Lokaal bestuur in een digitaliserende samenleving

Essay over een stap in de ontwikkeling: een handelingskader

05-10-2021

Prof. dr. Wouter Stol

Dr. Willem Bantema

THORBECKE ACADEMIE

NHL STENDEN

Inhoud

1. Inleiding

Gemeenten hebben maatschappelijke taken en verantwoordelijkheden, speciaal de zorg voor openbare orde en veiligheid. De samenleving digitaliseert en dus doen gemeenten nu hun werk in een digitaliserende samenleving. Daarop moeten zij zich instellen. Gemeenten zijn sinds ongeveer 2013 bezig met een inhaalslag op dit vlak. De eerste fase in zo'n proces is bewustwording. Inmiddels hebben gemeenten vooral door online aangejaagde ordeverstoringen gezien welke rol de online wereld reeds speelt in openbare orde en veiligheid − én dat dit om aanpassingen vraagt. Gemeenten moeten hun typische gemeentetaken, dus hun werk aan openbare orde en veiligheid, nu doen in een digitale context. Daarover gaat dit essay. Meer in het bijzonder gaat het over een specifieke stap in deze ontwikkeling: een handelingskader dat 'digibewuste' gemeenten kunnen gebruiken bij het ontwikkelen van concrete werkwijzen.

Diverse gemeenten hebben in hun beleid al aandacht voor digitalisering (Stol & Bantema 2020). Landelijk zien we die aandacht in de 'Agenda Digitale Veiligheid 2020-2024' van de Vereniging van Nederlandse Gemeenten (VNG 2020). Daarin staan als gemeentelijke taakgebieden: (1) informatiebeveiliging, (2) digitale incidenten en -crisis en (3) digitale criminaliteit. Het eerste taakgebied blijft in dit essay verder buiten beschouwing. Informatiebeveiliging is voor gemeenten weliswaar van groot belang, want ze hebben het beheer over belangrijke informatie én ze hebben een voorbeeldfunctie, maar informatiebeveiliging is tegelijk ook een algemene kwestie die geldt voor *iedere* organisatie. Het is, en daar draait het om, geen typische gemeentetaak zoals 'openbare orde en veiligheid'.

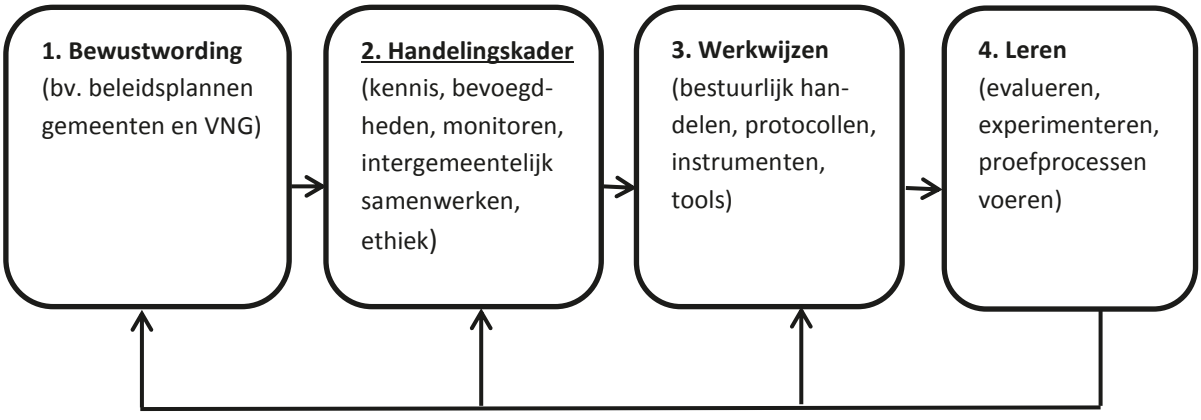
De twee typisch gemeentelijke taakgebieden (2 en 3) werken we hierna wat verder uit in *vier* gemeentelijke taakgebieden: (i) regie voeren op digitale weerbaarheid van mens en organisatie, (ii) eisen stellen aan digitale veiligheid bij vergunningplichtige activiteiten, (iii) optreden tegen het online aanzetten tot of aanjagen van een ordeverstoring en (iv) optreden bij cybercrises. Op die gebieden kunnen gemeenten verdere stappen zetten in de vorm van beleid en vooral concrete werkwijzen binnen het gemeentelijke handelingsrepertoire. Hierna zetten we een stap in die richting met het schetsen van een handelingskader dat kan dienen als referentie bij beleidsvorming en als plattegrond waarbinnen een handelingsrepertoire kan worden uitgewerkt. Het handelingskader is opgebouwd rond twee vragen: 'Waarmee gaan we aan de slag?' en 'Waarmee hebben we rekening te houden?' We hanteren daarbij een tijdshorizon van 5 à 10 jaar.

Om een antwoord te vinden op de vraag waarmee gemeenten aan de slag dienen te gaan, maken we gebruik van scenario's. De scenario's zijn overwegend gebaseerd op de inzichten die we de laatste vijf jaar hebben opgedaan in ons onderzoek op het gebied van rechtshandhaving en technologie, en op kennis van de literatuur over het gemeentelijke digitale veiligheidsdomein. Interviews met experts gebruikten we ter validering en aanvulling van de scenario's. Bij het ontwikkelen van de scenario's is rekening gehouden met maatschappelijke ontwikkelingen die gepaard gaan met digitalisering: een toenemende maatschappelijke complexiteit en (desondanks) een toename in orga-

nisatie- en informatievermogen bij burgers en organisaties. Uit de veertien scenario's die we schetsen destilleren we vervolgens vijf hoofdlijnen die dienen als aandachtsgebieden: vier inhoudelijke hoofdlijnen en ethiek als hoofdlijn die de andere vier doorsnijdt. De hoofdlijnen omvatten de in de scenario's terugkerende, expliciete of onderliggende thema's waarmee gemeenten aan de slag kunnen gaan, en blijkens de scenario's dus zouden moeten gaan, om slagvaardig te zijn in een digitale samenleving. De hoofdlijnen uit de scenario's zijn voor gemeenten dus aandachtgebieden. De vijf hoofdlijnen zijn: (A) een lijn die de andere vier doorsnijdt: het vaststellen van morele of ethische uitgangspunten (Wat voor gemeente willen we zijn?), (B) werken aan een kennispositie voor bestuurlijke handhaving in een digitale samenleving, (C) evalueren en waar nodig actualiseren van bevoegdheden, (D) op de hoogte blijven van wat er speelt in de samenleving ('monitoren') en (E) waar nodig realiseren van intergemeentelijke samenwerking. De vijf hoofdlijnen of aandachtsgebieden noemen we apart, maar ze staan niet los van elkaar. Ze beïnvloeden elkaar op vele manieren. Het uiteindelijke handelingskader (par. 6.2) is opgebouwd vanuit die hoofdlijnen.

Figuur 1 geeft schematisch weer welke plaats het handelingskader inneemt in het proces waarin gemeenten zich de bestuurlijke handhaving in een digitale samenleving verder eigen maken. Deze figuur impliceert niet dat gemeenten nog op geen enkel punt verder zijn gekomen dan 'bewustwording'. Overigens betekent het óók niet dat de bewustwording binnen alle gemeenten op alle fronten is voltooid. Sommige gemeenten zijn, al dan niet in een samenwerking, al bezig met het gestalte geven aan werkwijzen, zoals het monitoren van wat online gaande is (Bantema e.a. 2021) of het optreden bij een cybercrisis. Maar, gezien over alle 352 gemeenten, ligt de nadruk vermoedelijk op de fase van bewustwording en op het nadenken over hoe het bestuurlijk handelen in een digitale samenleving vorm kan krijgen. Het handelingskader waarin dit essay uitmondt, biedt gemeenten daarbij richtinggevende handvatten: een plattegrond of kader waarbinnen gemeenten concreet bestuurlijk handelen kunnen ontwikkelen in een verder digitaliserende samenleving.

Figuur 1: onderhavig handelingskader in de context van bestuurlijke ontwikkeling en digitalisering.



Gaande het schrijven van deze tekst spraken we met diverse betrokkenen in verschillende settings. We hadden diverse voortgangsgesprekken met vertegenwoordigers van de VNG, we hadden twee expertmeetings met overwegend burgemeesters (bijlage 2) en we hadden een serie interviews met experts van buiten de gemeenten (bijlage 3). De input uit deze gesprekken hebben we onder meer benut om de scenario's te toetsen en ideeën aan te scherpen. De verantwoordelijkheid voor de uiteindelijke tekst ligt uiteraard bij de auteurs.

2. De route naar een handelingskader voor gemeenten

Digitalisering is de maatschappelijke ontwikkeling die inhoudt dat informatie- en communicatietechnologie op steeds meer plaatsen en op steeds meer verschillende manieren een rol speelt in het dagelijks leven (Stol & Strikwerda 2017). Door digitalisering verandert de samenleving. Wanneer de samenleving verandert, is voor het bestuur de vraag of zij de ontwikkelingen op hun beloop laat of tracht om daarop vanuit haar taken en verantwoordelijkheden invloed uit te oefenen. Daaraan gaat uiteraard nog de vraag vooraf of het überhaupt mogelijk is om als bestuur richting te geven aan dergelijke maatschappelijke ontwikkelingen.

Een eerste vraag is dan of de veranderingen die de digitalisering brengt, uiteindelijk autonome gevolgen zijn van technologie of van intentioneel menselijk handelen. In het eerste geval heeft technologie een onafhankelijke kracht en zelfs een eigen moraal: de rationele moraal van berekening en efficiëntie. Mensen zijn dan uiteindelijk niet meer dan samengeperste grondstof voor een technologische machinerie. De tweede benadering is optimistischer. Veranderingen zijn dan het resultaat van menselijk handelen, van technologie*gebruik*. Dan kunnen dus ook menselijke waarden zoals vrijheid, gelijkheid en eerlijkheid richtingevend zijn. Voor bestuurders is deze visie de enige optie. Wat stelt besturen immers nog voor wanneer men meent dat veranderingen technologisch zijn gedetermineerd? Dan zijn we immers onderworpen aan de wetten van de technologie en ontstaat een ééndimensionale samenleving met de ééndimensionale mens die Marcuse voorzag (1964) en waarover Huxley schreef in zijn *Brave new world* (1932). Is het dus mogelijk dat mensen, en dus ook gemeentebestuurders, de ontwikkelingen weloverwogen richting geven? In zijn *Technics and Civilization* geeft techniekfilosoof Mumford (1934) daarop in zijn slotzin het enige antwoord dat voor bestuurders telt: 'Impossible? No: for however far modern science and technics have fallen short of their inherent possibilities, they have taught mankind at least one lesson: Nothing is impossible.'

De geschiedenis in eigen land bevat een hoopgevend praktijkvoorbeeld waarbij is ingegrepen op de negatieve gevolgen van een nieuwe technologie. De opmars van gemotoriseerd wegverkeer ging vanaf de jaren vijftig gepaard met een toename in het aantal verkeersdoden tot zo'n 3.200 per jaar begin jaren zeventig. Met tal van

maatregelen is die trend bijgestuurd tot ongeveer zeshonderd verkeersdoden per jaar nu. Daar zijn drie lessen uit te trekken. De eerste is dat het kan. De tweede les is dat zoiets een integrale aanpak vergt (bv. wettelijke maatregelen, veiliger infrastructuur, handhaving, educatie, veiliger technologie, cultuuromslag). Ten derde vergt het een lange adem en is het nooit klaar (denk aan nieuwe slachtoffers door e-bikes). Het voorbeeld toont misschien wel vooral dat technologische ontwikkelingen niet ongevoelig zijn voor begeleidend bestuurlijk ingrijpen. Dit is een praktijkantwoord op de vraag of bijsturen van technologische ontwikkelingen mogelijk is. Ja dus.

In de eerste alinea van deze paragraaf staat: 'Door digitalisering verandert de samenleving.' Daar staat dus *niet* dat de technologie de ontwikkelingen bepaalt. Het is maar net hoe zij wordt gebruikt. Digitalisering kan ongewenste gevolgen hebben, want mensen en organisaties kunnen de technologie zó gebruiken dat negatieve effecten optreden. Dat is de boodschap van bijvoorbeeld George Orwell in zijn roman *1984*. De dystopie die hij schetst is geen noodzakelijk gevolg van de technologie, maar het intentionele gevolg van een op onderdrukking beluste overheid. Zo gezien is Orwells verhaal in de kern optimistisch: het blijft mensenwerk, het kàn dus ook anders. Wat gewenste of ongewenste gevolgen zijn van technologiegebruik, is uiteraard afhankelijk van ethische en politieke opvattingen. Waar dat in deze notitie een rol speelt, proberen we daarover expliciet te zijn. Verder is ethiek een onderdeel van het uiteindelijke handelingskader.

We beogen in deze notitie vooruit te kijken. Maar, wanneer ontwikkelingen in de samenleving het resultaat zijn van menselijke intenties, hoe kunnen we dan ont-wikkelingen zien aankomen en daarop anticiperen? Het is immers niet eenvoudig te voorspellen welke intenties in een samenleving op enig moment de koers bepalen. Nog minder eenvoudig lijkt het om te voorspellen hoe dat over enige jaren zal zijn. Toch valt er wel het een en ander te voorzien, met name toekomstige fricties – in dit geval fricties die het gevolg zijn van digitalisering en die het openbaar bestuur aangaan. Fricties zijn tot op zekere hoogte te voorzien doordat onze samenleving zich behalve door verandering kenmerkt door stabiele trekken. Waar digitalisering gevolgen heeft die niet goed sporen met die stabiele trekken, ontstaat een wrijving die niet zelden bestuurlijke aandacht vergt.

De stabiliteit van een samenleving kunnen we ons voorstellen als gebaseerd op structuren die hun duurzaamheid ontlenen aan normen, regels, materie en hulpbronnen, waaronder macht en gezag (Giddens, 1984). Dat geeft vastigheid, maar sluit verandering niet uit − en dat moet ook niet want een onveranderbare samenleving is breekbaar. Wanneer mensen, om wat voor reden ook dingen anders gaan doen, kan het resultaat uiteindelijk een structurele verandering zijn. 'Uiteindelijk', want de basisprincipes zijn tamelijk robuust. Onze samenleving kent bijvoorbeeld wettelijk beschermd particulier eigendom en een geldeconomie inclusief vermogensdelicten. Daar heeft de digitalisering, inclusief bitcoin, niets aan veranderd. Elke samenleving vergt een zekere mate van orde evenals een zekere mate van veiligheid en een overheid of oppergezag met een bijzondere verantwoordelijkheid op die gebieden. Ook dat alles is ongewijzigd, ondanks internet, darkweb, social media en cybercrime. Een en ander neemt niet weg dat de digitalisering fricties met zich meebrengt omdat zij het bestaande uitdaagt. Precies daarover gaat deze notitie. Zij gaat over uitdagingen waarvoor de digitalisering

gemeenten stelt, oftewel: zij gaat over bestuurlijk relevante fricties. We hanteren daarbij een tijdshorizon van 5 à 10 jaar.

Doordat we focussen op fricties, ligt in deze notitie de nadruk op negatieve gevolgen van digitalisering. Het gaat over gevolgen waarmee de lokale overheid te kampen krijgt en niet over gevolgen die het de lokale overheid aangenaam en gemakkelijk maken. Daarmee is niet gezegd dat digitalisering vooral negatieve gevolgen heeft, maar wel dat gemeenten vooral een bestuurlijke, regulerende taak hebben als het gaat om de fricties (spanningen, dilemma's) die digitalisering met zich meebrengt. De gemeente heeft nu eenmaal niet primair als taak om te juichen voor wat goed gaat, maar heeft eerder als taak de samenleving te helpen met wat nog niet goed gaat.

We presenteren hierna in paragraaf 5 enkele scenario's. Een scenario is een veronderstelde ontwikkeling, dus niet geheel zeker maar wel met enige zekerheid te verwachten op basis van een onderbouwde redenering. Onze scenario's zijn veronderstelde ontwikkelingen die meekomen, of in elk geval kùnnen meekomen, met de digitalisering en die een bestuurlijk relevante frictie herbergen. Het gaat om fricties tussen de gevolgen van digitalisering en bestaande maatschappelijke principes of zo men wil: geldende waarden en normen. Een scenario wijst op een frictie, maar zegt niet of de oplossing ligt in veranderen, in handhaven van het bestaande of een mix daarvan. Het handelingskader komt aan bod in paragraaf 6. Dat kader laat gemeenten zien waarop ze zich kunnen voorbereiden en waarmee ze daarbij rekening dienen te houden. We bieden daarmee een kader waarbinnen gemeenten zowel beleid als concreet bestuurlijk handelen kunnen ontwikkelen (zie figuur 1).

Het basaalste scenario aangaande digitalisering en bestuur is reeds elders naar voren gebracht. In 2013 schreven Stol en Jansen 'de rol van de burgemeester in de online veiligheidszorg, is een vergeten onderwerp. Ten onrechte.' De gemeente heeft een taak in de veiligheidszorg (bestaand principe), maar vult die niet in waar het gaat om digitalisering (frictie). Het doemscenario was: de samenleving digitaliseert, gemeenten gaan niet mee en komen in de veiligheidszorg dus buitenspel te staan. Oftewel: 'Wanneer de burgemeester (...) zich niet oriënteert op het handhaven van orde en veiligheid in het digitale domein en zijn/haar eigen actieve rol daarin, verschrompelt gaandeweg de bestuurlijke bijdrage in lokaal veiligheidsbeleid' (Bantema & Stol 2020, p. 224). Gemeenten en andere partijen (bv. VNG, CCV) hebben de laatste jaren tal van acties ondernomen om dat doemscenario te voorkomen, naar het zich laat aanzien met succes want dàt gemeenten een rol hebben in digitale veiligheid is niet langer een punt van discussie. Die bewustwording dringt nu in het lokale bestuur snel door. De aandacht gaat vervolgens uit naar de invulling van die gemeentelijke rol (Bantema & Stol 2020; Stol & Bantema 2020). De houding van burgemeesters is zichtbaar veranderd. Waar zij enkele jaren terug afwijzend stonden tegenover een rol in de handhaving van online aangejaagde ordeverstoringen (Stol & Strikwerda 2017) voelt nu 71 procent van de burgemeesters zich verantwoordelijk voor bijvoorbeeld het voorkómen van online aangejaagde ordeverstoringen (Bantema e.a. 2020). Kortom, gemeenten en hun burgemeesters zijn in een volgende fase beland.

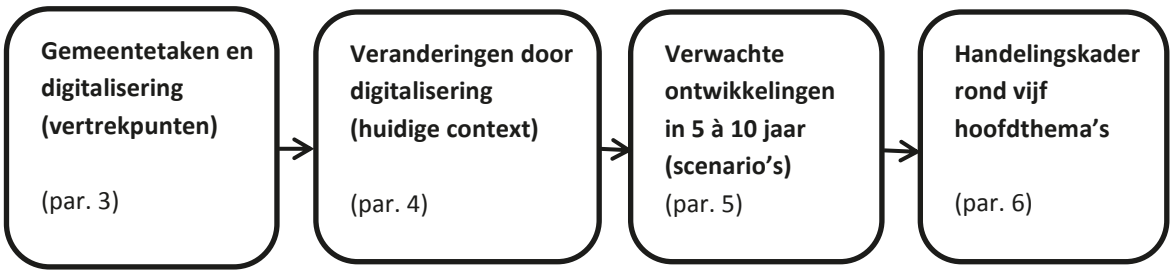
In deze notitie kijken we naar specifiekere scenario's dan het zo-even aangehaalde basale doemscenario. Dat vrij ruwe scenario luidde: 'door de digitalisering zijn

gemeenten straks in de veiligheidszorg overbodig'. De analyse was: in hun veiligheidsbeleid negeren gemeenten de digitalisering en staan daarom straks buitenspel. Gemeenten zijn echter inmiddels in actie gekomen om dat scenario te voorkomen en geven gaandeweg vorm en inhoud aan een bestuurlijke rol in digitale veiligheid. Om gemeenten daarbij te helpen, bespreken we in deze notitie enkele minder grove scenario's. Uitgangpunt daarbij is dus dat gemeenten óók in een gedigitaliseerde samenleving een rol hebben in de veiligheidszorg. Het eindproduct van deze exercitie bestaat uit een handelingskader dat gemeenten handvatten geeft bij het verder ontwikkelen van beleid en activiteiten waarmee zij hun rol in de digitale samenleving kunnen invullen.

In paragraaf 3 bespreken we dadelijk eerst de gemeentelijke taken in relatie tot digitalisering. Vervolgens kijken we in paragraaf 4 naar gevolgen van digitalisering voor maatschappelijke orde en veiligheid (de relevante context). We schetsen waar zich fricties met gemeentelijke verantwoordelijkheden voordoen of zijn te verwachten, en bespreken hoe gemeenten daarmee kunnen omgaan. We gaan niet in op details van de gemeentelijke taakuitvoering. Ook gaan we niet in op specifieke technologische ontwikkelingen zoals de zelfrijdende auto of blockchaintechnologie voor gemeentelijke vergunningverlening of specifieke dreigingen zoals ransomwareaanvallen. We hanteren niet een technologische maar eerder een sociologische blik, met aandacht voor maatschappelijke processen en principes, en met aandacht voor hoe de digitalisering, doordat zij op die processen en principes invloed heeft, betekenis heeft voor de rol van de gemeente in de veiligheidszorg.

Nadat in paragraaf 3 de gemeentelijke taken en in paragraaf 4 enkele relevante maatschappelijke gevolgen van digitalisering aan de orde komen, passeren in paragraaf 5 enkele concrete scenario's de revu. Die geven aan waarmee gemeenten in de komende 5 à 10 jaar te maken gaan krijgen. Na de scenario's benoemen we de hoofdlijnen die daaruit naar voren komen. In paragraaf 6 tot slot, schetsen we vanuit die hoofdlijnen een handelingskader voor gemeenten. Figuur 2 geeft deze opbouw in stappen weer.

Figuur 2: opbouw van dit essay



3. Gemeente en digitalisering

3.1 Gemeentefunctie inzake orde en veiligheid

De gemeentefunctie inzake openbare orde en veiligheid is een vorm van sociale controle: het toepassen van positieve of negatieve sancties met het oogmerk het gedrag van mensen in overeenstemming te houden of te brengen met standaards die binnen hun groep worden voorgestaan (Stol & Kop 2020). Als die standaards zijn verankerd in rechtsregels, spreken we van rechtshandhaving. Omdat de gemeente, net als bijvoorbeeld de politie, werkt op basis van wetten waarin haar mandaat is vastgelegd, spreken we van *formele* sociale controle.

Gemeenten hebben niet het monopolie op sociale controle inzake openbare orde en veiligheid. Iedereen die zorgt dat mensen zich gedragen in overeenstemming met de geldende waarden en normen daaromtrent, houdt zich bezig met sociale controle op het werkgebied van de gemeente. Dat begint al bij de opvoeding thuis en op school. Ook in ander verband spreken mensen elkaar aan, zoals actievoerders die bij een demonstratie anderen op grenzen wijzen, of ouders, leraren, influencers en vrienden die anderen aanspreken op ongewenst gedrag. We spreken dan van *informele* sociale controle. De gemeente heeft weliswaar een speciale wettelijke verantwoordelijkheid en bijbehorende bevoegdheden, maar ze doet het niet alleen. Formele en informele sociale controle vullen elkaar aan, versterken elkaar, kunnen niet zonder elkaar.

3.2 Digitalisering en gemeentelijke taakgebieden

De ‘Agenda Digitale Veiligheid 2020-2024’ van de Vereniging van Nederlandse Gemeenten (VNG 2020) noemt drie gemeentelijke taakgebieden: (1) informatiebeveiliging, (2) digitale incidenten en -crisis en (3) digitale criminaliteit. Stol en Bantema noemen eerst vijf (2019) en later zes (2020) gemeentelijke taakgebieden in relatie tot digitalisering. Eén daarvan is, net als in de VNG-agenda, de zorg voor een veilige informatiehuishouding (‘eigen huis op orde’). Die laten we hier verder buiten beschouwing, want een sterke informatiebeveiliging is een vereiste voor *alle* organisaties die privacygevoelige informatie beheren en niet typisch voor de gemeente als bestuurlijk orgaan. Een ander door Stol en Bantema genoemd taakgebied is ‘monitoren’ van maatschappelijke activiteiten en sentimenten in relatie tot orde en veiligheid. Bantema e.a. (2021) werken dat verder uit. Hun onderzoek voert ons hier tot de conclusie dat ‘monitoren’ *an sich* niet een gemeente*taak* is maar moet worden gezien als *instrument* of middel om andere taken uit te voeren. Dan resten er vier gemeentelijke taakgebieden in relatie tot digitalisering en bestuurlijke verantwoordelijkheid:

1. *Regie op digitale weerbaarheid van mens en organisatie.* De gemeente werkt hieraan middels acties die zij zelf uitvoert en vooral acties van anderen die zij stimuleert en regisseert. Dit taakgebied betreft weerbaarheid tegen cybercrime, maar ook omvat het weerbaarheid tegen andere verstoringen die ontstaan vanuit een digitale omgeving (bv. door systeemuitval).

2. *Eisen stellen aan digitale veiligheid bij vergunningplichtige activiteiten.* De gemeente is verlener van vergunningen. Bij elke vergunningverlening is aandacht voor veiligheid, dus ook voor digitale veiligheid. De gemeente stelt bij vergunningverlening eisen aan de digitale veiligheid en zorgt voor toezicht op de naleving. Te denken valt aan de digitale veiligheid van evenementen en de digitale veiligheid van andere bedrijfsmatige activiteiten binnen de gemeente.
3. *Optreden tegen het online aanzetten tot of aanjagen van een ordeverstoring.* Het kan gaan om een offline of online ordeverstoring, hoewel de gemeentelijke taak aangaande *online* openbare orde nog *terra incognita* is. Tot nu toe gaat dit dus om de *offline* openbare orde die door *online*-activiteiten wordt uitgedaagd (bv. een online oproep tot een straatrace).
4. *Optreden bij cybercrises.* Artikel 1 van de Wet veiligheidsregio's omschrijft een crisis als 'een situatie waarin een vitaal belang van de samenleving is aangetast of dreigt te worden aangetast'. Een cybercrisis is een crisis met een digitale oorzaak zoals een computerstoring, virus of hack. Een cybercrisis is doorgaans een crisis waarvan de *oorzaak in de digitale wereld* ligt, maar waarvan de *ontregeling ligt in de analoge wereld* (bv. wateroverlast, uitval elektriciteit). Een ontregeling kan zich echter ook online manifesteren. Net als voor ordeverstoring geldt voor cybercrises dat gemeentelijk optreden bij gevallen die zich uitsluitend online afspelen (en dus geen offline-effect hebben) nog onbekend is.

In termen van de veiligheidsketen (Liebregts 2016) ligt binnen de eerste twee taakgebieden het accent op proactie, preventie en preparatie, en binnen de andere twee op repressie en nazorg. De taakgebieden 1 en 2 (regie voeren, eisen stellen) zijn twee dimensies van werken aan digitale weerbaarheid. Ze hebben een preventief of preparatief karakter. De gemeentelijke activiteiten op deze gebieden moeten bijdragen aan het voorkómen van cybercrime, ordeverstoring of andere inbreuken op de maatschappelijke orde. Is een cybercrime eenmaal gepleegd, dan is het behandelen daarvan allereerst een verantwoordelijkheid binnen de strafrechtketen. In de nazorg echter kan de gemeente weer een rol vervullen, in elk geval in de vorm van maatregelen die herhaald slachtofferschap helpen voorkomen (nazorg in de vorm van opnieuw aandacht voor preventie). Betreft de verstoring van de maatschappelijke orde niet cybercrime maar een aantasting van de openbare orde, dan blijft de gemeente aan zet: zie taakgebied 3 en 4. De gemeente treedt dan reactief op, soms in vroeg stadium (bv. bij een online oproep tot een demonstratie) en soms als de verstoring van de openbare orde zich al volop manifesteert (bv. bij de plotse uitval van een nutsvoorziening).

Natuurlijk omvatten de vier taakgebieden allerlei *uitvoerende werkzaamheden* waarop de digitalisering effect heeft, zoals onderhouden van contacten met vergunningaanvragers (online loket) of regelen van inloopavonden (social media). De focus ligt hierna echter niet op dergelijke uitvoeringskwesties. Het gaat bijvoorbeeld niet over hoe je als organisatie digitaal contact met je omgeving onderhoudt, maar om bestuurlijke taken en verantwoordelijkheden.

Alle vier door ons genoemde taakgebieden vallen binnen het tweede en derde taakgebied van de Agenda Digitale Veiligheid 2020-2024' (VNG 2020). Bij haar taakge-

bieden noemt de veiligheidsagenda tien actielijnen. Hier is vooral de vijfde daarvan relevant: 'OOV-bevoegdheden en rollen voor de lokale bestuurders'. Deze actielijn houdt verband met zowel het tweede als het derde in de veiligheidsagenda genoemde taakgebied (en dus met alle vier door ons genoemde taakgebieden). Die vijfde actielijn omvat onder andere de aanpak van online aangejaagde ordeverstoringen en cybercrime – en ook weerbaarheid en de regierol van gemeenten maken daarvan onderdeel uit.

Zojuist hebben we taken benoemd, zoveel mogelijk los van concrete instrumenten om die taken uit te voeren.[1] Juist om die reden hebben we 'monitoren' er buiten gelaten. Ook bijvoorbeeld het bestrijden van nepnieuws valt buiten het overzicht want ook dat is een specifiek instrument, niet een taak. De essentie van instrumenten is dat aan de inzet ervan eisen gesteld dienen te worden vanuit ethiek (willen we dit?), legitimiteit (mag dit?) en effectiviteit (werkt dit?). We komen hierop terug in paragraaf 6.

4. De context[2]

4.1 Inleiding

Gemeenten hebben, zo zagen we zojuist, diverse taken en verantwoordelijkheden op het vlak van digitale veiligheid. Voor de vraag hoe en hoe eenvoudig (of juist lastig) gemeenten daaraan invulling kunnen geven, is van belang te zien in welke context zij dit werk hebben te verrichten. Het is de context van de gedigitaliseerde samenleving, natuurlijk. Maar wàt daarvan dienen gemeenten gezien hun taken in aanmerking te nemen? Daarover gaat deze paragraaf.

Enkele bijzondere kenmerken van onze gedigitaliseerde samenleving laten zich verenigen onder de noemer 'complexiteit' (Stol 2020). Dat is een relatief begrip. Wat nu complex is, is dat over enige tijd mogelijk niet meer. Dat neemt niet weg dat digitalisering nu zorgt voor ingewikkeldheden waarmee gemeenten dienen om 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. Het concept complexiteit in relatie tot digitalisering, werken we uit in paragraaf 4.2 tot en met 4.6.

Een ander aspect van de context waarin gemeenten hun werk verrichten, is dat de digitalisering nieuwe handelingsmogelijkheden biedt. Wat de gemeente daarmee kan

[1] 'Zoveel mogelijk' want te verdedigen valt dat 'regie voeren' eerder een instrument is dan een taak. Wij vatten 'regie voeren' op als de gemeentelijke taak om anderen te betrekken bij veiligheidsvraagstukken.

[2] Deze paragraaf bouwt voort op eerder werk (Stol 2020, 2021).

aanvangen, komt later aan bod; hier gaat het om de omgeving waarin de gemeente haar werk doet. Burgers en organisaties gebruiken de mogelijkheden die digitalisering biedt en dat vergroot hun handelingsrepertoire, waaronder hun vermogen tot sociale beïnvloeding en tot sociale controle. 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? In deze paragraaf bekijken we twee potenties van digitalisering die burgers en organisaties benutten en die hun mogelijkheden vergroten: organisatie- en informatievermogen. Dit werken we uit in paragraaf 4.7 tot en met 4.9.

4.2 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 mechanische. 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 steevast 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.

4.3 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 dingen en mensen (Internet of Everything). Niet alleen onze klassieke desktop-computers 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) èn 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.

4.4 Echtheidscomplexiteit

In de onlinewereld kunnen we niet eenvoudig vaststellen wie wie is danwel wat echt is of nep. 'Offline hebben we bijvoorbeeld identificatiepapieren met echtheidskenmerken, geld met echtheidskenmerken en gebouwen met echtheidskenmerken.' (Jansen e.a. 2019: 108). Online is dat niet op vergelijkbare wijze ontwikkeld. Offline kunnen we mensen herkennen, online kan je doorgaans 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 aankopen of online nieuwsberichten. De overheid moet omgaan met echtheidscomplexiteit bij opsporing en ordehandhaving.

4.5 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 (Stol 2020). 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.[3] 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 computer[4] of een handprothese[5] aan te sturen. 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 avatar[6] in de digitale wereld manifesteert. De Amerikaanse journalist Julian Dibbell beschreef in 1993, voor zover bekend voor het eerst, een virtuele aanranding.[7] 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

[3] http://edition.cnn.com/TECH/computing/9901/14/chipman.idg/, geraadpleegd 30 april 2020.
[4] https://www.umcutrecht.nl/nieuws/met-je-hersenen-een-apparaat-bedienen, geraadpleegd 30 april 2020.
[5] NRC Next, 1 mei 2020, katern Wetenschap, p. E10.
[6] Een digitaal verbeelde representatie van het menselijk lichaam.
[7] Zie ook Stol & Strikwerda (2017), paragraaf 2.4.2.

showed two male avatars attacking her daughter's female character.'[8] 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 Cybercrime-verdrag[9] stelde reeds twintig jaar geleden virtuele kinderporno strafbaar om te voorkomen dat een sfeer ontstaat waarin seks met kinderen normaal is.[10]

4.6 Ontwikkeling in complexiteit – een weging

Onze samenleving wordt nog immer complexer. De complexiteit van werktuigen en netwerken neemt al eeuwen toe (bv. Smith 1776; Elias 1939; Pieterson 1981). Er is geen reden te veronderstellen dat deze ontwikkeling binnenkort stopt. Echtheidscompexiteit neem voorlopig ook toe, getuige bijvoorbeeld ontwikkelingen in 'deepfake', een fenomeen waarbij getruukte 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 nepnieuws, trollaccounts 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. Het is dan ook geen toeval dat de digitalisering gepaard gaat met de ontwikkeling van echtheids- en betrouwbaarheidskenmerken, zoals echtheidscertificaten en referenties (bv. het 'slotje' in de adresbalk van een website of een lijst met 'reviews').

4.7 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

[8] https://www.bbc.com/news/technology-44697788, 3 juli 2018, geraadpleegd 12 mei 2020.
[9] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001.
[10] Verbonden aan deze problematiek is de vraag of robots mensenrechten hebben.

in een weiland bij Beverwijk, waarbij een dode viel. Vandaag de dag speelt digitale communicatie een rol bij veel, zo niet àlle demonstraties. Als we 'Beverwijk' beschouwen als illustratie van digitaal organisatievermogen, is deze ontwikkeling dus al 24 jaar zichtbaar. Wie anno 2021 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.

Mensen gebruiken de digitale mogelijkheden niet enkel om rellen te organiseren maar óók om bij te dragen aan openbare orde en veiligheid. Whatsapp-buurtpreventie-groepen zijn sinds de start van WhatsApp BuurtPreventie (WABP) op 1 juni 2015 een veelvoorkomend verschijnsel.[11] 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 (Lam & Kop 2020). In januari 2021 organiseren voetbalsupporters zich in Den Bosch, Maastricht en Alkmaar om te voorkomen dat relschoppers de stad vernielen of winkels plunderen.[12] Burgemeester Roemer van Alkmaar spreekt in dat verband van 'een mooi signaal'. 'Er werd gewoon een duidelijk statement gemaakt: "van andermans spullen blijf je af." De sociale controle mag best een beetje terugkomen' aldus Roemer.[13]

Dergelijke 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".[14] 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."[15] Het verschijnsel voetbalsupporters als ordedienst kreeg behalve genoemde lof ook rechtstatelijk gemotiveerde kritiek.[16]

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

---

[11] 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 17 maart 2021.

[12] https://www.nu.nl/binnenland/6112686/voetbalsupporters-door-het-hele-land-vormen-front-tegen-relschoppers.html, geraadpleegd 15 maart 2021.

[13] https://www.nhnieuws.nl/nieuws/279840/roemer-trots-op-burgerwacht-az-hooligans-buitengewoon-positief-signaal, geraadpleegd 15 maart 2021. Het twee maal achtereen schrijven van een openings-aanhalingsteken is uit het origineel.

[14] https://www.gelderlander.nl/binnenland/politie-over-pedojagers-dit-zijn-geen-helden-we-zijn-er-klaar-mee~a9664741/, geraadpleegd 17 maart 2021.

[15] 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.

[16] https://www.nhnieuws.nl/nieuws/279904/socioloog-kritisch-op-roemer-az-supporters-als-buurtwachten-kan-en-mag-absoluut-niet, geraadpleegd 17 maart 2021.

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 (2021) pleit in dit verband voor de politie als 'autoriteit fatsoenlijke rechtshandhaving'. Daaraan voegen wij toe: de burgemeester voert het gezag over ordehandhandhaving in de digitale samenleving, en is dus aan te spreken op het fatsoen ervan.

4.8 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.

Individuen 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 permanenter 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.

4.9 Organisatie- en informatievermogen gewogen

Digitalisering biedt burgers organisatie- en informatievermogen en zij kunnen die enerzijds gebruiken voor gecoördineerde ordeverstoringen en anderzijds voor het uitoefenen van gecoördineerde sociale controle. Digitalisering biedt uiteraard eveneens aan gemeenten nieuwe mogelijkheden, ook voor sociale controle (toezicht, ordehandhaving), maar die verandering is minder fundamenteel. De lokale overheid heeft namelijk van oudsher al een hoge organisatiegraad en beschikt van oudsher al over veel informatie. De digitalisering voegt daar wat aan toe, maar brengt geen radicaal andere

mogelijkheden, brengt gemeenten niet ineens in een wezenlijk andere positie. Burgers konden zich slechts moeizaam organiseren en hadden slechts beperkte mogelijkheden tot het verzamelen en analyseren van informatie, en al helemaal niet ad hoc. Nu hebben ze volop mogelijkheden daartoe. Kortom, wat organisatie- en informatievermogen betreft heeft de digitalisering voor burgers een grotere, principiëlere verandering gebracht dan voor gemeenten. Gemeenten zijn, net als bijvoorbeeld de politie en andere overheidsorganen, hun vanzelfsprekende dominante positie ten opzichte van burgers voor een niet onbelangrijk deel kwijtgeraakt. De digitalisering heeft burgers in zekere zin geëmancipeerd, of zo men wil: nieuwe machtsmiddelen verschaft.

Voor gevestigde organisaties ligt het anders. Zij hebben door de digitalisering, net als gemeenten, enig extra organisatievermogen. Het verandert hun positie niet wezenlijk, want ze hadden zich al goed georganiseerd. Vooral hebben gevestigde organisaties door de digitalisering een geheel nieuw *informatie*vermogen. Zeker de grotere spelers (verzekeraars, telecombedrijven, onlinewinkels, banken, reisorganisaties, autobedrijven, grootgrutters, etc.) beschikken vanwege de digitalisering, als bijproduct van hun primaire proces, over grote informatiebestanden die niet zelden interessant zijn voor vraagstukken van orde en veiligheid.[17] Daarnaast zijn er tal van kleine gespecialiseerde bedrijven die zich toeleggen op informatievermogen (bv. satelietdata, internetmonitoring). De gemeente heeft in haar omgeving ineens tal van spelers met een serieus en voor gemeenten interessant informatievermogen – ook relevant voor openbare orde en veiligheid.

Kortom, wat organisatie- en informatievermogen betreft, veranderen partijen in de omgeving van de gemeenten sterker en fundamenteler dan gemeenten zelf. Dat vraagt dat gemeenten zich bezinnen op hoe zij zich tot die andere partijen verhouden. In elk geval is een gemeente niet langer de partij die als enige georganiseerd en geïnformeerd is. Eerder is zij een partij die samenwerkt met anderen, die stimuleert en waar mogelijk en nodig regisseert.

Tot slot van deze paragraaf willen we kort stilstaan bij een schijnbare paradox: toenemend organisatievermogen in een complexer wordende omgeving. Zou het immers niet logischer zijn dat een complexe omgeving het organisatievermogen van mensen belemmert? Deze schijnbare tegenstelling laat zich als volgt begrijpen. Ten eerste zijn de *primaire* functies van de digitale mogelijkheden eenvoudig te gebruiken. Dat is de oppervlakte. Weinigen gebruiken geavanceerde opties, een enkeling begrijpt de onderliggende technologie. Ten tweede brengen mensen met hun alledaagse activiteiten via technologie, verbindingen tot stand waarvan zij geen weet hebben en waarvan zij het geheel niet kunnen overzien. Dat overzicht is ook niet nodig voor hun dagelijkse activiteiten. Mensen hebben en gebruiken veel mogelijkheden in een wereld die zij maar zeer ten dele overzien en doorgronden.

[17] Die grote informatieverzamelingen kunnen ook een bron van gevaar zijn. We denken dan aan datalekken en bijvoorbeeld verhandelen van persoonsgegevens voor criminele doeleinden.

5. Bestuurlijk relevante scenario's

5.1 Inleiding

In paragraaf 2 gingen we kort in op technologie in relatie tot maatschappelijke ontwikkelingen. Bestuurders kunnen niet afwachten wat de digitalisering ons brengt, ze hebben uit de aard van hun maatschappelijke rol geen andere keuze dan trachten de ontwikkelingen te sturen of minstens bij te sturen. Daarbij is het om te beginnen behulpzaam te zien waarheen ontwikkelingen (waarschijnlijk) gaan. We hanteren daarvoor scenario's aangaande 'digitalisering en de rol van gemeenten in openbare orde en veiligheid'. Een scenario omschreven we als 'een veronderstelde ontwikkeling, dus niet geheel zeker maar wel met enige zekerheid te verwachten op basis van een onderbouwde redenering'. Het gaat om scenario's die een bestuurlijk relevante frictie herbergen – een frictie tussen de gevolgen van digitalisering en bestaande maatschappelijke principes.

We bespreken daarbij niet of een ontwikkeling wenselijk is, maar beoordelen wel vanuit een sociologische maatschappijanalyse of een ontwikkeling logischerwijze is te verwachten. Een voorbeeld op politiegebied. Toen het zogenoemde darkweb opgang maakte was dat 'unpoliced area'. Nu kan men natuurlijk menen dat het goed is dat er plaatsen zijn zonder overheidstoezicht en dat dat zo moet blijven, maar een sociologische maatschappijanalyse toont dat geen westerse samenleving blijvend toestaat dat er gebieden zijn waar de overheid niets te vertellen heeft. Te verwachten was dan ook dat het ontbreken van politietoezicht op het darkweb geen lang leven beschoren was. Het zal niemand verbazen dat de politie inmiddels actief aanwezig is op het darkweb.

Lastiger dan voorspellen wat er zal gaan gebeuren (i.c. politietoezicht op het darkweb) is hoe dat te prioriteren en, als de prioriteit dat vraagt, hoe effectief te reageren. Prioriteren speelt hierna zeker een rol. Van sommige zaken valt nu eenmaal vrij zeker te zeggen dat ze moeten gebeuren en dus een hoge prioriteit hebben. Gemeenten *moeten* een rol hebben in digitale veiligheid – tenzij we gemeenten afschrijven als instituut met uitsluitend aandacht voor fysieke/offline veiligheidstaken, wat wij niet als reële optie zien. Het invulling geven aan die nieuwe rol heeft dus een hoge prioriteit en wordt nu dan ook opgepakt. Het principe is logisch en het was eenvoudig te voorzien. *Hoe* gemeenten die rol invullen, is echter afhankelijk van lokale mogelijkheden, van inzicht in effectiviteit en van politieke keuzes.

Zoals gezegd hanteren we een tijdshorizon van 5 à 10 jaar. Dat lijkt een flinke tijd: nog làng niet zo ver, nog minstens twee gemeenteraadsverkiezingen vanaf nu.[18] Maar de discussie over de rol van gemeenten in digitale veiligheid is ongeveer zeven jaar geleden aangevangen en het onderwerp is pas recent, vaak ook nog schoorvoetend (Stol

[18] 16 maart 2022 zijn de eerstkomende gemeenteraadsverkiezingen.

& Bantema 2020), op de gemeentelijke agenda gezet. Gemeenten hebben dus waarschijnlijk de genoemde 5 à 10 jaar hard nodig om de scenario's die we hierna behandelen, en de daarmee verbonden fricties, van een adequate reactie te voorzien.

In paragraaf 3 schetsten we gemeentelijke taakgebieden in relatie tot digitalisering. Kort gezegd gaat het om (1) regie op digitale weerbaarheid van mens en organisatie, (2) eisen aan digitale veiligheid bij vergunningplichtige activiteiten, (3) optreden tegen het online aanzetten tot of aanjagen van een ordeverstoring, en (4) optreden bij cybercrises. Op die taken hebben de scenario's betrekking.

In paragraaf 4 hebben we ingrediënten klaargezet waarop we hierna teruggrijpen. Problemen en dilemma's waarvoor de digitalisering gemeenten stelt, zijn gezien vanuit hedendaags perspectief niet zo eenvoudig. De complexiteit van de materie hebben we expliciet gemaakt met de begrippen (i) technische complexiteit, (ii) netwerkcomplexiteit, (iii) echtheidscomplexiteit en (iv) cyborgcomplexiteit. Daarnaast bespraken we 'organisatievermogen' en 'informatievermogen' als twee concepten die helpen om veranderingen te beschrijven en te begrijpen. Het concept complexiteit legt vooral nadruk op (onderliggende) omgevingskenmerken. Organisatie- en informatievermogen leggen meer de nadruk op in die omgeving handelende burgers en organisaties.

Voor het identificeren van scenario's hanteren we de zojuist genoemde elementen als denkkader, vooral de vier gemeentelijke taakgebieden, maar ook de zojuist gememoreerde ingrediënten uit paragraaf 4. We kijken naar gemeenterelevante ontwikkelingen die de digitalisering met zich meebrengt en die een frictie hebben met heersende principes op de gemeentelijke taakgebieden. Naarmate de frictie of potentiële frictie groter is, wordt het scenario beleidsrelevanter. We hebben geen vaste systematiek waarmee we uit alle mogelijkheden de relevante scenario's kunnen bepalen, laat staan berekenen. We baseren ons op ruim twee decennia ervaring met onderzoek naar de relatie tussen digitalisering en strafrechtspleging (bv. Stol e.a. 1999; Stol & Strikwerda 2017) en op onderzoek dat we sinds 2015 doen naar digitalisering in relatie tot gemeenten en veiligheidszorg (bv. Bantema e.a. 2018, 2021).

5.2 Scenario 1: Vervreemding van de leefwereld van burgers en bedrijven

Klassieke criminaliteit daalt. Digitale criminaliteit neemt toe. E-fraude en hacken scoren in slachtofferonderzoek fors hoger dan fietsdiefstal en al helemaal dan woninginbraak. Burgers en bedrijven zijn vandaag de dag ernstig digitaal kwetsbaar. Dat neemt de komende jaren nog verder toe. Gemeente Natte Meren onderkent de opkomst van digitale criminaliteit en noemt dat ook in haar beleidsplannen, maar het is nog steeds 'een bijkomende kwestie' terwijl voor burgers en bedrijven cybercrime het grootste criminaliteitsprobleem is. De gemeente komt traag in actie met preventieprojecten, veiligheidscoalities, voorlichting en veiligheidskeurmerken. Kortom: 'digitaal' is voor Natte Meren geen vertrekpunt voor integraal veiligheidsbeleid, maar eerder een paragraaf in een voor het overige analoog geïnspireerde veiligheidsbeleid – terwijl in rap tempo alles in de wereld digitaal wordt. De gemeente verliest zo het contact met de

leefwereld van burgers en bedrijven. Burgers en bedrijven herkennen zich niet meer in gemeentelijk veiligheidsbeleid, met grote onvrede als gevolg.

5.3 Scenario 2: Eigenrichting

Burgers in gemeente Berglanden organiseren zich structureel en ad hoc met digitale middelen om zelf te waken over hun offline veiligheid en de offline maatschappelijke orde. Dat past in de trend van burgerparticipatie, maar gesteund door die trend schiet het door. Burgers raken eraan gewend dat zij zelf het heft in handen nemen als iets hen niet zint. Ze zijn actief in online opsporing en ze organiseren zich langs digitale weg om 'op straat' in actie te komen. De gemeente Berglanden, die daarop geen proactief, regulerend antwoord heeft geformuleerd, rest niets anders dan (steeds weer) puinruimen als het weer eens uit de hand is gelopen, bijvoorbeeld in de vorm van online eigenrichting of eigenrichting op straat met digitaal georganiseerde knokploegen. In de gemeenteraad ontstaat discussie over de rol die de gemeente eigenlijk zou moeten spelen.

5.4 Scenario 3: Digitaal Haaksbergen

Tijdens het jaarfeest van gemeente Natte Meren hebben scholieren een kermisattractie gehackt en ontregeld, daardoor raakte een klein kind gewond. De ouders organiseren een actiegroep. Ze halen boven water dat in een andere gemeente tijdens een festival matrixborden zijn gehackt en demonstranten daarmee het publiek in paniek hebben gebracht. Ook achterhalen ze dat in nog weer een andere gemeente tijdens een dorspfeest de betaalgegevens van alle deelnemers zijn gelekt en daarna verkocht via het darkweb. De ouders vragen landelijk aandacht voor deze incidenten. Het leidt ertoe dat de burgemeester van Natte Meren moet aftreden omdat deze verzuimd heeft toezicht te houden op de digitale veiligheid van een evenement. Bovendien hebben alle drie gemeenten schadeclaims ontvangen.

5.5 Scenario 4: Virtuele kwetsbaarheid

In gemeente Berglanden is op een scholengemeenschap onrust ontstaan vanwege aanranding van aan avatar. Een scholiere heeft de zaak aangekaart en een filmpje online gezet waarin te zien is hoe haar avatar onzedelijk wordt betast door andere avatars. De pers duikt erop. Ouders zijn ongerust. De politie weigert een aangifte op te nemen want zij ziet geen strafbaar feit. De school roept nu de burgemeester op om maatregelen te nemen. De gemeente had nooit gedacht dat dit serieus zou worden en zit dus aan tafel zonder antwoorden op de vele vragen van scholen en ouders. De onrust neemt toe. Klasgenoten van het slachtoffer hebben de vermoedelijke daders aangevallen door kinderporno op zijn computer te plaatsen en dan daarvan beelden online te zetten. De gemeente loopt achter de feiten aan en is de regie volledig kwijt.

5.6 Scenario 5: Verstoring van de online orde

Sinds enige tijd zijn gemeenten vertrouwd geraakt met *online* aangejaagde verstoringen van de *offline* openbare orde. Dat geeft gemeenten al flink wat hoofdbrekens, maar het is slechts een deel van het verhaal. Er is ook een online openbare orde die kan worden verstoord. Voor de gemeenteraadsverkiezingen voert Berglanden Radicaal Klimaat-neutraal (BRK) intensief campagne via Facebook, Twitter, Signal en Telegram. Tegenstanders van BRK hebben zich verenigd in actiegroep Leefbaar Klimaat Berglanden (LKB). LKB bestookt de accounts van BRK met dermate veel berichten dat normale communicatie op die accounts niet meer mogelijk is. De online BRK- campagne raakt ontregeld. BRK spreekt van het ondermijnen van de online openbare orde, want de normale online-communicatie is ontregeld, en dus roept BRK de burgemeester op om die online orde te herstellen, desnoods met inzet van geweldsmiddelen. De burgemeester weet zo niet of dit inderdaad valt onder 'openbare orde' laat staan of het onder haar bevoegdheid valt die te herstellen. Zij vraagt advies aan het hoofd van de afdeling Openbare Orde en Veiligheid (OOV). Ook hij heeft zich hierin nog niet verdiept en moet dus het antwoord schuldig blijven. De pers heeft lucht gekregen van het relletje en vraagt om toelichting. Ook op de vraag waarom er geen draaiboek is voor dit soort situaties heeft de gemeente geen antwoord. In de pers verschijnen honende kritieken.

5.7 Scenario 6: Online geweldsmiddelen

Nieuwe gemeenteraadsverkiezingen naderen. Berglanden Radicaal Klimaatneutraal (BRK) heeft een sterk digitaal georganiseerde achterban en start net als vier jaar geleden een massale online-campagne. Leefbaar Klimaat Berglanden (LKB) ontregelt net als vier jaar geleden de BRK-campagne door het plaatsen van talloze berichten op de BRK-accounts. De gemeente heeft zich echter voorbereid. Zij weet de LKB-berichten die staan op de BRK-accounts te verplaatsen naar een account van de gemeente dat ooit is gebruikt voor inspraak bij een windmolenproject. De gemeente verdedigt de ingreep in essentie als volgt: (i) de online orde is verstoord want de berichten verstoren de normale gang van zaken en bovendien beschadigt dit het democratisch proces, (ii) de burgemeester is bevoegd want de ordeverstoorders zijn inwoners van gemeente Berglanden, (iii) het geluid van de tegenstanders is enkel verplaatst en kan nog steeds worden gehoord, het is de online versie van de methode Koppejan die op 20 maart 2021 nog werd gebruikt om demonstanten in Amsterdam, die waren ingesloten op de Leidsekade, in bussen te laden en naar de rand van de stad te verplaatsen. Niets bijzonders dus. Er ontstaat nu een publiek en vooral juridisch getint debat over online geweldsmiddelen. Op die verbreding had de gemeente niet gerekend. Zo'n bredere verdieping in online geweldsmiddelen is nooit uitgevoerd. De gemeente krijgt in de pers het verwijt van 'opportunistisch ad hoc beleid' en gebrek aan visie op ordehandhaving.

5.8 Scenario 7: Nepnieuws

Scenario 7a. Nepnieuws door een actiegroep

Een telecomprovider zoekt in Berglanden een plaats voor een 6G-zendmast en is daarover met de gemeente in overleg. Al voordat een besluit is genomen zijn de plannen breed bekend geworden en ontstaat onrust in de gemeente. NIMBY! Een groep bezorgde burgers is een actie gestart tegen het plan en opende de website www.Bergland6Gvrij.nl. De site staat vol berichten over hoe gevaarlijk 6G is. De berichten worden steeds extremer. In sommigen delen van het land zouden al kinderen overleden zijn door kanker als gevolg van een 6G-zendmast. Ook verspreidt 6G een nieuwe mutatie van het coronavirus. Complottheorieën worden verkondigd, ondersteund door deepfake filmpjes. Er is geen enkel bewijs voor alle beweringen, maar de actiegroep is niet voor rede vatbaar. Slim zijn ze wel, ze plegen geen strafbare feiten. Omdat de groep haar gang kan gaan ontstaat onrust in de gemeente. Het draagvlak voor de huidige coalitie kalft snel af, blijkt uit een betrouwbare peiling. Het hoofd van de gemeentelijke afdeling Externe Communicatie stelt de burgemeester voor om op www.berglanden.nl een pagina te openen met juiste informatie over 6G. 'Inwoners hebben daar recht op.' De oppositie stelt dat 'we als gemeente' niet voor elk onderwerp 'de waarheid' moeten willen gaan verkondigen. 'Dat past ons als gemeente niet.' De wethouder vraag de burgemeester om in deze casus een knoop door te hakken en voor de toekomst beleidssuitgangspunten te formuleren.

Scenario 7b. Nepnieuws door een politieke partij

In gemeente Berglanden zijn de lokale politieke partijen Berglanden Radicaal Klimaatneutraal (BRK) en Leefbaar Klimaat Berglanden (LKB) in een verkiezingsstijd verwikkeld. Inzet is de energietransitie, een politiek zwaartepunt in de gemeente èn onder de inwoners. De cruciale vraag is waarop Berglanden zal inzetten: windenergie, zonne-energie of aanhaken bij een landelijke lobby voor kernenergie. LKB start in de gemeente een voorlichtingscampagne over kernenergie. De campagneleider verzamelt zoveel mogelijk informatie en nieuwberichten waaruit blijkt dat kernenergie veilig, schoon en duurzaam is. Hij put onder meer uit de website van de Universiteit van Klow in Syldavië en van de Syldavische Eenheidspartij. Syldavië draait bijna geheel op kernenergie en voert veel propaganda hiervoor. LKB vertaalt de informatie naar het Nederlands, doet er nog een schepje bovenop en verspreid het geheel via social media, zoveel mogelijk gericht op lokale netwerken. BRK en een actiegroep van verontruste burgers roepen de burgemeester op om aan de 'leugenachtige berichten' van LKB een einde te maken of in elk geval uit te dragen dat het gaat om nepnieuws. De berichten zijn volgens hen 'aantoonbaar vals' en LKB 'ondermijnt daarmee het democratisch proces van de gemeenteraadsverkiezingen'. Dat wil de burgemeester toch niet verdedigen? Waar stáát de gemeente eigenlijk voor? De burgemeester trekt zich dit aan en verzoekt LKB vervolgens om geen valse informatie te verspreiden. LKB beroept zich op de vrijheid van meningsuiting en blijft 'alternatieve feiten' verkondigen. De burgemeester krijgt van steeds meer kanten het verwijt stiekem achter de nepberichten van LKB te staan.

Scenario 7c. Nepnieuws door een fake-bot

De in gemeente Berglanden bekende activist Archibald Hoover (zijn voornaam is eigenlijk John, maar hij noemt zich ook wel Aaron) voert actie tegen het plan van de gemeente om enkele Syldavische asielzoekers te huisvesten. Hij is digitaal goed onderlegd en pakt het dan ook langs die weg aan. Hij opent elke week een nieuw profiel op wisselende social media platforms, onder zijn eigen naam of onder een van zijn vele aliassen. Een digitale robot laat hij verder het werk doen. De chatbot wordt vrienden met inwoners van Berglanden en plaatst zoveel mogelijk berichten die asielzoekers geraffineerd in een kwaad daglicht stellen. Zo ontstaat bij de inwoners van Berglanden het beeld dat steeds meer inwoners tegen het plan van de gemeente zijn en wordt het gaandeweg salonfähig, ja zelfs de norm om die mening te verkondigen. De stemming in de gemeente neemt aldus gaandeweg steeds meer de kleur aan van het algoritme van de chatbot. Een stagiair op de afdeling Externe Communicatie ontdekt wat er gaande is en bespreekt het binnen de afdeling. Het afdelingshoofd stap naar haar collega van Openbare Orde en Veiligheid en samen lichten ze de burgmeester in. Die vraagt van hen advies, inclusief juridische en praktische handvatten voor te ondernemen acties.

5.9 Scenario 8: Cybercrisis

De elektriciteitscentrale in Berglanden is getroffen door malware en het systeem is ontregeld. Hele wijken zitten zonder stroom en of het daarbij blijft, weet niemand nog. Ook een deel van het industrieterrein zit zonder elektriciteit. De CISO pleegt overleg met het NCSC en schakelt experts in om technisch gezien te redden wat er te redden valt. De afdeling Externe Communicatie (EC) van de gemeente krijgt niet alleen telefoontjes van de pers en verontruste inwoners, maar ook van andere gemeenten, die zich afvragen of het virus ook hen zou kunnen raken – en wat mogelijk nog méér. Het grootste probleem blijkt nu ineens niet van technische of praktische, maar van communicatieve aard. De burgemeester vraagt aan het hoofd EC naar het communicatieplan want het is nog geen uur na de eerste melding en de landelijke pers staat in de hal met vragen over risico's voor andere gemeenten en vragen over risico's voor andere kritische infrastructuur zoals waterkeringen en waterzuiveringsinstallaties. Is het virus inderdaad gemaakt door Chinese studenten van een Nederlandse universiteit, zoals al direct op internet wordt beweerd? Het hoofd EC heeft geen communicatieplan richting de landelijke pers. De burgemeester moet improviseren. Nog dezelfde dag zet de pers online dat de gemeente niet goed was voorbereid. De gemeenteraad stelt kritische vragen.

5.10 Scenario 9: Informatiepositie

Gemeente Berglanden heeft een bloementeler vergunning verleend voor het kweken van een nieuwe, populaire sierplant, de bonte fidelia. De gemeente heeft een landelijke tuinbouworganisatie om advies gevraagd en op basis daarvan concrete voorwaarden gesteld aangaande bestrijdingsmiddelengebruik. Gezien de situatie op de huizenmarkt is immers te verwachten dat de grond over enige jaren voor woningbouw moet worden aangewend. Enkele burgers vertrouwen de plannen van de teler niet en verdiepen zich

in de fideliateelt. Ze starten een groep op Facebook en plaatsen daar informatie over fidelia's, inclusief publicaties van TNO en diverse universiteiten. Ze wobben de vergunning en gaan aan de slag met de vergunningsvoorwaarden. Ze interviewen experts in de fideliateelt, milieudeskundigen en toxicologen in binnen- en buitenland. Ze nemen grondmonsters en laten die analyseren in een lab van Wageningen University and Research (WUR). De grond blijkt nu schoon. De groep kent een hoogleraar van de WUR en vindt die bereid om een gedegen risicoanalyse te maken. Alle informatie bij elkaar maakt duidelijk dat de kans groot is dat, uitgaande van de vergunninsgvoorwaarden, het bewuste stuk land na één jaar fideliateelt minstens vijf jaar lang niet meer geschikt is voor woningbouw. De actie-groep gaat met de resultaten naar de pers, die vervolgens breed uitmeet dat de gemeente 'naïef en amateuristisch' heeft gehandeld.

5.11 Scenario 10: Monitoren

Scenario 10a. Stelselmatig informatie verzamelen

Een medewerker van de afdeling OOV van gemeente Berglanden hoort tijdens een verjaardagsfeest dat een groep burgers onder de codenaam 'Hieperdepop' een demonstatie voorbereidt. Die zou over een maand moeten plaatsvinden tijdens het bevrijdingsfestival, want dat zou veel publiciteit opleveren. Volgens het verhaal zou het gaan om een demonstratie tegen politiegeweld en zouden de actievoerders politiegeweld willen uitlokken en filmen. Eén van de aanvoerders zou de bij de politie en gemeente bekende Evert Zwijnstra zijn, op internet bekend als 'Don Harley', die geregeld rondvertelt dat hij de gemeente nog wel eens te grazen zal nemen omdat hem een parkeervergunning voor zijn motorfiets is geweigerd. De maandag daarop zoekt de OOV-medewerker op internet en vindt inderdaad een website waarop 'Don Harley' het heeft over manifestatie 'Hieperdepop', maar het verhaal wordt hem nog niet echt duidelijk. Hij besluit het in de gaten te houden en bezoekt de site herhaaldelijk om te zien of 'Don Harley' nog meer over de actie loslaat en of er meer organisatoren zijn. Activiteiten en uitspraken van 'Don Harley' noteert hij in een notitieblok. Na twee weken wordt hij gebeld door Evert Zwijnstra die hem vraagt waarom hij gegereld zijn website bezoekt. Het was allemaal van meet af aan een opzetje, de beheerder van de site heeft alle bezoeken secuur gelogd en zeven daarvan herleid tot de gemeente. Hij heeft naar zijn zeggen 'de gemeente ontmaskerd als stiekeme gluurder'. Een bevriende jurist gaat de gemeente nu aanklagen wegens schending van artikel 8 EVRM, de Grondwet en de GDPR.

Scenario 10b: Identificeren van een aanstichter

De marktmeester stuurt een appje aan Yarim Kwaliç van de afdeling OOV van gemeente Berglanden. Hij hoorde namelijk van één van de marktkooplui dat op Snapchat, Telegram en Instagram twee personen met de namen 'Idéfix' en 'Bobbie' oproepen tot het in brand steken van de marktkraam van één van de kooplieden, een slager. Ze loven zelfs een beloning uit. De marktmeester vermoedt dat het een actie is van extremistische veganisten. Die hebben al eerder bij die kraam gedemonstreerd. Yarim weet nog van de demonstratie. Die mondde uit in een vechtpartij en dreigementen over en weer.

Er volgt intern beraad waarbij ook de burgemeester aanwezig is. Die vraagt dezelfde dag nog aan het hoofd van het Cybercrimeteam van de politie of zij de identiteit van 'Idéfix' en 'Bobbie' kan vaststellen, zodat hij hen aan het gemeentehuis kan uitnodigen voor een gesprek om het conflict te sussen. De politie stelt vast dat het gaat om één persoon die gebruik maakt van twee accounts: Jean-Pierre du Bouvier, een in de gemeente bekende dierenactivist. De burgemeester vraagt Yarim om Jean-Pierre uit te nodigen voor een gesprek om met hem te spreken over methoden die wel en niet geoorloofd zijn. Als Yarim Jean-Pierre belt om hem namens de burgemeester uit te nodigen, houdt de activist zich op de vlakte en gaat niet op de uitnodiging in. Kort daarop wordt Yarim gemaild door een advocaat die vraagt op basis van welke bevoegdheid de burgemeester de politie heeft opgedragen om de identiteit van 'Idéfix' en 'Bobbie' vast te stellen. Het gaat hier wel om een inbreuk op artikel 8 EVRM, zo betoogt de advocaat, dus wil hij geen 'vaag geklets', maar 'een specifieke wettelijke bevoegdheid' vernemen, per mail. Hij kondigt al vast nadere juridische stappen tegen de gemeente aan. De burgemeester vraagt Yarim om advies.

5.12 Scenario 11: Netwerkcomplexiteit

De actiegroep «WOZ-GCT», beter bekend als «GCT» ('Geen Cent Teveel'), maakt via sociale media reclame onder inwoners van gemeente Natte Meren. Volgens het principe 'no-cure-no-pay' maakt GCT voor een inwoner van de gemeente bezwaar tegen de WOZ-beschikking. De groep richt zich elk jaar intensief op één gemeente, zodat er vanwege de vele berichten een sfeer ontstaat waarin extreem veel mensen zich aanmelden en de gemeente overbelast raakt − wat volgens hun filosofie allemaal bijdraagt aan het succcespercentage. Deze keer is Natte Meren doelwit. GCT pleegt geen strafbare feiten. Via social media worden burgers benaderd met wervende teksten ('500 Euro minder dankzij GCT!'). Deze teksten komen van inwoners uit enkele Nederlandse gemeenten die eerder doelwit waren. Wanneer je op de 'aanmeld-link' klikt, kom je uit bij een website op een server in de gemeente Rohrbach in Oostenrijk. Gemeente Natte Meren voorziet een administratieve én publicitaire chaos. Ze wil in gesprek met GCT, maar heeft behalve de website (www.wozgct.at) en een e-mailadres (info@wozgct.at) geen bereikbaarheidsgegevens. Op een gemeentelijke mail aan dat mailadres, wordt niet gereageerd. De burgemeester vraagt advies aan haar wethouders.

5.13 Hoofdlijnen in de scenario's: aandachtsgebieden

Hierboven schetsten we enkele situaties die zich gezien de huidige context (par. 4), in de komende 5 à 10 jaar bij gemeenten kunnen voordoen. Het zijn concrete scenario's op incidentniveau, gebeurtenissen die zich in de alledaagse bestuurlijke praktijk kunnen voordoen, en ook zijn te verwachten. Het zijn scenario's op het gebied van de gemeentelijke taken in een digitale samenleving (par. 3), tegen een achtergrond van maatschappelijke ontwikkelingen die met die digitalisering gepaard gaan (par. 4). Door de scenario's heen lopen enkele rode draden, die we in deze paragraaf benoemen. Dat geeft op een wat abstracter niveau munitie voor discussie over scenario's en over waarop gemeenten zich kunnen voorbereiden. Het zijn geen voorspellingen waarvan we zeker

weten dat ze uitkomen maar serieuze mogelijkheden die om die reden vragen om voorbereiding. Op basis van de hoofdlijnen uit de scenario's, komen we tot een 'handelingskader' (par. 6). Dat bestaat uit de eerder genoemde vier gemeentelijke taakgebieden en de vijf hoofdlijnen die dienen als aandachtsgebieden. Op elk van de taakgebieden kunnen gemeenten aandacht geven aan de vijf aandachtsgebieden, teneinde zich verder te ontwikkelen als lokaal bestuur in de digitale samenleving. De vijf aandachtsgebieden zijn op te vatten als een nadere uitwerking op de Agenda Digitale Veiligheid 2020-2024 (VNG 2020). Het gaat om vier inhoudelijke aandachtsgebieden en, niet in de laatste plaats, ethiek. De vier inhoudelijke aandachtsgebieden die volgen uit de scenario's zijn:

Kennispositie. Aangezien echtheidscomplexiteit nog steeds toeneemt en burgers beschikken over een solide organisatie- en informatievermogen, en daarvan gebruik maken, hebben gemeenten niet langer een monopoliepositie in kennis of zelfs maar specialistische kennis over actuele onderwerpen. Dat roept voor hen de vraag op (i) hoe zij een serieuze kennispositie behouden of ad hoc opbouwen, op de grote verscheidenheid aan onderwerpen waarmee zij te maken krijgen, en (ii) of gemeenten een rol hebben in het bestrijden van nepnieuws en zo ja hoe zij dat dan gaan doen.

Bevoegdheden. De huidige bestuurlijke bevoegdheden zijn gegeven met het oog op een analoge werkelijkheid. Gemeenten kunnen enkel een rol blijven spelen op het veiligheidsdomein als ze kunnen handelen in een digitale context. Derhalve moet worden nagegaan (i) of online optreden een grond kan vinden in bestaande bevoegdheden (geen wetswijziging vereist), (ii) of van bestaande bevoegdheden een digitale variant nodig is (aanpassen van bestaande wetgeving) en (iii) of speciaal voor de digitale context nieuwe bevoegdheden nodig zijn (geheel nieuwe wetgeving).

Monitoren. Om goed te kunnen functioneren moeten gemeenten weten wat er in hun gemeente speelt en dienen zij dus daarover informatie te vergaren. Al snel komt dat neer op het verzamelen van persoonsgegevens. De verleiding om veilig van achter het eigen bureau informatie over burgers te verzamelen is groot. Maar het is een evidente misvatting dat alles wat mensen over zichzelf online zetten, door de overheid onbeperkt mag worden verzameld en naar eigen inzicht mag worden gebruikt. Dat betekent dat gemeenten afgewogen protocollen moeten hebben voor het verzamelen van informatie over burgers (waarom, wat en hoe) én zich daarover geregeld zullen moeten verantwoorden, gevraagd èn uit eigen beweging. Dit vergt naast ethische afwegingen ook juridische expertise. Artikel 8 EVRM en de GDPR, plus de uit deze rechtsregels voortvloeiende eisen aan overheidsoptreden, zijn het voornaamste juridische referentiekader.

Intergemeentelijk samenwerken. De verdere vernetwerking van de samenleving en vooral het grensoverschrijdende karakter van digitale netwerken, maakt dat overheden, willen zij hun slagkracht behouden, niet kunnen blijven vasthouden aan oude geografische grenzen. Strafrechtelijke handhaving bijvoorbeeld, is door de jaren heen steeds meer landelijk georganiseerd en internationaal georiënteerd. Zo regelt het Cybercrimeverdrag dat verdragspartijen samenwerken in de opsporing en daartoe aanspreekpunten voor elkaar beschikbaar hebben. De vraag is hoe in bestuurlijke hand-

having kan worden samengewerkt in kwesties die vanwege de digitalisering de klassieke geografische grenzen doorsnijden dan wel overstijgen.

Deze vier aandachtsgebieden zijn inhoudelijke pijlers voor een gemeentelijk handelingskader. Ze zijn voor gemeenten het antwoord op de vraag (zie par.1) 'Waarmee gaan we aan de slag?' Hierna formuleren we per inhoudelijk hoofdthema enkele aandachtspunten en presenteren we ethiek als thema dat de andere thema's doorsnijdt. Dat geeft dan een antwoord op de vraag waarmee gemeenten bij het ontwikkelen van werkwijzen rekening hebben te houden.

6. Lokaal bestuur in een digitale samenleving

6.1 Inleiding

Gemeenten doen hun werk in een omgeving waarin burgers en bedrijven vanwege de digitalisering tal van nieuwe mogelijkheden hebben en die ook gebruiken: organisatie- en informatievermogen. Ook gemeenten hebben vanwege de digitalisering nieuwe mogelijkheden, maar ze zijn hun van oudsher relatief begunstigde positie inzake organisatie- en informatievermogen blijvend kwijt. Verder is de omgeving waarin gemeenten hun taken uitvoeren complexer, wat nieuwe vraagstukken van openbare orde en veiligheid met zich meebrengt. De dimensie 'echtheidscomplexiteit' is daarvan het fundamenteelste probleem omdat het twijfel zaait over wat waar of echt is, en daarmee geweld doet aan het vermogen van mensen om zich te oriënteren in hun leefomgeving, met soms dwalingen als gevolg en discussies die niet kunnen worden beslecht met rationele of wetenschappelijke argumenten. Dat speelt onder burgers, maar ook in de politiek. Moet de gemeente opstaan als hoeder van de waarheid: dwalingen en nepnieuws opsporen en corrigeren? De dimensie 'netwerkcomplexiteit' betekent dat veel OOV-vraagstukken al gauw een grensoverschrijdende karakter hebben, terwijl gemeentetaken en -strategieën van oudsher sterk fysiek-geografisch zijn begrensd. Anders dan 'echtheidscomplexiteit' plaatst dat de gemeente voor vraagstukken van een meer zakelijke aard: organisatie- en samenwerkingskwesties, die ondanks hun meer zakelijke karakter nog steeds om een antwoord vragen.

Gemeentetaken zijn verantwoordelijkheden en daarbij horen bevoegdheden. De typische gemeentetaak, waarover het hier gaat, is de zorg voor openbare orde en veiligheid. De orde kan worden verstoord en de veiligheid aangetast. Digitalisering geeft een nieuwe dimensie daaraan. De maatschappelijke orde en de maatschappelijke veiligheid kennen nu beide een fysieke én digitale dimensie − te onderscheiden maar niet te scheiden. De openbare orde en veiligheid in onze samenleving kunnen via de fysieke en via de digitale dimensie worden aangetast. Nog niet alle verschijningsvormen daarvan zijn tot het repertoire van gemeenten gaan behoren: van gemeentelijk optreden tegen de aantasting van *de online openbare orde* zijn nog geen voorbeelden bekend. Vanwege

de digitalisering zien gemeenten zich nu vooral voor kwesties geplaatst waarin de fysieke openbare orde wordt bedreigd met 'digitaal' in een initiërende of versterkende rol: de 'digitaal aangejaagde' verstoring van de openbare orde. De recente casus 'Bodegraven', waarbij online verdachtmakingen omtrent satanisch kindermisbruik leidden tot offline ordeverstoringen, is hiervan een voorbeeld. 'Drie mannen die online complotverhalen verspreiden over een satanisch-pedofiel netwerk en rituele kindermoorden in Bodegraven moeten daar onmiddellijk mee stoppen. Dat heeft de rechter bepaald in een kort geding dat was aangespannen door de gemeente Bodegraven-Reeuwijk. De beweringen leidden er afgelopen winter toe dat complotdenkers de begraafplaats in Bodegraven overstelpten met bloemen.'[19] Overigens heeft op veiligheidsgebied de 'geheel digitale variant' zich inmiddels wel een plek verworven in het gemeentelijk repertoire. Er zijn immers gemeenten die beleid maken en uitvoeren over weerbaarheid tegen bijvoorbeeld hacken – een delict dat zich geheel in de digitale wereld afspeelt.

Of het nu gaat om online aangejaagde of geheel online bestaande problemen, gemeenten nemen momenteel digitale dimensies van openbare orde en veiligheid op in hun oriëntatie en beleid. Terugkerende vragen daarbij zijn welke maatregelen juridisch toelaatbaar zijn (mag dit?), welke maatregelen effectief zijn (werkt dit?), welke maatregelen wenselijk zijn (willen we dit?) en welke mogelijkheden (kennis, vaardigheden, capaciteit, budget) een gemeente heeft om maatregelen te realiseren (kunnen we dit?).

De scenario's (par. 5) schetsen verschillende situaties waarvoor gemeenten zich de komende jaren gesteld zullen zien. Uiteraard niet steeds precies dát verhaal, maar wel de elementen die de gemeente voor een probleem plaatsen. Bijvoorbeeld: of het nu gaat om 6G of wat anders, gemeenten komen voor de vraag hoe ze omgaan met indringend nepnieuws; of het nu gaat om fideliateelt of wat anders, gemeenten krijgen te maken met digitaal georganiseerde actiegroepen die zich een kennispositie verwerven die die van de gemeente verre overklast, enzovoorts. We hebben uit de scenario's vijf aandachtsgebieden afgeleid die op hoofdlijnen weergeven waarop gemeenten kunnen anticiperen, willen zij althans effectief opereren in een gedigitaliseerde samenleving: kennispositie, bevoegdheden, monitoren, intergemeentelijk samenwerken en ethiek. Hierna komt bij elk van deze vijf aan de orde in welke richting gemeenten zich kunnen ontwikkelen om effectief te zijn in de digitale samenleving. We eindigen dat spoor niet met een stappenplan op uitvoeringsniveau. Daarvoor is het nog te vroeg. De stap die we hierna zetten, is wat daaraan juist voorafgaat: de stap die bij elk aandachtsgebied een richting schetst en vooral enkele aandachtspunten markeert, en aldus een kader aanreikt voor te ontwikkelen concrete werkwijzen: een handelingskader met in de basis vier gemeentelijke taakgebieden en vijf aandachtsgebieden die gelden voor elk van die vier.

[19] https://nos.nl/artikel/2387610-complotdenkers-bodegraven-moeten-stoppen-met-beschuldigingen, geraadpleegd 27 juli 2021.

6.2 Een handelingskader ... en verder

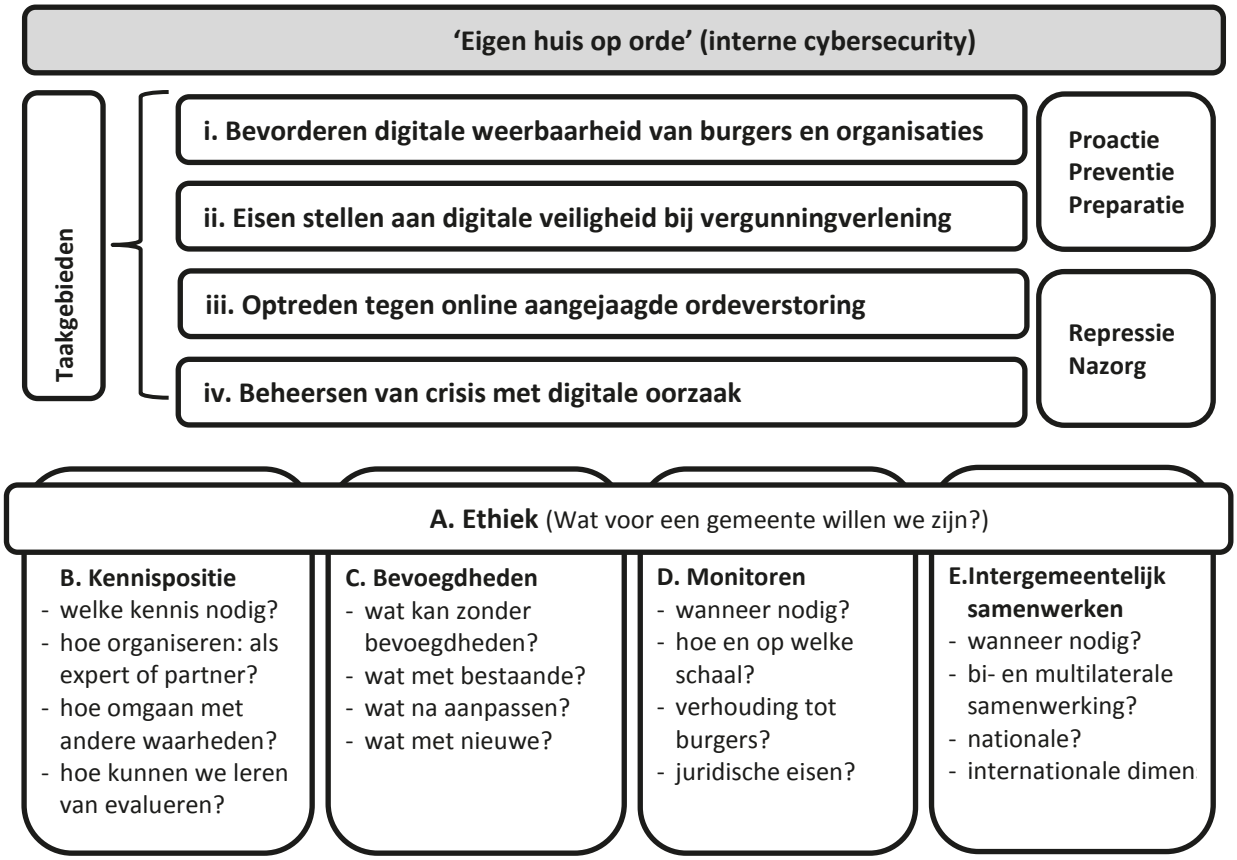
Bij aanvang van dit essay noemden we de drie taakgebieden uit de Agenda Digitale Veiligheid 2020-2024 (VNG 2020). Informatiebeveiliging (‘eigen huis op orde’) lieten we vervolgens buiten beschouwing omdat het weliswaar belangrijk is, maar geen typsiche bestuurlijke gemeentetaak. De dan resterende taakgebieden zijn: (a) digitale incidenten en -crisis en (b) digitale criminaliteit. In paragraaf 3.2 kwamen we voortbordurend daarop tot een wat gespecificeerdere indeling met vier taakgebieden: (i) bevorderen digitale weerbaarheid van mens en organisatie, (ii) eisen stellen aan digitale veiligheid bij vergunningplichtige activiteiten, (iii) optreden tegen het online aanzetten tot of aanjagen van een ordeverstoring, en (iv) beheersen van cybercrises. Bij de eerste twee ligt het accent op proactie, preventie en preparatie, bij de andere twee op repressie en nazorg. Daarbij heeft repressie in vroeg stadium, dus online, de voorkeur en niet pas wanneer op straat ‘de stenen er uit gaan’.

In een variëteit aan scenario’s zagen we dat gemeenten bij het werken aan de vier taakgebieden aanlopen tegen vraagstukken in relatie tot: (A) Ethiek, (B) kennispositie, (C) bevoegdheden, (D) monitoren en (E) intergemeentelijk samenwerken. Om hun handelend vermogen te versterken hebben zij op die vijf aandachtsgebieden stappen te zetten. 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.

Figuur 3 geeft een schematische presentatie van het handelingskader. Dat handelingskader is voor gemeenten een vertrekpunt voor het zetten van de laatste stap: het ontwikkelen van concrete werkwijzen oftewel een handelingsrepertoire, bijvoorbeeld vastgelegd in protocollen. Aldus vergroten gemeenten hun vermogen tot handelen in een digitaliserende samenleving.

Vertrekpunt voor gemeenten zijn hun vier taakgebieden i t/m iv. Op elk van die gebieden kunnen zij een handelingsrepertoire uitwerken, steeds met inachtneming van de vijf aandachtsgebieden ‘ethiek’, ‘kennispositie’, ‘bevoegdheden’, ‘monitoren’ en ‘intergemeentelijk samenwerken’. Gaat een gemeente aan de slag met één van de taakgebieden, bijvoorbeeld met ‘bevorderen digitale weerbaarheid’, dan dienen de vijf aandachtsgebieden de gemeente daarbij tot handvat. Ethiek en daarmee de vraag ‘Wat voor een gemeente willen we zijn?’ heeft daarbij een aparte positie. Dat dient beter niet per taakgebied te worden uitgewerkt, maar vraagt eerder om behandeling op in elk geval gemeenteniveau, uiteraard voorafgaand aan het op een bepaald taakgebied uitwerken van een handelingsrepertoire. Bij de vetgedrukte kopjes van de aandachtsgebieden A t/m E staan aandachtspunten. Die dienen als handvatten bij het ontwikkelen van concrete werkwijzen. Hierna bespreken we de vijf aandachtsgebieden, waarbij per aandachtsgebied de bijbehorende aandachtspunten aan bod komen (par. 6.2.1 t/m 6.2.5).

Figuur 3: handelingskader met vier gemeentelijke taakgebieden, uitgaande van 'eigen huis op orde'.



6.2.1 Ethiek

De overheid heeft als wellicht 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 aangaande 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' (Stol 2021). Voor gemeenten ligt dat niet anders. Wij pleiten daarom voor de gemeente als '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.

In het huidige debat over rechtshandhaving valt het geluid te horen dat 'ondermijning' geen prerogatief is van criminelen, ophitsers en complotdenkers, maar dat ook de overheid zelf het vertrouwen in de rechtsstaat geweld aan doet door zonder een daartoe strekkende bevoegdheid onschuldige burgers als verdachten te behandelen (vgl. de toeslagenaffaire en het eerdergenoemde monitoren door het LIMC en de NCTV[20]). Allereerst dient het lokale bestuur dus te waken over de waarden en normen in haar eigen bestuurlijke handhaving. Direct daarop, want daarover gaat het hier, volgt dat zij ten aanzien van digitalisering expliciteert welke waarden en normen gelden in haar gemeente, en welke eisen de gemeente dus ook stelt aan de digitalisering van anderen in haar gemeente. We beperken ons hier tot veiligheid (andere thema's zijn bijvoorbeeld inclusiviteit en gelijkheid). Wanneer een gemeente expliciet maakt wat gemeentelijke waarden en normen zijn aangaande digitale veiligheid, kunnen digitale praktijken van de gemeente, van inwoners, van organisatoren van evenementen, van scholen, instellingen en van ondernemers daarop worden beoordeeld.

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?

6.2.2 Kennispositie

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, ondergraaft dat haar slagvaardigheid en geloofwaardigheid.

Gezien op hoofdlijnen kunnen gemeenten op twee manieren reageren. (a) Ze kunnen trachten hun eigen kennisinfrastructuur en -vaardigheden te verstevigen en (b) ze kunnen 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: gemeenteparticipatie) 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

[20] Ook het met ANPR-camera's zonder wettelijke grondslag vastleggen van gezichten van bestuurders en bijrijders, past in dit rijtje (NRC, 4 augustus 2021, p.1).

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 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, 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, maar dan is het verschil minder principieel. Indien een gemeente en haar 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 nepnieuws. De ditalisering dwingt gemeenten als het ware tot een expliciete kennisstrategie. We noemen vier onderdelen daarvan, 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 èn 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.

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 'nepnieuws' 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 (vgl. par. 5.8, scenario 7a en 7b).

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.

6.2.3 Bevoegdheden

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.

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. In de politiepraktijk bijvoorbeeld was het tot zo'n dertig jaar geleden gebruikelijk om een verdachte voor een gesprek uit te nodigen' (bv. op straat: 'ik wil je hierover even spreken, kom je vanmiddag om vier uur even naar het bureau?'). In een proces verbaal stond dan zoiets als 'heden, verscheen vrijwillig aan het bureau ...'. Omdat de status van de aanwezigheid (wel of niet aangehouden, wel of niet verdachte, welke rechten?) daarmee onduidelijk bleef, is deze praktijk op een zeker moment vrij abrupt veranderd, afgeschaft, geformaliseerd, wat voor alle partijen meer duidelijkheid schiep. Te verwachten valt dat deze beweging, het formaliseren van de relatie tussen overheid en burger, ook in bestuurlijk overheidsoptreden verder ingang vindt. Bevoegdheden zijn dus 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.

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. In de scenario's kwamen we bijvoorbeeld tegen een bevoegdheid om de identiteit van een aanstichter te laten achterhalen (par. 5.11, scenario 10b) en de bevoegdheid tot online ingrijpen door opruiende teksten naar een minder zichtbare plek te verplaatsen (par. 5.7, scenario 6). Aandacht is vereist voor (a) mogelijkheden die voorafgaan aan het gebruik van bevoegdheden (bv. voorlichting, het gesprek aangaan), (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.

6.2.4 Monitoren

Met de studie van Bantema e.a. (2021) is het onderwerp 'monitoren' hoog op de politieke agenda geraakt. 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.[21] Deze discussie past in het bredere maatschappelijke debat over de verhouding tussen overheid en burger en in een nog bredere maatschappelijke context, namelijk 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, het gebruik van gender-aanduidingen, registreren van etniciteit in landelijke statistiek, lbhtiq+-acceptatie, en de toeslagenaffaire, om er maar een paar te noemen. 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, welke weerstand vanwege de digitalisering snel kan worden georganiseerd en ruim geïnformeerd. De verleiding om vanachter een bureau speurdersactiviteiten te verrichten is desalniettemin kennelijk groot. Zo bleek eerder al dat het Land Information Manoeuvre Centre (LIMC) van Defensie online informatie over de Nederlandse bevolking verzamelde, evenals de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).[22] 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 niemands 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

[21] NRC 19 mei 2021, www.vpngids.nl
[22] Resp. NRC 15 november 2020 en NRC 9 april 2021.

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)[23] verzamelen van informatie over een persoon is daarom nu toepassing van artikel 126j Wetboek van Strafvordering 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 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 GDPR 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 Zwolsmancriterium als richtsnoer. 'Een antwoord op de vraag hoe ver 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 Pw. Anders is voor het betreffende optreden een afzonderlijke wettelijke voorziening vereist.'[24] (Stol & Strikwerda 2018, p.9-10). 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

[23] 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)

[24] 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).

haar gebruikers (vgl. 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.[25] 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 (Bantema e.a. 2021) 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 dus op de hoogte kunnen stellen en 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 dichtbijbestuur. 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' (Bantema e.a. 2021, p. 116). Ook de vraag wat voor een lokaal bestuur je als gemeente wilt zijn (ethiek) verdient hier een plaats.

(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

[25] ECLI:NL:HR:2017:584

bevoegdheden zijn vereist, kunnen gemeenten gebruik maken van de ervaringen die binnen de strafrechtspleging zijn opgedaan.

6.2.5 Intergemeentelijk 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 (par. 5.12, scenario 11). Ook een techbedrijf kan een rol spelen, wat een gemeente voor de vraag plaatst of zij bijvoorbeeld Facebook tot optreden kunnen dwingen. Eerder zagen we dat 59 procent van de burgemeesters meer willen samenwerken met sociale mediaplatforms, terwijl niet meer dan 15 procent van de burgemeesters aangeeft ooit contact te hebben gezocht met een dergelijk platform (Bantema e.a. 2020).

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 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.

Literatuur

Bantema, W., S.M.A. Twickler, S.A.J. Munneke, M. Duchateau en W.Ph. Stol (2018) *Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*. Den Haag: Sdu (reeks Politie en Wetenschap, nr. 103).

Bantema, W. en W.Ph. Stol (2020). Hoe burgemeesters kunnen bijdragen aan een digitaal veilige samenleving. In C. de Poot, E.Lievens, W. Stol & L. De Kimpe (red.) (2020) *Cahier Politiestudies*, jaargang 2020/3, themanummer Politie en Cybercrime, pp. 223-237.

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

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).

Elias, N. (1984, oorspr. 1939). *Het civilisatieproces.* Utrecht/Antwerpen: Het Spectrum.

Giddens, A. (1984). *The Constitution of Society.* Cambridge: Polity Press.

Huxley, A. (1932) *Brave New World.* London: Vintage.

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).

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.

Liebregts, J. (2016) De ketenbenadering. In W. Stol, C. Tielenburg, W. Rodenhuis, E. Kolthoff, M. van Duin en S. Veenstra, *Basisboek Integrale Veiligheid*, Den Haag: Boom criminologie, pp. 53-68.

Marcuse, H. (1964) *One Dimensional Man. Studies in the Ideology of Advanced Industrial Society.* Boston: Bacon Press.

Mumford, L. (1934) *Technics and Civilization*. New York: Harcourt Brace Jovanovich Publishers.

Pieterson, M. (1981). *Het technisch labyrinth.* Meppel: Boom.

Smith, A., (1987, oorspr. 1776). *The wealth of nations.* Harmondsworth: Penguin Books.

Stol, W.Ph. en J. Jansen (2013). Politie in een digitaliserende samenleving. Waar staat de politie nu, wat vraagt aandacht? *IPA Actief*, nr. 342, zomer 2013, p. 17.

Stol, W.Ph. en L. Strikwerda (2017) *Strafrechtspleging in een digitale samenleving.* Den Haag: Boom Juridisch.

Stol, W.Ph. & L. Strikwerda (2018) Online vergaren van informatie voor opsporings-onderzoek. Een beknopte evaluatie van voorgestelde wetgeving. *Tijdschrift voor Veiligheid*, 17, 1/2, 8-22.

Stol, W.Ph. en W. Bantema (2019). De gemeente en de digitaal veilige stad. In J.W. Sap & E. Kolthoff (red.) *De veilige stad als collectief doel.* Nijmegen: Ars Aequi Libri, pp. 123-130.

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 Criminologe, pp. 363-385.

Stol, W.Ph. en N.Kop (2020) De politie. In M. Bolhuis, Y. Schoenmakers & G. Beijers (red.) (2016) *Actoren in de strafrechtspleging.* Den Haag: Boom criminologie, pp. 15-34.

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.

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

Bijlage 1 – opzet bestuurlijke expertmeeting

Deel 1 (30 minuten)

Welke ontwikkelingen komen door de digitalisering de komende 5 tot 10 jaar op gemeenten af, en kunnen gemeenten daarop anticiperen?

Deel 2 (45 minuten)

We hebben scenario's ontwikkeld die gemeenten voor een probleem kunnen plaatsen. Bij elk scenario is de vraag of het reëel is (1) en zo ja of en hoe gemeenten zich daarop kunnen voorbereiden en wat daar eventueel voor nodig is.

1. Gemeenten moeten zich meer en meer verantwoorden over privacy en over het verzamelen van en omgaan met informatie van burgers.

Een medewerker OOV hoort via via van een demonstratie die wordt voorbereid. Het doel ervan zou zijn om uit te lokken tot politiegeweld. Een medewerker OOV houdt de voorbereidingen van het evenement in de gaten en bezoekt de website herhaaldelijk om meer informatie te krijgen. Na 14 dagen wordt de ambtenaar plots gebeld door de beheerder van de website om te vragen waarom hij geregeld de website bezoekt. De bezoeken zijn secuur gelogd en zeven zijn herleidbaar tot de gemeente. Een jurist gaat nu namens de actiegroep de gemeente aanklagen voor schending van onder andere de AVG en artikel 8 EVRM.

2. Burgers organiseren zich steeds beter en hebben, bijvoorbeeld in actiegroepen, een zeer sterke kennispositie. Het is moeilijk voor gemeenten om op alle actuele onderwerpen zo'n sterke kennispositie te hebben. Dat maakt het lastig om beleid te verdedigen of nepnieuws te ontkrachten. Er zijn nu twee varianten:

a. De gemeente ziet zich gesteld tegenover een serieuze actiegroep met solide kennis van zaken. Die groep heeft daardoor een publicitair en juridisch sterk verhaal dat ingaat tegen een besluit van de gemeente.

b. De gemeente ziet zich gesteld tegenover een groep die met een digitale robot nepberichten verspreid, welke berichten een besluit van de gemeente ondermijnen.

3. Gemeenten kunnen alleen een rol blijven spelen in veiligheid als ze ook online kunnen handelen. Is van oude bevoegdheden een nieuwe variant nodig of moeten er nieuwe bevoegdheden komen? Waar schuurt het nu?

In gemeente Natte Meren plaats een drill-rapper herhaaldelijk liedjes op sociale media. Deze liedjes hebben al geleid tot ernstige geweldplegingen. Uit veiligheid voor de omgeving geeft de gemeente de rapper een gebiedsverbod én verplaatst zij de liedjes van social media náár de website van de rapper. Zo is de ontstane onrust ingedamd maar kan hij zijn muzikale expressie continueren.

4. Vernetwerking samenleving en grensoverschrijdende karakter van digitale netwerken.

Het bedrijf ‘Zelfdoding Wij Helpen’ maakt via sociale media reclame onder inwoners van Berglanden. Andere gemeenten zijn geen doelwit. Er zijn geen strafbare feiten maar er is wel een volksgezondheidsrisico vanwege de toch al lange wachtlijsten in de psychische zorg. De reclames komen van inwoners uit verschillende Nederlandse gemeenten. Wanneer je op een link klikt, kom je op een website met een server in de gemeente Rohrbach in Oostenrijk. Het aantal zelfdodingen in Berglanden is in een half jaar verdubbeld, evenals de wachtlijst voor psychische hulp.

Bijlage 2 – respondenten expertmeeting

	Deelnemers
17 juni **10.30-12.00uur** 5 deelnemers	Wim Willems, wethouder gemeente Apeldoorn
	Melis van de Groep, burgemeester gemeente Bunschoten
	Mark van Stappershoef, burgemeester gemeente Goirle
	Hans Ubachs, burgemeester gemeente Best
	Iris Meerts, burgemeester gemeente Wijk bij Duurstede
17 juni **13.30-15.00** **7 deelnemers**	Martijn Vroom, burgemeester gemeente Krimpen aan den IJssel
	Franc Weerwind, burgemeester gemeente Almere
	Cornelis Visser, burgemeester gemeente Katwijk
	Marco Out, burgemeester gemeente Assen
	Frans Backhuijs, burgemeester gemeente Nieuwegein
	Nanning Mol, burgemeester gemeente Laren
	Kees van Rooij, burgemeester gemeente Meierijstad

Bijlage 3 – respondenten interviews

Naam	Functie	Wanneer
Reijer Passchier	Universitair docent Staats- en bestuursrecht (Universiteit Leiden)	22-06
Jan-Jaap Oerlemans	Bijzonder hoogleraar Inlichtingen en Recht (Universiteit Leiden)	24-06
Hanne van Aert	Burgemeester gemeente Loon op Zand	08-07
Peter-Paul Verbeek	Hoogeleraar Filosofie van Mens en Techniek (UT)	08-07
Jeroen van den Hoven	Hoogleraar Ethiek en Technologie (TU Delft)	14-07
Cees van de Sanden	Advocaat gespecialiseerd in bestuurs- en privacyrecht	07-09

THORBECKE
ACADEMIE

NHL STENDEN