burgers en hun belangen- en actiegroepen. Dit versterkt hun positie. Kennis is macht. Wanneer gemeenten daarop niet reageren, neemt de kans toe dat burgers en actiegroepen in debatten over lokale besluiten en lokaal beleid, de gemeente in kennispositie overklassen. Het toegenomen organisatie- en informatievermogen stuwt zo gezien de kwaliteit van gemeentelijke besluitvorming op. In die context is een keer bakzeil moeten halen geen schande, maar als een gemeente te vaak in moeizame debatten verzeild raakt, op besluiten moet terugkomen of wordt teruggefloten, ondergraft dat haar slagvaardigheid en geloofwaardigheid.

Overheden kunnen hier op reageren door (a) te trachten hun eigen kennisinfrastructuur en -vaardigheden te verstevigen en (b) te trachten aan te sluiten bij de nieuwe vermogens in hun omgeving. Het eerste vraagt het ontwikkelen van het vermogen om, op wat voor terrein ook, snel een gedegen kennispositie op te bouwen. Het tweede vraagt relatiemanagement en samenwerkingsvaardigheden om burgerparticipatie (of zo men wil: gemeente-participatie) te optimaliseren.

Het eerste is een expertmodel en het tweede is een participatiemodel. Een gemeente kan voor bepaalde onderwerpen kiezen voor het ene model en voor andere onderwerpen voor het andere. In beide modellen werkt de gemeente samen met anderen. In het expertmodel ligt samenwerking voor de hand met deskundigen van andere kennisinstellingen, overheidsinstellingen of van bedrijven, steeds lokaal, nationaal en internationaal. In het participatiemodel ligt allereerst samenwerking voor de hand met lokale belanghebbenden, en kan daarna als coalitie

⁵⁶ Stol, W. & Bantema, W. (2021). *Lokaal bestuur in een digitaliserende samenleving. Essay over een stap in de ontwikkeling: een handelingskader*. Onderzoeksgroep Cybersafety.

⁵⁷ Stol, W.Ph. (2021) Digitalisering en de rol van de politie. Naar een 'autoriteit fatsoenlijke rechtshandhaving'. *Panopticon*, vol. 42 nr. 2, pp. 161-168.

worden samengewerkt met deskundigen van kennisinstellingen, et cetera. Het risico van het expertmodel is dat het in wezen competitief is en er dus partijen kunnen opstaan die de kennis-concurrentie aangaan. Het risico van het participatiemodel is dat slagkracht of snelheid verloren gaat.

Het toetsen van de digitale veiligheid van evenementen bijvoorbeeld, leent zich goed voor het expertmodel. Kwesties die de inrichting of het gebruik van de openbare ruimte aangaan, alsook digitale weerbaarheid en het gebruik van slimme technologie in de stad (smart cities), lenen zich daarentegen beter voor een participatief model. Gemeentelijk bestuur in Nederland is 'dichtbijbestuur' en een participatieve kennisstrategie sluit daarop goed aan, hoewel er altijd een situatie kan zijn of ontstaan waarin een gezamenlijke kennisstrategie niet of niet meer vruchtbaar is. Dat doet zich voor wanneer geen overeenstemming bestaat over de grondslag van kennis (bv. wetenschap als kennissysteem) én het doet zich voor wanneer binnen een gedeeld kennissysteem geen overeenstemming bestaat over een meetmethode of een grenswaarde. Indien gemeente en burgers verschillende kennissystemen hanteren (bv. wetenschap versus geloof in een complottheorie) rest al gauw slechts nog een competitief of zo men wil een 'meerstemmig kennismodel', inclusief de kwalificatie desinformatie. De digitalisering dwingt gemeenten als het ware tot een expliciete kennisstrategie. Hier komen vier onderdelen aan bod, in willekeurige volgorde.

Het eerste onderdeel is het ontwikkelen en vaststellen van uitgangspunten en uitvoeringsplannen voor participatief veiligheidsbeleid. Daarbij wordt uitgewerkt in welke gevallen en hoe het door de digitalisering ontwikkelde organisatie- en informatievermogen van burgers en bedrijven wordt aangesproken en ingezet, en zo nodig gestimuleerd. Waar de gemeente kiest voor het expertmodel, is er de keuze tussen expertise in eigen huis of via samenwerking met anderen.

Het tweede onderdeel van de kennisstrategie in relatie tot digitalisering betreft de digitale weerbaarheid van personen en organisaties in de gemeente. Hier gaat het om het mobiliseren van kennis en om het organiseren van kennistoepassing. Het concept 'regierol' wordt hierbij uitgewerkt in actieplannen. Dit tweede onderdeel bouwt voort op het eerste omdat het ook bij een regierol draait om het aanspreken, inzetten en zo nodig stimuleren van capaciteiten van burgers en organisaties binnen de gemeente. Dit is een belangrijk onderdeel en zal vooral aandacht krijgen vanuit collega's van het lectoraat 'digitale weerbaarheid van mens en organisatie'.

Het derde onderdeel is het vaststellen hoe praktisch om te gaan met discussies die worden gevoerd vanuit verschillende kennisgrondslagen. De gemeente dient te bepalen hoe zij omgaat met waarheden en feiten die zijn gebaseerd op een kennisgrondslag die zij zelf niet hanteert of die zij zelfs expliciet afwijst. Zij geeft beargumenteerd aan welke positie zij inneemt tegenover 'desinformatie' en 'deepfake', of zij daarop intervenieert en zo ja, hoe. Hierbij dient onderscheid gemaakt te worden tussen 'fakeberichten' in het publieke debat en 'fakeberichten' die de rechtsstaat of het openbaar bestuur raken. Dat dit een spannend

vraagstuk is blijkt onder andere uit recent nieuws rondom de aanpak van desinformatie door de overheid tijdens de Corona-epidemie.⁵⁸

Het vierde onderdeel van een gemeentelijke kennisstrategie in relatie tot digitalisering, is een evaluatiestrategie, met het oog op een PDCA-cyclus. Van de eerdere onderdelen is dan steeds de vraag of de aanpak leidt tot het gewenste maatschappelijke resultaat. Dat kan gebaseerd zijn op interne evaluaties, maar bijvoorbeeld ook gebaseerd zijn op onderzoek naar effectiviteit van een specifieke aanpak. In de Citydeal 'Lokale Weerbaarheid Cybercrime' worden bijvoorbeeld enkele projecten op het gebied van cyberweerbaarheid wetenschappelijk onderzocht op hun effectiviteit. Als onderzoeksgroep, waaronder het lectoraat 'Bestuur in een Digitaliserende Samenleving' zijn we hierbij betrokken. Ook breder dan cyberweerbaarheid kan beleid en kunnen bestuurlijke maatregelen en werkwijzen om veiligheid te vergroten onderzocht worden op hun effectiviteit. Een behulpzaam instrument in de communicatie betreft een handreiking door BZK over hoe bestuurders kunnen omgaan met desinformatie en onder andere hoe je beter wel of niet kunt reageren.⁵⁹ Er is nog veel meer onderzoek nodig naar effectieve online communicatie, ons lectoraat zal daar ook waar mogelijk een bijdrage aan leveren. Gezien de juridische complexiteit bij de bestuursrechtelijke aanpak (onder andere anonimiteit van daders en grondrechten) en de kosten die met die aanpak gepaard zijn is dit waarschijnlijk de meest vruchtbare en effectieve route op de langere termijn.

⁵⁸ <https://www.nrc.nl/nieuws/2023/04/25/desinformatie-over-vaccins-werd-gewist-maar-wie-besloot-wat-a4163066>
⁵⁹ <https://open.overheid.nl/documenten/ronl-68101d81f62e93a6467511bcfe165e91ce9da39b/pdf>

3.4 Bevoegdheden inzetten

Geen verantwoordelijkheid zonder bevoegdheid. Daar gemeenten een verantwoordelijkheid hebben (en voelen) voor veiligheid en openbare orde in een digitale context, dienen ze te beschikken over bevoegdheden waarmee ze die verantwoordelijkheid daadwerkelijk kunnen nemen, waarna ze daarover verantwoording afleggen. Dat veel kan worden geregeld in goed overleg, dus zonder het gebruik van bevoegdheden, betekent niet dat bevoegdheden overbodig zijn. Wanneer een samenleving haar overheid ergens voor verantwoordelijk houdt, moet die overheid uiteindelijk ook over de bijbehorende doorzettingsmacht beschikken. Anders gezegd, als je verantwoordelijk bent moet je ook bevoegd zijn.

Er bestaat, in bestuurlijke kringen en daarbuiten, een vrij grote consensus over de informele aanpak: liever bijvoorbeeld een online actievoerder uitnodigen voor een goed gesprek dan meteen zwaaien met bevoegdheden en sancties. Het is niettemin denkbaar dat hierin verandering komt en dat de relatie tussen overheid en burger in de bestuurlijke aanpak verder geformaliseerd wordt. Bevoegdheden zijn niet enkel een *ultimum remedium* voor wanneer andere middelen falen, maar zijn ook een reguliere basis voor overheidsoptreden dat niet is gebaseerd op informele verhoudingen. Tijdens de corona-epidemie zijn er meerdere voorbeelden geweest waarbij naar aanleiding van een stopgesprek beelden online zijn gezet die tot nog meer onrust en verontwaardiging hebben geleid.

Bevoegdheden kan men afleiden uit wat de wet nadrukkelijk toebedeelt of uit wat de wet niet verbiedt. Sinds de 'crisis in de opsporing' in de jaren negentig, ligt in Nederland op strafrechtelijk gebied de nadruk op de eerste benadering, hoewel met name de digitalisering heeft gemaakt dat politie en justitie ook weer meer oog hebben voor de tweede benadering. Verschil met de jaren negentig is echter dat daarover nu meer wordt gesproken en van nieuwe werkwijzen wordt gezegd dat de rechter over de rechtmatigheid ervan hoort te oordelen. Er lijkt daarmee vanwege de veranderingen door digitalisering een praktijk te zijn gegroeid bestaande uit een legalistisch fundament aangevuld met 'legitiem pragmatisme'.

Voor haar optreden in relatie tot digitalisering is het zaak dat de gemeente inventariseert wat haar verantwoordelijkheden zijn plus de daarbij benodigde mogelijkheden en bevoegdheden. Niet voor álles is een specifieke bevoegdheid nodig. Wél dienen gemeenten steeds te bestuderen of een bepaalde aanpak al dan niet specifieke bevoegdheden vereist, om direct te gebruiken of om achter de hand te hebben. Zeker wanneer gemeenten bij online aangejaagde ordeverstoringen online in actie willen komen, of wanneer zij online cybercrime willen verstoren of activiteiten van burgers willen monitoren, is het zaak de juridische mogelijkheden daartoe te kennen en de bruikbaarheid en reikwijdte van specifieke bevoegdheden te hebben bepaald. Aandacht is vereist voor (a) mogelijkheden die voorafgaan aan het gebruik van bevoegdheden (bv. voorlichting, het gesprek aangaan)⁶⁰, (b) het toepassen van bestaande bevoegdheden in de

online omgeving, (c) het aanpassen van bevoegdheden zodat deze ook in een digitale omgeving toepasbaar zijn, (d) nieuwe bevoegdheden die optreden in een online omgeving mogelijk maken. Bij elk van deze opties is plaats voor een experimentele benadering, evaluaties en proefprocessen. De vraag is wel hoever een bestuur kan en moet gaan met bestuursrechtelijke experimenten wanneer de rechter en onderzoeken kritisch zijn over de gekozen invalshoek en maatregelen. De discussie over bevoegdheden in een digitale samenleving zal altijd raken aan ethische vragen (willen we dit wel), over kennis gaan (hebben we genoeg kennis in huis om dit uit te voeren), over monitoring (bijvoorbeeld controle rond 'online gebiedsverboden'), maar ook vragen over samenwerking (lokaal of beter landelijk, samenwerking tussen publieke en private partijen). Deze tekst is grotendeels al in 2021 tot stand gekomen maar heeft niet aan actualiteit ingeboet. In zekere zin is het tijdonafhankelijk en in allerlei contexten toe te passen.

Inmiddels is discussie in volle gang en heeft er op 11 april 2023 zelfs een rondetafelgesprek plaatsgevonden in de Tweede Kamer over digitale gebiedsverboden (zie mijn position paper in hoofdstuk 4). Tijdens Covid-19 hebben gemeenten uitkomsten uit de wetenschap niet afgewacht en hebben ze zelfs bestuursrechtelijke experimenten uitgevoerd om online aangejaagde ordeverstoringen aan te pakken. In Utrecht en Haarlem zijn bestuursrechtelijke maatregelen toegepast, Amsterdam wil experimenteren met mogelijkheden in de Gemeentewet en in de gemeente Almelo is zelfs een speciaal APV-artikel gemaakt (verbod) waarmee online

aangejaagde ordeverstoringen expliciet aangepakt worden. Ons lectoraat kan, zeker op het terrein van uitvoerbaarheid en handhaafbaarheid, aanvullend onderzoek verrichten (zie ook hoofdstuk 4).

3.5 Monitoren van (on)veiligheid

Met de studie van onder andere Bantema e.a. (2021) is het onderwerp 'monitoren' hoog op de politieke agenda geraakt.⁶¹ Met name de bevinding dat gemeenten nepaccounts gebruiken om burgers in de gaten te houden, wekte veel verontwaardiging en is onderwerp van discussie. De landelijke overheid werkt aan richtlijnen.⁶² Deze discussie past in het bredere maatschappelijke debat over de verhouding tussen overheid en burger en in een nog bredere maatschappelijke context; die van de beweging richting meer inclusiviteit. Die beweging is zichtbaar in onderwerpen zoals zwarte piet, het Nederlandse koloniale verleden, de slavenhandel, teruggave van roofkunst, institutioneel racisme, lbhti+ -acceptatie, de toeslagenaffaire, stikstofproblematiek en aardbevingsschade in Groningen. Een overheid die burgers in de gaten houdt zonder daarover expliciet verantwoording af te leggen, past niet in deze beweging en kan serieuze weerstand verwachten. Die weerstand zal als gevolg van de digitalisering snel worden georganiseerd en goed geïnformeerd zijn. De verleiding om vanachter een bureau speurdersactiviteiten te verrichten is toch kennelijk groot. Zo bleek eerder al dat het Land

Information Manoeuvre Centre (LIMC) van actie-groep? *Defense* online informatie over de Nederlandse bevolking verzamelde, evenals de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).⁶³ De legitimatie voor het monitoren is 'veiligheid' en men kan steeds twee argumenten vernemen waarom het mag: het gaat om het verzamelen van niets anders dan openbaar beschikbare informatie en/of met het verzamelen van de informatie wordt niemand's privacy geschonden.

Politie en justitie gebruikten het eerste argument ooit ook (we hoorden het argument bijvoorbeeld eens gebruikt worden door cyber-officieren van justitie), maar zij hebben dat pad met reden verlaten. Artikel 8 EVRM beschermt namelijk het privéleven van burgers tegen inmenging door de overheid. Voor het 'stelselmatig' (d.w.z. vaker dan twee keer)⁶⁴ verzamelen van informatie over een persoon is daarom nu toepassing van artikel 126j Sv vereist. Dat is een bijzondere opsporingsbevoegdheid die vereist dat sprake is van een verdachte en dat de officier van justitie de opdracht tot het monitoren geeft. Naast een onderbouwde verdenking is dus ook een toetsing vereist. Kortom, dat informatie over burgers online beschikbaar is, betekent niet dat deze dus daarom door de overheid mag worden verzameld. Informatie over maatschappelijke ontwikkelingen en bewegingen is in zichzelf geen persoonsinformatie en kan dus in principe door de

⁶⁰ Er staan inmiddels verschillende handreikingen online bij het CCV op het dossier 'online aangejaagde ordeverstoringen'

⁶¹ Bantema, W., S. Westers, M. Hoekstra, R. Herregodts, S. Munneke (2021). *Black box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk*. Den Haag: Sdu (reeks Politie en Wetenschap).

⁶² NRC 19 mei 2021, www.vpngids.nl. Deze richtlijnen zijn waarschijnlijk al uit bij deze presentatie van dit boekje.

⁶³ Resp. NRC 15 november 2020 en NRC 9 april 2021.

⁶⁴ Volgens de niet-openbare 'Leidraad bevoegdheden informatievergaring op internet' dienen politiemensen overleg te voeren met de OvJ indien zij vaker dan twee maal een zoekslag doen die betrekking heeft op personen, hetzij verdachten hetzij derden die niet worden verdacht. (Stol & Strikwerda 2017, p. 293)

overheid zonder beperkingen worden verzameld. De vraag is echter wat te doen met de bron van de informatie (de afzender). Is de informatie te herleiden tot een persoon dan geniet die persoon privacybescherming op basis van artikel 8 EVRM, de AVG en de Grondwet.

Het is overigens niet gezegd dat de overheid geen enkele inbreuk mag maken op iemands persoonlijke levenssfeer. In het strafrecht geldt het Zwolsman-criterium als richtsnoer. 'Een antwoord op de vraag hoever de politie op grond van haar algemene taakstelling mag gaan, geeft de Hoge Raad in 1995 in het Zwolsman-arrest: indien niet meer dan 'een beperkte inbreuk op de persoonlijke levenssfeer' wordt gemaakt, kan het optreden steunen op artikel 3 Politiewet. Anders is voor het betreffende optreden een afzonderlijke wettelijke voorziening vereist.⁶⁵ Te verdedigen is dat naar analogie hiervan een dergelijke ruimte ook geldt voor gemeenten, wat betreft hun algemene taakstelling.

In de discussie is ook te vernemen dat de overheid altijd al waarnemingen deed aangaande maatschappelijke fenomenen en personen die daarmee zijn verbonden, en dat dit dus nu ook online mogelijk moet zijn, conform het motto 'wat offline geldt, geldt ook online'. Natuurlijk behoren gemeenten te weten wat er in hun gemeente speelt en dus dienen zij zich daarvan op de hoogte te stellen. Burgers verwachten ook van het lokale bestuur dat het weet wat er speelt. Maar een taak, verwachting

of verantwoordelijkheid betekent niet dat dus alle middelen om dat te bereiken zijn toegestaan. Welke middelen mogen worden gebruikt, is een afzonderlijk vraagstuk. Hier is de vraag dus op welke wijze gemeenten zich op de hoogte mogen stellen van wat er in hun gemeente speelt. Er is reden om aan te nemen dat dit online anders is dan offline, want de impact van het overheidsoptreden doet ertoe. Gezien de verwevenheid tussen technologie en haar gebruikers (zie - cyborgcomplexiteit) en gezien de digitale informatiedichtheid, heeft 'monitoren' langs digitale weg al snel een grotere impact dan langs analoge weg, en grijpt dus al snel dieper in op de persoonlijke levenssfeer, én zal dus eerder restricties kennen. Een voorbeeld hiervan vinden we wederom in de sfeer van het strafrecht, waar de rechter bepaalde dat politiemensen niet zonder meer een in beslag genomen smartphone mogen uitlezen vanwege de 'meer dan een beperkte inbreuk op de persoonlijke levenssfeer' die dat is voor de eigenaar van de smartphone.⁶⁶ Er is dan een toetsing door de OvJ vereist. We kennen geen vergelijkbare uitspraak over een in beslag genomen papieren notitieboekje. Voor monitoren kent het handelingskader voor gemeenten verschillende dimensies: geografisch, maatschappelijk/ethisch en juridisch.

(a) Om te beginnen gaat het niet om een lokaal vraagstuk, maar om iets wat de hele Nederlandse samenleving aangaat. Het monitoren door gemeenten moet daarom voor alle gemeenten identiek en voor burgers kenbaar en voorspelbaar

geregeld worden. Dat vergt meer intergemeentelijke coördinatie, uitwisseling en samenwerking en dus een landelijke regeling. De uitvoering is echter lokaal, waarbij de vraag is op welke schaal dat te organiseren. Een gemeente kan tot op zekere hoogte zelf monitoren en ze kan daarvoor samenwerkingsverbanden aangaan met buurgemeenten en/of de politie.

(b) De maatschappelijke dimensie geeft een eerste inhoudelijke richting. Van alle gemeenten mag worden gevraagd dat zij weten wat er speelt in hun gemeente. Ze moeten zich hoogte zijn digitaal hoort daar nu eenmaal bij. De maatschappelijke ontwikkelingen wijzen er evenwel op dat een overheid die haar burgers met achterdocht of als potentiële dader benadert, en helemaal een overheid die dat in het verborgene doet (en dat is vooral online gemakkelijk), serieus weerstand oproept. Dat strookt niet met de Nederlandse traditie van dichtbij bestuur. Openheid over werkwijzen ligt zo gezien voor de hand. Niet goed valt in te zien wat voor gemeenten overwegende nadelen zijn van openheid op dit vlak. Gemeenten kunnen hieraan werken 'door te communiceren over doelstellingen van monitoring (expliciet) en door aan te geven hoe de gemeente werkt en welke vuistregels daarbij gehanteerd worden'.⁶⁷ Ook de vraag wat voor een lokaal bestuur je als gemeente wilt zijn (ethiek) verdient hier een plaats. Dit raakt ook aan bevoegdheden, want als gemeenten niet weten wat er speelt en dit ook niet kunnen controleren dan heeft het weinig zin om zogenaamde 'online gebiedsverboden' in te stellen om online aangejaagde ordeverstoringen aan te pakken.

(c) De Europese en nationale wetgever hebben de persoonlijke levenssfeer van burgers beschermd tegen een te grote inmenging van de overheid. Het Zwolsman-criterium is een door de Hoge Raad vanuit het strafrecht gegeven richtlijn voor hoever de overheid mag gaan op basis van haar algemene taakstelling. Voor verdergaande inmenging is dan een bijzondere wettelijke grondslag vereist. Het is niet te verwachten dat gemeenten wel mogen wat de politie niet mag. Voor de ruimte die de overheid heeft op basis van een algemene taakstelling en dus voor de vraag wanneer bijzondere bevoegdheden zijn vereist, kunnen gemeenten gebruik maken van de ervaringen die binnen de strafrechtspleging zijn opgedaan.

(d) Momenteel is er binnen de politie en maatschappij ook discussie over wat de politie wel en niet mag op basis van hun algemene taakstelling (artikel 3 Politiewet). Vanuit de praktijk wordt aangegeven dat het onduidelijk is wanneer er meer dan een geringe inbreuk wordt gemaakt op de persoonlijke levenssfeer van burgers en er sprake is van stelselmatig handelen. Ook is het onduidelijk in hoeverre de politie aanwezigheid mag zijn in besloten omgevingen zoals Telegram-groepen, onrechtmatig handelen door de politie ligt dan op de loer.⁶⁸ Als lectoraat zijn we van mening dat deze discussie om veel meer vraagt dan om een helder juridisch kader. Om te beginnen is het al ingewikkeld om in de veelheid platformen en vanuit verschillende criteria vast te stellen of een groep open of besloten is (zie meer in hoofdstuk 4). We pleiten voor meer inzicht in perspectieven buiten het hier

⁶⁵ HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, in het bijzonder r.o. 5.1 en 5.2, en 6.4.2 t/m 6.4.5. Een tweede jurisprudentieel criterium aangaande de reikwijdte van art. 3 Pw is dat dit artikel geen grondslag biedt voor een opsporingshandeling die zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing (zie bijv. Borgers, 2017 en HR 20 december 2011, ECLI:NL:HR:2011:BP0070, in het bijzonder r.o. 2.6).

⁶⁶ ECLI:NL:HR:2017:584

⁶⁷ Bantema e.a., 2021, p. 116

⁶⁸ <https://www.politie.nl/nieuws/2022/september/27/00-onduidelijkheid-over-online-gegevensvergaring.html>

en nu, bijvoorbeeld door ook het burgerperspectief en maatschappelijke legitimiteit in de discussie te betrekken. Daarnaast zijn er ook vragen te stellen over het gezag van de burgemeester ten aanzien van 'opsporing' ten behoeve van de 'openbare orde' bij het achterhalen van NAW-gegevens of bijvoorbeeld IP-adressen. Het is de vraag op basis van welke bevoegdheid de burgemeester dat kan en mag doen. Ook hier is mogelijk meer aandacht nodig voor het huidige juridische kader. Deze discussie speelt ook bij het reguleren van demonstraties.⁶⁹

3.6 Samenwerken

De toenemende netwerkcomplexiteit maakt dat lokale problemen landelijke en internationale verbindingen kunnen hebben, bijvoorbeeld doordat de veiligheid of de openbare orde wordt bedreigd vanuit een andere gemeente of zelfs een ander land. Ook een techbedrijf kan een rol spelen, wat een gemeente voor de vraag plaatst of zij bijvoorbeeld Facebook tot optreden kunnen dwingen. Eerder kwam naar voren dat 59% van de burgemeesters meer willen samenwerken met sociale mediaplatforms, terwijl 15% van de burgemeesters aangeeft ooit contact te hebben gezocht met een dergelijk platform.⁷⁰

Hier lijkt de aangewezen weg dat gemeenten zich organiseren. Immers, in een digitale samenleving is het al snel niet adequaat om problemen op te lossen vanuit gemeenten afzonderlijk omdat vanwege de vernetwerking van de samenleving, alle gemeenten bij openbare orden en veiligheidsvraagstukken

te maken kunnen krijgen met dezelfde externe partijen, zowel landelijk als internationaal. Als het nodig is voor een openbare orde- of veiligheidskwestie waarvan het belang het lokale overstijgt, moet niet één gemeente afspraken maken met relevante partijen, maar 'de gezamenlijke Nederlandse gemeenten' in een (bestaand of nieuw) samenwerkingsverband. Het kader dat hier nodig is, bestaat uit een samenwerkingsarrangement van waaruit een gemeente die dat nodig heeft, namens alle gemeenten kan worden vertegenwoordigd. Een vraag namens allen heeft meer gewicht en een regeling die eventueel volgt, staat dan meteen alle gemeenten ter beschikking. Een dergelijke voorziening kan mogelijk tegelijk dienen als locatie waar bijvoorbeeld werkwijzen worden ontwikkeld en wetgeving wordt onderzocht. Het gaat weliswaar om een bovengemeentelijk te coördineren actie, maar niet om een klassieke opschalingsstructuur want dat veronderstelt een voorziening die pas in actie komt wanneer repressie is vereist. Het samenwerkingsarrangement is vooral proactief en preventief van aard.

Vorenstaande neemt niet weg dat zich ook situaties zullen voordoen waarin samenwerking tussen twee of enkele gemeenten de aangewezen weg is. Dat vraagt dan om arrangementen die voorzien in het snel tot stand kunnen brengen van maatwerk in intergemeentelijke samenwerking inzake openbare orde en veiligheid in een digitale context. Het is goed om te zien dat naast samenwerking tussen gemeenten, waar de VNG ook een belangrijke rol

speelt, ook via het Ministerie van Justitie & Veiligheid onderzocht wordt of er een meldpunt ingesteld kan worden dat gemeenten kan ondersteunen bij het snel offline kunnen halen van onrechtmatige online content.

3.7 Conclusie

In dit hoofdstuk is bewust niet ingegaan op specifieke taakgebieden van bijvoorbeeld gemeente en politie. Doel van dit hoofdstuk was om een vijftal hoofdlijnen en aanverwante kernvragen te presenteren. Wanneer gemeenten en politie deze vragen verder uitwerken zijn zij beter voorbereid op de digitaliserende samenleving waar ze al middenin zitten en die nog verder zal digitaliseren de komende jaren. Wetenschappelijk en toegepast onderzoek kan ook een bijdrage leveren aan goed en effectief bestuur in een digitaliserende samenleving. Bijvoorbeeld door aandacht te vragen voor wat er op ons afkomt (agenderen), onderzoek te doen naar bevoegdheden in een digitale samenleving, bijdragen aan kennis over effectieve werkwijzen, maar ook het bestuur een spiegel voorhouden over wat goed en ethisch verantwoord bestuur in een digitale samenleving behelst. Technisch is er namelijk veel meer mogelijk dan we als samenleving willen en wenselijk vinden. In het laatste hoofdstuk wordt ingegaan op de huidige werkzaamheden van het lectoraat en op enkele thema's waar het lectoraat mee aan de slag wil gaan samen met collega's van NHL Stenden, Thorbecke Academie en andere lectoren, andere hogescholen en kennisinstellingen, waaronder universiteiten, studenten en de werkpraktijk.

⁶⁹ <https://nos.nl/artikel/2466880-onderzoek-politie-verzamelt-op-grote-schaal-data-van-demonstranten>

⁷⁰ Bantema, W., Westers, S. & Munneke, S. (2020). *Niet bevoegd, wel verantwoordelijk? Handhavingsmogelijkheden bij online aangejaagde ordeverstoringen*. Boom Bestuurskunde: Den Haag.



Hoofdstuk 4

Het lectoraat Bestuur in een Digitaliserende Samenleving

4.1 Inleiding

In dit hoofdstuk staat het lectoraat 'Bestuur in een Digitaliserende Samenleving' centraal. In de tweede paragraaf wordt aandacht besteed aan de kenniskring en het team rondom het lectoraat en wordt er ook aandacht besteed aan samenwerkingen van het lectoraat met andere partijen. In paragraaf drie is aandacht voor recent afgeronde en lopende onderzoeken van het lectoraat gevolgd door aandacht voor recente valorisatie (paragraaf 4). In de vijfde paragraaf komen de onderzoekslijnen van het lectoraat aan bod waarmee duidelijk wordt in welke richting het onderzoek en onderwijs zich de komende jaren gaan bewegen. Er wordt afgesloten met enkele concluderende opmerkingen (paragraaf 6).

4.2 Missie en team

4.2.1 Missie en samenwerking

Het lectoraat 'Bestuur in een Digitaliserende Samenleving' maakt deel uit van de onderzoeksgroep Cybersafety. Het is de missie van de onderzoeksgroep om met praktijkgericht onderzoek de veiligheid in de gedigitaliseerde samenleving te bevorderen. De onderzoeksgroep wil haar missie bereiken door middel van hoogwaardig, onafhankelijk en praktijkgericht veiligheidskundig onderzoek. Ons onderzoek draagt bij aan:

1. Kwaliteit en toekomstbestendigheid van onderwijs en professionalisering
2. Kennisontwikkeling en het delen van kennis en
3. Oplossing voor de beroepspraktijk en maatschappelijke vraagstukken.

De onderzoeksgroep Cybersafety kent twee lectoraten en één cross-over onderzoekslijn: de lectoraten Digitale Weerbaarheid van Mens en Organisatie (collega lector Jurjen Jansen) en Bestuur in een Digitaliserende Samenleving en daarnaast een cross-over met het lectoraat Organisations an Social media dat zich richt op 'digital citizenship'. In aanvulling op algemene visie van de onderzoeksgroep Cybersafety richt het lectoraat 'Bestuur in een Digitaliserende Samenleving' zich op de kennisontwikkeling over de online inzet en effectiviteit van bevoegdheden en over het verantwoord gebruik van technologie door overheden om bij te dragen aan (digitale) veiligheid. Er wordt toekomstgericht en agenderend onderzoek uitgevoerd naar veiligheidsuitdagingen, naar innovatieve en effectieve vormen van handhaving in het digitale domein en de juridische en ethische aspecten daarin. Bijzondere aandacht is er voor het betrekken van burgerperspectieven als randvoorwaarde voor goed en effectief bestuur in een digitaliserende samenleving.

Het lectoraat is betrokken bij verschillende samenwerkingen. Zo zijn we vertegenwoordigd bij de City Deal 'Lokale weerbaarheid en cybercrime' (sinds 2020) en bij de City Deal 'Slimme Stad, zo doet je dat'. In deze laatste City Deal willen we meedenken over ethiek en het burgerperspectief op technologie in de stad (dit sluit aan bij onze nieuwe onderzoekslijn die in paragraaf 4.5 aan bod komt). Daarnaast is de onderzoeksgroep Cybersafety aangesloten bij het SPRONG-netwerk om cyberweerbaarheid te vergroten (samen met HHS en Saxion) en zijn we betrokken bij evaluaties van projecten rondom de eerst genoemde City Deal, een deel hiervan zal door het lectoraat 'Bestuur in een Digitaliserende Samenleving' worden uitgevoerd. Als lector is Willem Bantema aangesloten

bij twee lopende aanvragen voor een lectorenplatform op het gebied van veiligheid en een aanvraag voor een lectorenplatform op het gebied van toekomstbestendig bestuur. Dit laatste netwerk sluit goed aan bij de toegenomen aandacht (ook binnen ons lectoraat) voor burgerperspectieven en ethiek als een belangrijke voorwaarde voor goed en effectief bestuur. Daarnaast wordt actief samengewerkt met een lectorennetwerk rond recht in de praktijk. Samengevat vervult het lectoraat 'Bestuur in een Digitaliserende Samenleving' in de volle breedte een belangrijke spilfunctie tussen de Thorbecke Academie en haar opleidingen en andere hogescholen en sluit dit ook aan bij het multidisciplinaire karakter en brede interesse van de kenniskring van het lectoraat.

Eveneens wordt op verschillende momenten samengewerkt met partijen zoals de politie, met de VNG en ook met het Nederlands Genootschap van burgemeesters (NGB), in ieder geval door jaarlijks een dag onderwijs te verzorgen binnen het vak de 'cyberburgemeester'. Het lectoraat werkt ook actief samen met de Rijksuniversiteit Groningen, zowel in juridische onderzoeken maar momenteel ook met sociaalpsychologen, om interventies en werkwijzen in een digitaliserende samenleving een meer wetenschappelijke basis te kunnen geven (zie het project Connect en online interacties tussen politie en burgers). Het lectoraat werkt ook samen met AKD-advocaten in onderzoek maar ook bij het verzorgen van workshops en (vak)publicaties. Sommige samenwerkingen zijn ad hoc, andere meer duurzaam, ook intern wordt gezocht en gewerkt aan relevante samenwerkingen.

4.2.2 Teamleden die onderzoek doen binnen het lectoraat



Laura Postma (1997) is sinds 2023 aangesloten bij het de onderzoeksgroep Cybersafety. Na een uitstap naar het zuiden van Nederland voor de Bachelor Politicologie aan de Radboud Universiteit in Nijmegen, volgde de master Criminaliteit & Veiligheid in Groningen. Met studeren en wetenschappelijk onderzoek was Laura nog niet klaar: zo heeft ze nadien een tweede master in de vorm van Eerste-graadsdocent Maatschappijleer/MAW behaald.

Laura draagt binnen de onderzoeksgroep bij aan verschillende nieuwe en lopende onderzoeken. Haar expertise richt zich met name op motieven achter online aangejaagde ordeverstoringen, escalaties, collectieve onrust en complottheorieën. Haar onderzoek is vooral van kwalitatieve aard, zoals thematische analyses en (sociale) media-analyses. Daarnaast is Laura geboeid door het gedrag van radicale groepen en psychologische processen die spelen tijdens radicalisering. Oftewel: *'Waardoor radicaliseren mensen in hun gedachte en wat drijft hen om opruiende berichten de wereld in te slingeren?'*

Haar eerste kwalitatieve onderzoek bouwt voort op bovenstaande gedachte. Een inhoudsanalyse van (sociale) media berichten naar anti-institutionalisme (wantrouwen jegens de overheid, media en wetenschap) stond daarin centraal. Met behulp van thematische analyse heeft ze vijf hoofdthema's met drijfveren geïdentificeerd: verveling & sensatie, complot, zelfverdediging, natuur & spiritualiteit en een aanvullend thema van mobilisatie & opruiing. Laura is gestart als docent Maatschappijleer en MAW, maar tegenwoordig is ze naast de onderzoeksgroep werkzaam bij de opleiding Integrale Veiligheidskunde. Haar dagelijkse werkzaamheden bestaan uit het coördineren van derdejaars stages, begeleiding van studenten en verzorgen van kennissavakken op gebied van criminaliteit en veiligheid.

Momenteel is Laura betrokken bij een verkennende studie naar de inmenging van vreemde mogendheden in de Nederlandse verkiezingen en wat gemeenten daar lokaal tegen kunnen doen en is zij eveneens betrokken bij een onderzoek naar mogelijkheden om online aangejaagde ordeverstoringen, in het bijzonder drillrap-problematiek, preventief aan te kunnen pakken.



Suzanna Twickler (1959) is sinds 2017 betrokken bij de onderzoeksgroep Cybersafety. Ze heeft een bestuurlijke en juridische achtergrond. Ze studeerde bestuurswetenschappen (HBO) en rondde een universitaire studie rechten af aan de Rijksuniversiteit Groningen. Ze werkte circa 25 jaar voor diverse overheden waarbij in een aantal van deze banen onderzoek werd verricht. De expertise van Suzanna zit onder andere in het natte milieu en specifiek de handhaving ervan. De laatste jaren heeft zij expertise ontwikkeld op het gebied van bestuursrecht en privaatrecht in relatie tot de regulering van online aangejaagde ordeverstoringen. Zo leverde ze een belangrijke bijdrage aan het onderzoek 'burgemeesters in cyberspace' en was de drijvende kracht achter het onderzoek naar de mogelijkheden die de APV biedt op online aangejaagde ordeverstoringen aan te pakken. Op dit moment is Suzanna een belangrijke spil tussen de opleiding HBO-rechten en het lectoraat en onderzoeksgroep. Zo begeleidt zij onder andere afstudeerders die de privaatrechtelijke en bestuursrechtelijke mogelijkheden op de aanpak van online aangejaagde ordeverstoringen verder onderzoeken.

Suzanna is ook actief betrokken bij afstudeeropdrachten van HBO-Rechten die raken aan het onderzoek van het lectoraat. Op dit moment doet een aantal studenten afstudeeronderzoek voor het lectoraat. De onderwerpen die worden onderzocht zijn: (1) Of het als burgemeester mogelijk is om via het strafrecht preventief te handhaven indien berichten op het internet ervoor zorgen dat de openbare orde in een gemeente wordt of dreigt te worden verstoord. Het strafrecht, en dan met name artikel 131 opruiing, werkt repressief dus hoe kan vooraf al ingegrepen worden? Dit wordt nader onderzocht. (2) Ook wordt bekeken hoe het civiele recht kan helpen bij de oplossing van dit vraagstuk, waarbij leidend is de uitspraak van de kort gedingrechter in de zaak van de gemeente Bodegraven (ECLI:NL:RBDHA:2021:6769). (3) Een ander onderzoek gaat over de bevoegdheden van data-analyse bureaus bij het scannen van sociale media in opdracht van overheden. Hoeveel mogen deze bureaus gaan met hun dataverzameling zonder de privacywetgeving te overtreden? (4) Daarnaast worden twee andere onderzoeken worden uitgevoerd voor het team Privacy en Security van de Concernstaf van NHL Stenden Hogeschool. Hier worden aspecten van de Algemene verordening gegevensbescherming nader onderzocht in relatie tot bepaalde werkzaamheden van de hogeschool.



Sipke de Vries (1994) is sinds 2020 werkzaam als docent-onderzoeker bij de onderzoeksgroep Cybersafety. Hij studeerde af aan de Rijksuniversiteit Groningen waar hij zijn meestersdiploma behaalde. In zijn afstudeeronderzoek onderzocht Sipke of de vernieuwde Wet gemeenschappelijke regelingen successen zou brengen voor gemeenten. Zijn specialisatie is openbaar bestuur, zoals gemeenterecht en staatsrecht. Met die kennis wil hij de onderzoeksgroep verder helpen in de bestuurlijke kant van Cybersafety. Naast zijn werk als onderzoeker is Sipke docent bij de Thorbecke Academie. In die hoedanigheid begeleidt hij studenten bij afstudeerscripties en doceert hij vakken aan verschillende opleidingen.

In de afgelopen jaren heeft Sipke een bijdrage geleverd aan verschillende onderzoeken op het gebied van bestuur en digitalisering. Zo was hij een drijvende kracht in een regionale verkenning naar de aanpak van online aangejaagde ordeverstoringen voor NHSV en was hij eveneens betrokken bij het onderzoek naar de juridische mogelijkheden die de APV biedt voor het aanpakken van online aangejaagde ordeverstoringen. Ook leverde hij een bijdrage aan publicaties over deze onderzoeksthema's.



Denise de Boer (1996) is sinds 2023 onderzoeker bij de onderzoeksgroep Cybersafety. Als onderzoekster heeft Denise zich toegelegd op het bestuderen van de verschillende juridische aspecten die digitalisering met zich meebrengt voor het openbaar bestuur. Haar expertise ligt op het gebied van bestuursrecht, privacy, openbare-ordebevoegdheden en crisismaatregelen. Binnen de onderzoeksgroep draagt ze vooral bij aan de juridische aspecten van de verschillende onderzoeken. Denise heeft HBO-Rechten gestudeerd aan de NHL Hogeschool, waar ze de minoren 'Recht en internet' en 'International Law' heeft gevolgd. Ze heeft haar master Nederlands recht, richting staats- en bestuursrecht afgerond aan de Rijksuniversiteit Groningen. In haar masterthesis heeft ze onderzocht hoe maatregelen tijdens crises zich verhouden tot grondrechten, door de avondklok onder de mensenrechtelijke loep te leggen. Ze begon haar loopbaan als gemeentejurist en is als crisisfunctionaris aangesloten geweest bij een veiligheidsregio in het kader van de coronamaatregelen. In 2022 heeft ze de overstap gemaakt, en is ze docent geworden aan de Thorbecke Academie. In haar rol als docent begeleidt ze studenten Integrale Veiligheidskunde tijdens diverse projecten ten aanzien van de overheid, geeft ze verschillende juridische vakken en begeleidt ze studenten tijdens hun stages.



Anna Bartelds MA (1985) is sinds september 2021 verbonden aan de onderzoeksgroep Cybersafety. Zij heeft onder andere onderzoeken verricht naar privacy en ethische aspecten rondom smart city toepassingen en online interventies tegen online aangejaagd geweld (Project Connect). In 2015 rondde Anna haar master Midden-Oostenstudies af aan de Rijksuniversiteit Groningen. Voorafgaand aan deze master heeft ze de bachelor Internationale Betrekkingen en Internationale Organisatie behaald met als specialisatie conflicten in het Midden-Oosten. Na haar opleiding is Anna werkzaam geweest bij de afdelingen Openbare Orde en Veiligheid en het Sociaal Domein van de gemeente Groningen. Hier heeft Anna zich onder andere bezighouden met de aanpak van polarisatie en radicalisering, en gezondheidsbeleid.

Sinds 2018 is Anna werkzaam binnen de NHL Stenden als docent-onderzoeker voor de opleiding Integrale Veiligheidskunde. Als docent begeleidt Anna studenten binnen de minor *Criminal Mindhunters: Criminologie in de praktijk* bij onderzoeken naar sociaal-politiek geweld en is zij afstudeerbegeleider van meerdere studenten.



Willem Bantema (1984) is sinds 2017 aangesloten bij de onderzoeksgroep Cybersafety. Sinds 2022 is hij lector op het terrein van 'Bestuur in een Digitaliserende Samenleving'. Na zijn studie sociologie aan de Rijksuniversiteit Groningen (afstudeerrichting kwantitatiefs beleidsonderzoek) rondde hij een promotieonderzoek af aan de Juridische Faculteit van de RUG waar hij naleving en de handhaving van het rookverbod in cafés onderzocht. Daarna was hij postdoc betrokken bij het interdisciplinaire onderzoeksteam 'Handhaving van Onderop' waar eveneens nalevingsmotieven centraal stonden (waarom houden mensen zich aan de wet en het recht of waarom overtreden ze het juist). Vanaf 2018, mede door het uitkomen van het onderzoek 'burgemeesters in cyberspace' is er een landelijke discussie gaande over de rol van burgemeesters in cyberspace en er is op dit gebied aan bewustzijn gewonnen. Dat blijkt onder andere uit de grote aandacht in landelijke en regionale media en het opnemen van het thema 'online aangejaagde ordeverstoringen' op de cyberwegenkaart van het CCV. Het onderzoek over online monitoring door gemeenten (2021) leidde tot vragen in de Tweede Kamer en aanvullend onderzoek door het Ministerie van BZK en J&V. Nu 'online gebiedsverboden' op de kaart staan is Willem als expert uitgenodigd door de vaste Tweede Kamercommissie Digitale zaken

voor een rondetafelgesprek. De komende jaren wil hij met het lectoraat anticiperen op nieuwe ontwikkelingen, kennis blijven valoriseren onder verschillende doelgroepen en nadrukkelijker aandacht vragen voor ethische en burgerperspectieven op digitalisering om bij te dragen aan goed en effectief bestuur in een digitaliserende samenleving.

4.3 Recent afgeronde en lopende projecten

Er zijn in 2022 verschillende projecten afgerond. In dit hoofdstuk worden de belangrijkste uitkomsten getoond van de onderzoeken die we voor regio IJsselland en voor Noord-Holland Samen Veilig (NHSV) hebben uitgevoerd. In het eerste onderzoek stonden de juridische en praktische mogelijkheden van de APV als instrument in de strijd tegen online aangejaagde ordeverstoringen centraal. In het project voor NHSV is de bestaande regionale aanpak in kaart gebracht en zijn suggesties voor interventies aangedragen en is er een blik vooruit geworpen op de beleidsontwikkeling door gemeenten op dit terrein.

4.3.1 Project online orde (Noord-Holland Samen Veilig – afronding april 2022)

Samenvatting

Gemeenten zien al langere tijd dat het aantal online aangejaagde ordeverstoringen toeneemt en zijn zoekende in wat zij mogen en kunnen op het gebied van online signaleren en interveniëren. De onderzoeksgroep Cybersafety van NHL-Stenden Hogeschool heeft in de tweede helft van 2021, in opdracht van Noord Holland Samen Veilig (NHSV), onderzoek gedaan naar online signalering en toegepaste (online) interventies van gemeenten. Het onderzoek is uitgevoerd in de eenheid Noord-Holland en maakt deel uit van de City Deal (Lokale Weerbaarheid Cybercrime). Dit onderzoek is bedoeld om ervaringen bij gemeenten met online aangejaagde ordeverstoringen in kaart te brengen en daarmee de lokale en regionale aanpak van online aangejaagde ordeverstoringen te versterken.

Voor de resultaten is er met een gemêleerd gezelschap van ambtenaren en bestuurders gesproken uit in totaal twaalf gemeenten, waarvan een aantal buiten de eenheid Noord-Holland. Elk van die gemeenten heeft onderhand ervaring met fysieke ordeverstoringen die een online karakter of oorsprong hebben. Elk van die gemeenten lijkt zich nu ook bewust te zijn van de urgentie van deze problematiek. Iedere gemeente (h)erkent knelpunten bij online signalering. Dit kan bijvoorbeeld de wijze van signaleren, de complexiteit van de duiding en inschatting van openbare orde gevolgen van online oproepen zijn, of de samenwerking met de politie. Daarnaast vinden gemeenten de hoeveelheid online platforms en het besloten karakter een knelpunt. Ook merken zij dat er intern een gebrek is aan capaciteit, kennis en ervaring op dit gebied, waardoor gemeenten het gevoel hebben achter de feiten aan te lopen.

(Online) interventies die gemeenten reeds inzetten zijn vooral communicatief, zoals het reageren op een online conversatie of het communiceren over een ordeverstoring waarvan de gemeente op de hoogte is. Ook maakten enkele burgemeesters online en fysiek afspraken met inwoners van de eigen gemeente, bijvoorbeeld in stopgesprekken met online aanjagers. Daarnaast zijn er enkele gevallen geweest waarin de burgemeester uitgenodigd werd om tijdelijk deel te nemen aan WhatsApp-groepen om op te hoogte te worden gehouden over ontwikkelingen op een bepaalde plek.

De aanpak van online aangejaagde ordeverstoringen is in veel gevallen fysiek en reactief. Gemeenten zetten pas na of tijdens een fysieke ordeverstoring hun interventies in (al staan in de rapportage een aantal mooie uitzonderingen!). Gemeenten lijken daarnaast terughoudend te zijn met het toepassen van online interventies. Ook wordt de aanpak van de online aangejaagde ordeverstoringen in veel gemeenten niet geëvalueerd.

Hoewel de gemeenten nu ervaring hebben met online aangejaagde ordeverstoringen is een waarschuwing gepast: het stopt hier niet. Gemeenten moeten adaptief zijn en actief jurisprudentie en casuïstiek volgen, om mee te kunnen bewegen met de maatschappelijke ontwikkelingen. Er wordt dus aan de gemeenten aangeraden om een transitie te maken van reactief naar meer preventief. Dit vraagt om een nieuwe benadering en werkwijze.

Gemeenten wordt geadviseerd om visie en beleid te ontwikkelen rondom online signalering, te meer doordat enkele gemeenten vooralsnog volledig lijken te leunen op de online signalerings-bevoegdheden van de politie. Dit beleid moet duidelijke afspraken bevatten over wie wat wanneer doet en met welke middelen. Ook kunnen gemeenten onderling meer samenwerken en kennis uitwisselen over zowel signalering als toegepaste interventies. Tijdens dit onderzoek kwam in de media naar voren dat er gemeenten zijn die experimentele juridische interventies inzetten, zoals een 'online gebiedsverbod'. Wanneer deze nieuwe routes juridisch standhouden, is dit een belangrijke uitbreiding van de gemeentelijke interventiemogelijkheden.

Tot slot heeft NHSV mede op basis van én gedurende dit onderzoek een interventiekaart ontwikkeld: een inzichtelijke weergave van interventies die gemeenten kunnen toepassen bij online aangejaagde ordeverstoringen. Daarnaast heeft NHSV een handreiking gemaakt die kan helpen bij online signalering. Dit is een mooie eerste stap voor beleidsontwikkeling in de eenheid Noord-Holland.

Het project leverde naast een rapportage nog een factsheet op en indirect ook een aanvullende handreiking naar online monitoring.⁷¹ en onder andere het vakblad Binnenlands Bestuur besteedde er aandacht aan.⁷² Het onderzoek heeft belangrijke lessen opgeleverd voor gemeenten die hun aanpak van online aangejaagde ordeverstoringen willen verbeteren of beleid gaan ontwikkelen op dat terrein.

4.3.2 Project APV en online aangejaagde ordeverstoringen (afgerond oktober 2022)

'Waar het mondiale het lokale treft, waarom niet gewoon lokale regels opnemen op online aangejaagde ordeverstoringen aan te pakken? Kan dat? Werkt dat?' Na 'Burgemeesters in cyberspace' en het onderzoek niet bevoegd, wel verantwoordelijk werd de urgentie en de wens om online in te kunnen grijpen niet kleiner. In de media is er veel aandacht geweest voor gemeenten die creatief gebruik hebben gemaakt van mogelijkheden die er zijn om online in te grijpen, denk aan Utrecht, Amsterdam, Haarlem en Almelo. In die laatste gemeente is zelfs de APV aangepast om daarmee online aangejaagde ordeverstoringen aan te kunnen pakken. Nog voor al deze gemeenten initiatieven hadden ontplooid op dit terrein startten wij een verkennend onderzoek naar de mogelijkheden van de APV om online aangejaagde ordeverstoringen aan te pakken (nog voor Covid-19). Dat onderzoek werd uitgevoerd

op verzoek van het Districtelijk Veiligheidsoverleg van IJsselland. Het onderzoek maakte gebruik van interviews met gemeenten, expertmeetings en literatuuronderzoek. We hebben ook gemeenten betrokken die experimenteerden met bevoegdheden in het digitale domein. Binnen het onderzoek is samengewerkt met de Open Universiteit (Karianne Albers) en met AKD-advocaten (Marietta Buitenhuis). Onderstaand staan de belangrijkste uitkomsten van het onderzoek.⁷³

Waar er enkele jaren geleden nog een grote terughoudendheid onder burgemeesters was om een actieve rol aan te nemen bij het voorkomen van online aangejaagde ordeverstoringen, blijkt uit recenter onderzoek dat steeds meer burgemeesters een actieve rol voor zichzelf zien weggelegd.⁷⁴ Zo blijkt dat 71% van de burgemeesters zich verantwoordelijk voelt voor het voorkomen van online aangejaagde ordeverstoringen. Maar welke bevoegdheden hebben burgemeesters in het digitale domein? Eerder is al gebleken dat burgemeesters handelingsverlegen zijn. Burgemeesters die zien dat er online iets fout gaat, hebben het idee dat zij pas kunnen ingrijpen als het op straat daadwerkelijk uit de hand loopt. Burgemeesters hebben het idee dat zij een beperkt handelingsrepertoire hebben, omdat zij geen expliciete bevoegdheden hebben tot online preventief ingrijpen.⁷⁵ Tegelijkertijd kunnen zij wel achteraf

⁷¹ <https://nh-sv.nl/kennisbank/cyber/project-online-orde/>
⁷² <https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/uw-online-oproep-heeft-consequenties>
⁷³ Bantema, W., Twickler, S. M. A. & De Vries, S. (2022). Juridische grenzen en kansen bij openbare-ordehandhaving. Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen. Leeuwarden: Onderzoeksgroep Cybersafety
⁷⁴ Bantema, Twickler, Munneke, Duchateau en Stol, *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*, Politie en Wetenschap 103, 2018.
⁷⁵ Bantema, Westers & Munneke, *Niet bevoegd, wel verantwoordelijk*, Den Haag 2020.

bestuurlijk verantwoordelijk worden gehouden voor de gevolgen die een verstoring heeft gehad op de openbare orde. Vanuit de praktijk lijkt de roep om bevoegdheden om ook online en preventief in te kunnen grijpen na een aanloopfase van meerdere jaren toe te nemen. Uit een onderzoek komt naar voren dat de helft van de ondervraagde burgemeesters aangeeft wel iets te zien in het daadwerkelijk opleggen van een last onder dwangsom tegen online uitingen waarvan verwacht wordt dat die tot ordeverstoringen kunnen leiden. Uit de juridische analyse in datzelfde onderzoek komt naar voren dat dit onder andere niet kan omdat er niet een wettelijk voorschrift wordt overtreden.⁷⁶ Uit eerder onderzoek komt naar voren dat onder andere door grondrechten, jurisdictieproblemen, wetgeving die gericht is op het fysieke (lokale) domein en door een onduidelijke relatie tussen online gedragingen en de openbare orde, de burgemeester zijn bevoegdheden niet online kan toepassen.⁷⁷ Tot voor kort betrof het vooral een wetenschappelijke discussie over bestuursrechtelijke handhaving online want een bestuurlijke praktijk op dit terrein is tot in 2021 uitgebleven. In dat specifieke jaar hebben meerdere gemeenten ordeverstoringen gezien die via sociale media georganiseerd werden en die verband hielden met coronamaatregelen zoals het instellen van de avondklok. Verscheidende gemeenten hebben toen geëxperimenteerd met het opleggen van een last onder dwangsom tegen online uitingen waarvan verwacht werd dat deze bij herhaling wederom zouden leiden tot ordeverstoringen. Een

voorbeeld is de last onder dwangsom op basis van de APV in de gemeente Utrecht in november 2021.⁷⁸

Dit onderzoek werd gestart voordat gemeenten experimenteerden met toepassen van bestuursrechtelijke bevoegdheden online, maar sluit er wel bij aan. Specifiek is ervoor gekozen het spanningsveld en de mogelijkheden op te zoeken die de Algemene Plaatselijke Verordening (APV) biedt om rechtsregels op te nemen die het mogelijk maken om op te treden tegen online aangejaagde ordeverstoringen. De gedachte is dat er mogelijk aanknopingspunten zijn binnen de huidige regelgeving die een grondslag kunnen bieden voor de handhaving van online aangejaagde ordeverstoringen. De APV is één van de mogelijkheden die in dit onderzoek concreet onderzocht wordt. De vraag is in hoeverre het mogelijk is om op lokaal niveau (op gemeenteniveau) regels te stellen met verboden en of beperkingen ten aanzien van online gedragingen.

Het onderzoek ging specifiek in op de vraag in hoeverre de Algemene Plaatselijke Verordening (APV) mogelijkheden biedt voor het opnemen van regels die het mogelijk maken om op te treden tegen online aangejaagde ordeverstoringen. De focus van het onderzoek is in samenwerking met de opdrachtgever - het Districtelijk Veiligheids-overleg IJsselland - tot stand gekomen. Het doel van het onderzoek is het vergroten van handelingsperspectief van gemeenten bij het voorkomen van online aangejaagde ordeverstoringen. Daartoe

worden de mogelijkheden die de APV biedt onderzocht en zo concreet mogelijk uitgewerkt aan de hand van de volgende onderzoeksvraag: *In hoeverre kan de gemeente op grond van de APV (preventief) online optreden tegen online aangejaagde ordeverstoringen?*

Het onderzoek bestaat uit een juridische analyse/bronnenonderzoek en een empirisch deel waarbij zeven (groeps) interviews zijn afgenomen en daarnaast is een expertmeeting met wetenschappers en een focusgroep met praktijkjuristen en gemeenteamttenaren georganiseerd. De interviews, focusgroep en expertmeeting hebben plaatsgevonden tussen december 2021 en april 2022. Uit de resultaten komt naar voren dat gemeenten veel niet-juridische interventies inzetten om online aangejaagde ordeverstoringen aan te pakken, zoals communicatie met ouders (in het geval van jongeren) en het in gesprek gaan met ordeverstoorers of ze waarschuwen. Wat betreft de APV en bestuursrechtelijke mogelijkheden is geput uit praktijkcasussen en uit aanvullende juridische analyses die tot nieuwe juridische voorstellen hebben geleid.

Bestuursrechtelijke experimenten

Uit de praktijkverkenning komt onder andere naar voren dat een van de gemeenten een bestaand APV-artikel over 'uitdagend gedrag' toepaste op online gedrag dat eerder al tot ordeverstoringen in de gemeente had geleid en waarbij de last onder dwangsom werd opgelegd om herhaling van die ordeverstoring te voorkomen. Het APV artikel is hierbij ook van toepassing geacht op 'online uitdagend gedrag'. Uit het onderzoek komt naar voren dat dit gezien kan worden als een beperking van een grondrecht, de vrijheid van meningsuiting,

die alleen bij een wet in formele zin (vastgesteld door het parlement en niet een gemeente) mag worden beperkt en niet door een wet van een lagere overheid. Daarnaast is er discussie over jurisdicties, want in dit geval legde burgemeester uit gemeente X een last onder dwangsom op aan een inwoner uit gemeente Y. In het onderzoek wordt dit jurisdictie vraagstuk niet gezien als een groot juridisch probleem zolang duidelijk is waar het effect op de openbare orde zich voordoet.

Een ander praktijkvoorbeeld betreft een combinatie van strafrecht en bestuursrecht. De gedachte erachter is dat wanneer opruiing plaatsvindt (Artikel 131 Sr), automatisch ook de openbare orde wordt verstoord (artikel 172 GW). Een dwangsom kan dan herhaling van dit gedrag voorkomen op een vergelijkbare wijze als het eerder genoemde voorbeeld maar dan via twee wetten in formele zin. Bij deze interventie is er onder experts vooral discussie over handhaving en het monitoren van openbare accounts op basis van artikel 10 van de Grondwet en is actieve samenwerking binnen de driehoek een vereiste omdat in dit geval alleen de politie wettelijk digitaal mag monitoren en niet de gemeente.

Een derde casus die vermeld moet worden betreft een Belgisch APV-artikel waarbij de werking van de APV niet alleen de fysieke publieke ruimte betreft, maar ook de virtuele publieke ruimte expliciet geformuleerd en benoemd is. Dit komt tegemoet aan de discussie over wetgeving en regelgeving die gericht is op het fysieke domein en de Belgische casus is ter inspiratie meegenomen bij de juridische voorstellen en constructies die het onderzoek heeft opgeleverd.

⁷⁶ Bantema, Westers & Munneke, *Niet bevoegd, wel verantwoordelijk*, Den Haag 2020.

⁷⁷ Bantema, Twickler, Munneke, Duchateau en Stol, *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*, Politie en Wetenschap 103, 2018.

⁷⁸ 'Online gebiedsverbod voor man die opriep tot rellen Utrecht', utrecht.nl, 26 november 2021.

Concrete bestuursrechtelijke voorstellen

De aanvullende juridische ontwerpen die uit het onderzoek naar voren zijn gekomen zijn gericht op (1) opleggen van een online gebiedsverbod op basis van de Gemeentewet (172a, 172 lid 3 en 172 lid 1) en APV, (2) het uitbreiden van de APV met pre-criminele fase, de zogenaamde Veluwse methode, en (3) het uitbreiden van de reikwijdte van de APV naar het virtuele domein zoals in de Belgische APV is gedaan.

Opleggen van een online gebiedsverbod, naar analogie van het bekende gebiedsverbod lijkt het meest kansrijk via een lichte bevelsbevoegdheid op basis van artikel 172a van de Gemeentewet – al mag niet worden afgeweken van wettelijke voorschriften (zoals de Grondwet) en het mag alleen als de APV geen mogelijkheden biedt en dat is nu het geval. Een mogelijkheid voor de APV zou kunnen liggen in het uitbreiden van de verblijfsontzegging naar de virtuele publieke ruimte binnen de APV. Bij dit voorstel zijn meerdere kanttekeningen in te brengen. Zo spelen grondrechten bij dat voorstel een belangrijke beperkende rol want het gaat om online uitingen die niet gedaan mogen worden en zijn ook uitvoerbaarheid en handhaving een aandachtspunt, omdat ook daar weer grondrechten in het geding zijn (schenden van de privacy bijvoorbeeld).

Bij de tweede en Veluwse methode, waarbij een via de APV een voor-en nafase van een misdrijf strafbaar gesteld kunnen worden, speelt de onderbouwing een grote rol. In hoeverre kan aangetoond worden dat er bij een specifieke online gedraging ook sprake is van een (dreigende) verstoring van de openbare orde en in hoeverre is het duidelijk wat de overtreder moet doen om verbeuring van de dwangsom te voorkomen? Daarnaast kan toezien op naleving juridische en organisatorische problemen

opleveren en spelen grondrechten ook hier weer een rol (schenden van de privacy als het online gedrag moet worden gemonitord).

Bij de derde denkrichting, waarbij de reikwijdte van de APV wordt uitgebreid naar het virtuele domein, is gebruik gemaakt van de formuleringen uit het Gemeenschappelijke Algemeen Politiereglement van de 19 Brusselse gemeenten en het uitbreiden van het begrip openbare plaats of voor publieke toegankelijke gebouwen. Wanneer wordt vastgesteld dat een APV is gericht op het fysieke domein en niet te voorzien is dat ook de online publieke ruimte hiertoe behoort, kan het expliciet benoemen van die plek een oplossing zijn. Het onderzoek biedt daartoe mogelijkheden.

Conclusie

Concluderend zijn in het onderzoek verschillende juridische mogelijkheden naar voren gekomen die al dan niet in de praktijk zijn toegepast. Uit het onderzoek is gebleken dat er verdeeldheid is onder experts, maar dat men over het algemeen terughoudend is over de APV als route. Belangrijkste reden hiervoor is dat een APV in zijn algemeenheid geen grondrechten mag beperken. Dat mag, hoge uitzonderingen daargelaten, alleen bij een wet in formele zin. In de expertmeeting kwam vooral naar voren dat we wetten in formele zin hebben, die toegepast kunnen worden bij online openbare ordeverstoringen en daarbij wordt verwezen naar het Wetboek van Strafrecht en het Burgerlijk Wetboek. Bestuursrechtelijk is er momenteel geen wet in formele zin die burgemeesters de bevoegdheid geven om online op te treden tegen online aangejaagde ordeverstoringen dan alleen de Gemeentewet, maar de redactie van deze artikelen is zo algemeen, dat het niet kan dienen als basis om grondrechten te beperken.

Uit eerder onderzoek bleek dat online inzet van bevoegdheden door burgemeesters in het kader van de openbare orde onder andere door grondrechten, jurisdictieproblemen, wetgeving die gericht is op het fysieke domein en door een onduidelijke relatie tussen online gedragingen en de openbare orde, niet toegepast kunnen worden door de burgemeester.⁷⁹ Op basis van het huidige onderzoek kan gesteld worden dat een burgemeester van gemeente X in principe kan optreden tegen online gedragingen van een inwoner uit gemeente Y als het effect voor de openbare orde in zich in zijn gemeente voordoet of voor lijkt te doen. Jurisdictie lijkt inmiddels meer een organisatorisch dan een juridisch vraagstuk. Datzelfde geldt in zekere zin ook voor de relatie tussen online gedragingen en de openbare orde – hoe meer casuïstiek zich voordoet hoe aannemelijker deze relatie gemaakt kan worden. Dit terwijl in 2018 de relatie tussen online gedragingen en de openbare orde nog onduidelijker was. Doordat er sprake is van een onduidelijke relatie tussen online gedragingen en mogelijke ordeverstoringen blijven grondrechten en de weging en toetsing van die online gedragingen een belangrijk aandachtspunt en is onderbouwing van die relatie belangrijk. Dat geldt ook wanneer de Gemeentewet aangepast zou worden op dit punt. Wanneer ervoor wordt gekozen om een wet in formele zin of in de APV expliciet te verwijzen naar het online domein als onderdeel van de publieke of openbare ruimte is het voor burgers duidelijk en voorzienbaar wat de regels zijn. Wanneer dit niet het geval is en bestaande regels ruim worden opgevat geeft dat lokale overheden allicht te veel ruimte (zoals in

⁷⁹ Bantema, Twickler, Munneke, Duchateau en Stol, *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*, Politie en Wetenschap 103, 2018.

Utrecht met de APV) om artikelen naar eigen interpretatie en inzichten toe te passen met inbegrip van online gedragingen en de relatie met de openbare orde. De wijze waarop de 19 Brusselse gemeenten verwijzen naar het online domein in hun Gemeenschappelijke Algemeen Politiereglement kan als voorbeeld en inspiratie dienen voor Nederlandse gemeenten en voor de wetgever.

Hoe nu verder? Het Ministerie van Justitie en Veiligheid liet eerder weten dat het aan gemeenteraden is om verder te verkennen of de APV mogelijkheden biedt om de problematiek van online aangejaagde ordeverstoringen van de openbare orde het hoofd te bieden. Uit het onderzoek kwam juist naar voren dat een wet in formele zin het meest voor de hand ligt op basis van discussie over grondrechten die niet via de APV beperkt kunnen worden. In dat geval is de landelijke politiek aan zet als men het belangrijk genoeg vindt om er wetgeving voor te ontwikkelen. Gemeenten kunnen ook het verzoek van het Ministerie van J&V volgen om te experimenteren binnen de huidige bevoegdheden. Als de rechter de handelswijze van de gemeente afkeurt en de wetgever het belangrijk genoeg vindt zouden regels gesteld worden bij een wet in formele zin, bijvoorbeeld de Gemeentewet. De gemeenten die niet kunnen wachten kunnen direct aan de slag gaan en de mogelijkheden die dit onderzoek biedt benutten.

Bovenstaande tekst is geschreven naar aanleiding van ons onderzoek (samenvatting) dat in oktober 2022 werd gepubliceerd. Uit de praktijk destijds

is gebleken dat gemeenten inderdaad niet kunnen wachten. Zo heeft onder andere de gemeente Amsterdam heeft aangekondigd te willen experimenteren met bevoegdheden in een online domein en heeft de gemeente Amelo zelfs een nieuw APV artikel opgenomen dat expliciet ingaat op het verbieden van het verstoren van de openbare orde via het gebruik van technologie, waaronder het internet en sociale media. In de gemeente Utrecht is inmiddels enige juridische duidelijkheid, volgens de rechtbank mag de gekozen constructie niet omdat het APV-artikel gaat over een verbod om bepaald gedrag niet te vertonen op een openbare plaats wordt daarmee niet bedoeld op een virtuele plaats, ook niet als deze publiek of openbaar toegankelijk is. Naar aanleiding van dit onderzoek en de actualiteit zijn er veel valoriserende activiteiten gaande op dit terrein die besproken worden in de volgende paragraaf. Dit gaat onder andere over de visie van het lectoraat om maatregelen en de APV zoals die in Almelo is opgenomen.

4.3.3 Connect (afrondding uiterlijk juni 2023)

Uit onderzoek blijkt dat gemeenten vooral fysieke en reactieve interventies inzetten om ordeverstoringen te voorkomen, terwijl de wens en noodzaak aanwezig is om meer preventief en online in te grijpen aan de voorkant. Dit project draagt bij aan onderbouwde kennis en inzicht in online interventiemogelijkheden.

Steeds vaker wordt in Amsterdam en de Amstelland-gemeenten gezien dat online opjutten en uitdagen leidt tot ernstige geweldsincidenten. Een voorbeeld hiervan zijn spanningen tussen drillrapgroepen en daaruit voortvloeiende verstoringen van de openbare orde en het geweld. Amsterdam wil beter inzicht in hoe online groepsdynamiek kan leiden

tot geweld op straat en op basis daarvan kunnen de-escaleren, interveniëren en manieren vinden om toekomstig geweld te voorkomen of te verminderen. Er is veel ervaring met de rol die wijkagenten, jongerenwerkers en straatcoaches offline kunnen spelen om contact met jongeren te leggen en hun te bieden wat nodig is (grenzen stellend en perspectief biedend). Een steeds groter deel van het leven van jongeren speelt zich echter online af. Professionals zien daarom de noodzaak om meer online aanwezig te zijn en om beter te begrijpen wat daar speelt en daarop inspelen. Daarom helpt ons lectoraat met dit project om de online gereedschapskist en handelingskader voor Amsterdam en de andere gemeenten verder te vullen door een overzicht te genereren van ervaringskennis en evidence- en practice-based mogelijkheden om online aangejaagde ordeverstoringen verder te beperken en vroegtijdig in de kiem te kunnen smoren. Met dit project beogen we een online interventiematrix op te leveren om online opjutting en uitdaging tegen te gaan.

Het project bestaat uit drie fasen. In de eerste fase wordt een literatuurreview uitgevoerd op basis van wetenschappelijke literatuur en grijze literatuur (bv. evaluaties en beleidsdocumenten). Dit mondt uit in een overzicht van de bestaande interventiemogelijkheden online en offline en wat daarvan geleerd kan worden ten aanzien van effectiviteit en mechanismen (waarom werkt het). In de tweede fase – die deels gelijk opgaat met de eerste fase, vindt een inventarisatie plaats van best practices en concrete ervaringen uit de praktijk. Dit wordt vooral gedaan door interviews/focusgroepen met verschillende beroepsgroepen te houden die ervaring hebben met online interventies. Ook betrekken we de credible messengers om gebruik te maken van

hun ervaringskennis. Deze fase draagt bij aan het in kaart brengen van wat er al in de praktijk gebeurt maar niet wordt vastgelegd (evaluaties vinden vaak niet plaats) en draagt ook bij aan afstemming van interventies op de praktijk als aanvulling op de eerste fase.

De derde fase van het project is gericht op het samenbrengen van de inzichten en het ontwikkelen van een handelingskader. Dat kader geeft enerzijds een overzicht van mogelijke werkwijzen en interventiemogelijkheden. Anderzijds is het kader een hulpmiddel voor de analyse en het beter begrip van de online groepsdynamiek die kan uitmonden in geweld en openbare ordeverstoringen. Het kader biedt bovendien inzicht in wat de randvoorwaarden zijn voor een effectieve inzet van de geschetste online-interventiemogelijkheden. Zo komt het eindproduct tot stand: een online interventiematrix die in toekomstige projecten verder zal groeien. Dit onderzoek komt voor juli 2023 uit en wordt eveneens gepresenteerd op conferentie van het CCV in juni.⁸⁰

4.3.4 Intelligence (afrondding in juni)

In de afgelopen jaren is het bewustzijn rondom buitenlandse inmenging in verkiezingen toegenomen, met name naar aanleiding van de verkiezingen in de Verenigde Staten. Maar ook in Europa zijn er aanwijzingen dat buitenlandse actoren invloed uitoefenen op democratische processen. Wereldwijd speelt ongewenste buitenlandse inmenging niet alleen op nationale verkiezingen, maar is er ook reden tot zorg voor lokale verkiezingen. De verspreiding van onjuiste informatie kan leiden tot een vertekend beeld van

politieke partijen en kandidaten, wat de uitkomst van verkiezingen kan beïnvloeden. Dit verkennende onderzoek zal zich richten op ongewenste buitenlandse inmenging in verkiezingen door middel van misinformatie en desinformatie. Het doel is om te begrijpen welke maatregelen kunnen worden genomen om deze vorm van inmenging te tegen te gaan en om de Nederlandse democratie beter te kunnen beschermen.

Er wordt een verkennend literatuuronderzoek uitgevoerd, waarbij het lokale en internationale perspectief op ongewenste buitenlandse inmenging door middel van het verspreiden van valse informatie in kaart wordt gebracht. Daarnaast wordt aandacht besteed aan mogelijke interventies door de (lokale) overheid, zowel preventief als reactief om handelingsperspectief te vergroten. Wanneer de tijd het toelaat zullen enkele interviews worden gehouden met griffiers om te kijken in hoeverre dit vraagstuk leeft (bewustzijn) en te kijken in hoeverre de geschetste interventies aansluiten bij de lokale werkpraktijk.

4.3.5 NAOB – leergang handelingsperspectief online aanjaging

Sinds 2023 verzorgt ons lectoraat samen met de Noordelijke Academie voor het Openbaar Bestuur (NAOB) een leergang over handelingsperspectief op online aangejaagde ordeverstoringen. Collega Avelien Haan (Bestuurskunde en Overheidsmanagement) schreef een korte bijdrage over haar ervaringen en de meerwaarde van de leergang voor het lectoraat en voor de beroepspraktijk (tekst opgesteld op 31 maart 2023).

⁸⁰ <https://hetccv.nl/agenda/cybercongres-city-deal-lokale-weerbaarheid-cybercrime/>

"Voor de Noordelijke Academie voor Openbaar Bestuur heeft Willem Bantema een college-reeks ontwikkeld, gericht op OOV-adviseurs en medewerkers bij de veiligheidsdiensten. De Noordelijke Academie voor Openbaar Bestuur (NAOB) is een samenwerking van de Thorbecke Academie (NHL Stenden) en de Faculteit Rechtsgeleerdheid en Campus Fryslân (RUG). De NAOB verzorgt opleidingen training en inspiratie voor adviseurs bij de lokale en regionale overheden. Digitalisering als belangrijk thema mag bij de NAOB natuurlijk niet ontbreken! In de collegereeks staat het thema Online Ordehandhaving centraal. In een reeks colleges neemt Willem Bantema de deelnemers mee langs de belangrijkste ontwikkelingen en nieuwste inzichten op basis van onderzoek. Met de deelnemers bespreken we de urgentie en aanpak van de vormen waarin de openbare orde online wordt bedreigd. We bespreken de dilemma's die ze in de praktijk tegenkomen bij het voorkomen en ingrijpen bij bedreigingen van de openbare orde.

De wisselwerking wetenschap en praktijk levert boeiende inzichten op. Van een heel aantal vormen van online bedreiging van de openbare orde, weten de deelnemers van gemeenten en politie goed aan te geven wat het inhoudt en in welke mate het zich voordoet en of daar wel of niet zicht op is. Een deel van de vormen hoort duidelijk bij de gemeente en wordt vooral preventief aangepakt (cyberpesten bijvoorbeeld) en daar waar de schade voor personen groter is, is veelal een route voor repressie/handhaving in beeld (online bedrog/haatzaaien). Maar dat wat de deelnemers de meeste zorgen baarde zijn de indirecte dreigingen (aanzetten tot zelfbeschadiging bijvoorbeeld) en informatiemanipulatie. Die zijn ofwel in het privé-domein ofwel zo breed verspreid dat er weinig

grip op is. Van de verschillende vormen waarden de deelnemers online informatiemanipulatie (met ondermijning en polarisatie tot gevolg) als het meest urgent en bedreigend voor de openbare orde. In de gesprekken kwamen we met de deelnemers tot een start van een aanpak hiervoor, die in ieder geval breed, samen en preventief moet zijn.

Veel overheden zijn bezig met online signalering en dat levert regelmatig dilemma's op: hoever mag je gaan om aan informatie te komen? Met de deelnemers hebben we een casus uitgespit waarin informatie uit een privé-account wordt gebruikt om in te grijpen om ordeverstoringen te voorkomen. Als de politie zoiets doet, is er een heldere bevoegdheidsstructuur en iemand die de afweging maakt welk belang op dat moment voorgaat, dat van de maatschappij of dat van de individu. Voor dreigingen in de openbare orde, is een dergelijke structuur er niet – terwijl het heel goed denkbaar zou zijn dat op dat moment de burgemeester een afweging moet maken tussen het openbare-ordebelaag of het waarborgen van de privacy. Waarden die in de discussie tegenover elkaar kwamen te staan zijn: de transparante overheid of de veilige samenleving. Het belang van de veilige samenleving gaat volgens de deelnemers al snel voor. Dit roept ook weer een vraag op: als informatiemanipulatie als belangrijk wordt gezien, zouden we dan niet meer gewicht moeten toekennen aan de transparante overheid?

Door zo met elkaar van gedachten te blijven wisselen kunnen wetenschap en praktijk elkaar versterken. Als onderzoekers krijgen we meer zicht op wat aan kennis en informatie nodig is voor de praktijk en we kunnen de praktijk ondersteunen met het ontrafelen van casussen en dilemma's. Zo blijft het onderzoek van het lectoraat relevant en toepasbaar".

4.3.6 Het afstudeeronderzoek van nieuwe lectoraat collega's

Het lectoraat is sinds februari 2023 versterkt met twee nieuw collega's (zie 4.2.2), namelijk Laura Postma en Denise de Boer. Beide hebben expertise die relevant is voor het lectoraat en heel goed aansluit bij de vraagstukken waar het lectoraat aan werkt. Om ze extra in het zonnetje te zetten zijn ze beide gevraagd een samenvatting van hun afstudeerscriptie aan te leveren. Die zijn onderstaand weergegeven. Laura komt onder andere tot de conclusie dat er bij de coronarellen te weinig aandacht was voor het opruiende en mobiliserende karakter van sociale media. Denise de Boer keek met een ander perspectief naar het vraagstuk en vroeg zich af hoe de avondklok zich verhoudt tot grondrechten. Dit toont eens te meer het multidisciplinaire karakter en verscheidenheid aan achtergronden binnen ons lectoraat.

Corona ontbrandt diffuus anti-institutionalisme (Laura Postma, 2021)

Met anti-institutionalisme wordt het wantrouwen in de overheid, media en de wetenschap bedoeld. Corona vormde een broeinest voor dit sentiment: in sommige gevallen raken protestacties zo verhit dat geweld wordt ingezet. Dit sentiment was ook aanwezig in de rellen van Amsterdam op 17 januari en een week later in Eindhoven. In beide gevallen mondde een anti-lockdown demonstratie uit in rellen, plunderingen en vernielingen. De groep die het anti-institutionalisme in Amsterdam en Eindhoven vertoonde was zeer divers. Daardoor

bestaat onduidelijkheid over de beweegredenen die schuilgaan achter het sentiment.

In dit onderzoek staat deze nog onverklaarde motivatie centraal, in de volgende onderzoeksvraag: *Wat houdt het anti-institutionalisme in Nederland in, welke motivatie ligt aan het sentiment van anti-institutionalisme ten grondslag en kan het flashpoints-model de sentimenten en motivatie van anti-institutionalisme tijdens anti-lockdown demonstraties in Amsterdam en Eindhoven verklaren?* Ter beantwoording van deze onderzoeksvraag volgt de toepassing van het flashpointsmodel op de rellen in Amsterdam en Eindhoven. Dit model is gericht op het verklaren van collectieve onrust, dat in het algemeen verschillende eigenschappen kent (uiting van onderliggende gevoelens, heeft een variabel voorkomen en moet 'collectief' zijn). Het handelen van een eenling is daarmee uitgesloten.⁸¹

Hoe staan de begrippen anti-institutionalisme en collectieve onrust met elkaar in relatie? Anti-institutionalisme is zoals gesteld een sentiment van wantrouwen. Wanneer dit sentiment in de praktijk geuit wordt, noemen we dit collectieve onrust. Collectieve onrust is daarmee een fysieke uitingvorm van anti-institutionalisme. De toepassing van het flashpointsmodel is een logische stap in de verduidelijking van het sentiment anti-institutionalisme. De geselecteerde rellen in Amsterdam en Eindhoven zijn een typerend voorbeeld van zowel het onderliggende sentiment anti-institutionalisme als van de uitingvorm collectieve onrust. Weten-

⁸¹ King, M. (1990). Flashpoints: Studies in Disorder. *American Journal of Sociology*, 96(2), 475-477; Ministerie van Justitie en Veiligheid & Wetenschappelijk Onderzoek- en Documentatiecentrum. (2018). *Links-extremisme in beeld. Een verkennend onderzoek naar links-extremistische groeperingen in Nederland*. Bureau Beke: Arnhem.

schappelijk onderzoek maakt duidelijk dat een tal van psychologische en sociale elementen van invloed kunnen zijn op het voorkomen van collectieve onrust.⁸² Het flashpointsmodel groepeerde verschillende invloedfactoren samen in een model met zeven niveaus. Zo is er in het model aandacht voor structurele ongelijkheidsprocessen, politiek-ideologische polarisatie en institutionele regelgeving. Ook groepsdynamiek, voorgaande negatieve ervaringen en de locatie van het protest zijn elementen die zijn opgenomen in het model. Daarnaast zijn zogenaamde triggerfactoren in het model verwerkt, die een vreedzame demonstratie doen escaleren (King & Waddington, 2013)⁸³.

Het flashpointsmodel vormt de theoretische basis. Dit model is vervolgens toegepast op de cases en data door gebruik te maken van een thematische analyse. Thematische analyse is een methode waarin algemene datapatronen worden samengevoegd in overkoepelende thema's.⁸⁴ In deze thematische analyse stond een triangulatie van databronnen centraal. De dataset is een combinatie van kranten-artikelen, beeldmateriaal, een documentaire-reeks en social-media statements afkomstig van het platform Telegram. De databronnen zijn vervolgens getranscribeerd en gecodeerd. Op basis van de coderingen zijn overkoepelende thema's opgesteld, die enerzijds de motivatie voor deelname aan anti-

lockdown demonstraties onderbouwen. Anderzijds zijn ook de verschillende niveaus van het flashpointsmodel in de thema's herkenbaar. Met behulp van de thematische analyse zijn in totaal vijf hoofdthema's met drijfveren geïdentificeerd: verveling & sensatie, complot, zelfverdediging, natuur & spiritualiteit en een aanvullend thema van mobilisatie & opruiing. Een beknopte inhoudelijke bespreking van deze thema's en sub thema's volgt. Uit de analyse blijkt dat verveling & sensatie een deel van de demonstranten aanzet tot anti-institutionalisme. De gevoelens van onvrede die hen drijven zijn vrij oppervlakkig. De frustratie ligt niet in een diep wantrouwen in de overheid, maar heeft specifiek te maken met de ontregeling van het dagelijks leven als gevolg van corona. Deze groep verveelde demonstranten gebruikt de demonstraties om mannelijkheid en status op een alternatieve manier te profileren.

Het tweede motief voor anti-institutionalisme kan betiteld worden als het geloof in complottheorieën rondom het handelen van de overheid tijdens de coronacrisis. Verscheidene individuen die deze complottheorieën aanhangen, sluiten zich aan bij anti-lockdown protestacties. Organisatoren spelen hierin een mobiliserende rol. Zij linken de demonstraties namelijk aan QAnon en de Great Reset. De aansluiting van complotaanhangers blijft niet

zonder consequenties. Social-media statements wijzen erop dat enkele complotaanhangers de inzet van geweld tijdens anti-lockdown demonstraties accepteren als laatste beschermingsmiddel tegen de corrupte elite.

De noodzaak van zelfverdediging, de derde motivatie, ontstaat door het samenspel van een verzetsstrijd en de opvatting dat de overheid buitensporig geweld uitlokt. Er is volgens deze groep sprake van onvrijheid en een oorlogssituatie. De opvatting die heerst is dat de overheid zelf, door inzet van Romeo's, probeert deze onvrijheid te verstevigen. Verzet daartegen is nodig. Voor hen neemt verzet de vorm aan van aanwezigheid en het gebruik van geweld tijdens de anti-lockdown demonstraties.

Een vierde domein kent de naam natuur & spiritualiteit. Dit betreft een groep die pleit voor handelen op basis van gevoelens in plaats van op basis van rationele redeneringen en wetenschap. Deze groep komt op de anti-lockdown demonstraties af om hun zorgen over de te rationele inrichting van de maatschappij te uiten. Het gevoel van verbinding met gelijk-denken is voor deze demonstranten een belangrijke motivator voor hun aanwezigheid bij de demonstraties.

Een laatste overkoepelend thema dat meerdere malen terugkeert in de data heeft betrekking op (online) mobilisatie en opruiing. Voor beide demonstraties komt de mobiliserende rol van sociale media in de dataset naar voren. Enerzijds vormen online-groepen een centrale plaats waar verscheidene groepen zich concentreren en elkaar kunnen inlichten of opvattingen kunnen uitwisselen. Daarbij is communicatie via platformen als Telegram

redelijk anoniem. De stap tot gewelddadige opruiing lonkt. Ook tijdens de fysieke protestacties spelen de platformen een rol. Ter bewijsgaring streamen demonstranten beeldmateriaal van de politie. Hiermee is de motivatie voor aanwezigheid tijdens de anti-lockdown demonstraties besproken.

In deze scriptie ligt de focus ook op de vraag welke rol het flashpointsmodel speelde in Amsterdam en Eindhoven. De verschillende niveaus uit het model zijn herkenbaar in de gevonden thema's. Zowel de motivatie natuur & spiritualiteit als de motivatie complot zijn gebaseerd op gevoelens van achterstelling en machteloosheid. Beide motivaties vertonen gelijkenissen met het structurele niveau. In het thema motivatie – natuur & spiritualiteit zijn daarbij verwijzingen gevonden naar een afkeurende politieke reactie, oftewel het politiek-ideologische niveau. Dit gaat ook op voor het sub-thema institutionele reactie – voorbeeld stellen. In de motivatie 'Romeo's lokken geweld uit' komen de meeste niveaus samen. Zowel factoren van het institutionele, culturele en contextuele niveau zijn herkenbaar in dit specifieke sub-thema. Er zijn geen noemenswaardige resultaten gevonden voor het situationele en interactie-level. Het flashpointsmodel sluit daarmee aan op de geïdentificeerde thema's. Ook op de geselecteerde cases van collectieve onrust, Amsterdam en Eindhoven, past het model. De scriptie verheldert dat Amsterdam het startpunt vormde voor het thema zelfverdediging. Voornamelijk culturele en contextuele factoren bleken dominant in de escalatie op het Museumplein. In Eindhoven stond zelfverdediging nogmaals centraal. De fysieke locatie, een gebrek aan mankracht en triggerfactoren vormen hierop een aanvulling. Het situationele level en de triggerfactoren waren in Amsterdam zo goed als afwezig. De inhoudelijke

⁸² Adang, O., Livingstone, A., Stott, C. & Schreiber, M. (2008). TACKLING FOOTBALL HOOLIGANISM. A Quantitative Study of Public Order, Policing and Crowd Psychology. *Psychology, Public Policy and Law*, 14(2), 115-141 ; Stott, C. & Drury, J. (2017). Contemporary understandings of riots: Classical crowd psychology, ideology and the social identity approach. *Public Understanding of Science*, 26(1), 2-14; Waddington, D. (2008). The Madness of the Mob? Explaining the 'Irrationality' and Destructiveness of Crowd Violence. *Sociology Compass*, 2(2), 675-687.

⁸³ King, M. & Waddington, D. (2013). Riots and social protest in an age of austerity. *Policing and Society*, 23(1), 1-5.

⁸⁴ Braun, V. & Clarke, V. (2012). Thematic Analysis. In Cooper, H., Camic, P. M., Long, D. L., Panter, A. T., Rindskopf, D. & Sher, K. J. (Red.). *APA Handbook of Research Methods in Psychology; Vol 2. Research Designs Quantitative, Qualitative, Neuropsychological, and Biological* (pp.57-71). American Psychological Association.

analyse van krantenartikelen en sociale-media statements maakte de bestudering van de twee case en bijbehorende beweegredenen mogelijk. De veelzijdigheid in databronnen reikt aanbevelingen aan. Beleid kan gebaat zijn bij de bevinding dat traditionele platformen en sociale media een ander beeld schetsen van de beweegredenen voor aanwezigheid bij coronademonstraties. De social-media statements tonen motivaties die in de traditionele media onderbelicht blijven. Krantenartikelen geven invulling aan de motivatie zoals beschreven in het thema verveling en sensatie. Het beeld dat ontstaat uit de thema's zelfverdediging en complot wordt in de traditionele media nauwelijks geschetst. Zonder social-media statements waren deze thema's niet aan de oppervlakte gekomen. De factor sociale media dient mede daarom te worden toegevoegd aan het flashpointsmodel. In het model is momenteel onvoldoende aandacht voor sociale media terwijl de opruiende en mobiliserende werking van online Telegramgroepen in zowel Amsterdam als Eindhoven groot bleek. Online speculaties, ongerustheid over de samenleving en corona-onzekerheid vormen de vonken die het anti-institutionalisme in vuur en vlam zetten.

De avondklokrellen in mensenrechtelijk perspectief (Denise de Boer, 2021)

In deze scriptie wordt de wijze waarop een maatregel zoals de avondklok zich verhoudt tot het grondrecht en het verdragsrecht behandeld. Over de grondslag van die maatregel is in de maatschappelijke en juridische praktijk veel kritiek geweest, waarbij deze maatregel in kort geding zelfs onrechtmatig werd verklaard. In het kader van de voorgenomen modernisering van het staatsnoodrecht wordt daarom onderzocht of de wijze waarop de avondklok juridisch is ingebed in overeenstemming

is met de Grondwet en het Europees Verdrag betreffende de Rechten van de Mens, en of binnen het Nederlands recht alternatieve mogelijkheden bestaan om een dergelijke maatregel in te stellen. Het onderzoek is uitgevoerd aan de hand van een analyse van juridische literatuur, wetgeving en parlementaire documenten.

Hoewel het instellen van een avondklok geen vrijheidsontneming in de zin van art. 15 Grondwet oplevert, wordt daarmee wel direct het recht op bewegingsvrijheid zoals gegarandeerd in art. 2 Vierde Protocol (hierna: VP) van het Europees Verdrag betreffende de Rechten van de Mens (hierna: EVRM) beperkt. Daarnaast beperkt de maatregel het recht op de eerbiediging van de persoonlijke levenssfeer van art. 8 EVRM en art. 10 Grondwet (hierna: Gw), en indirect de vrijheid van vergadering en betoging en het belijden van godsdienst en levensovertuiging als gegarandeerd door artikelen 9 en 10 EVRM en 6 en 9 Gw.

Voor het instellen van een maatregel met een dergelijke invloed op de mensenrechten is een deugdelijke juridische basis nodig, dient sprake te zijn van een legitieme doelstelling, moet de maatregel proportioneel en subsidiair zijn en moet de maatregel voldoende voorzienbaar en kenbaar zijn gemaakt. Uit het onderzoek vloeit voort dat de maatregel zoals deze in Nederland op basis van de Wet buitengewone bevoegdheden burgerlijk gezag (hierna: Wbbbg) - en later de Tijdelijke wet vertoeven in de openlucht - heeft gegolden, voldoet aan de eisen die het nationale en het verdragsrecht daaraan stellen.

Waar voor de beperking van de verdragsrechten geldt dat een noodverordening voldoende wettelijke basis kan zijn, is dat voor de beperking van

grondrechten niet zonder meer het geval. Het (geven van aanwijzingen ten aanzien van het, of voorzien in het) vaststellen van een noodverordening biedt daarom geen waardig alternatief. De noodverordening zou onder omstandigheden passend zijn om de periode tussen het bekend worden van de noodzaak van een maatregel en het uitvaardigen van een nationale maatregel bij Wbbbg.

Hoewel de Wet buitengewone bevoegdheden burgerlijk gezag als juridische grondslag de toetsing van het Gerechtshof Den Haag heeft doorstaan, is die grondslag stevig bekritiseerd. Daarbij is mede van belang dat de Wbbbg niet gecreëerd is met het oog op infectieuze ziekten: de achterliggende gedachte betreft de uitwendige en inwendige veiligheid van de staat, waarmee eigenlijk bedoeld werd op binnenlandse of buitenlandse vijanden. Het creëren van een specifieke bevoegdheid met het oog op de bestrijding van de verspreiding van infectieziekten, als *lex specialis*, brengt met zich mee dat het parlement de mogelijkheid heeft zich te buigen over de mate waarin zij dergelijke maatregelen in de toekomst willen toestaan, onder welke omstandigheden dat wenselijk geacht wordt, de wijze waarop een maatregel kan worden ingesteld en het daartoe bevoegde gezag.

⁸⁵ <https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/uw-online-oproep-heeft-consequenties>

⁸⁶ <https://ibestuur.nl/nieuws/online-ordeverstoringen-wat-kan-binnen-de-ap>

⁸⁷ <https://www.tubantia.nl/almelo/deskundigen-maken-gehakt-van-online-gebiedsverbod-van-almelo~a32663f9d/> ;<https://www.rtvooost.nl/nieuws/2169790/expert-zet-vraagtekens-bij-almelose-aanpak-online-oproerkrakers-moet-dit-wel-in-de-apv>

⁸⁸ <https://www.nrc.nl/nieuws/2023/02/07/halsema-geeft-niet-op-en-probeert-alsnog-een-online-gebiedsverbod-in-te-voeren-a4156425>

⁸⁹ Buitenhuis, M. & Bantema, W. (2023). *De burgemeester, burgervader handhaver van de openbare orde en sheriff van het internet. Kunnen burgemeesters met een internetverbod optreden tegen een verstoring van de openbare orde met aanleiding in het onlinedomein. Gemeentestem, 2023-8.*

4.4 Valoriserende activiteiten

Er zijn diverse valoriserende activiteiten geweest sinds er gesproken wordt van het lectoraat 'Bestuur in een Digitaliserende Samenleving'. Zo is er aandacht besteed aan het onderzoek dat we hebben uitgevoerd voor Noord-Holland Samen Veilig (NHSV) naar de regionale aanpak van online aangejaagde ordeverstoringen.⁸⁵ Daarnaast is er veel aandacht geweest voor het verschijnen van ons onderzoek naar de mogelijkheden de APV biedt om online aanjaging aan te pakken.⁸⁶ Vervolgens heb ik als lector nog op verschillende momenten gereageerd op het nieuws rondom de aanpak van gemeenten, bijvoorbeeld als reactie op de APV van de gemeente Almelo⁸⁷ en het voornemen van de gemeente Amsterdam om de Gemeentewet creatief toe te passen.⁸⁸ Tevens heb ik samen met Mariëtta Buitenhuis van AKD een opiniebijdrage geschreven voor de Volkskrant in het afgelopen jaar om de maatschappelijke discussie over 'online gebiedsverboden' verder aan te zwengelen. Dit is gebaseerd op een wetenschappelijke publicatie die we samen schreven.⁸⁹ Hieruit komen ook verschillende vragen naar voren die aanvullend onderzoek behoeven.

Net als in overige jaren is er ook veel gedaan aan kennisoverdracht. Zo zijn er lezingen verzorgd voor het VNG Juridische congres (oktober 2022), voor een congres van het RBO en het RIEC in

Noord-Nederland, een presentatie voor cyber-burgemeesters, een lezing voor het Ministerie van BZK, een lezing op een congres over radicalisering en extremisme en een lezing voor de Raad van Toezicht van NHL Stenden Hogeschool. Recentelijk is er een lezing verzorgd op de Kennis-dag van NHL Stenden (Research Talk), voor een congres van studenten van Dorknoper (Rijksuniversiteit Groningen) en er zullen nog meer lezingen volgen in 2023. Dit jaar zal voor het vierde achtereenvolgende jaar weer een bijdrage worden geleverd aan het vak 'de cyberburgemeester' dat via PLBQ en het Nederlands Genootschap van Burgemeesters wordt aangeboden. Bij dit vak verzorgt het lectoraat elk jaar een hele dag onderwijs waarin actuele kennis uit eigen en andere onderzoek wordt toegepast op de werkpraktijk van burgemeesters. Dat is een mooie verbinding tussen kennis en praktijk met directe doorwerking. Het meest uniek in 2023 is de bijdrage die recent is geleverd aan de Tweede Kamer waar een rondetafelgesprek heeft plaatsgevonden over de toekomst van 'online gebiedsverboden'. Hiertoe zijn de bestuurlijke praktijk, experts en de uitvoeringspraktijk gevraagd in verschillende deelsessies (de lector nam deel). Vooraf werd gevraagd de inbreng samen te vatten in 2 A4 als een position paper. Onderstaand heb ik deze integraal opgenomen omdat het een mooi beeld geeft van een groot deel van ons portfolio op dit specifieke terrein en onze visie op de toekomst op dit specifieke terrein:

4.4.1 Position paper – Onderzoeksgroep Cyber-safety – NHL Stenden Hogeschool/Thorbecke Academie

Ik wil met deze position paper argumenten voor- en tegen ter overweging meegeven. Dat gaat verder dan alleen de juridische kijk op het vraagstuk.

1. Noodzakelijkheid en wenselijkheid

Hoe groot is het probleem? Uit onderzoeken die in twee regio's zijn uitgevoerd blijkt dat gemeentebtenaren aangeven dat online aangejaagde ordeverstoringen vaker voorkomen dan voor Covid-19.⁹⁰ Naast online aangekondigde demonstraties komen ook ook drillrap-problematiek en pedojagen naar voren. De verspreiding van desinformatie is een ander vaker gehoord voorbeeld. In Coronatijd zagen gemeenten ook een toename in het verspreiden van desinformatie.

Het is niet te verwachten dat de ordeverstoringen die online aangejaagd de komende jaren zullen verminderen. Naast Project X in Haren (2012) zijn er nog oudere voorbeelden van het gebruik van technologie voor het organiseren van rellen. In 1997 organiseerden hooligans bijvoorbeeld per SMS een vechtpartij bij Beverwijk, waarbij één dode viel. Vandaag de dag speelt digitale communicatie een rol bij veel ordeverstoringen en demonstraties.⁹¹ Wie dus anno 2023 nog verrast is, heeft niet opgelet. Na de lange aanloop waarin het fenomeen is gegroeid, zijn online aangejaagde ordeverstoringen tegenwoordig geen bijzonderheid meer. Eerder lijken nu

ordeverstoringen die niet online worden aangejaagd de uitzondering. Het is te verwachten dat dit zich de komende jaren nog verder gaat ontwikkelen. Zo bezien lijkt handhaving zeker noodzakelijk. Het is goed om te beseffen dat de fenomenen in Coronatijd een heel ander karakter hebben dan voorbeelden zoals Project X in Haren. Eén van die verschillen is de toename van interactie tussen online en offline, zo wordt er ook tijdens rellen gefilmd (live) en opnieuw gedeeld waardoor er weer nieuwe spanningen ontstaan.⁹² De mogelijke komst van de Metaverse en de toenemende mogelijkheden van kunstmatige intelligentie kunnen ook weer nieuwe dimensies en spanningen opleveren.⁹³

Er zijn al middelen om als gemeente op te kunnen treden tegen online aangejaagde ordeverstoringen. Dit betreft onder meer het in gesprek gaan met burgers of organisaties en via het maken van afspraken en stopgesprekken de situatie te beëindigen. Daarnaast biedt het strafrecht mogelijkheden via de aanpak van opruiing (achteraf) en kan ook achteraf schade worden verhaald op overtreeders.⁹⁴ Er zijn ook privaatrechtelijke mogelijkheden die in bepaalde omstandigheden benut kunnen worden.⁹⁵ Meer onderzoek naar deze route is nodig. Ten aanzien van wenselijkheid en noodzaak wil ik nog twee overwegingen meegeven. Ten eerste is de burgemeester verantwoordelijk voor de handhaving

van de openbare orde en veiligheid. We zien tegelijkertijd dat er steeds meer online onveiligheid plaatsvindt⁹⁶ en dat bij vrijwel elk openbare ordezaakstuk sociale media en het internet een rol spelen. Wanneer de keuze wordt gemaakt om de burgemeester geen bevoegdheden toe te kennen in het online domein zal diens lokale positie in het veiligheidsbeleid op (korte) termijn door ontwikkelingen tenietgedaan worden. Ten aanzien van de wenselijkheid is het ook nodig om maatschappelijk debat hierover te voeren en daarnaast behoeften en ervaringen van alle burgemeesters in kaart te brengen. Uit eerder onderzoek blijkt namelijk dat er onderling veel verschil in opvattingen bestaat.⁹⁷

2. Bestuursrechtelijke juridische grondslag voor optreden door burgemeesters

NHL Stenden hogeschool heeft meerdere onderzoeken gedaan op dit terrein. Complicerende factoren bij de online inzet van bevoegdheden zijn de diffuse en indirecte relatie tussen online gedragingen en offline effecten (causaliteit), wetgeving die stamt uit een pre-internet tijdperk en het feit dat alle gedragingen op het internet uitingen zijn en dat de meeste daarvan worden beschermd door de vrijheid van meningsuiting.⁹⁸ In Utrecht heeft de gemeente naar analogie een bestaand APV artikel toegepast waarbij men vooral is teruggefloten omdat het artikel niet bedoeld zou zijn

⁹⁰ Zie: S. de Vries & W. Bantema, Aanpak in kaart. Inzicht in een regionale aanpak van online aangejaagde ordeverstoringen. Leeuwarden: Onderzoeksgroep Cybersafety 2022; W. Bantema e.a., Juridische grenzen en kansen bij openbare-ordehandhaving. Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen. Onderzoeksgroep Cybersafety 2022.

⁹¹ Zie onder andere: W. Stol & W. Bantema, Lokaal bestuur in een digitaliserende samenleving. Essay over een stap in de ontwikkeling: een handelingskader. Onderzoeksgroep Cybersafety 2021.

⁹² H. Moors e.a., Avondklokrellen, lokale dynamiek in een mondiale crisis. Emma 2022.

⁹³ Onder andere: B.W. Schermer & J. van Ham, Regulering van immersieve technologieën. WODC 2021.

⁹⁴ ECLI:NL:RBOVE:2018:3656.

⁹⁵ ECLI:NL:RBDHA:2022:10082.

⁹⁶ Zie onder andere: M. Huijstee e.a., Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Rathenau Instituut 2021.

⁹⁷ W. Bantema e.a., Niet bevoegd, wel verantwoordelijk? Handhavingmogelijkheden bij online aangejaagde ordeverstoringen, Den Haag: Boom Bestuurskunde, 2020.

⁹⁸ Zie ook al ons onderzoek in 2018: W. Bantema e.a., Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld. Den Haag: SDU Uitgevers 2018.

voor virtuele openbare ruimten. Een herformulering van dat artikel kan dat oplossen (zie bijvoorbeeld gemeente Almelo) maar gaat wel voorbij aan het feit dat grondrechten niet beperkt kunnen worden via een APV. Het is dus niet afdoende om de tekst aan te passen. Nieuwe experimenten met de APV zullen naar verwachting juridisch weinig opleveren.⁹⁹ Als de politieke conclusie is dat burgemeesters bevoegdheden moeten krijgen zal daarvoor nieuwe wetgeving in het leven geroepen moeten worden, bijvoorbeeld door de Gemeentewet aan te passen.

3. Handhaving en uitvoering

Naast een juridische grondslag dient er ook rekening te worden gehouden met handhaving en uitvoering. Uit de regionale verkenningen van NHLs komt naar voren dat gemeenten problemen zien rond de capaciteit bij de uitvoering, maar ook in de kennis en kunde van het personeel om te kunnen signaleren en interveniëren. Ook wordt verwezen naar het grensoverschrijdende karakter van de online oproepen tot ordeverstoringen. Daarnaast kunnen ook de anonimiteit van online oproepen en het controleren van een dergelijke maatregel tot problemen leiden.¹⁰⁰ Uit eerder onderzoek blijkt dat gemeenten geen bevoegdheid hebben om personen online te monitoren.¹⁰¹ Naast organisatorische en kennisvraagstukken spelen ook hier vraagstukken rondom grondrechten en privacy bij de controle van 'online

gebiedsverboden'. Tot slot is ook de vraag in hoeverre gemeenten zijn toegerust op de massaliteit van het internet en bijvoorbeeld de toename van geautomatiseerde trollenlegers en of gemeenten in staat zijn om de berichten offline te krijgen.¹⁰²

Ter overweging

Gezien de maatschappelijke ontwikkelingen rondom veiligheid en digitalisering is het bijna ondenkbaar dat burgemeesters op termijn geen zeggenschap krijgen over online vraagstukken die raken aan hun gemeentelijke openbare orde. Tegelijkertijd zijn maatschappij en gehele burgemeestersgilde nog onvoldoende geraadpleegd ten aanzien van wenselijkheid en behoeften en is het ontwikkelen van uitgebalanceerde wetgeving die burgemeesters helpt om de orde te handhaven en tegelijkertijd de burgers beschermd tegen willekeur van de overheid – nog een hele opgave. Hoe dan ook zou het politieke en maatschappelijke debat zich niet moeten richten op creatief gebruik van het recht in het hier en nu maar zich eerder op een effectieve en uitvoerbare route op de lange termijn. Mochten burgemeesters daarin een rol krijgen dan is een bredere aanpak en nieuwe wetgeving essentieel.

⁹⁹ W. Bantema e.a., Juridische grenzen en kansen bij openbare-ordehandhaving. Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen. Onderzoeksgroep Cybersafety 2022.

¹⁰⁰ M. Buitenhuis & W. Bantema, De burgemeester: burgervader, handhaver van de openbare orde en sheriff van het internet? (deel 2). Kunnen burgemeesters met een internetverbod optreden tegen een verstoring van de openbare orde met aanleiding in het onlinedomein. Gemeentestem 2023-8.

¹⁰¹ W. Bantema e.a., Black box van online monitoring: een wankel fundament onder een stevige praktijk. Den Haag: Sdu uitgevers 2021.

¹⁰² <https://www.volkskrant.nl/columns-opinie/wat-moet-je-als-burgemeester-als-toffepeer01-online-oproept-om-bij-de-dorpspomp-een-avondje-te-rellen~b03a63e9/>

4.5 Onderzoekslijnen en onderzoeksthema's van het lectoraat

4.5.1 Inleiding

De onderzoeken van het lectoraat zijn de eerste vijf jaar vooral gericht geweest op bevoegdheden en online monitoring door gemeenten. In die onderzoeken zijn naast juridische en organisatorische vragen ook verschillende ethische vraagstukken blootgelegd en er is duidelijk naar voren gekomen dat op deze terreinen gemeenten op zoek zijn naar meer handelingsperspectief en er ook te winnen is een capaciteit en kennis en kunde van medewerkers op dit terrein. Onderzoek kan bijdragen aan inzicht in fenomenen en vergroot van bewustzijn (en anticiperen) ten aanzien van digitalisering en ontwikkelingen op dat gebied, in randvoorwaarden voor (effectief) beleid en – meer nodig dan ooit – zal dit lectoraat aandacht vragen voor maatschappelijke en burgeropvattingen over handelen en beleid in een digitaliserende samenleving en dit betrekken als een van de randvoorwaarden voor effectief en goed bestuur in een digitaliserende samenleving. Dit is samen te vatten in de volgende lijnen die conceptueel van elkaar te scheiden zijn maar in de praktijk met elkaar samenhangen en soms zelfs door elkaar lopen:

- A. Anticiperen op uitdagingen in digitalisering en maatschappij
- B. Bijdragen aan effectief en goed bestuur en beleid in een digitaliserende samenleving
- C. Betrekken van het maatschappelijke en burgerperspectief bij beleid en bestuur

4.5.2 Anticiperen op uitdagingen in digitalisering en maatschappij

Het gaat hierbij om het oog hebben voor maatschappelijke ontwikkelingen en technologische ontwikkelen, inschatten wat de gevolgen daarvan zijn en kennis en informatie continu uit te wisselen met verschillende stakeholders. Wanneer bijvoorbeeld duidelijk is dat er gevolgen zijn voor de veiligheid en we het noodzakelijk achten dat er beleid of maatregelen nodig zijn, is vaak voorafgaand aan beleid en uitvoering aandacht en discussie nodig voor bevoegdheden en verantwoordelijkheden. We zien dat deze discussie bijvoorbeeld naar voren is gekomen (en nog steeds gaande is) wanneer het gaat om de rol van burgemeesters bij de aanpak van online aangejaagde ordeverstoringen en de rol en bevoegdheden van gemeenten bij online signalering van onveiligheid. Het anticiperen op wat gaat komen staan centraal in deze onderzoekslijn. Mogelijke vragen hierbij zijn, los van het thema, wat zijn de gevolgen van fenomeen X voor de veiligheid van gemeenten (bijvoorbeeld). Ik wil hier twee voorbeelden aandragen van thema's waar het lectoraat een belangrijke rol ziet weggelegd in de agendering. Onderzoeken zoals 'burgemeesters in cyberspace' en 'black box van online monitoring' zijn voorbeelden van onderzoeken die goed passen bij de agenderende kracht van ons lectoraat. De nieuwe verkennende studie naar de lokale effecten en handelingsperspectieven ten aanzien van buitenlandse inmenging bij verkiezingen (of breder) past ook goed in dit rijtje. In ieder geval wil ik hier nog een aantal thema's noemen die goed passen bij de agenderende en signalerende functie die ons lectoraat vervult.

Digitale veiligheid van evenementen

In veel gemeenten is evenementenveiligheid op zijn meest een speerpunt in veiligheidsbeleid en op zijn minst een aandachtspunt. De gemeente en met name de burgemeester heeft bevoegdheden om voorwaarden te stellen aan evenementen en al dan niet een vergunning te verlenen. Openbare orde en veiligheid maakt een belangrijk onderdeel uit van de afweging om evenementen al dan niet doorgang te laten vinden. Wanneer bepaalde risico's over het hoofd worden gezien kan dat grote gevolgen hebben.

Evenementen staan door verschillende ontwikkelingen in de spotlights. Zo is recentelijk veel aandacht geweest voor de vreugdevuren in Den Haag, waar eerder een vergunning voor werd afgegeven in 2018. Het gevolg was een grote vonkenregen en meerdere branden in Den Haag en uiteindelijk het politiek aftreden van de burgemeester. Daarnaast worden in toenemende mate evenementen vergund. Dit maakt dat evenementen een reëel en frequent veiligheidsrisico zouden kunnen vormen voor de openbare orde en veiligheid binnen gemeenten. Daarnaast zijn er signalen dat door een tekort aan handhavingscapaciteit ook steeds vaker technologie, zoals drones, worden ingezet om tegen lagere kosten alsnog voor voldoende veiligheid te kunnen zorgen.

Tegenwoordig omvat veiligheid ook digitale veiligheid. Het is dus voor de handhaving van de openbare orde van belang dat evenementen vooraf ook op hun *digitale* veiligheid worden beoordeeld.

Opvallend genoeg is er nog maar weinig aandacht voor de digitale (veiligheids)aspecten van evenementen. Uit een recent onderzoek blijkt dat geen van de 27 willekeurig geselecteerde gemeenten in openbare beleidsstukken aandacht besteedt aan de digitale veiligheid van evenementen.¹⁰³ Een gesprek met burgemeesters op de Lochemconferentie van het NGB van februari 2019 liet zien dat burgemeesters zoekende zijn en er behoefte is aan meer duidelijkheid over verantwoordelijkheden en bevoegdheden op dit specifieke thema. Hoewel er bij ons weten geen evenementen door digitale oorzaak zijn uitgelopen op een ramp of crisis, is door verdergaande digitalisering dit wel een reëel risico waar op zijn minst expliciet rekening mee moet worden gehouden. Als bij de beoordeling vooraf veiligheidsaspecten over het hoofd worden gezien, kan dat tot problemen leiden tijdens het evenement en dus ook de politie voor extra werk plaatsen. Gebrek aan aandacht voor digitale veiligheid vóóraf, kan er toe leiden dat tijdens het evenement problemen ontstaan doordat apparatuur (bv. een kermisattractie, vuurwerk, tekstbord) door onbevoegden wordt ontregeld of overgenomen. Maar ook valt te denken aan ticketfraude, het platleggen van optredens en diefstal van content of vertrouwelijke gegevens (privacy inbreuk) bij gebruik van veiligheidsapps.

Er zijn bij ons weten nog geen evenementen vanwege een digitale oorzaak uitgelopen in een ramp of crisis. Er was bijvoorbeeld nog geen 'Haaksbergen digitaal' en er is nog geen evenement vanwege een hack of DDoS-aanval op een ramp

¹⁰³ Stol, W.Ph. en W. Bantema (2020). Stadsbestuur en digitale veiligheid. Een analyse van beleidsplannen. In M. Malsch en J. W. Sap (red.) *Orde en verwarring in de stad*. Den Haag: Boom Criminologie, pp. 363-385.

uitgedraaid. Het is evenwel onverstandig om de primeur daarvan af te wachten. Vandaar dit onderzoeksvoorstel over de digitale veiligheid van evenementen. Complicerende factoren rondom dit thema zijn onbekende risico's, een laag bestuurlijk bewustzijn en onduidelijkheid over verantwoordelijkheid. Veel verschillende actoren spelen een rol bij evenementen, zoals evenementenorganisatie, derden voor apparatuur, de gemeente, politie, de Veiligheidsregio en mogelijke andere actoren.

Samengevat is er hard onderzoek nodig op dit terrein. We kennen geen gemeente die expliciet aandacht besteedt aan de digitale veiligheid van evenementen en een actieve bestuurlijke aanpak ervan najaagt. Ook bijzonder is dat digitale veiligheid en/of cyber aansluit bij een breder bekende en erkende openbare orde portefeuille van evenementenveiligheid, terwijl in veel gemeenten digitale veiligheid en of cyber een afzonderlijk beleidsdomein is. Daarnaast zijn er mogelijk ook risico's bij nieuwe en moderne typen evenementen (LAN-parties, hackevenementen) die in de toekomst steeds vaker op gemeentelijk grondgebied kunnen plaatsvinden. In een verkenning voor de VNG hebben we aangegeven dat we digitale veiligheid van evenementen als een centrale gemeentetaak zien. Het is niet relevant of deze nu valt onder 'eigen huis op orde' of onder de 'regierol en cyberweerbaarheid' binnen gemeenten, belangrijk is dat gemeenten hier mogelijk een belangrijke bijdrage kunnen leveren aan een grotere (digitale) veiligheid van evenementen.

¹⁰⁴ Zie ook: Ter Varst, L., Groenendaal, J., Bantema, W., & Cools, F. (2023). *Bestuurlijke bevoegdheden cyber. Bevoegdheden en interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio bij (dreigende) digitale incidenten*. Arnhem: NIPV.

Het is dus hoog tijd om hier verder onderzoek naar te doen. Ons lectoraat kan hierbij ondersteunen door aandacht te besteden aan vragen over de soorten evenementen en eventuele risico's die daarbij spelen, aandacht te besteden aan de actoren die een rol spelen en hun visie op digitale veiligheid van evenementen. In het bijzonder valt dan te denken aan de organisatoren van evenementen en gemeenten die een centrale rol spelen in de vergunningverlening. Als inzichtelijk is welke evenementen er zijn welke typen digitale risico's te onderscheiden zijn is vervolgens de vraag hoe groot die risico's zijn en hoe deze verminderd kunnen worden. Vanzelf komen er dan ook vragen over verantwoordelijkheid en bewustzijn van risico's. Onder andere is de vraag of gemeenten hier een belangrijk rol zouden kunnen spelen en hoe organisatoren van evenementen, indien nodig (we verwachten van wel) gemotiveerd kunnen worden om hun evenementen meer digitaal veilig te organiseren. Mocht de gemeente hier een centrale rol spelen dan is eveneens de vraag hoe zijn dat moeten vormgeven en of er voldoende kennis en expertise is om dit te kunnen controleren en handhaven.¹⁰⁴ Uiteraard zal ook naar de mogelijkheden en rollen van andere partijen worden gekeken. Op dit moment voeren onze studenten op verschillende plekken ook opdrachten en kleine onderzoeken uit op dit terrein. We werken graag samen met andere organisaties om dit vraagstuk op de kaart te zetten en verder bij te dragen aan effectief beleid en werkwijzen om de digitale veiligheid te vergroten.

Metaverse

Een heel ander thema dan digitale veiligheid van evenementen betreft de zogenaamde metaverse. Dit is iets wat nog niet erg leeft maar waarin we al veel kunnen leren van technieken die al op kleine schaal worden toegepast. We hanteren de definitie van het Rathenau Instituut hier als uitgangspunt. De metaverse is te beschouwen "als een visie op de digitale omgeving van de toekomst, waarin we met elkaar contact hebben, werken en leven".¹⁰⁵ We gaan kort in op een aantal uitdagingen die technologische ontwikkelingen met zich meebrengen.

Het bekendste Nederlandse onderzoek is van de hand van Considerati,¹⁰⁶ die voor het WODC ingingen op de kansen en risico's bij de regulering van immersieve technologie. Deze technologie (zowel *virtual reality* en *augmented reality*) maken deel uit van de 'metaverse'. De volgende vraagstukken komen naar voren: (1) Schadelijke en illegale gedragingen in virtuele werelden, (2) schadelijke gevolgen door het gebruik van immersieve technologieën in de fysieke wereld, (3) schadelijke effecten door het gebruik/misbruik van immersieve technologieën; (4) sociaal-maatschappelijke vraagstukken en (5) misbruik door derden.

Bij het eerste aspect gaat het over *virtual reality*. Door gebruik van technologie kunnen we ons op een andere manier representeren. Naast ons fysieke lichaam kunnen we ook plaatsnemen in een virtueel lichaam. Zo kan je op die manier bijvoorbeeld voetbalwedstrijden of winkels bezoeken of gaan werken in verschillende delen van de virtuele

wereld. De ervaringen zullen onze fysieke ervaringen dichterbij benaderen dan het huidige internet. Er zijn al veel toepassingen hiervan, bijvoorbeeld in de game-wereld en in het onderwijs. Binnen Thorbecke Academie van NHL Stenden Hogeschool worden dit onder andere al benut binnen HBO-rechten om deelname aan rechtszaken na te bootsen. De VR-hoofdsets zijn nog duur en nog niet voor iedereen toegankelijk. Bij deze toepassing is het op termijn allicht mogelijk om je tussen virtuele werelden te bewegen. *Virtual reality* kan onder andere leiden tot nieuwe juridische vraagstukken want wat is de juridische status van het virtuele lichaam en wat betekent dit voor aanranding. Klassieke uitingsdelicten zoals belediging en bedreiging kunnen ook plaatsvinden. Heel concreet kan bijvoorbeeld gedacht worden aan het maken van een avatar (een virtuele representatie van een persoon) naar het uiterlijk van een echt persoon. Virtuele aanranding kan dan heel dichtbij komen en als echt worden ervaren. In het huidige recht, nog voor dat dit speelt, zien we al voorbeelden die hieraan doen denken. Voor het tweede aspect, dat we hier kort zullen noemen, gaat het vooral over afleiding door immersieve technologie en bijvoorbeeld gevaren in het verkeer.

Bij het derde aspect gaat het om de relatie tussen immersieve technologie en moraliteit. Daar is nog relatief weinig over bekend. Worden mensen bijvoorbeeld agressiever of angstiger door immersieve ervaringen en of kunnen mensen afwijkend gedrag gaan vertonen na het hebben van (extreme) virtuele seksuele ervaringen? Dit was

de belangrijkste reden volgens de onderzoekers van Considerati om het onderzoek naar immersieve technologie uit te voeren. Zaken als verslaving en vervreemding zijn effecten die niet nieuw zijn als we bijvoorbeeld kijken naar de game industrie.

Bij het vierde aspect, gaat het om *augmented-reality* en nieuwe vraagstukken op sociaal-maatschappelijk vlak. AR-systemen brengen een omgeving tot stand waarbij een virtuele laag over de fysieke omgeving komt te liggen. Zo ontstaat een nieuw type hybride omgeving, die zowel fysiek als virtueel is.¹⁰⁷ Hierdoor wordt het mogelijk om bijvoorbeeld een virtueel standbeeld op straat te zien. Er zijn al voorbeelden hiervan. Denk bijvoorbeeld aan het spel Pokémon Go, waarbij je via je mobiele telefoon animatiefiguren over straat ziet lopen. Dit leidde onder andere tot ongewenste bezoeken op private plekken en zelfs grote ordeverstoringen op plekken waar zogenaamde zeldzame Pokémons zouden zitten, ook biedt het kansen aan cybercriminelen om gebruikers te volgen.¹⁰⁸ Dit roept vragen op over privacy en omgangsvraagstukken op het sociale vlak. Dit is begrijpelijk door de grote hoeveelheid camera's, chatdiensten, enzovoort die hier een rol kunnen spelen. Het meest spannende aspect is dat personen naar hetzelfde kunnen kijken maar wel verschillende dingen zien, omdat zij een andere aangevulde werkelijkheid zien of ervaren.

Daarnaast is het, nu ook al, lastig vast te stellen wat echt is en wat nep (zie ook hoofdstuk 2 en 3).

Tot slot kan de technologie ook gebruikt worden om anderen te misleiden en te manipuleren, bijvoorbeeld door het gebruik van data (effecten van waarnemingen kunnen worden gemeten). Dit biedt ook kansen voor mensen met minder goede bedoelingen zoals cybercriminelen. In lijn met ons onderzoek naar burgemeesters in cyberspace is ons lectoraat ook geïnteresseerd in de juridische vraagstukken die er op ons afkomen en wat dit betekent. Onder andere kan de strafrechtelijke normering van ongewenste gedragingen tot problemen leiden. Zo is bijvoorbeeld virtuele aanranding niet strafbaar, het misbruiken van echte personen in virtuele omgevingen is niet strafbaar gesteld. De worsteling met het recht met het eerste aspect komt naar voren in een veel eenvoudiger zaak. Zo is er in 2018 een zaak waarbij iemand een Pokémon spel bewerkt waarbij de stenen in het spel niet meer op de Pokémon komen maar op het hoofd van een bestaande agent die op de Pokémon was geplakt. Deze agent deed aangifte. De verdachte werd uiteindelijk vrijgesproken van bedreiging en opruiing.¹⁰⁹ Dit onder meer omdat het ging om het dreigen met het gooien van virtuele stenen naar virtuele figuurtjes. In de ogen van de rechter zijn deze figuurtjes geen personen, noch maken zij onderdeel uit van het openbaar gezag, zodat er niet sprake was van strafbare bedreiging en opruiing. Volgens Considerati gaat het verder nog om juridische vragen over het misbruiken van beelden van personen, afleiding door het gebruik van technologie, effecten van technologie op mens

¹⁰⁵ Definitie van Rathenau Instituut, zie: <https://www.rathenau.nl/nl/digitalisering/wat-de-metaverse>.

¹⁰⁶ B.W. Schermer & J. van Ham, Regulering van immersieve technologieën. WODC 2021.

¹⁰⁷ Snijders, D., S. Horsman, L. Kool, R. van Est (2020). Responsible VR. Protect consumers in virtual reality.

The Hague: Rathenau Instituut.

¹⁰⁸ <https://blog.sbo.nl/veiligheid/pokemon-go-onschuldig-spelletje-cybersecurity-nachtmerrie/>

¹⁰⁹ ECLI:NL:RBROT:2018:5142

en gedrag en sociaal maatschappelijke veranderingen die het gevolg kunnen zijn. Ook vragen over intellectueel eigendom kunnen een rol spelen – wat als een student NHL Stenden Hogeschool helemaal virtueel namaakt en in verschillende virtuele ruimten gebruikers toelaat om activiteiten te verrichten die, laten we het voorzichtig zeggen, in strijd zijn met de normen en waarden van de fysieke NHL Stenden Hogeschool. Ons lectoraat zal de ontwikkelingen nauwgezet volgen op dit terrein en het vraagstuk ook verder uitwerken.

4.5.3 Bijdragen aan effectief en goed bestuur en beleid in een digitaliserende samenleving

Deze lijn sluit aan bij eerder genoemde kernvragen rond bestuur in een digitale samenleving. Wanneer gemeente en politie besluiten dat ze ergens verantwoordelijk voor zijn is de vraag welke bevoegdheden ze hebben, zouden moeten hebben en welke andere maatregelen mogelijk ingezet kunnen worden. Het lectoraat heeft hier de nodige aandacht aan besteedt in relatie tot bevoegdheden van burgemeesters en andere interventies die door gemeenten ingezet kunnen worden om online aangejaagde ordeverstoringen aan te pakken. Recent komt dit ook naar voren in het project Connect waar we proberen de gemeente Amsterdam te helpen bij hun preventieve online aanpak van onder andere drillrap-problematiek die daar speelt. We dragen samengevat bij aan kennis over effectieve en uitvoerbare werkwijzen. Dit betekent dat er ook veel aandacht is voor organisatorische randvoorwaarden. In het bijzonder willen we hierbij aandacht vragen voor ethiek als een van de randvoorwaarde. In hoofdstuk drie is dit al beschreven als een belangrijke randvoorwaarde voor beleid van gemeenten en politie (en andere organisaties). Ethiek speelt niet alleen in relatie tot veiligheid maar ook breder.

Beleid wat effectief is maar in strijd is met wat burgers en de maatschappij wenselijk en belangrijk vinden zal op termijn de legitimiteit van het overheidsoptreden kunnen schaden. Daarom vinden wij het belangrijk dat de opvattingen van maatschappij en inwoners in relatie tot overheidsbeleid en digitalisering worden meegenomen in de gekozen aanpak en of beleid. Om het thema extra gewicht te geven en te laten zien hoe belangrijk we het vinden hebben we een derde lijn toegevoegd om dat te benadrukken. In het eerste voorbeeld is het perspectief van de burger expliciet meegenomen in een experimenteel onderzoek waar ons lectoraat bij betrokken is.

Online interacties tussen overheid en inwoners

Eerder in hoofdstuk drie is aandacht besteed aan bevoegdheden in het digitale domein. Er blijkt weinig bekend te zijn over een effectieve inzet van niet-juridische interventies (overwegend communicatie) om te kunnen de-escaleren. In het project 'Connect' dat ons lectoraat uitvoert in opdracht van de gemeente Amsterdam wordt gekeken naar literatuur over effectieve (online) interventies en best practices. Online interventies worden relatief weinig ingezet of worden niet als dusdanig bestempeld omdat ze al in een vroeg stadium plaatsvinden. Mede door verwachte juridische problemen en koudwatervrees lijkt er niet een ontwikkelde praktijk van online interventies te zijn en is er eveneens weinig literatuur over de effectiviteit van online interventies in handhavingsrelaties. Dit was voor ons reden om in het verlengde van het project 'Connect' in dit geval via Politie en Wetenschap een vervolgstudie te starten (de Rijksuniversiteit Groningen was deze keer voortrekker van het voorstel) om deze wetenschappelijke en praktische lacune op te vullen (en het voorstel voor dat project

is gehonoreerd). In dit geval is het project gericht op de politieorganisatie maar uit eerder onderzoek in de context van openbare orde en gemeenten zien we dat ook daar weinig wordt gedaan met communicatieve interventies via sociale media (bijvoorbeeld om ordeverstoringen te voorkomen) en dat we ook weinig weten over werkzaamheid. De meerwaarde van het onderzoek gaat dus breder dan de politie en kan relevant zijn voor een breed palet aan toezicht en handhavingsrelaties.

In het voorstel is onder andere de vraag gesteld hoe de politie haar handhavende rol online kan waarmaken zonder voor opschudding te zorgen. Welke factoren beïnvloeden de effectiviteit van online interacties tussen politie en burgers? De politie mengt zich al langer in het debat op sociale media, met name als het gaat om online opruiming. In 2015 bijvoorbeeld belden agenten aan bij mensen die online haatzaaiende berichten postten over vluchtelingenopvang in Leeuwarden. Politiechef Dros postte na het online aangejaagde geweld op Koningsdag 2021 een bericht op Facebook: "Jij, toetsenbordheld op sokken. Het is niet de vraag of, maar wanneer we je komen halen." Politiechef Schäfer-Poels besloot rondom de Rotterdamse coronarellen in 2021 om een aantal hatelijke reageerders op Instagram een persoonlijk bericht te sturen: "Wat is er gebeurd dat je zo kwaad bent op de politie?".

Het recht loopt achter op maatschappelijke ontwikkelingen op digitaal gebied, waardoor juridische interventies problematisch kunnen zijn. Zelfs als juridische interventies houdbaar zijn, blijken deze in de praktijk niet altijd uitvoerbaar en daadwerkelijk handhaafbaar. Dit beperkt de effectiviteit van dergelijke juridische interventies. Communicatie kan in die gevallen een heel krachtig instrument zijn,

met als voordelen dat men deels buiten problematische juridische kaders blijft en mogelijk wel aan de "voorkant" het gedrag van burgers preventief kan beïnvloeden en bijsturen. Ook wanneer je niet weet wie ergens achter zit biedt communicatie aanvullende kansen die het recht niet biedt. Doel van het nieuwe project is om de essentiële stap van pionierswerk naar evidence-informed blauwe inzet op sociale media te kunnen maken. Daarmee wordt beoogd kennis te produceren die kan bijdragen aan de beleidsvorming rondom actuele problemen (zoals wanneer en hoe te reageren op doxing) en rondom de ontwikkeling van digitalisering bij zowel criminaliteit alsook bij openbare-ordevraagstukken en politiewerk in het algemeen. De lessen die dit project gaat opleveren zijn breder toepasbaar dan alleen op de politie. Ook voor gemeenten kan dit veel relevante resultaten opleveren die kunnen bijdragen aan online werken op het terrein van onder andere de openbare orde en veiligheid.

Om de effectiviteit van politie-inzet te waarborgen, is het bovendien van belang dat de gebruikte methode niet schadelijk is voor het algemene vertrouwen van burgers in de politie en de mate waarin de politie door burgers als legitiem wordt gezien. Het is daarom van belang om ook burgerervaringen perspectieven mee te nemen. Dit nieuwe project dat in het najaar van 2023 start beoogt de bestaande kennis over de invloed van burgerperspectieven uit te breiden naar het online domein. We zullen dit onderzoek niet een isolement uitvoeren maar ook nadrukkelijk, zoals het hoort, studenten betrekken bij het thema van dit onderzoek via afstuderen en kleine onderzoeksopdrachten. De uitkomsten van dit onderzoek zullen ook de weg naar het onderwijs en de beroepspraktijk terugvinden.

Nieuwe vragen over de uitvoering van bestuursrechtelijke online handhaving

Ons lectoraat wil ook de komende jaren nog een belangrijke bijdrage richten aan vraagstukken over online handhaving, al dan niet via het bestuursrecht. Samen met Marietta Buitenhuis schreef ik hier een artikel over.¹¹⁰ De belangrijkste conclusies en vragen die een vervolg vereisen komen hier aan bod. Als eenmaal een juridische basis is gevonden voor het opleggen van het online gebiedsverbod, dan wordt het bij de uitvoering pas echt spannend. Zolang regels niet uitvoerbaar en handhaafbaar zijn kan gesteld worden dat ze amper nut hebben.

Wie zit er achter een oproep en bekendmaking van de maatregel

Eén van de uitdagingen die zich vanuit de bestuursrechtpraktijk bij een online gebiedsverbod voordoet, manifesteert zich bij de bekendmaking. Een probleem hierbij is dat men niet in alle gevallen weet wie er achter het opruiende bericht schuilgaat. Veel mensen die zich op het internet begeven doen dat anoniem of onder een alias. Het bekendmaken van een online gebiedsverbod zonder te weten van wie achter de gedraging of uitlating schuilgaat zal uitermate lastig zijn. Daarvoor zal veelal toegang tot een IP-adres moeten worden verschaft. Voorstelbaar is dat de burgemeester om het online gebiedsverbod te kunnen bekendmaken en handhaven, bij een socialemidiaplatform of internet-service-provider gegevens betreffende de naam, adres en

woonplaats (hierna: 'NAW-gegevens') en IP-adresgegevens moet opvragen. Nu het duidelijk is dat dit persoonsgegevens betreffen, dient voor het delen van deze gegevens een wettelijke grondslag te bestaan. Onder omstandigheden kan een grondslag daarvoor worden gevonden in een onrechtmatige daad.¹¹¹ Dit zal zich niet zomaar bij iedere verstoring van de openbare orde voordoen. Als het afdwingen van de NAW- en IP-adresgegevens via een onrechtmatige daad niet mogelijk is, zal daarvoor in een separate wettelijke grondslag moeten worden voorzien. In lijn met deze rechtspraak is het allerm minst zeker dat burgemeesters zomaar beschikking zullen krijgen over de IP-adressen van personen waarvan wordt aangenomen dat zij met hun berichten de openbare orde verstoord hebben. Dit aspect is wel essentieel voor een de uitvoering. Daar komt nog bij dat het verkrijgen van het IP-adres niet voldoende zal zijn om de overtreder te vinden. Om te achterhalen van wie binnen het huishouden de berichtgeving afkomstig is, zal ook toegang moeten worden verschaft tot de (fysieke) router.

Handhaving online gebiedsverbod

Gemeenten hebben zorgen geuit over de regels rondom en handhaafbaarheid van online ordeverstoringen. Een van de routes voor de handhaving van het verbod is de strafrechtelijke, bij de overtreding van een op grond van de APV of de Gemeentewet gebaseerde maatregel.¹¹² Dit gebeurt in samenwerking met de politie en het OM. Een andere route

is om het online gebiedsverbod bestuursrechtelijk te handhaven. Daarvoor zal niet kunnen worden ontkomen aan online monitoring (het in de gaten houden van het internet over wat er online gezegd wordt). Onlangs bleek uit onderzoek dat 95% van de gemeenten aan enige vorm van online monitoring doet, waarbij 60% van de gemeenten dit toepast binnen het openbare orde domein.¹¹³ De Ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Justitie en Veiligheid (J&V) werken momenteel aan een handreiking om het juridisch kader voor online monitoring te verhelderen.¹¹⁴ Naast de juridische mogelijkheden en beperkingen rondom online monitoring, spelen ook organisatorische belemmeringen een rol. Zo blijkt uit onderzoek dat gemeenten zich zorgen maken over de organisatorische capaciteit en specifieke kennis die online monitoring vraagt.¹¹⁵ Te denken valt aan juridische kennis, maar ook aan de vereiste kennis om online signalen goed te kunnen duiden. Een complicerende factor voor de gemeente is dat soms moeilijk is vast te stellen wie bij online gedrag waar verantwoordelijk voor is. Dat geldt zeker bij online groepen en groepsdynamiek. Stelselmatige monitoring zonder specifieke wettelijke grondslag komt al snel in strijd met artikel 8 EVRM wanneer er om de overtreding van een online gebiedsverbod te controleren gebruik wordt gemaakt van monitoringstools. In dit verband kan er ook aanvullende aandacht worden

besteed aan de informatie-uitwisseling binnen zogenaamde digikamers.¹¹⁶

Randvoorwaarden AVG

Verder kan niet voorbij worden gegaan aan de randvoorwaarden uit de Algemene Verordening Gegevensbescherming (hierna: de 'AVG'), waarvan we voor de politie een pendant kennen in de Wet politiegegevens. Voor het opleggen van een online gebiedsverbod is het nou eenmaal noodzakelijk om persoonsgegevens te raadplegen en daarmee verwerken. De gegevensverwerking door de burgemeester moet voldoen aan de voorwaarden die de AVG daaraan stelt. Zo dient de gegevensverwerking noodzakelijk en transparant te zijn, te voldoen aan de beginselen van proportionaliteit en subsidiariteit en gelden er documentatievereisten.¹¹⁷ Verder moet de verwerking voldoen aan de beginselen van doelbinding en moet er een grondslag voor de gegevensverwerking te bestaan. Met name de verwerkingsgrondslag vraagt voor het kunnen opleggen van een 'online gebiedsverbod' aandacht. Voor de verwerking moeten worden teruggevallen op de grondslag dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.¹¹⁸ De AVG vereist dat deze grondslag moet worden

¹¹⁰ Zie meer uitgebreid M. Buitenhuis en W. Bantema, 'De burgemeester: burgervader, handhaver van de openbare orde en sheriff van het internet? (deel 2), Kunnen burgemeesters met een internetverbod optreden tegen een verstoring van de openbare orde met aanleiding in het online domein?', Gst. 2023/8.

¹¹¹ Artikel 6:162 BW, zie Gerechtshof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352; bekrachtigd door de Hoge Raad in HR 25 juni 2022, ECLI:NL:HR:2021:985.

¹¹² Artikel 184 Wetboek van Strafrecht.

¹¹³ W. Bantema e.a., 'Black Box van gemeentelijke online monitoring', 2021.

¹¹⁴ Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Monitoring sociale media en naleving AVG door overheden, 29 april 2022. <https://www.rijksoverheid.nl/documenten/kamerstukken/2022/04/29/kamerbrief-over-monitoring-sociale-media-en-naleving-avg-door-overheden>

¹¹⁵ Thorbecke Academie NHL Stenden, 'Juridische grenzen en kansen bij openbare orde handhaving - Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen', 27 oktober 2022.

¹¹⁶ <https://hetccv.nl/onderwerpen/cybercrime/database-lokale-cyberprojecten/digikamer-voor-gemeenten/>

¹¹⁷ Artikel 5 AVG.

¹¹⁸ Artikel 6, lid 1 onder e, AVG.

vastgesteld bij Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.¹¹⁹ De vraag kan worden gesteld of al bestaande wettelijke grondslagen een basis kunnen bieden voor het verwerken van persoonsgegevens ten behoeve van het opleggen van een 'online gebiedsverbod' door de burgemeester. In dat kader kan er bijvoorbeeld worden gedacht aan de algemene handavingsgrondslag in de Gemeentewet.¹²⁰ In de jurisprudentie is nog geen antwoord gegeven op de vraag of deze grondslag specifiek genoeg is. Onze verwachting is dat wanneer er een enkele keer een online gebiedsverbod wordt opgelegd mogelijk een basis kan worden gevonden in deze al bestaande wettelijke grondslag. Het stelselmatig opleggen daarvan rechtvaardigt echter geen beperking van de vrijheid van meningsuiting, privacy en in sommige gevallen het demonstratierecht.¹²¹ In die gevallen zal er in een meer specifieke wettelijke grondslag moeten worden voorzien. Overigens is er ook nog veel meer aandacht en onderzoek nodig voor een effectieve implementatie van de AVG. Uit nieuw onderzoek blijkt dat er bij gemeenten nog veel winst te halen is in de uitvoering en naleving van deze wetgeving.¹²²

Offline halen ongewenste content

Met het opleggen van een online gebiedsverbod is de reeds geplaatste ongewenste content nog niet verwijderd. Om een bericht van het internet te krijgen en om te voorkomen dat deze door anderen wordt gedeeld, kan een burgemeester een 'Notice and Take Down' (hierna: 'NTD')-verzoek indienen. Voor het offline halen van de content dient behoorlijk wat aan de hand te zijn. Daarvoor moet komen vast te staan dat de informatie strafbaar of onmiskenbaar in strijd met de wet (onrechtmatig) is. Aan die eis zal niet zomaar bij ieder bericht dat op het internet wordt geplaatst worden voldaan. Indien vast komt te staan dat sprake is van een strafbare of onmiskenbaar in strijd met de wet zijnde gedraging dan dient het internetplatform, afhankelijk van de situatie, binnen maximaal tien dagen op de klacht te reageren. Indien het bericht ernstige schade berokkent, moeten de gegevens soms al binnen 24 uur ontoegankelijk worden gemaakt. De vraag is of dat op tijd genoeg is om op een online aangejaagde ordeverstoring te reageren of om deze te voorkomen. Een ander bekend probleem over de NTD-procedure is dat bepaalde sociale media platforms – Telegram is daar een bekend voorbeeld van – zich weinig aantrekken van dergelijke verzoeken. De gemeente Bodegraven-Reeuwijk probeerde daarom een platform in een civiele procedure in kort geding te dwingen om onrechtmatige content toch offline te halen. De vordering werd afgewezen, omdat het platform zich volgens de voorzieningenrechter voldoende

had ingespannen om de content van het account in kwestie offline te halen.¹²³

Duidelijk is dat de nu geldende termijnen te lang zijn om adequaat op een dreigende verstoring van de openbare orde te kunnen reageren. Op dit moment wordt gewerkt aan een register waarin gemeenten ongewenste content kunnen melden, waarna de verzoeken tot offline halen gebundeld kunnen worden ingediend.¹²⁴ Als er geen gehoor wordt gegeven aan een NTD-verzoek, kan de burgemeester een verzoek indienen bij de officier van justitie (hierna: de 'OVJ') om informatie offline te laten halen.¹²⁵ De OVJ kan dan met tussenkomst van een rechter-commissaris een communicatiedienst bevelen om bepaalde informatie tijdelijk ontoegankelijk te maken. Een dergelijk verzoek kan enkel worden gericht aan een aanbieder van een communicatiedienst, waar een sociale media platform zoals Facebook in beginsel ook onder kan vallen. Platforms kunnen strafrechtelijk vervolgd worden indien zij het bevel niet opvolgen.¹²⁶

4.5.4 Betrekken van het maatschappelijke en burgerperspectief bij beleid en bestuur

"Over privacy voeren we veelal het verkeerde debat", durft Prins te stellen. "Het gaat niet uitsluitend over wat wel of niet mag. Het gaat ook over de positie en verantwoordelijkheid van betrokken organisaties. Het gaat over beheer, de

vraag wanneer je iets mag delen, hoe lang je iets moet of mag bewaren, dat soort vragen. Die gaan veel verder dan 'het mag niet op grond van de privacy'. Dat is een dooddoener.¹²⁷ De uitdaging die voor ons ligt is om voor dit moment, tegen de achtergrond van de huidige maatschappelijke discussies, de juiste balans voor de strategische positie van privacy ten opzichte van de huidige behoefte aan veiligheid, c.q. de gepercipieerde onveiligheid, te vinden.¹²⁸ Bij onze lijn gaat het onder andere over dit soorten vragen waarin ook privacy en het maatschappelijke en burgerperspectief daarop, centraal zullen staan.

Deze derde lijn sluit enigszins aan bij het genoemde voorbeeld van burgerinteracties en effectiviteit van online interventies, maar is wel een verschil. Om extra aandacht te vragen voor het maatschappelijke en burgerperspectief op legitimiteit van overheids-handelen en bestuur in een digitaliserende samenleving. Dit perspectief wordt met name spannend als het gaat om mogelijkheden die digitalisering biedt voor controle en toezicht. Specifiek denken wij dan aan het gebruik van slimme technologie in de stad (smart cities), online monitoring van gemeente en politie (onder andere) maar ook aan de actualiteit rond 'online gebiedsverboden'. Voordat gewerkt kan worden aan toekomstbestendige werkwijzen en beleid dient eerst inzicht te worden verkregen in burgerperspectieven op specifieke werkwijzen (1),

¹¹⁹ Artikel 6, lid 3, AVG.

¹²⁰ Artikel 172, lid 1, Gemeentewet.

¹²¹ Artikel 10 Grondwet en artikel 8 EVRM.

¹²² <https://www.wodc.nl/actueel/nieuws/2023/02/09/overheden-hebben-meer-aandacht-voor-naleving-privacynormen-maar-vanzelfsprekend-is-het-nog-niet>

¹²³ Rechtbank Den Haag 4 oktober 2022, ECLI:NL:RBDHA:2022:10082

¹²⁴ AG connect, 'Gemeenten hopen op bevoegdheid om online-opruiming aan te pakken', 15 september 2022. <https://www.agconnect.nl/artikel/gemeenten-hopen-op-bevoegdheid-om-online-opruiming-aan-te-pakken>

¹²⁵ Artikel 125p Wetboek van Strafvordering.

¹²⁶ Artikel 54a Wetboek van Strafvordering.

¹²⁷ <https://www.mr-online.nl/prins-verkeerd-debat-privacy/>

¹²⁸ https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_20071101_veiligheid_en_privacy.pdf

omstandigheden waaronder dit als meer of legitiem en rechtvaardig wordt gezien (2) en de manier waarop dit betrokken kan worden als randvoorwaarde voor de ontwikkeling van effectieve interventies en beleid (3).

Burgerperspectief op online monitoring in (besloten) online groepen

Dit voorbeeld geldt niet alleen voor de politie maar ook voor het handelen van de gemeente bij het online signaleren en monitoren van openbare orde en veiligheidsvraagstukken. Een groot deel van het maatschappelijk leven speelt zich online af. Aldus moet de politie ook online zichtbaar en aanspreekbaar zijn. We zien dat gemeenten die behoefte ook voelen. Dat roept direct vragen op over hoe en waar de politie aanwezig kan of moet zijn en welke informatie mag worden verzameld, voor welke doeleinden en hoeveel inbreuk op grondrechten daarbij acceptabel kan worden geacht. De politie wil niet alleen rechtmatig optreden in juridisch-technische zin, maar ook legitiem in maatschappelijke zin. Daarvoor is van belang dat zij ook het perspectief van de burger meeweegt.

De politie hecht er belang aan het perspectief van de burger – wiens belangen worden beschermd en wiens rechten (mogelijk) worden aangetast – mee te nemen. Uit de literatuur komt echter naar voren dat voor het laatst in 2001 onderzoek is gedaan naar het burgerperspectief op privacy in relatie tot politiewerk.¹²⁹ In dat onderzoek was er aandacht voor cameratoezicht en huiszoekingen,

het internet speelde destijds nog een beperkte rol in politiewerk. Daarnaast richtte dat onderzoek zich volledig op het domein van de opsporing terwijl we in dit onderzoek juist zien dat informatievergaring ook het terrein van de openbare orde en veiligheid een steeds grotere rol gaat spelen.

Bij de politie geldt dit bijvoorbeeld bij het gebruik van *Open Source Intelligence* (OSINT) om bij te dragen aan een goede informatiepositie voor haar optreden en zodoende de belangen van burgers te beschermen. Door middel van OSINT maakt zij tegelijkertijd inbreuk op de rechten van burgers, waaronder het recht op privacy en (mogelijk ook) het recht op vrijheid van meningsuiting. Hoe kijken burgers aan tegen online gegevensvergaring door de politie in online groepen en de spanningen die zich hierbij met grondrechten (kunnen) voordoen? Daarnaast is er weinig literatuur over wat online (besloten) groepen precies zijn en dit onderzoek kan bijdragen aan inzicht hierin vanuit het perspectief van de gebruikers (de burgers). Om het recht beter aan te laten sluiten bij maatschappelijke ontwikkelingen en opvattingen is inzicht in perspectief van de burger eveneens relevant.

De politie is samen met het Ministerie van Justitie & Veiligheid bezig met het verkrijgen van meer houvast voor online gegevensvergaring met een niet-strafvorderlijk karakter: wat mag de politie wel en niet, in welke omstandigheden en op basis van welke juridische grondslagen? Deze juridische invalshoek is van belang maar ook eenzijdig in die zin dat de stem van de burger ontbreekt. Voor

¹²⁹ Vedder, H. & Koops, E.J. (2001). Hoever mag de overheid gaan bij het maken van inbreuken op de privacy van burgers om misdaad op te kunnen sporen?

gemeenten geldt dat naar aanleiding van onderzoek van ons lectoraat momenteel wordt gewerkt aan een handreiking voor online monitoring via de Ministeries van J&V en BZK. Er wordt dus vooral gezocht naar juridische oplossingen en het perspectief van de burger is vooralsnog onzichtbaar en niet expliciet betrokken als onderdeel van de toekomstige werkwijze. Dit laat eens te meer zien dat meer onderzoek op dit terrein relevant en nodig is.

Wat maakt een groep besloten?

Ook binnen de politie is men zoekende naar handvatten voor het begrip besloten of afgeschermd omgeving. Dat is relevant, wanneer een opsporingsambtenaar (persoons)gegevens vergaart in een besloten of afgeschermd omgeving, is er eerder sprake van een meer dan geringe inbreuk op de persoonlijke levenssfeer. Uit onderzoek komt naar voren dat bijvoorbeeld de grootte van de groepen wordt gezien als criterium om de mate van openheid en besloten te bepalen. *'Je moet een goede afweging maken als het gaat om besloten groepen. Wanneer is een groep nu besloten? Wij moeten als overheid respect hebben voor de privacy van burgers. Als wij aan de voorkant kunnen nagaan hoeveel mensen er in zo'n groep zitten en wat de aard van de groep is, dan kunnen we ook inschatten welke mate van privacy mensen denken te hebben. Als het deurgebeleid is dat je een hekel moet hebben aan de coronamaatregelen en je komt binnen bij een groep van driehonderd man, dan is de mate van privacy'schending gering, dus dan durven wij te verkopen dat je dat op basis van artikel 3 kunt doen. Maar*

¹³⁰ Landman, W. & Groothuis, S. (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring*. Den Haag: Sdu Uitgevers (p. 73).

*als het bijvoorbeeld gaat om een groep van zes personen of een groep Urkers, dan kun je het niet doen ten aanzien van privacy, los van het feit dat je er niet inkomt.*¹³⁰ Tevens komt naar voren dat men zich afvraagt of naast de grootte ook bijvoorbeeld de aard van de groep of de doelstelling waarmee de politie aanwezig is, uitmaakt voor de aanwezigheid en deelname aan besloten groepen. Uit meerdere onderzoeken van onze studenten komt naar voren dat er stelregels zijn over de grootte van de groepen in relatie tot beslotenheid. In één van die onderzoeken stelt een wijkagent dat bij groepen die groter zijn dan 100 personen al niet meer van beslotenheid wordt gesproken. Onbekend is in hoeverre dergelijke vuistregels bij de politie of bij het Openbaar Ministerie ook daadwerkelijk in beleid zijn vastgelegd en belangrijker, of dit overeenkomt met afwegingen die burgers maken en hun opvattingen hierover.

Om het perspectief van de burger betekenis te geven is het van belang om op basis van de relevante juridische kaders en literatuur het wettelijk perspectief op politieaanwezigheid in (besloten) online bronnen te duiden. Hoe verhoudt het burgerperspectief zich tot de bestaande juridische kwalificaties, definities en bevoegdheden, waarbij de kanttekening gemaakt moet worden dat dit wettelijk perspectief nog niet is uitgekristalliseerd. Ook vanuit dit perspectief rijzen er nog tal van vragen, zoals: wanneer er sprake is van open en gesloten bronnen, waar liggen de grenzen tussen gegevensvergaring voor openbare orde en veiligheid en opsporing en vervolging en is deze grens in de

praktijk wel altijd te trekken, hoe de bevoegdheden van politie en gemeenten zich in dit domein verhouden en lopen deze al dan niet door elkaar heen en of er momenteel überhaupt een juridische basis is voor (verborgen) politieaanwezigheid in besloten groepen. (Zie over bestaande onduidelijkheden in het wettelijk kader onder andere de Commissie Koops en in de literatuur verschenen beschouwingen hierop zoals die van Oerlemans). Hierbij valt overigens op dat vanuit juridisch perspectief de discussie zich voornamelijk richt op onderzoek in open bronnen terwijl zowel vanuit politie als vanuit gemeenten er meer en meer (de wens tot) aanwezigheid in gesloten bronnen lijkt te bestaan.

Open bronnen kenmerken zich doordat 'in beginsel eenieder toegang kan verkrijgen en dat voor zover toegang gebonden is aan een account is het verkrijgen van een account een (semi-) geautomatiseerd proces waarbij niet bepaalde groepen worden uitgesloten van registratie'. Bij afgeschermd of besloten bronnen vindt er juist wel controle plaats op wie toegang wil tot de bron.¹³¹ Uitgaande van deze omschrijvingen is een bron waarvoor je een connectie nodig hebt (en toestemming voor toetreding) een besloten bron. De vraag is of dit onderscheid toereikend genoeg is om de verscheidenheid aan soorten groepen en de snelheid waarmee digitale ontwikkelingen elkaar opvolgen te kunnen omvatten. Naast aandacht voor het burgerperspectief en het juridische perspectief

kan ook het technische aspect relevant zijn als aanvullend perspectief. Hierin spelen aspecten zoals toegangscontrole en verificatie in online groepen mogelijk een rol. Hieruit volgen bijvoorbeeld de volgende vragen: is een groep (meer) besloten als leden zichzelf kunnen toevoegen met een account met een alias als gebruikersnaam? Als andere leden van de groep mensen kunnen uitnodigen tot de groep, is die groep dan wel gesloten en in hoeverre speelt grootte van de groep hierin een rol? Naast vragen over acceptatie van politie (kan ook gemeente of jongerenwerk zijn) in soorten online groepen, kunnen inzichten vanuit burgers ook bijdragen aan een beter begrip van de infrastructuur en vormgeving van soorten online groepen en de keuzes die burgers hierbij al dan niet bewust maken en hun overwegingen die daarbij centraal staan.

Burgeracceptatie van de online aanwezigheid van gemeente en politie

Wat is er bekend over de acceptatie en opvatting over aanwezigheid van politie in groepen op sociale media? Allereerst dient opgemerkt te worden dat het burgerperspectief op privacy in relatie tot politiewerk een onderbelicht thema is waar zelden over is geschreven. De laatste keer dat een onderzoek naar het burgerperspectief op dit terrein is uitgevoerd is meer dan 20 jaar geleden.¹³² In dat enquête-onderzoek zijn burgers bevraagd over de acceptatie van privacy-inbreuken door de politie op het gebied van cameratoezicht, huiszoekingen en telefoontaps (als middel). Het valt direct op dat er

geen aandacht is besteed aan online aanwezigheid door de politie. Het internet heeft inmiddels een grote rol in het politiewerk gekregen. Ook blijkt dat het genoemde onderzoek zich vooral richtte op bevoegdheden van de politie op het gebied van opsporing. Met uitzondering van één scenario/vignette, was er slechts zijdelings aandacht voor het domein van de openbare orde en veiligheid. Uit dat onderzoek blijkt dat met name doelstelling van het onderzoek (variatie van zware en minder zware delicten) uitmaakt voor de mate waarin privacy-inbreuken door de politie geaccepteerd worden door burgers.

Uit een eerste verkenning van de literatuur hebben we geen studies gevonden waar de acceptatie van politie in soorten online groepen centraal staat. Afgelopen jaar hebben onze studenten vanuit NHL Stenden wel al onderzoek verricht naar de acceptatie van online monitoring van gemeenten in besloten groepen.¹³³ Zij maakten hierin gebruik van een vragenlijst die is ingevuld door 50 studenten van verschillende opleidingen binnen de Thorbecke Academie. Uit de enquête volgt dat 64% van de respondenten het helemaal gerechtvaardigd vinden dat een medewerker van de gemeente meekijkt in besloten groepen met een duidelijke weergave van hun gemeentelijke organisatie. Hierbij vindt slechts 7% het niet gerechtvaardigd. In dit geval is de gemeente duidelijk herkenbaar bij de leden van de (besloten)groep. Op het moment dat een gemeente minder herkenbaar wordt hebben de studenten meer moeite om dit als gerechtvaardigd te zien. Wanneer de gemeente gebruik maakt van

een nepaccount dan vindt ruim 60% van de respondenten het niet meer gerechtvaardigd. Deze kleine (en selecte) steekproef lijkt er op te wijzen dat hoe herkenbaarder de gemeente is tijdens online monitoring hoe meer gerechtvaardigd de studenten de deelname van de gemeente aan besloten groepen vinden. Dat geldt mogelijk ook voor de politie.

De studenten hebben daarnaast nog een vergelijking gemaakt tussen groepen met een verschillend karakter en doel vanuit de gebruikers. Zo vergeleken ze een besloten anti-corona protestgroep, een modeltrein hobbyclub, een besloten voetbalsupportersgroep van een grote club en een besloten groep waar handel plaatvindt in gestolen voorwerpen. Uit de vergelijking blijkt dat de aard of doel van de groep een rol kan spelen in de rechtvaardiging van online monitoring door gemeente. Zo vinden studenten het gebruik van een nepaccount of een alias meer gerechtvaardigd in bijvoorbeeld de besloten groep waarin wordt gehandeld in gestolen voorwerpen dan in de groep waarin wordt gesproken over modeltreinen. Dit resultaat is in lijn met wat Koops en Vedder concluderen in de context van opsporing en acceptatie van privacy-inbreuken door de politie, waar naar voren kwam dat privacy-inbreuken door de politie meer geaccepteerd worden wanneer er sprake is van zware misdrijven in vergelijking met lichte delicten. Dat stemt overeen met nog weer ouder onderzoek, naar de introductie van videosurveillance op de snelweg, dat leidde tot de conclusie dat burgers een inbreuk op hun privacy tolereren als dat 'de prijs is die voor een grotere

¹³¹ Onder andere: Oerlemans, J.J. & Schuurmans, Y.E. (2019). Internetonderzoek door bestuursorganen. *Nederlands Juristenblad*, 94(20), 14158-1466 & Oerlemans, J.J. (2018). Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk. *Platform Modernisering Strafvordering*.

¹³² Vedder, H. & Koops, E.J. (2001). Hoeveer mag de overheid gaan bij het maken van inbreuken op de privacy van burgers om misdaad op te kunnen sporen?

¹³³ Brokaar, J., Luchtenberg, K. & Altenberg, S. (2021). *Verwachtingen van privacy door inwoners*. Leeuwarden: NHL Stenden Hogeschool.

veiligheid betaald moet worden.¹³⁴ De eerder genoemde studenten vinden online monitoring in alle besloten groepen meer gerechtvaardigd wanneer dit gebeurt op een open en transparante manier (in vergelijking met het gebruik van een nepaccount of alias) en is dit verschil groter in de groepen die minder met veiligheid te maken hebben terwijl bijvoorbeeld in de groep over gestolen voorwerpen het gebruik van een alias en het gebruik van een bedrijfsaccount of persoonlijk account weinig verschil maken in de mate van rechtvaardiging en acceptatie van online monitoring door de gemeente.

Aansluitend bij het onderzoek van Koops en Vedder kunnen nog een aantal variabelen worden aangedragen die mogelijk relevant zijn voor het burgerperspectief. Er is onder andere (aanvullend) een onderscheid gemaakt in uitvoerder (de politie versus een particuliere organisatie), bereik (grote of kleine kans op verzamelen gegevens van niet-daders) en effectiviteit van de inzet van het middel en het gebruik van gegevens (niet voor andere doelen of ook voor andere doelen gebruikt). Van deze variabelen komt alleen naar voren dat men privacy inbreuken door de politie meer geneigd is te accepteren inbreuken door particuliere beveiligingsbedrijven (uitvoerder). De overige variabelen lijken geen grote rol te spelen. Er zijn wel achtergrondvariabelen die relevant zijn. Hoger opgeleiden zijn overwegend kritischer over privacy-inbreuken door de politie dan lager opgeleiden. Daarnaast lijken ouderen meer te hechten aan de uitvoerder (liever politie dan een particulier beveiligingsbedrijf) dan jongeren.

Er zijn verschillende spannende aspecten aan het burgerperspectief. Zo is het verfrissend en meer toekomstgericht om zonder het recht als uitgangspunt te nemen te kijken naar concepten als 'online groepen' vanuit het perspectief van de burger en dus de gebruiker. Daarnaast is er weinig bekend over de mate waarin burgers overheid en politie accepteren in soorten (besloten) groepen welke factoren daarop van invloed zijn. Welke criteria zijn daarbij doorslaggevend. Wat betekenen de uitkomsten van burgerperspectief voor zowel de typologie van online (besloten) groepen en voor de maatschappelijke legitimiteit van online gegevensvergaring door de politie (en gemeenten/jongerenwerk) in deze groepen?

Hierbij moet onder andere aandacht besteed worden aan de vraag hoe het burgerperspectief zich verhoudt tot maatschappelijke legitimiteit. Te denken valt onder andere aan het maken van een typologie van online groepen die kan worden gebruikt voor beleid (bijvoorbeeld een handelingskader) en uitvoering, maar de uitkomsten kunnen ook duidelijke aanknopingspunten bieden voor de uitvoering van gemeente of politiewerk in een online omgeving, óók in relatie tot een bepaald doel zoals 'informatievergaring voor een specifieke openbare ordekwestie' of 'informatievergaring voor het opbouwen van een kennispositie over maatschappelijke verhoudingen' – afhankelijk van waarop burgers accenten leggen.

¹³⁴ Van Treeck, R. & W. Stol (1996). Automobilisten voorstander van videosurveillance. Enquête langs de ringweg rond Amsterdam. *Algemeen Politieblad*, 145, 16, 8-9.

Andere voorbeelden van vraagstukken waar het burger en maatschappelijke perspectief ontbreekt
Het getoonde voorbeeld ten aanzien van online monitoring in soorten online groepen – in het voorbeeld toegepast op de politie – is al heel specifiek. Er zijn veel meer voorbeelden te noemen waarin het burgerperspectief en het maatschappelijke perspectief op digitalisering relevant is en meegenomen zou kunnen en moeten worden. Digitalisering leidt tot nieuwe kansen en nieuwe bedreigingen. Ten aanzien van die online onveiligheid en digitale bedreigingen biedt technologie overheden ook mogelijkheden. De inzet van die technologische mogelijkheden vragen niet alleen om een verandering van het recht maar ook vragen over 'willen we dit wel' en dus ook het ethische perspectief. Voor een goede afweging van verschillende belangen en perspectieven is het burgerperspectief en maatschappelijke perspectief een belangrijk onderdeel in onze ogen.

Bij het genoemde voorbeeld van online monitoring kan ook het gemeenteperspectief worden betrokken. Uit eerder onderzoek is gebleken dat burgemeesters geen expliciete bevoegdheden hebben om online te monitoren op basis van de algemene taakstelling van burgemeesters ten behoeve van de openbare orde. Uit recent nieuws kwam naar voren dat de politie veel gegevens van demonstranten verzameld, soms zelfs van vrienden of familieleden van demonstranten. Naast de vraag of dit juridisch kan en mag (dit is twijfelachtig) is ook hier maatschappelijke discussie op zijn plek over de vraag of in welke mate dergelijke praktijken noodzakelijk en wenselijk zijn. Ten aanzien van de openbare

¹³⁵ <https://www.mensenrechten.nl/themas/vrijheid-van-meningsuiting/demonstratie>

orde en veiligheid is eveneens de vraag op welke basis en juridische grondslag burgemeesters als gezaghebber over de politie een de online identiteit van online opruiers en demonstranten mag achterhalen, in zekere zin gaat het dan op een opsporing ten behoeve van de openbare orde. Ook hier geldt dat het goed is om burgerperspectieven te betrekken bij een verder onderzoek naar juridische mogelijkheden en eventuele nieuwe wetgeving op dit gebied (waar iets voor te zeggen is).

Een relevant en onderbelicht onderzoek op dit terrein is uitgevoerd door het College voor de Rechten van de Mens in 2018.¹³⁵ In het onderzoek werd gekeken hoe Nederlanders aan kijken tegen de grenzen van de vrijheid van meningsuiting en het demonstratierecht, waarbij ook nadrukkelijk aandacht werd besteed aan uitingen op sociale media. Uit dat onderzoek blijkt onder andere dat de Nederlandse bevolking over het algemeen vindt dat iedereen in Nederland vrij moet zijn om zijn of haar mening te kunnen uiten, al dan niet in de vorm van een demonstratie. Die mening sluit aan bij de uitgangspunten van deze vrijheidsrechten. De steun hiervoor is echter deels ook afhankelijk van de context en inhoud van de uitingen. Zo vinden mensen dat er een groot verschil is tussen online en offline zeggen wat je wilt. Het grootste deel van de bevolking is van mening dat mensen in het openbaar moeten kunnen zeggen of schrijven wat zij willen. Slechts een kleine groep is het daarmee oneens. Er is echter een groot verschil als het gaat om de berichtgeving op social media: dan vindt slechts bijna een kwart van de bevolking nog dat men moet kunnen zeggen wat men wil. Het merendeel van de

Nederlanders heeft er geen bezwaar tegen wanneer berichten op online platforms verwijderd worden door de platforms zelf, als die beledigend zijn voor bepaalde personen of bevolkingsgroepen. Over overheidsregulering, zoals nu gaande is bij 'online gebiedsverboden' gaat het in 2018 nog niet.

In de conclusie en in de toelichting op de resultaten blijkt dat ook het College voor de Rechten van de Mens zoekende was met het vaststellen van de betekenis van de uitkomsten – wat betekenen de uitkomsten voor het recht of voor de samenleving? In de toelichting wordt aangegeven dat het College het belangrijk vindt dat deze vrijheidsrechten beschermd blijven, ook wanneer meningen en demonstraties tegen de meerderheidsopinies ingaan. Het is hun ogen alleen aan de onafhankelijke rechter om te bepalen of een bepaalde uiting strafbaar (of op een andere manier onrechtmatig) is of niet. Ook bij uitingen op het internet geldt vrijheid van meningsuiting. Bij het verwijderen van bepaalde uitingen online moet men waken voor censuur. Het College benadrukt dat iedereen vrij is om te zeggen wat hij of zij denkt of voelt, mits dat binnen de grenzen van de wet gebeurt. Eveneens verwijzen ze naar risico's wanneer de regulering volledig aan de grote sociale-mediaplatformen wordt overgelaten.

In 2023 is deze discussie nog minstens zo relevant en zou in onze ogen (zie ook de position paper) het burgerperspectief meer betrokken moeten worden in de discussie over 'online gebiedsverboden'. Hier kan onder andere aandacht besteed worden aan de mate en de omstandigheden waarin al dan niet online ingrijpen door platformen of overheden als

gerechtvaardigd wordt gezien. Bij de duiding van uitkomsten uit burgeronderzoeken is het belangrijk om bij het onderzoeksproces en ook achteraf als de uitkomsten bekend zijn, veel aandacht te besteden aan het betrekken van verschillende perspectieven voor het duiden van de resultaten en dat geldt zeker wanneer een poging wordt gedaan om individuele burgerperspectieven te vertalen naar maatschappelijke legitimiteit. Ook rond de smart cities en de slimme stad lijkt meer aandacht te komen voor het burgerperspectief in relatie tot technologie en besluitvorming over technologie. Onder andere collega Bart Wernaart van Fontys Hogeschool richt zich op manieren om burgers te betrekken bij technologie en zet ook nadrukkelijk in op het betrekken van moeilijk bereikbare burgers.¹³⁶

4.6 Tot besluit

Het is en blijft voor overheden koorddans in een digitaliserende samenleving. Doordat het recht achter loopt op maatschappelijke ontwikkelingen en daardoor in sommige gevallen sprake is van meer (online) onveiligheid zien overheden zich genoodzaakt en vinden ze het eveneens gerechtvaardigd om de grenzen van het recht op te zoeken en er soms bewust overheen te gaan met het oog op het publieke belang van openbare orde en veiligheid. Omdat er technisch veel meer mogelijk is dan juridisch mag is de vraag hoe die overwegingen tot stand komen en hoe breed ze worden gedragen vanuit de burger en de maatschappij. Naast dat ons lectoraat wil bijdragen aan zicht op veiligheidsuitdagingen, op rollen en verantwoordelijkheden van verschillende partijen willen we ook inzicht bieden in randvoorwaarden voor effectieve

handhaving. Die randvoorwaarden moeten verder gaan dan alleen organisatorische en juridische aspecten – overheden moeten beter hun best doen om de burger en maatschappij serieus te betrekken. Wanneer gemeenten bijvoorbeeld experimenteren rondom 'online gebiedsverboden' is de vraag of alle gemeenten dit een goed idee vinden en onder welke voorwaarden burgers dit als gerechtvaardigd zien. Veiligheid is maar een van de (publieke) waarden en de kunst is om een balans te vinden tussen verschillende waarden en belangen. Ons lectoraat wil met onderzoek, onderwijs en kennisproducten (die deels discussie stimuleren) bijdragen aan een meer evenwichtig bestuur in een digitaliserende samenleving.

Hierbij sluit ik dit boekwerk af dat is geschreven ter gelegenheid van mijn lectorale rede (30 mei 2023). We zoeken doorlopend nieuwe samenwerkingspartners. We zijn onder andere voortdurend in gesprek met het onderwijs, de praktijk en met andere onderzoekers en kennisinstellingen. Schroom niet om contact met ons op te nemen. Ons lectoraat werkt multidisciplinair en is te paaen voor verrassende samenwerkingen en perspectieven. We beperken ons niet tot onderzoek maar dragen onze kennis ook graag via verschillende producten en lezingen over aan studenten, de beroepspraktijk en de maatschappij. Vraag gerust naar de mogelijkheden. We zijn te bereiken via: willem.bantema@nhlstenden.com

¹³⁶ <https://www.scienceguide.nl/2023/01/de-sstraat-op-om-alles-burgers-bij-onderzoek-te-betrekken/>

Dankwoord

November 2016 belde ik met lector Wouter Stol om meer informatie te verkrijgen over de vacature voor docent-onderzoeker Cybersafety. Eerder had ik de vacature terzijde gelegd. Door de verwijzing naar Cybersafety moest ik denken aan een baan gericht op cybersecurity en dat sloot niet echt aan bij mijn achtergrond als gepromoveerd rechtssocioloog aan de Rijksuniversiteit Groningen. Uiteindelijk besloot ik toch te bellen. Wouter wist me te overtuigen om te gaan solliciteren en zoals bekend werd ik aangenomen en startte ik per februari 2017 – ruim zes jaar geleden.

Ik werd al snel projectleider op twee projecten waarbij ik vooral heel veel plezier haalde uit het meerdere malen benoemde project 'burgemeester in cyberspace'. Het project was zoals gezegd een opmaat tot meer mooie projecten en kansen binnen NHL Stenden Hogeschool/Thorbecke Academie. Wouter heeft mij hierin altijd gestimuleerd en ondersteund waardoor we zelfs landelijk op de kaart staan met ons bestuurlijke onderzoek in relatie tot digitalisering. Dank voor de steun en de verschillende samenwerkingen en inspiratie op dit terrein Wouter, dat waardeer ik zeer.

Samen met collega Jurjen Jansen geef ik leiding aan de onderzoeksgroep Cybersafety, waar ik me volop bezig hou met onderzoek en onderwijs vanuit het lectoraat 'Bestuur in een Digitaliserende Samenleving'. Gelukkig hoef ik dat niet alleen te doen. Dat doe ik samen met gedreven en enthousiaste collega's vanuit verschillende achtergronden (zie CV eerder), te weten: Sipke de Vries, Suzanna Twickler, Denise de Boer, Anna Bartelds en Laura Postma. Het is een plezier om met jullie samen te werken, zonder jullie geen lectoraat. Ook collega's Sander Ebberts, Saskia Westers, Joyce Kerstens, Kimberly Bluhm en

Maike Berkenpas wil ik bedanken voor de prettige samenwerking en de levendige gedeelde kenniskring die we samen vormen binnen de onderzoeksgroep Cybersafety. Marja Blok-Goudberg hoort ook in dit rijtje thuis, zij regelt veel achter de schermen en draagt sterk bij aan een goede sfeer binnen onze onderzoeksgroep en is van het 'eerste uur'. Ook Jurjen Jansen wil ik bedanken voor de prettige samenwerking en voor het 'samen navigeren in een digitale samenleving', eveneens de titel van onze gezamenlijke inauguratie op 30 mei 2023. Het is fijn dit avontuur samen met jou aan te gaan, ook gezien de vergelijkbare thuissituatie met een jong gezin.

Daarnaast wil ik graag de collega's van de opleiding Integrale Veiligheidskunde bedanken voor het mogelijk maken van de verbinding tussen onderzoek en onderwijs. We zullen ook de komende tijd volop samenwerken aangezien ik nog een deel van mijn aanstelling onderwijs verzorg binnen opleiding. Ook de collega's binnen de Thorbecke Academie wil ik bedanken en ook uitnodigen om te komende tijd actief samen op te blijven trekken. Het onderzoek van ons lectoraat raakt aan recht, bestuur en (inter)nationale veiligheid en bestrijkt daarmee alle opleidingen van de Thorbecke Academie. In het bijzonder wil in de teamleiders bedanken – Marika Toutenhoofd, Lucinda Wondel en Edou Hilverda. Ook wil ik graag Richard Delger, onze academiedirecteur, bedanken voor het vertrouwen en voor deze

mooie kans om verder te bouwen aan het lectoraat. Natuurlijk gaat mijn dank ook uit naar het College van Bestuur van NHL Stenden Hogeschool, te weten Erica Schaper, Oscar Couwenberg en Marco Otto. Ik wil jullie danken voor het gestelde vertrouwen en het mogelijk maken van deze mooie kans.

Vanuit onderzoek wil ik de Rijksuniversiteit Groningen bedanken voor de mooie samenwerkingen. Zo is er in de beginfase veel samengewerkt met professor Solke Munneke en zijn collega's bij verschillende juridische onderzoeken en werken we momenteel veel samen met professor Tom Postmes en Hedy Greijdanus vanuit de Rijksuniversiteit Groningen (sociale psychologie). Rond bevoegdheden en het recht heb ik het afgelopen jaar veel met Marietta Buitenhuis samengewerkt. Dank voor deze mooie en productieve samenwerking die nog steeds gaande is. Vanuit de praktijk wil ik een bijzonder woord van dank wijden aan Marieke Verhagen-Dales die samen met ons het project 'online orde' startte via de City Deal 'Lokale Weerbaarheid en Cybercrime'. Destijds was dit heel vernieuwend en avontuurlijk en ik waardeer het lef dat jullie hebben getoond om 'online aanjaging' bestuurlijk aan te jagen. Dat geldt ook voor Rob Bats en Marleen Veldhuis vanuit regio IJsselland, zij maakten onderzoek naar de APV in relatie tot online aangejaagde ordeverstoringen mogelijk. Momenteel werken we fijn samen met de gemeente Amsterdam

via Jorieke de Wit en haar team, jullie ook dank voor het vertrouwen en ik kijk uit naar de afronding van het onderzoek (Connect).

Ook kijk ik met veel plezier terug op de mooie samenwerking met PBLQ bij het vak 'de cyber-burgemeester (Peter van Enk), met Joost Keemink van het NGB (verschillende vakpublicaties), met Wouter Jong (de befaamde Lochemconferenties), met Kato Vierbergen (VNG), met Axel Weggelaar, Jouri Vig, Patrick van den Brink, Sten Meijer (CCV) en het netwerk van Cyberburgemeesters (o.a. Astrid Nienhuis, Iris Meerts). Daarnaast dank aan de collega lectoren binnen NHL Stenden Hogeschool en de lectorennetwerken rondom bestuur, recht en veiligheid waar ik actief bij betrokken ben. Ik verwacht veel van die samenwerkingen de komende jaren. Vanuit de Noordelijke Academie voor het Openbaar Bestuur (NAOB) wil ik Avelien Haan bedanken voor de mooie samenwerking. Tot slot wil ik nog Marcel Spruit en Emiel Kerpershoek (HHS) bedanken voor de vruchtbare samenwerking in het Kiem Project (SIA) rondom smart cities en kijk ik uit naar het verder gezamenlijk verkennen van dat boeiende onderzoeksterrein.

Tot slot wil ik mijn familie en vrienden bedanken voor hun support door de jaren heen. In het bijzonder wil ik stilstaan bij mijn vrouw Floor, met haar steun, liefde en begrip kan ik de wereld aan. Onze prachtige kinderen Arthur en Jasmijne heb ik graag om me heen en ik bewonder hun jaloersmakende nieuwsgierigheid in de wereld om hun heen. Zij zijn een grote inspiratie. Dankzij dit fijne gezin blijf ik de wereld in het juiste perspectief zien en weet ik wat het belangrijkste is in het leven. Allicht worden jullie soms moe van de verhalen over burgemeesters, over digitalisering en recent veel over 'online gebiedsverboden'. Ik wil jullie vragen ook de komende jaren vragen goed te luisteren want er staat nog veel te gebeuren op dit terrein, het raakt de levens van ons allemaal en ik ben er ook nog lang niet over uitgesproken.



Illustratie: Tymo Grijsma

Bestuurlijk koorddansens in een digitaliserende samenleving

Dr. Willem Bantema is lector Bestuur in een Digitaliserende Samenleving aan NHL Stenden Hogeschool. Het lectoraat is gepositioneerd binnen de onderzoeksgroep Cybersafety van de Thorbecke Academie. Daarnaast is hij docent binnen de opleiding Integrale Veiligheidskunde.

