De veilige stad als collectief doel

Jan Willem Sap & Emile Kolthoff (red.)

De veilige stad als collectief doel

Onder redactie van
Jan Willem Sap & Emile Kolthoff

Ars Aequi Libri
Nijmegen 2019

Inhoudsopgave

De gemeente en de digitaal veilige stad

Wouter Stol en Willem Bantema

Wie spreekt over de veilige stad, heeft het ook over de *digitaal* veilige stad. Politie en justitie werken al geruime tijd aan het bestrijden van cybercrime en daarmee aan het bevorderen van een digitaal veilige samenleving.[1] Maar zij alléén kunnen niet zorgen voor digitale veiligheid. Terecht zeggen bijvoorbeeld burgers en bedrijven dat die verantwoordelijkheid vooral ligt bij andere partijen dan de politie.[2] Zij denken dan allereerst aan financiële instellingen, eigenaren van websites, digitale dienstverleners zoals internet service providers (ISP's) en niet in de laatste plaats aan zichzelf. De politie komt volgens burgers en bedrijven in die twee onderzoeken op de laatste plaats. Natuurlijk spelen ook anderen een rol in het bewaken van de digitale veiligheid, zoals ICT-producenten, online marktplaatsen, techgiganten zoals Facebook en Google, stichtingen zoals het meldpunt kinderporno op internet en diverse onderdelen van de landelijke overheid. Gemeenten echter, bleven lange tijd buiten beschouwing als partij met een rol in het bevorderen van digitale veiligheid. Dat is inmiddels veranderd. In kringen van lokaal bestuur wordt sinds 2014 gesproken over wat hun bijdrage kan zijn aan een digitaal veilige samenleving.[3] In enkele jaren is dat vervolgens uitgegroeid van een non-issue tot een hot topic.

Voor zover valt na te gaan, schrijft Vols in 2010 in zijn masterscriptie als eerste over de vraag of cyberspace tot de openbare ruimte moet worden gerekend – en dus of de burgemeester ook daar een verantwoordelijkheid heeft.[4] Het werk krijgt echter geen vervolg en het thema blijft op de achterrond. In de zomer van 2013 noemen Stol & Jansen 'de rol van de burgemeester in de online veiligheidszorg' dan ook 'een vergeten onderwerp'.[5] In september 2014 organiseert de Thorbecke Academie van de toenmalige NHL Hogeschool samen met het Nederlands Genootschap voor Burgemeesters (NGB) en de gemeente Leeuwarden een kennisconferentie over de rol van de burgemeester in cyberspace.[6] De tenneur onder de aanwezige burgemeesters is dat zij geen rol voor zichzelf zien in de digitale wereld.[7] Dat weerspiegelt het tijdsbeeld. Stol & Strikwerda observeren in 2017: '(...) de notitie *Burgemeester & Veiligheid* van 8 april 2009, door de minister van Binnenlandse Zaken en Koninkrijksrelaties op 9 april 2009 aangeboden aan de voorzitter van de Eerste Kamer der Staten-Generaal, "beschrijft de maatschappelijke en bestuurlijke context waarbinnen de burgemeester invulling moet geven aan zijn veiligheidsportefeuille". De woorden cyber, internet, digitaal en digitale komen in het stuk niet voor. Die woorden komen ook niet voor in het in 2010 gepubliceerde *Zakboek openbare orde en veiligheid*, van het Nederlandse Genootschap van Burgemeesters

1 W.Ph. Stol, R.J. van Treeck & A.E.B.M. van der Ven, *Criminaliteit in cyberspace*. Den Haag: Elsevier, 1999; W.Ph. Stol & L. Strikwerda, *Law Enforcement in Digital Society*. The Hague: Eleven International Publishing, 2019.

2 S. Veenstra, R. Zuurveen & W.Ph. Stol, *Cybercrime among companies.* Den Haag: Eleven International Publishing, 2016, p. 188; M.M.L. Domenie, E.R. Leukfeldt, J.A. van Wilsem, J. Jansen & W.Ph. Stol, *Victimisation in a Digitised Society.* Den Haag: Eleven International Publishing, 2013, p. 83.

3 W.Ph. Stol & L. Strikwerda 2019, a.w., p. 54.

4 S. Vols, 'Virtuele handhaving van de openbare orde'. Groningen: Rijksuniversiteit Groningen, 2010.

5 W.Ph. Stol & J. Jansen, 'Politie in een digitaliserende samenleving', *IPA-actief*. Nr. 342, zomer 2013, p. 11-17, met name p. 17.

6 https://www.burgemeesters.nl/node/4050, geraadpleegd 10 januari 2019.

7 *Leeuwarder Courant*, 11 september 2014, p. 28.

(Van Bennekom & Jong, 2010).'[8] Een subsidieaanvraag in 2015 van NHL Hogeschool bij RAAK voor een onderzoek naar de (on)mogelijkheden van virtuele ordehandhaving werd niet gehonoreerd, onder meer omdat het onderwerp niet urgent is en het onderzoek te weinig is opgebouwd vanuit concrete vragen uit de praktijk. In het rapport 'Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht' van de Adviesraad Internationale Vraagstukken, dat gaat over internet en overheidsingrijpen, komt het woord 'gemeente' niet voor.[9] Kortom, 'digitale veiligheid' en 'lokaal bestuur' zijn in die jaren niet of nauwelijks met elkaar verbonden.

Een herhaalde subsidieaanvraag voor hetzelfde onderzoek wordt in 2016 door het programma Politie en Wetenschap gehonoreerd. Aldus doen Bantema, Twickler, Munneke, Duchateau & Stol in 2017 'een verkenning naar de mogelijkheden en onmogelijkheden van de burgemeester om preventief online op te treden in gevallen waarbij de openbare orde verstoord wordt of dreigt verstoord te raken door wat online gebeurt.'[10] De onderzoekers voeren een juridische analyse uit en behandelen de rol van de gemeente bij ordehandhaving in een digitale omgeving, onder meer op basis van interviews met 25 experts en 14 burgemeesters. Uitkomsten komen verderop aan bod. Eén van de effecten van het onderzoek is dat het thema wat de gemeente kan doen aan digitale veiligheid een prominentere plaats krijgt op de agenda van lokaal veiligheidsbeleid. De onderzoekers bespreken het onderwerp tijdens diverse themadagen aangaande gemeentelijk veiligheidsbeleid, waarbij vertegenwoordigers van gemeenten en soms van landelijke organisaties aanwezig zijn, zoals de Vereniging Nederlandse Gemeenten (VNG) vertegenwoordigers van de G40, het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en het NGB. De bredere vraag 'Wat kan de gemeente bijdragen aan digitale veiligheid?' mag tijdens die bijeenkomsten rekenen op grote belangstelling. Zelfs cybercrimebestrijding, wat tot die tijd niets voor de gemeente leek, is nu binnen het gemeentelijk blikveld geraakt. Zo is bijvoorbeeld de burgemeester van Den Helder 'de komende vier jaar provinciaal aanspreekpunt voor het tegengaan van cybercrime'.[11] 'De gemeente Leeuwarden wil het komende jaar verder werk maken van het terugdringen van cybercrime bij het mkb en ook bij de inwoners.'[12] Gemeentes organiseren bijeenkomsten tegen cybercrime, zoals in de gemeentes Maassluis en Scherpenzeel, met een openingswoord van respectievelijk burgemeester Haan en burgemeester Van Rhee-Oud Ammerveld.[13] Kortom, gemeenten en burgemeesters manifesteren zich vandaag de dag nadrukkelijk als speler in het veld voor digitale veiligheid.

8 R. van Bennekom, R. & W. Jong (red.), *Zakboek openbare orde en veiligheid*. Den Haag: Nederlands Genootschap van Burgemeesters, 2010; W.Ph. Stol & L. Strikwerda, *Strafrechtspleging in een digitale samenleving*. Den Haag: Boom juridisch, 2017, p. 55-56.

9 Adviesraad internationale vraagstukken (AIV), *Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht*. Rapport no. 92. Den Haag: Ministerie van Buitenlandse Zaken, 2014.

10 W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.Ph. Stol, *Burgemeesters in cyberspace*. Den Haag: Sdu, 2018, p. 10.

11 *Noordhollands Dagblad*, 8 januari 2019, sectie Helderse Courant, p. 1.

12 *Leeuwarder Courant*, 29 december 2018, Editie Zuid, p. 20.

13 *AD/Rotterdams Dagblad*, 14 november 2018, Rotterdam Waterweg Editie, p. 6; *De Rijnpost*, 21 november 2018, RP1 Editie p. 12.

'Project X' en oude principes

De enigszins in internet en ordevraagstukken ingevoerde lezer mist in de vorige paragraaf wellicht een verwijzing naar 'project X' op 21 september 2012 te Haren, ook wel de Facebookrellen genoemd. Project X is echter geen treffende illustratie bij het hierboven besproken thema. Sterk vereenvoudigd voorgesteld heeft project X gemeenten geleerd dat wat online begint (bv. een oproep tot een feest) wel eens op straat uit de hand kan lopen. Het heeft gemeenten daarentegen niets geleerd over de bestuurlijke bevoegdheden en andere mogelijkheden om *online* maatregelen te nemen. Project X was uiteindelijk vooral een offline probleem waarbij de Mobiele Eenheid (ME) het op straat opnam tegen relschoppende jongeren.

Dat een gemeente er rekening mee moet houden dat online communicatie aan de basis ligt van een offline ordeverstoring, is nauwelijks een nieuw inzicht te noemen. Digitale communicatie, toen nog per sms, speelde bijvoorbeeld een rol bij de supportersrellen in Beverwijk in 1997. Hooligans van de voetbalclubs Ajax en Feijenoord spraken af te gaan vechten, hetgeen uitmondde in een massale vechtpartij in een weiland bij Beverwijk, waarbij één dode viel. Het vermogen om via digitale communicatie mensen op de been te brengen werd in 2003 nog eens, maar dan op ludieke wijze, gedemonstreerd in zogenoemde flashmobs. 'Dat is een (grote) groep mensen die plotseling op een openbare plek samenkomt, iets ongebruikelijks doet en daarna weer snel uiteenvalt. Flashmobs worden veelal georganiseerd via moderne communicatiemiddelen zoals het internet.'[14] De eerste flashmob was in mei 2003 in New York, daarna waaide het fenomeen snel over naar Europa. De eerste Nederlandse flashmobs waren in Amsterdam en Rotterdam op 8 en 9 augustus 2003. In Rotterdam staken tientallen deelnemers plotseling een paraplu op en hielden die twee minuten hoog, ook al viel er geen druppel regen.

Project X in 2012 heeft dus niet een nieuw organisatieprincipe getoond. Het heeft gemeenten enkel nog eens laten zien dat een online oproep tot ongeregeldheden kan leiden, serieuze offline gevolgen kan hebben en dat het dus vanwege de gemeentelijke verantwoordelijkheid voor orde en veiligheid, ook zaak is om online signalen in acht te nemen. De Adviesraad Internationale Vraagstukken heeft het over 'de mobilisatiefunctie van internet'.[15]

Ons thema is welke mogelijkheden de gemeente heeft tot het ondernemen van actie *in de online omgeving*, met als doel een bijdrage te leveren aan de veiligheid in de samenleving. Dat vraagt van een gemeente dat zij de blik niet zozeer richt op wat er uiteindelijk op straat uit de hand kan lopen en hoe daarbij op te treden (bv. de ME inzetten) maar dat zij de blik richt naar wat zij *online* al kan ondernemen om te voorkómen dat orde en veiligheid op straat worden bedreigd.

Een nieuwere en weinig toegepaste variant is dat een gemeente online maatregelen neemt om te voorkomen dat de *online openbare orde* wordt verstoord. Dat is meteen ook een vrij complexe variant omdat dan eerst dient te worden bepaald of er online een openbare orde bestaat, of die kan worden verstoord en zo ja of de gemeente de instantie is om die orde te handhaven. Dat brengt de discussie naar onontgonnen terreinen waarover Bantema e.a. concluderen: 'Hoewel we dus in onze samenleving kunnen besluiten dat in cyberspace geen plaats is voor bestuurlijke handhaving, lijkt die keuze niet echt logisch. Het zou een tamelijk radicale breuk zijn in het handhavingsbeleid en de voordelen van zo'n keuze zijn niet

14 Bron: https://nl.wikipedia.org/wiki/Flashmob, geraadpleegd 10 januari 2019.

15 Adviesraad Internationale Veiligheid (AIV), *Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht*. Rapport no. 92. Den Haag: Ministerie van Buitenlandse Zaken, 2014, p. 61.

eenvoudig in te zien. Een nadeel van een keuze voor bestuurlijke handhaving in alle delen van onze samenleving, en dus ook in cyberspace, is wel meteen duidelijk: de uitvoering van die keuze is nog niet zo eenvoudig, dat laat ons onderzoek in elk geval zien. Maar een principiële keuze moet bij voorkeur niet worden ingegeven door uitvoeringsperikelen. Eerder is het zaak om de uitvoeringsperikelen die een principiële keuze met zich meebrengt te bestuderen en op te lossen. Het verdient aanbeveling om op die weg verdere stappen te zetten.'[16]

In afwachting van verdere helderheid aangaande het onontgonnen terrein van bestuurlijke handhaving van de openbare orde *in* cyberspace, zijn wel al enkele terreinen te identificeren waarop gemeenten nu al kunnen acteren en terreinen die minder ingewikkeld zijn dan bestuurlijke handhaving van de openbare orde in cyberspace en waar handelingsperspectieven met nader onderzoek binnen handbereik lijken te zijn. Die terreinen passeren hierna de revu als gemeentelijke *work packages* voor veiligheid in een digitale samenleving.

Vijf gemeentelijke work packages voor digitale veiligheid

De gemeente kan met verschillende *work packages* bijdragen aan digitale veiligheid. We bespreken er vijf, niet per se in volgorde van urgentie. Natuurlijk zijn er dwarsverbanden tussen de vijf, maar omwille van het overzicht presenteren we ze hier apart.

Informatiebeveiliging
Ten eerste dient de gemeente natuurlijk haar ICT en vooral de daarop vastgelegde informatie effectief beschermen. Zij dient weerbaar te zijn tegen cybercrime en ook anderszins het lekken van informatie tegen te gaan. De gemeente heeft een voorbeeldfunctie en zal dat dus beter moeten doen dan gemiddeld. Bij het bepalen van wat er moet gebeuren en hoe dat te doen, kan de gemeente zich baseren op inzichten en standaards uit de informatiebeveiliging. Afgezien van de voorbeeldfunctie is dit allemaal niet gemeentespecifiek; de andere *work packages* zijn dat wel.

Regierol
Ten tweede kan de gemeente een stimulerende rol vervullen voor wat andere partijen doen aan het vergroten van de digitale veiligheid. De gemeente kan burgers en bedrijven in haar werkgebied voorlichting geven over hoe zij kunnen bijdragen aan digitale veiligheid, zoals hierboven de gemeenten Maassluis en Scherpenzeel. Vanuit haar klassieke 'regierol'[17] kan de gemeente partijen bij elkaar brengen in coalities die sterker zijn dan de som der delen. De gemeente kan bijvoorbeeld scholen met digitaal vaardige leeringen of studenten in een project koppelen aan MKB-ondernemers die niet weten hoe ze zich digitaal kunnen beveiligen of daarvoor geen tijd hebben. Talloze verbindingen kunnen worden gelegd om de digitale weerbaarheid in een gemeente te vergroten en de kansen voor cybercriminelen te verkleinen. Hierbij heeft de gemeente dus niet zozeer de rol van expert maar vooral die van bemiddelaar of regisseur.

16 W. Bantema e.a., a.w., 2018, p. 136.

17 C. Tielenburg & W.Ph. Stol, 'Rijk, provincie, gemeente en andere bestuursorganen', in: W.Ph. Stol, C. Tielenburg, W. Rodenhuis, E. Kolthoff, M. van Duin & S. Veenstra (red.), *Basisboek Integrale Veiligheid*. Den Haag: Boom criminologie, 2016, p. 199-213, met name p. 209.

Bestuurlijke maatregelen

Het derde *work package* is wat ingewikkelder. Het gaat om het nemen van maatregelen in situaties waarbij door activiteiten in cyberspace de offline openbare orde wordt bedreigd.[18] Bij 'maatregelen' kunnen we denken aan het toepassen van formele bevoegdheden en aan het acteren op andere wijze. Als de activiteiten op internet waartegen de gemeente in actie zou willen komen, strafbare handelingen zijn (bv. discriminatie, opruiing), is het strafrecht het eerst aangewezen instrument en zijn politie en justitie de eerst aangewezen partijen om in actie te komen. Gaat het om andere online activiteiten die de offline openbare orde (dreigen te) verstoren, dan is de burgemeester als eerste aan zet. Artikel 172 lid 1 Gemeentewet stelt immers dat 'De burgemeester is belast met de handhaving van de openbare orde'. Lid 2 voegt daaraan toe: 'De burgemeester is bevoegd overtredingen van wettelijke voorschriften die betrekking hebben op de openbare orde, te beletten of te beëindigen. Hij bedient zich daarbij van de onder zijn gezag staande politie.' En lid 3 luidt: 'De burgemeester is bevoegd bij verstoring van de openbare orde of bij ernstige vrees voor het ontstaan daarvan, de bevelen te geven die noodzakelijk te achten zijn voor de handhaving van de openbare orde.' Een cruciale vraag is nu of bestaande bevoegdheden, ooit geschreven vanuit en voor toepassing in een fysieke wereld, zich laten vertalen naar toepassing in de digitale ruimte. Bijvoorbeeld: kan de burgemeester op grond van artikel 172a Gemeentewet (gebiedverbod) aan een persoon het verbod opleggen om zich op bepaalde online fora of websites te begeven, ofwel een digitaal gebiedsverbod?

Hun verkenning leidt Bantema e.a. tot de conclusie dat de burgemeester niet zomaar op grond van bestaande openbare-ordebevoegdheden online kan optreden tegen activiteiten die de offline openbare orde (dreigen te) verstoren: 'grote problemen kunnen zich voordoen rond vraagstukken als het noodzakelijkheidsvereiste, de subsidiariteit, de evenredigheid, de voorspelbaarheid van de grondrechtenbeperking, de grondwettelijke eis dat een maatregel die grondrechten beperkt daar ook specifiek voor is bedoeld en op is afgestemd (de leer van de bijzondere beperkingen) en de vraag naar de causaliteit. Bepaalde grondrechten, met name de vrijheid van meningsuiting en het recht op bescherming van de persoonlijke levenssfeer zullen bovendien steeds harde grenzen stellen aan wat wel en niet mag, welke vorm van regulering ook wordt gekozen. Daarnaast betekent aansluiting bij de offline verstoring in de fysieke wereld ook dat wordt aangesloten bij de territoriale begrenzing van gemeentelijke bevoegdheden op dit punt. Probleem is hier dat de offline verstoring weliswaar territoriaal bepaald kan zijn, maar dat dit niet hoeft te gelden voor de online aanleiding.'[19] Bantema en collega's wijzen op een andere route. Dat gemeenten niet proberen om vigerende wetgeving te gaan toepassen op een situatie waarvoor ze niet is ontworpen maar 'dat we regels maken die ook bedoeld zijn om in de online wereld te werken en die daarop zijn afgestemd'.[20] Zo gezien is niet de burgemeester maar de wetgever aan zet.

Maar de burgemeester staat ook weer niet geheel met lege handen waar het gaat om optreden tegen online activiteiten die de offline openbare orde (dreigen te) verstoren. Onder het kopje 'andere wegen dan bestuursrechtelijke handhaving' spreken Bantema e.a. over 'slimme handhaving door burgemeesters, zonder dat zij gebruikmaken van formele

18 De situatie dat door online activiteiten de openbare orde *in* cyberspace (de online openbare orde) wordt verstoord, blijft hier, zoals gezegd, buiten beschouwing.

19 Bantema e.a., a.w., 2018, p. 122.

20 Bantema e.a., a.w., p. 121.

bevoegdheden.'[21] De lijst met instrumenten is echter kort: (i) online in gesprek gaan met de personen achter de uitingen die de offline orde (dreigen te) verstoren; (ii) al dan niet op basis van de Notice and Take Down[22] procedure contact opnemen met digitale dienstverleners om de uitingen die in strijd zijn met de gebruikersvoorwaarden van het bewuste platform offline te laten verwijderen; (iii) het online verspreiden van uitingen die de gewraakte uitingen tegenspreken of nuanceren; (iv) het opleggen van een dwangsom om bijvoorbeeld een online aangekondigd illegaal offline feest te voorkomen. Het zijn slechts enkele instrumenten en ook nog eens niet meer dan summier uitgewerkt. De tweede van deze vier instrumenten lijkt de slimste omdat de burgemeester dan een beroep doet op private partijen met het verzoek om hun gebruikersvoorwaarden te handhaven, en daarmee niet alléén maar in samenwerking met andere partijen optreedt. Aandachtspunt is dan weer wel dat een gemeentelijk initiatief om bepaalde uitingen offline te laten halen, een effect heeft dat zich tot (ver) buiten de gemeente uitstrekt. Kortom, voor het derde *work package* heeft de burgemeester dus niet al een uitgekristalliseerde set gereedschappen maar een begin is gemaakt en nader onderzoek zal de bestaande set moeten completeren, concretiseren en op legitimiteit en effectiviteit evalueren.

Monitoren

Het vierde *work package* betreft het zogenoemde 'monitoren' van internet. Een gemeente die er alert op is dat ordeverstoringen online kunnen beginnen, zal de behoefte voelen om te overzien ('monitoren') wat van hetgeen zich online afspeelt mogelijk de offline orde binnen de gemeente kan verstoren. 'Alle geïnterviewde burgemeesters vinden een informatiepositie in cyberspace erg belangrijk, maar ze verschillen wel over de vraag wie die werkzaamheden of taak zou moeten vervullen. Na Project X blijken de meeste gemeenten veel te doen om ook in cyberspace te voorzien in hun informatiepositie, maar de manier waarop zij dat vormgeven en de intensiteit ervan verschilt.'[23] Twee aspecten zijn hierbij van belang. Ten eerst is de vraag hoe gemeenten het praktisch gesproken organiseren om het internet te overzien. Is dat een taak van iedere gemeente afzonderlijk? Is het een taak voor de grotere gemeenten of van een landelijke instantie? Een politietaak? Internet kent geen geografische grenzen en dus dient in relatie tot 'monitoren' ook te worden nagedacht over internationale samenwerking. Immers, een gemeente kan via 'monitoren' zicht krijgen op lokale dreigingen maar ook op grensoverschrijdende voornemens tot ordeverstoring. Ten tweede is de vraag hoe ver gemeenten met 'monitoren' kunnen gaan zonder in strijd te komen met artikel 8 EVRM. Voor het door de politie stelselmatig vergaren van informatie over een bepaald persoon is inmiddels duidelijk dat artikel 8 EVRM vereist dat een dergelijke informatievergaring is gebaseerd niet op een algemene taakstelling (art. 3 Pw) maar op een specifieke bevoedgheid (i.c. art. 126j Sv).[24]

21 Bantema e.a., a.w., p. 125.

22 Voor meer informatie over de NTD-procedure, zie: https://ecp.nl/activiteiten/werkgroep-notice-and-takedown/, geraadpleegd 10 januari 2019.

23 Bantema e.a., a.w., p. 126.

24 B.J. Koops, 'Public investigations in internet open sources: Procedural-law issues', *Computer Law and Security Review*, jaargang 29, nummer 6, 2013, p. 654-665; J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen*, jaargang 38, nummer 5, 2012, p. 35-49; J.J. Oerlemans, *Investigating Cybercrime*. Amsterdam: Amsterdam University Press, 2017; W.Ph. Stol & L. Strikwerda, 'Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving', *Tijdschrift voor Veiligheid*, jaargang 17, nummer 1/2, 2018, p. 8-22. J.J. Oerlemans, Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk, *Platform Modernisering Strafvordering*, 2018-18.

Analoog redenerend is voor het gemeentelijk monitoren van internet de vraag op grond van welke specifieke bevoegdheid de gemeente kan 'monitoren' als dat het stelselmatig vergaren van persoonsgegevens omvat. Oerlemans schrijft in dit verband: 'Binnen het bestuursrecht zijn drie uitspraken van de Rechtbank Amsterdam beschikbaar, waaruit blijkt dat de gemeente Amsterdam een *scraper*[25] heeft ingezet om webpagina's van Airbnb vast te leggen om na te gaan of een bewoner ten onrechte zijn woonboot meer dan het toegestaan aantal dagen verhuurde. De Rechtbank Amsterdam achtte de inzet van het middel rechtmatig op grond van de algemene onderzoeksbevoegdheid in artikel 3:2 van de Algemene wet bestuursrecht (Awb).'[26] Het is nog maar de vraag of die lijn stand houdt. Oerlemans merkt bijvoorbeeld op dat de wetgever in de memorie van toelichting van het wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering, er op lijkt te wijzen dat het inzetten van een crawler als stelselmatige vastlegging kwalificeert en dus een specifieke wettelijke grondslag vergt.[27] Ook Stol en Strikwerda pleiten voor het expliciet reguleren van zoekmethoden die zijn gebaseerd op geavanceerde technologie omdat het op burgers inzetten van geavanceerde technologie op zichzelf al een ingrijpende inbreuk op de privacy is, los van het daarmee bereikte resultaat.[28] De aangehaalde auteurs voeren discussie over strafvordelijke bepalingen, een vertaling naar het bestuursrecht zal nog nader moeten worden uitgewerkt.

Evenementenveiligheid

Het vijfde *work package* heeft betrekking op de digitale veiligheid van evenementen. Artikel 174 lid 1 Gemeentewet bepaalt dat 'De burgemeester is belast met het toezicht op de openbare samenkomsten en vermakelijkheden alsmede op de voor het publiek openstaande gebouwen en daarbij behorende erven.' Deze gemeentelijke verantwoordelijkheid roept twee vragen op. De eerste is of het artikel tevens ziet op evenementen in de digitale wereld. Deze vraag is lastig te beantwoorden vanwege territoriale complicaties: welke burgemeester zou bevoegd zijn? Als onze samenleving toezicht nodig acht op evenementen in cyberspace (hetgeen op termijn te verwachten is) dan dient allereerst de verantwoordelijkheidstoewijzing te worden geregeld. De tweede vraag is of artikel 174 Gemeentewet inhoudt dat gemeenten toezicht dienen te houden op de digitale veiligheid van evenementen op het gemeentelijk grondgebied. Daarop moet het antwoord wel 'ja' zijn want elk evenement waarbij genetwerkte digitale apparatuur een rol speelt in de aansturing van beweging, dataopslag, beeld of geluid, herbergt een digitaal veiligheidsrisico. Een veiligheidsincident kan ontstaan door een storing of aanval. In de voor gemeenten ontwikkelde Keuzewijzer Evenementenveiligheid van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) komen de woorden cyber, internet, digitaal en digitale niet voor.[29] In het door het Instituut Fysieke Veiligheid

25 'Een *crawler* is kortgezegd een programma dat binnen ingestelde condities (zoals welke bronnen moeten worden doorzocht en op welke woorden of andere zoektermen moet worden doorzocht) gegevens van internet verzamelt, zoals webpagina's die voldoen aan de criteria, en deze vervolgens indexeert. Als daarbij ook gegevens worden vastgelegd, wordt gesproken van een 'scraper' (Oerlemans, a.w., 2018, p. 9).

26 Oerlemans, a.w., 2018.

27 Memorie van toelichting van het wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering, Kamerstuk 07-02-2017, p. 247.

28 Stol & Strikwerda, a.w., 2018.

29 https://docplayer.nl/1531349-Keuzewijzer-evenementenveiligheid.html, geraadpleegd 10 januari 2019 (de Keuzewijzer is niet gedateerd).

gepubliceerde 'procesmodel evenementenveiligheid'[30] komen van die vier de woorden 'digitaal' en digitale' elk één maal voor, niet inhoudelijk echter, maar verwijzend naar het digitaal indienen van een aanvraag. Voor zover bekend, is digitale veiligheid binnen gemeenten niet werkelijk een aandachtspunt bij de beoordeling van evenementen. Van de digitale veiligheid van evenementen dient dus werk te worden gemaakt, om te beginnen met een onderzoek naar de digitale risico's van hedendaagse evenementen, naar de verdeling van verantwoordelijkheden tussen de evenementenbranche en de overheid, en naar de mogelijkheden om als gemeente aandacht te besteden aan de digitale veiligheid van evenementen middels vergunningsvoorwaarden en toezicht.

Aan de slag

'De veilige stad' wil tegenwoordig ook zeggen 'de *digitaal* veilige stad'. Aan digitale veiligheid kan iedereen een bijdrage leveren. Wij keken naar de bijdrage die de gemeente als lokale overheid daaraan kan leveren. Het onderwerp is de laatste paar jaar op de lokale politieke agenda geraakt. Dat is een begin; vervolgens is er nog veel te doen. We hebben vijf *work packages* benoemd en besproken die de aandacht van gemeenten vergen. De eerste twee, het op orde brengen plus houden van de eigen informatiebeveiliging en het gestalte geven aan de gemeentelijke regierol bij het streven naar een digitaal veilige gemeente, zijn wellicht niet altijd even eenvoudig, maar ze kennen niet echt fundamentele knelpunten. Daarmee kunnen gemeenten dus direct en voortvarend aan de slag. Met de andere drie *work packages* kunnen gemeenten ook al aan de slag, maar die drie terreinen voeren gemeenten tevens naar serieuze vraagstukken, bijvoorbeeld aangaande bevoegdheden, territorialiteit en verantwoordelijkheden. Met name die drie *work packages* vergen dan ook nader onderzoek. Buiten beschouwing hebben we hier gelaten de situatie van orde en ordehandhaving in een online omgeving. Daarmee is niet gezegd dat 'een online openbare orde' niet bestaat of dat een dergelijke orde niet zou moeten worden gehandhaafd, maar wel dat dit onderwerpen zijn voor een nog wat verdere toekomst.

30 Instituut Fysieke Veiligheid (IFV), *HEV 2018: procesmodel evenementenveiligheid*. Arnhem: IFV, 2018.