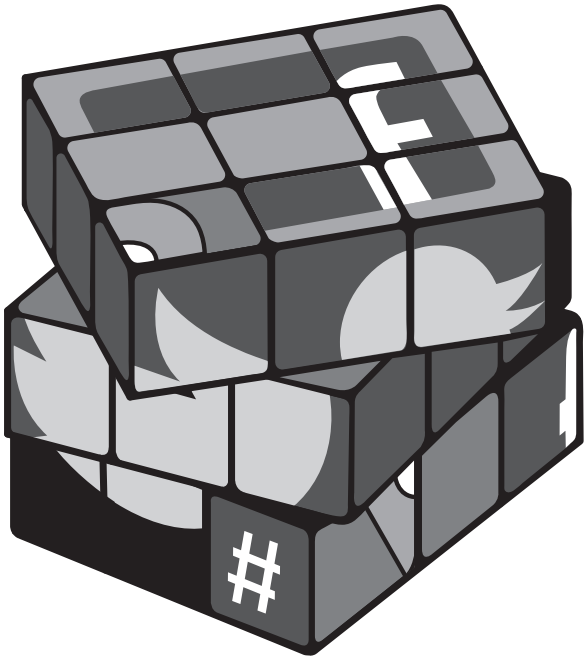
POLITIE & Wetenschap

Black Box van gemeentelijke online monitoring

Een wankel fundament onder een stevige praktijk

Bantema, Westers, Hoekstra, Herregodts & Munneke



rijksuniversiteit groningen

NHL STENDEN hogeschool

Black box van gemeentelijke online monitoring

Black box van gemeentelijke online monitoring

Een wankel fundament onder een stevige praktijk

W. Bantema

S. Westers

M. Hoekstra

R. Herregodts

S. Munneke

POLITIE & Wetenschap

NHL STENDEN hogeschool

rijksuniversiteit groningen

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:
Sdu Klantenservice
Postbus 20025
2500 EA Den Haag
tel.: (070) 378 98 80
website: www.sdu.nl

Omslagontwerp: Imago Mediabuilders, Amersfoort
Afbeelding omslag: Tymo Grijpma

ISBN: 9789012407052
NUR: 600

Inhoudsopgave

Ten geleide

Cybersafety Research Group
NHL Stenden Hogeschool / Rijksuniversiteit Groningen
www.cybersciencecenter.nl

Auteurs

Dr. Willem Bantema
Saskia Westers, MSc
Dr. Maarten Hoekstra
Mr. Dr. Rianne Herregodts
Prof. Mr. Dr. Solke Munneke

Met dank aan de klankbordgroep

Dr. Mr. B. van Caem – Adviseur onderzoek Direct operatiën, Kennis en Innovatie, Politie
Dr. W. Jong - Onderzoeker en adviseur crisisbeheersing
Mr. M. Viersma - Beleidsmedewerker Politiebestel, Bevoegdheden en Informatiefunctie J&V
Prof. Dr. J.J. Oerlemans - Bijzonder hoogleraar inlichtingen en recht
R. Poulissen-Jorritsma, MA - Strategisch beleidsadviseur Bureau Regioburgemeesters

1. Introductie op het onderzoek

1.1 Maatschappelijke relevantie 'gemeentelijk online monitoren'

Gemeenten hebben steeds vaker te maken met online aangejaagde ordeverstoringen. Zo verzamelden op 1 juni 2020 duizenden demonstranten zich in Amsterdam voor een vreedzaam protest tegen racisme en discriminatie. De massale opkomst bij dit protest op De Dam bracht echter, zo luidden de commentaren, aanmerkelijke risico's met zich mee voor de volksgezondheid en ook voor de openbare orde en veiligheid. Dat leidde vervolgens tot stevige kritiek op het functioneren van burgemeester Halsema. Waarom had de gemeente de opkomst bij deze demonstratie niet goed ingeschat? Waarop Halsema vervolgens liet optekenen: "Onze informatiepositie was niet goed; de driehoek beschikte niet over realistische aantallen."[1] Had de informatiepositie van de burgemeester in dit specifieke geval versterkt kunnen worden als men zich een beter beeld gevormd had van wat op sociale media gaande was? Deze studie gaat in op de wijze waarop Nederlandse gemeenten[2] in het algemeen dergelijke openbare en online bronnen monitoren met het oog op de handhaving van de openbare orde. Tot nu toe is er namelijk weinig bekend over de instrumenten die gemeenten inzetten en de praktische knelpunten en bestuursrechtelijke grenzen waar zij tegenaan lopen. Het is niet eens precies bekend wie zich exact met monitoring bezighouden en welke doeleinden gemeenten precies onderscheiden. Deze studie probeert hier licht op te schijnen.

In het domein van het strafrecht wordt online monitoring door de politie, weliswaar met allerlei juridische beperkingen, al jaren en met succes toegepast. Rechercheurs zoeken actief op internet naar strafbare feiten en de verblijfplaatsen van veroordeelden. Ook wordt getracht digitaal bewijsmateriaal veilig te stellen. Daarnaast wordt binnen politie-eenheden gezocht naar informatie die wijst op mogelijke verstoringen van de openbare orde. Denk hierbij aan voorbeelden uit het verleden over signalen die duiden op vechtafspraken tussen rivaliserende groepen voetbalfans. Ook is het aannemelijk dat de politie via Twitter en Facebook op het spoor komt van 'fuck-coronafeesten' en

1 *Parool*. Halsema erkent, we zaten er finaal naast. 2 juni 2020, Bron: https://www.parool.nl/amsterdam/halsema-erkent-we-zaten-er-finaal-naast~bca3aa9f/?referer=https%3A%2F%2Fwww.ecosia.org%2F.

2 Voor de leesbaarheid wordt in dit rapport het containerbegrip 'gemeenten' gebruikt zonder een onderscheid te maken tussen de juridische, bestuurlijke en ambtelijke dimensies en componenten. Vooral in het juridische deel (hoofdstuk 4) zal met meer precisie worden aangegeven over welke gemeentelijke organen exact wordt gesproken. Hetzelfde geldt overigens voor de term 'politie'.

andere groepsbijeenkomsten die een bedreiging vormen voor de openbare orde en veiligheid. Maar wat doen gemeenten eigenlijk op dit gebied? Zij hebben immers een minstens zo belangrijke taak bij het voorkomen en handhaven van ordeverstoringen. Monitoren zij dan ook wat er gebeurt op sociale media en analyseren zij dan ook welk dreigingsniveau daarvan uitgaat? En aan welke regelingen zijn zij eigenlijk gebonden?

Al lange tijd wordt onderkend dat sociale media een belangrijke factor zijn bij verstoringen van de openbare orde.[3] Neem bijvoorbeeld het terugkerend hooliganisme rondom de jaarwisseling in Den Haag. Of breng de rellen in de gemeente Haren (project X), de blokkeerfriezen, de treitervloggers en de door vloggers aangejaagde rellen in Utrecht van de zomer van 2020 nog eens in herinnering. Bij al deze gebeurtenissen speelden sociale media een cruciale rol in zowel de dynamiek van escalatie als in de bestuurlijke aanpak die moest leiden tot de-escalatie. Inwoners worden door elkaar via sociale media geïnformeerd over op handen zijnde activiteiten. Er kan echter ook via digitale informatiekanalen sprake zijn van opruiing of zelfs het aanzetten tot geweldpleging. Zo bezien is het goed voor te stellen dat ook gemeenten de behoefte voelen om het gedrag van inwoners op internet te monitoren. Het is bekend dat dergelijke monitoring al wordt uitgevoerd door de politie, maar er is op voorhand geen reden om aan te nemen dat de politie wél en de gemeente niet kan monitoren wat op internet gaande is. Waar de openbare orde in het geding is, heeft immers niet alleen de politie maar ook elke Nederlandse gemeente, en in het bijzonder elke Nederlandse burgemeester een belangrijke taak te vervullen. Gemeenten zijn zich hiervan bewust en nemen de nodige maatregelen.[4] Om zich concreet van deze taak te kwijten, is een goede informatiepositie van de gemeenten vanzelfsprekend van cruciaal belang. Gebruikelijk is dat de gemeente informatie over op handen zijnde verstoringen van de openbare orde ontvangt via de politie, het Openbaar Ministerie en eigen personeel zoals bijzondere opsporingsambtenaren en jongerenwerkers. Dit onderzoek laat zien dat signalen over mogelijke verstoringen van de openbare orde niet alleen vanuit de 'veiligheidshoek' komen maar dat evenzeer vanuit de reguliere online communicatie tussen gemeenten en burgers relevante signalen worden opgevangen.[5] Deze informatie-uitwisseling, die te vatten is onder de parapluterm (gemeentelijke) communicatie, maakt derhalve een wezenlijk onderdeel uit van deze studie.

Het lijkt dus op het eerste gezicht volkomen begrijpelijk dat gemeenten informatie uit openbare online bronnen (o.a. Twitter en Facebook), gebruiken om invulling te geven aan hun verantwoordelijkheid voor de openbare orde en veiligheid maar dat is het niet.

3 Zie o.a.: R.H. Johannink, I. Gorissen & N.K. Van As (2013). 'Sociale media: factor van invloed op onrustsituaties?' *Politiekunde, 52* en C. Rizza, Â.G. Pereira & P. Curvelo (2014). '"Do-it-yourself justice": considerations of social media use in a crisis situation: the case of the 2011 Vancouver riots.' *International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 6*(4), 42-59.

4 Gemeente Amsterdam (2019). *Agenda Digitale Veiligheid van de gemeente Amsterdam*. Bron: https://amsterdamlogistics.nl/wp-content/uploads/2019/11/agenda_digitale_veilig-heid_amsterdam.pdf.

5 Door medewerkers van een communicatieafdeling of een zogenaamde Newsroom.

Dataverzameling door overheidsorganisaties is, ter bescherming van het individu, gebonden aan allerlei wetgeving zoals de (Europese) Algemene Verordening Gegevensbescherming (AVG) en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Ook zijn er vanuit ethisch en technisch oogpunt redenen te bedenken waarom er terughoudend omgegaan zou moeten worden met het verzamelen en interpreteren van dergelijke gegevens. Recente voorbeelden laten zien dat dataverzameling door gemeenten op juridische grenzen stuit. In Amsterdam oordeelde de rechter dat camera's, bedoeld voor milieuvraagstukken, niet gebruikt mochten worden voor het opsporen van criminelen.[6] De gemeente Amsterdam bracht ook probleemjeugd in kaart door een analyse te maken van hun profielen op sociale media. Volgens de Autoriteit Persoonsgegevens (AP) was dit te ingrijpend en maakte het een te grote inbreuk op de privacy van de jongeren.[7] Deze voorbeelden maken duidelijk dat er juist redenen zijn om gemeentelijke monitoring van onlinebronnen nauwlettend te onderzoeken. Daarom wordt met dit onderzoek in kaart gebracht of gemeenten online monitoren, hoe ze dit doen en op welke knelpunten en grenzen ze stuiten. Het perspectief van de politie wordt om drie redenen meegenomen in deze studie. Ten eerste heeft de politie veel ervaring opgedaan met online monitoring en zijn werkwijzen reeds geïnstitutionaliseerd. Ten tweede opereren politie en gemeenten in hetzelfde domein (openbare orde en veiligheid), waarbij ook uitwisseling van informatie plaatsvindt. Ten derde maken politie en gemeenten (deels) gebruik van dezelfde instrumenten waarover in de context van de politie reeds de nodige literatuur is verschenen. Kortom: onderzoekers, ambtenaren en bestuurders kunnen veel leren van de politiepraktijk.

1.2 Kennisbehoefte, doelstelling en vraagstelling

Aanleiding voor het onderzoek is het eerder afgeronde onderzoek 'Burgemeesters in cyberspace', waarbij de mogelijkheden van burgemeesters om bij een (dreigende) openbare ordeverstoring hun bevoegdheden te vertalen naar en preventief toe te passen in de digitale wereld.[8] Uit dat onderzoek blijkt dat die vertaling en toepassing online ingewikkeld is. Naast de aandacht voor bevoegdheden kwam zijdelings aan bod dat een aantal gemeenten heel actief is bij het monitoren van online gedrag, terwijl andere zich nog aan het bezinnen zijn op hun rol aldaar. De gemeenten die actief zijn, monitoren op verschillende manieren. Zo werd er verwezen naar het inzetten van een gespecialiseerde analist of het opzetten van zogenaamde 'Newsrooms'. Newsrooms worden gebruikt om in contact te blijven met burgers en gebruiken monitoringtools

6 *Trouw*. Politie Amsterdam loerde onterecht in data van milieucamera's. 16 oktober 2019. Bron: https://www.trouw.nl/nieuws/politie-amsterdam-loerde-onterecht-in-data-van-milieucamera-s~bba1398a/.

7 *NRC Handelsblad*. Amsterdam in de fout met gegevens hangjongeren. 16 mei 2018. Bron: https://www.nrc.nl/nieuws/2018/05/16/amsterdam-in-de-fout-met-gegevens-hangjongeren-2-a1603291.

8 W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.ph. Stol (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld* (reeks politie en wetenschap). Den Haag: Sdu.

zoals OBI4wan om te scannen op trefwoorden in online openbare bronnen zoals sociale media.[9]

Het 'Burgemeesters in cyberspace'-onderzoek heeft, naast veel interessante gegevens, ook veel praktische vragen opgeroepen over hoe het monitoren binnen gemeenten georganiseerd is en welke gemeentelijke afdelingen erbij betrokken zijn. Ten eerste is er weinig bekend over de intensiteit waarmee gemeenten monitoren, hun drijfveren en eventuele grenzen en knelpunten die ze daarbij ervaren. Ten tweede is er wetenschappelijk nog weinig bekend over de implicaties van het juridische kader waarbinnen gemeenten monitoractiviteiten verrichten. Artikel 8 EVRM (eerbiediging van het privé- en gezinsleven) en de AVG (privacy) lijken daarbij in het bijzonder relevant. Het geldende recht stelt strenge eisen aan de verwerking van persoonsgegevens. De stringente eisen ten aanzien van specifieke methoden en besloten groepen zouden tot gevolg kunnen hebben dat er meer nadruk en focus komen te liggen op het gebruik van openbare bronnen voor het (preventief) handhaven van de openbare orde en veiligheid door gemeenten.[10] Ten derde roept het onlinegedrag van gemeenten steeds meer vragen op over de ethische kant van de zaak. Uit verschillende recente nieuwsberichten is gebleken dat 'veiligheid boven alles' binnen het veiligheidsdomen het adagium is terwijl andere publieke waarden evenzeer moeten worden afgewogen. Door COVID-19 komt daar nog een gezondheidsbelang bij. Bovendien is het de vraag of door intensieve maatregelen de veiligheid wel echt gediend is.[11] Een morele afweging over wat goed is voor de maatschappij als geheel en voor het individu in het bijzonder lijkt vaak achterwege te blijven. Ten vierde is onbekend welke organisatorische en technische knelpunten en dilemma's gemeenten ervaren. Hierbij valt te denken aan vraagstukken of er voldoende menskracht voorhanden is en of de techniek voldoet. Tot slot blijkt uit de recente evaluatie van de demonstratie op De Dam dat de gemeente Amsterdam in de ogen van de onderzoekers te veel op de (niet adequate) informatiepositie van de politie heeft geleund.[12] Ook in dat licht bezien, is het de moeite waard om de gemeentelijke praktijk van online monitoring onder de loep te nemen.

Dit onderzoek is een eerste verkenning van de gemeentelijke praktijk van online monitoring in het kader van de openbare orde en veiligheid. Ook wordt er geïnventariseerd met welke knelpunten en grenzen gemeenten te maken hebben. Daarbij spelen naast het juridische vraagstuk dus evenzeer de organisatorische, technische en ethische as-

9 Frankwatching (2018). *Newsrooms bij gemeenten: de 4 grootste misverstanden*. Bron: https://www.frankwatching.com/archive/2018/12/11/newsrooms-bij-gemeenten-de-4-grootste-misverstanden/

10 Waarbij verder de gedachte, die in dit onderzoek overigens niet specifiek getoetst wordt, zich kan opdringen dat steeds strengere eisen die aan de monitoring bij de politie worden gesteld in nieuwe wetgeving er mogelijk toe leiden dat de gemeentelijke monitoringspraktijk, waar de spelregels minder duidelijk zijn, aan aantrekkingskracht wint.

11 Zie als voorbeeld SyRI: een systeem gebruikt door de overheid waar persoonlijke gegevens worden gekoppeld om fraude op te sporen.

12 A. Boin, K. Nooy & P. van der Velden (2020). *Een verkeerde afslag: een analyse van de 1 juni demonstratie in Amsterdam*.

pecten van het monitoren door gemeenten. Uiteindelijke doel is om beleidsmatige aanbevelingen te formuleren. De centrale vraag van deze studie luidt derhalve:

In hoeverre geeft de huidige gemeentelijke praktijk wat betreft online monitoring van open bronnen in het domein van openbare orde en veiligheid reden tot heroverweging?

Daarbij zijn de volgende onderzoeksvragen geformuleerd:

1. Wat is er vanuit de literatuur bekend over online monitoring?
2. In hoeverre en op welke wijze monitoren gemeenten online en met welke intenties en doelstellingen doen zij dit?
3. Welke knelpunten en dilemma's ervaren gemeenten op dit moment bij het online monitoren?
4. Aan welke juridische grenzen zijn gemeenten gebonden wat betreft online monitoren?

Voordat wordt ingegaan op de methoden die leiden tot beantwoording van de vragen worden eerst vier kernbegrippen aangestipt.[13]

1.3 Kernbegrippen

Ten eerste wordt het begrip 'openbare orde' kort toegelicht. Ten tweede wordt een toelichting gegeven op de betekenis van 'open bronnen' en ten derde wordt nader ingegaan op de definitie en verschijningsvormen van 'social media'. Ten vierde en ten slotte is er aandacht voor het kernbegrip 'monitoren'.[14]

1.3.1 *Openbare orde*

Dit onderzoek gaat over het monitoren van internet met het oog op het in kaart brengen van verstoringen van de openbare orde of ernstige dreigingen van verstoringen.[15] Er zijn meerdere omschrijvingen van openbare orde mogelijk, afhankelijk van de vraag of het begrip in strafrechtelijke,[16] civielrechtelijke[17] dan wel bestuursrechtelijke zin

13 De termen 'Monitoren' en 'monitoring' worden in dit rapport door elkaar gebruikt.

14 Met het oog op de doelgroep van deze studie (bestuurders en practitioners) wordt ervoor gekozen om soms ingewikkelde begrippen toch kort en bondig te formuleren. Mogelijk gaan daarbij in de optiek van specialisten verbijzonderingen of details verloren.

15 De paragraaf is een zeer verkorte weergave van de inzichten van: M.A.D.W. de Jong, W. van der Woude, W.S. Zorg, J.L.W. Broeksteeg, R. Nehmelman, I.U. Tappeiner & H.R.B.M. Kummeling (2017). *Orde in de openbare orde. Een onderzoek naar verbetering van de toepasbaarheid en inzichtelijkheid van het openbare-orderecht*.

16 Strafrechtelijke handhaving is primair gericht op opsporing, vervolging en bestraffing van strafbare feiten. Het punitieve element speelt daarin een leidende rol.

17 Hierbij wordt verwezen naar de civielrechtelijke aanpak van Satudarah Motorcycle-Club enkele jaren geleden. Zie: ECLI:NL:HR:2020:1789.

wordt bedoeld. Dit onderzoek richt zich op de burgemeestersbevoegdheden zoals die in de Gemeentewet zijn vastgelegd. Daarmee is de optiek dus een bestuursrechtelijke. 'Openbare orde' wordt omschreven als het niveau van rust zoals dat bij 'normale gang van zaken' in het openbare gemeenschapsleven geldt. Met 'orde' wordt een situatie van rust en regelconform gedrag bedoeld. Met de term 'openbare' wordt van oudsher gedoeld op publiek toegankelijke ruimte en gebouwen. Het zijn niet alleen landelijk beleid en daaruit voortvloeiende regelgeving die invullen wat onder openbare orde wordt verstaan maar ook juist de invulling door gemeentelijke ambten, waaronder de gemeenteraad en de burgemeester. Vanzelfsprekend is ook lokale regelgeving en besluitvorming sterk bepalend voor het gewenste niveau van rust dat dus zal verschillen van gemeente tot gemeente.[18] De vraag of sprake is van een verstoring van de openbare orde, hangt af van de invulling van dat begrip, waarbij de feitelijke context van grote invloed is. Van verstoring is volgens de auteurs van dit onderzoek sprake in geval van een aantasting van enige betekenis van de normale gang van zaken in of aan de openbare ruimte.

1.3.2 *Open bronnen*

Voor het begrip open bron[19] sluit het onderzoek, overeenkomstig anderen aan bij het werk van de Commissie-Koops die de volgende omschrijving hanteert: "Open bronnen kenmerken zich doordat in beginsel eenieder er toegang toe kan verkrijgen en dat voor zover toegang gebonden is aan een account, het verkrijgen van een account een (semi-)geautomatiseerd proces is waarbij niet bepaalde groepen worden uitgesloten van registratie. Open bronnen staan tegenover afgeschermde bronnen die zich kenmerken doordat er een controle plaatsvindt op wie degene is die toegang wil tot de bron." [20, 21, 22] Op internet is over veel mensen informatie beschikbaar die voor iedereen toegankelijk is, dus ook voor de gemeenten en politie. Denk bijvoorbeeld aan persoonsgegevens op het openbare gedeelte van een LinkedIn-profiel of een Twitteraccount. Verder kan de opzet van sociale media (welke personen hebben een connectie met elkaar, wie reageert op een geplaatst bericht) inzicht geven in netwerken rond personen of groepen.[23] Open bronnen zijn dus beschikbaar zonder te hoeven inloggen op een website. Zodra het account alleen toegankelijk is voor specifiek geïnteresseerden (de connecties op het platform), dan is het een afgeschermde bron. Het gegeven

18 Onderzoek van W. Bantema et al. (2018) liet zien dat openbare orde een begrip is, waarbij sommige burgemeesters problemen zo breed formuleren dat het valt onder het begrip openbare orde en veiligheid en dat ze dientegenvolge hun bevoegdheden kunnen gebruiken.

19 De termen 'open bronnen' en 'openbare bronnen' worden in deze studie aan elkaar gelijkgesteld.

20 O.a.: J.J. Oerlemans & Y.E. Schuurmans (2019). Internetonderzoek door bestuursorganen. *Nederlands Juristenblad, 94* (20), 1458-1466.

21 E.J. Koops, R.J. Verbeek, B.W. Schermer, M.J. Grapperhaus, A. Kuijer, D. Ven-Laheij ... & Viersma, M. (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving,* p. 152.

22 J.J. Oerlemans (2018). 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk.' *Platform Modernisering Strafvordering.*

23 Vrij naar: W.Ph. Stol & L. Strikwerda (2018). Online vergaren van informatie voor opsporingsonderzoek. *Tijdschrift voor Veiligheid, (17)* 1-2, 8-22.

dat individuele toestemming wordt verkregen, maakt de informatie dus 'niet-openbaar'. Voorbeelden van openbare bronnen zijn sommige socialemedia-accounts, nieuwsartikelen en reacties daarop en openbare discussiefora. De term 'open bron' suggereert dat iedereen vrij is om de data naar eigen wens en inzicht te gebruiken. Dat is echter niet het geval en gesuggereerd is daarom wel dat de term 'publiekelijk toegankelijke bron' beter op zijn plaats is. Deze term is echter minder ingeburgerd bij de doelgroep.

1.3.3 *Sociale media*

Voor een praktische omschrijving van het begrip 'sociale media' sluit dit rapport aan bij de gemeente Amsterdam dat beschrijft dat 'sociale media' een verzamelnaam is voor allerlei internettoepassingen waarmee het mogelijk is om informatie met elkaar te delen, zowel tekst als beeld. Dit kan via websites of speciale apps. Het is een virtuele plek waar mensen met elkaar in contact komen.[24] Anderen leggen niet zozeer de nadruk op de functies maar benadrukken juist de integratie van technologie, sociale interactie en 'content-creatie'.[25] Dit betekent dat de 'binding' tussen de mensen die informatie met elkaar creëren en delen via allerlei systemen centraal staat.[26]

Sommige informatie is openbaar toegankelijk, andere niet. Zo zijn Facebookgroepen veelal openbaar (al worden die steeds beter afgeschermd), terwijl WhatsApp-berichten vooral in beslotenheid worden verstuurd. Sociale media hebben, volgens deskundigen, de wereld van de openbare orde en veiligheid en die van opsporing van criminaliteit revolutionair veranderd.[27, 28] Het betreft dan ook een breed palet aan fora, weblogs, kennispagina's en sociale netwerken. Anderen zien de toegevoegde waarde van socialemediagebruik van overheden in het feit dat daardoor een meer horizontale en open manier van communiceren ontstaat hetgeen de interactie met de burgers eenvoudiger maakt.[29] Voor deze studie is het goed te beseffen dat vanuit bestuurlijk perspectief sociale media als een open informatiebron worden beschouwd terwijl deze voor de gebruikers juist vooral een samenwerkingsplatform en communicatiekanaal zijn.[30]

---

24 Gemeente Amsterdam (2016). *Verkenning Social Media en Jeugd en Veiligheid.* Bron: https://static.nrc.nl/2018/hangjongeren-privacy/1116uitlegstuk.pdf.

25 S.M. Zavattaro (2013). 'Social media in public administration's future: A response to Farazmand.' *Administration & Society, 45* (2), 242-255.

26 Zie ook: M. Yang (2013). 'The collision of social media and social unrest: Why shutting down social media is the wrong response.' *Northwestern Journal of Technology and Intellectual Property, 11* (7), 708-728.

27 M. den Hengst, T. ten Brink, & J. ter Mors (2017). *Informatiegestuurd politiewerk in de praktijk*. Deventer: Vakmedianet.

28 Zie: J. Bakker, H. Tops, D. Nonahal, & F. Willemsen (2016). *Toepassing Social Media Data-Analytics voor het Ministerie van Veiligheid en Justitie. Toelichting, beschrijving en aanbevelingen.* Coosto.

29 J.I. Criado, F. Rojas-Martín & J.R. Gil-García (2017). 'Enacting social media success in local public administrations.' *International Journal of Public Sector Management, 30* (1), 31-47.

30 Zie ook: A.D. Murray (2016). 'The legal challenges of social media.' In: Gillies Lorna and Mangan, David, (Eds.) Mapping the rule of law for the internet. Edward Elgar Publishing, UK.

1.3.4 *Monitoring*

Voor de leesbaarheid worden de termen 'sociale media surveillance' (zoals wel gebruikt in het veiligheidsdomein) en 'monitoring' voorlopig aan elkaar gelijkgesteld. Omdat surveillance een sterke 'blauwe' connotatie heeft, is gekozen voor de term 'monitoring' die vooral bij het vocabulaire van gemeenten, de primaire doelgroep van deze studie, aansluiting vindt. Overwogen is om een Nederlandse term zoals 'observeren of observatie' te hanteren. Probleem daarvan is dat deze termen ongewild begripsverwarring kunnen opleveren met de gelijknamige opsporingsmethode, namelijk het systematisch volgen van een persoon of groep. Daarbij zou vervolgens de valkuil zich aandienen dat we in een louter juridische discussies terechtkomen. In essentie gaat het bij monitoring[31] om de volgende vragen: wat wordt door wie, waar gezegd, hoe vaak en waarom? Hoe belangrijk is het onderwerp? Wat zijn de sentimenten op internet? Daarbij worden vier vormen van monitoring bij gemeenten onderscheiden, te weten:

1. Monitoren van risico's: veiligheidsrisico's tijdig zien aankomen en dus meer tijd hebben om te anticiperen. Bijvoorbeeld bij evenementen of ter voorkoming van project X. Vooral belangrijk voor crisiscommunicatie.
2. Monitoring van vragen en problemen: vragen aan en opmerkingen over de gemeente actief opsporen en voorzien van een antwoord of advies door middel van 'webcare'. Burgers vinden het normaal dat bedrijven dat doen en verwachten dat inmiddels ook van de gemeente.
3. Analyse van issues. Opkomende issues opsporen en uitdiepen. Beelden en meningen over overheidsinitiatieven tijdig in het vizier krijgen. Zien welke issues door bepaalde fracties worden opgepikt. 'Broodjes aap detecteren' en 'debunken'. Actief achterhalen welke beïnvloeders actief zijn op beleidsterreinen en met welke standpunten.
4. Analyse van reputatie-uitingen. Zien of gemeenten in de ogen van mensen de goede dingen doen en die goed doen, wat van invloed is op de slagkracht van het college van B&W, individuele bestuurders en de ambtelijke organisatie.[32]

De eerste twee vormen zijn het 'passief' in de gaten houden van openbare bronnen. Een vervolgstap is een verwerking en analyse van deze openbare bronnen om deze in een groter geheel te plaatsen (de laatste twee vormen van monitoring). In dit onderzoek wordt monitoring als parapluterm gebruikt waaronder alle vier genoemde vormen van monitoring worden geschaard. Om met de veelheid van informatie uit open bronnen te kunnen werken, worden technische instrumenten ingezet. Dergelijke instrumenten, zogeheten 'monitoringstools', zijn veelal op de markt gezet door commerciële partijen. Middels 'datascience' en 'data-analytics' worden verbanden in de infor-

31 Ontleend aan: A.J. Meijer & D. van Berlo (2011). 'Big Brother of gesprekspartner? Monitoren van communicatie van burgers via social media.' *Bestuurswetenschappen, 6*, 90-98.

32 D. Kok, (red) (2013). *Sociale gemeenten. De kracht van nieuwe media*. Delft: Academische Uitgeverij Eburon.

matie gevonden en gevisualiseerd. Ook claimt men toekomstvoorspellingen te kunnen doen.[33]

In hoofdstuk 2 wordt nader ingegaan op het gebruik van monitoringstools en monitoring van openbare bronnen bij de politie en gemeente op basis van de literatuur. Eerst wordt nader ingegaan op de methodologische verantwoording van het voorliggende onderzoek.

1.4 Methodologische verantwoording

1.4.1 *Inleiding*

De aanleiding van de studie is gelegen in de kennislacune over de wijze waarop online monitoring door gemeenten plaatsvindt, terwijl de praktijk en actualiteit juist vragen om een nadere beschrijving en duiding van het fenomeen. Het onderzoek als geheel heeft dan ook een overwegend verkennend en beschrijvend karakter.[34] Daarbij is sprake van een iteratief proces in die zin dat tijdens het verzamelen van de gegevens voorlopige analyses zijn gemaakt op grond waarvan de methoden van onderzoek werden doorontwikkeld en nieuwe gegevens werden verzameld.[35] Vanuit verschillende disciplines en gezichtspunten zoals de juridische wetenschappen, de organisatiekunde en de leer van de ethiek wordt aan dit onderzoek invulling gegeven.[36] De impliciete verwachting was dat deze drie gezichtspunten de belangrijkste spanningsvelden en dilemma's die gemeenten in de dagelijkse praktijk van online monitoren ervaren, bloot kunnen leggen.

Wat betreft de validiteit dienden zich vier vragen aan die bij de drie empirische onderdelen van deze studie in samenhang zijn besproken:[37] Ontleend aan: F. van der Zee (2004). *Kennisverwerving in de empirische wetenschappen. De methodologie van wetenschappelijk onderzoek.* Groningen: BMOOO. is het correcte onderzoeksdesign toegepast? Is de steekproef op de juiste wijze getrokken? Is gebruikgemaakt van het juiste meetinstrument? Zijn de juiste analysetechnieken toegepast? De volgende paragraaf licht de methoden per deelvraag toe en verantwoordt de belangrijkste methodologische keuzen in het onderzoek. Daarnaast worden bij de drie onderdelen telkens de maatregelen besproken die zijn getroffen om de betrouwbaarheid te waarborgen. De gebruikte methoden staan vermeld in tabel 1.

33 Zie o.a.: M. den Hengst, T. ten Brink & J. ter Mors (2017).
34 Zie o.a.: B. Baarda (2009). *Dit is onderzoek. Handleiding voor kwantitatief en kwalitatief onderzoek.* Groningen: Uitgeverij Noordhoff.
35 Bijvoorbeeld: M.H. van IJzendoorn (1988). 'De navolgbaarheid van kwalitatief onderzoek I: methodologische uitgangspunten.' *Nederlands Tijdschrift voor Opvoeding, Vorming en Onderwijs, 4*(5), 280-288.
36 S.V. van Thiel (2007). *Inleiding Bestuurskundig onderzoek.* Bussum: Uitgeverij Coutinho.
37 Ontleend aan: F. van der Zee (2004). *Kennisverwerving in de empirische wetenschappen. De methodologie van wetenschappelijk onderzoek*. Groningen: BMOOO.

Tabel 1. Methodenmatrix per deelvraag

	Literatuurstudie	Interviews	Vragenlijst	Juridisch bronnenonderzoek
1: Wat is bekend?	x			
2: Werkwijze en doelstellingen	x	x	x	x
3: Knelpunten en dilemma's	x	x		x
4: Juridische grenzen	x		x	x

De deelvragen zijn middels vier onderzoeksmethoden beantwoord, te weten: een literatuurstudie, interviews, een vragenlijst en een juridisch bronnenonderzoek (zie tabel 1). Na de tabel volgt per methode een toelichting op de belangrijkste overwegingen.

1.4.2 *Literatuurstudie*

De literatuurstudie richt zich vanzelfsprekend met name op de eerste deelvraag, te weten: wat is er in de literatuur[38] bekend over online monitoren? Bij het beschrijven van de huidige praktijk met betrekking tot online monitoren wordt zowel bij de politie als bij de gemeenten gerefereerd aan de doelstellingen, de werkwijze en de knelpunten en dilemma's. Het zoekproces kan worden geduid als een combinatie van methoden en benaderingen waarbij enerzijds gaandeweg het zoekproces het aantal bronnen (sneeuwbalmethode) vermeerderde en anderzijds de precisie van gehanteerde zoektermen en zoekfuncties kon toenemen waarbij gestreefd is naar een actueel en volledig overzicht.

1.4.3 *Interviews*

Er zijn tien groepsinterviews afgenomen, waarvan twee bij de politie en acht bij Nederlandse gemeenten. Bij de keuze van de gemeenten is gestreefd naar een grote geografische spreiding en een balans tussen grote gemeenten enerzijds en kleinere gemeenten anderzijds. Ook speelde de beschikbaarheid van respondenten een rol bij de selectie.[39] Om de betrouwbaarheid te optimaliseren, zijn de volgende maatregelen genomen:

De semi-gestructureerde interviews zijn waar mogelijk op locatie gehouden en afgenomen op basis van een uitgebreid interview protocol, zie Bijlage I. Bij de interviews waren overwegend twee onderzoekers aanwezig.

38 Dit betreft literatuur van zowel wetenschappelijke, praktische als journalistieke aard.
39 Daarbij werd onder andere een beroep gedaan op de contacten die eerder werden gelegd in het onderzoek 'Burgemeesters in cyberspace' van W. Bantema et al. (2018).

De interviews zijn, met toestemming van de betrokkenen, integraal opgenomen op geluidsdrager en getranscribeerd middels 'transcriptieonline.nl'. Daarna zijn de interviews thematisch geanalyseerd met het softwareprogramma 'Atlas.ti'. De resultaten zijn geanonimiseerd verwerkt in het onderzoeksrapport. Op basis van een zogenaamde 'peer-debriefing' werden na elke interview het protocol en de methoden waar nodig aangepast.

1.4.4 *Vragenlijst*

De opzet van de vragenlijst volgt in grote lijnen de opzet van de interviews die op haar beurt weer op hoofdlijnen de uitkomsten van de literatuurstudie volgde. De vragenlijst diende om een breed beeld te krijgen van de mate waarin gemeenten online monitoren en de wijze waarop zij dit doen. Vervolgens is gevraagd naar de knelpunten en dilemma's die zij ervaren op juridisch, organisatorisch en ethisch vlak. De vragenlijst is in een iteratief proces binnen het projectteam ontwikkeld en ter validatie voorgelegd aan twee gemeentelijke OOV-adviseurs en een jurist.[40] De vragenlijst heeft een sterk verkennend karakter. De eerste inzichten uit de interviews en juridische analyses zijn meegenomen. De vragenlijst heeft daarmee niet tot doel het 'bestaande' juridisch kader te toetsen, maar eerder input en inspiratie te geven voor de juridische analyse. Deze iteratie vindt overal plaats in het onderzoek. Al hoewel het onderzoek een sterk rechtssociologisch karakter kent, is het juridisch kader dus allerminst een gegeven bij aanvang van dit onderzoek. De digitale vragenlijst is via e-mail onder in totaal 349 unieke gemeenten verspreid,[41] met daarbij het verzoek om de vragenlijst door te sturen naar 1) een vertegenwoordiger van de 'afdeling Communicatie' en 2) een vertegenwoordiger van de 'afdeling Openbare Orde en Veiligheid'.[42, 43] In totaal hebben 273 gemeentelijke medewerkers de vragenlijst ingevuld. Daarvan hebben 134 respondenten de vragenlijst vroegtijdig afgebroken. Een deel van die respondenten is wel meegenomen in de analyses. De antwoorden van de respondenten die minimaal tot vraag 10 hebben ingevuld (vragen over bij welke afdeling ze werken en de doelen van monitoring) zijn op inhoudelijke gronden meegenomen. Van die 134 respondenten[44] bleven er dan nog 70 over – in totaal resteren er dan 209 respondenten. Daarnaast zijn er 13 respondenten die aangeven dat zij niet aan monitoring doen en hebben slechts een de eerste paar vragen van de vragenlijst beantwoord. Dit betekent dat er uiteindelijk analyses zijn gedaan op basis van maximaal 196 respondenten – waarvan er in 40 gevallen zowel een medewerker OOV als een communicatiemedewerker van dezelfde gemeente de vragenlijst heeft

40 De gehanteerde vragenlijst is opgenomen als Bijlage II.
41 Dat zijn de gemeenten die via een algemeen en publieke toegankelijk e-mailadressenbestand zijn benaderd en enkele gemeenten die (aanvullend) wie het gemeentelijke netwerk van het CCV toegevoegd konden worden.
42 Deze groepen zijn benaderd omdat eerder werd geconstateerd dat vraagstukken op het gebied van openbare orde en veiligheid zowel vanuit het vakgebied zelf als vanuit de discipline communicatie wordt benaderd.
43 Wanneer het gaat over een specifieke afdeling binnen de gemeente of een discipline wordt dit afgekort als OOV.
44 Uit analyse blijkt dat de antwoorden van de respondenten die de vragenlijst volledig en niet-volledig hebben ingevuld niet systematisch van elkaar verschillen.

ingevuld. Dat betekent dat, uitgaande van het maximale aantal van 196 er in totaal 156 verschillende gemeenten aan het onderzoek hebben meegewerkt. Dat betekent dat bij de vragen die gebaseerd zijn op 196 respondenten 156 gemeenten vertegenwoordigd zijn (45% van het totaal aantal geselecteerde gemeenten). De 'afdelingen' Communicatie (53%) en OOV (45%) zijn in min of meer gelijke mate vertegenwoordigd in dit onderzoek en 2 procent van de respondenten (*N*=3) gaf aan voor beide afdelingen te werken. Hoewel het onderscheiden van de twee gemeentelijke afdelingen geen doel van dit onderzoek is, zullen eventuele verschillen tussen deze groepen in hoofdstuk 3 kort worden benoemd.

1.4.5 *Juridisch bronnenonderzoek*

In dit deel van het onderzoek is gekozen voor een tweezijdige benadering. In de eerste plaats is het geldende juridische kader in kaart gebracht. Bij de bespreking van het juridisch kader voor de monitoring van uitlatingen in online openbare bronnen wordt bijvoorbeeld aandacht besteed aan de vraag wat de grondslag voor deze handelingen is en onder welke voorwaarden monitoring in overeenstemming is met de eisen die de AVG en artikel 8 EVRM stellen. Op basis van de geldende regels is het mogelijk aanbevelingen te doen (aandachtspunten, voorwaarden en eisen te formuleren) voor een gemeentelijke werkwijze die binnen de grenzen van het recht blijft. In de tweede plaats is de bestaande gemeentelijke praktijk, zoals die uit de enquêteresultaten naar voren komt, vanuit het juridisch perspectief bekeken. Dat zegt iets over de juridische grenzen van de huidige praktijk. Juist daar waar nu beperkingen worden gesignaleerd, is het zaak de werkwijze binnen de grenzen van het recht te brengen en aanbevelingen tot verbetering te doen.

1.5 Leeswijzer

In dit eerste hoofdstuk zijn de achtergrond, de doelstellingen en de aard van de voorliggende studie naar online monitoren door gemeenten besproken. Ook zijn de onderzoeksvragen gepresenteerd en zijn per onderzoeksvraag de voornaamste essentiële overwegingen geschetst die aan de aan de gehanteerde methoden ten grondslag liggen.

Hoofdstuk 2 (de literatuurstudie) behandelt eerst de wijze waarop de (Nederlandse) politie gebruikmaakt van online monitoring, omdat daar voor gemeenten veel lering uit valt te trekken. Daarbij besteden de achtereenvolgende paragrafen aandacht aan 1) de intenties en doelstellingen, 2) de werkwijze(n) en instrumenten en 3) de ervaren knelpunten en dilemma's. Vervolgens gaat het hoofdstuk in op de bekende en minder bekende aspecten van monitoring door gemeenten waarbij het zojuist genoemde drietal onderdelen wederom zichtbaar zullen zijn. Hoofdstuk 2 sluit af met een samenvatting die voor de inhoud van de empirische hoofdstukken leidend is. Hoofdstuk 3 kan worden beschouwd als het empirische hart van deze studie. Het gaat ten eerste in op de mate waarin en de wijze waarop gemeenten online monitoren en met welke intenties

en doelstellingen zij dit doen. Ten tweede worden de ervaren knelpunten en dilemma's van gemeenten in kaart gebracht. Daarbij komen juridische, ethische en technisch-organisatorisch aspecten aan bod. Hoofdstuk 4 gaat dieper in op de juridische grenzen waaraan gemeenten gebonden zijn wat betreft online monitoren. Het laatste deel, hoofdstuk 5, bevat de conclusies en beantwoordt daarmee de hoofdvraag van deze studie, zijnde 'In hoeverre geeft de huidige gemeentelijke praktijk wat betreft online monitoring van open bronnen in het domein van openbare orde en veiligheid reden tot heroverweging?'

2. Literatuuronderzoek naar de praktijk van politie en gemeenten

2.1 Inleiding

Dit hoofdstuk beantwoordt de tweede onderzoeksvraag van deze studie, te weten: wat is er vanuit de literatuur bekend over online monitoring? Met het oog op een goed begrip van dit hoofdstuk is het goed om te vermelden dat de inzichten in dit hoofdstuk moeten worden opgevat als verkenningen voor bestuurders en bestuursadviseurs. Het hoofdstuk geeft namelijk een breed beeld en is niet zozeer bedoeld als uitputtende juridische, technische, wetenschappelijke of maatschappelijke analyses.[45] Bovendien is het raadzaam om te beseffen dat informatie die wordt gebruikt voor openbare orde en veiligheid soms via algemene en op communicatie gerichte monitoring of analyses op de radar komt (zie ook hoofdstuk 1). In de praktijk lopen algemene communicatie en dienstverlening enerzijds en inhoudelijke en concrete handhavingsvraagstukken anderzijds dus door elkaar maar worden deze invalshoeken in dit hoofdstuk afzonderlijk behandeld.

Paragraaf 2.2 gaat eerst uitgebreid in op de praktijk bij de politie omdat men daar al langer bekend is met online monitoring en er dus relatief veel informatie beschikbaar is. Ook werken politie en gemeenten nauw samen waardoor ze goed van elkaars inzichten gebruik kunnen maken. Dit uit zich niet alleen in de strategische en tactische samenwerking in de 'driehoeken' waarin de burgemeesters, de politiechefs en de officieren van justitie zitting hebben, maar ook in de uitwisseling van informatie op operationeel niveau. Politie en gemeenten kunnen kortom veel van elkaar leren. De reeds beschikbare informatie over monitoring door gemeenten staat centraal in paragraaf 2.3. Net als bij de paragraaf over de politie komen achtereenvolgens de intenties en doelstellingen, de werkwijze en instrumenten en geconstateerde knelpunten en dilemma's aan bod. Paragraaf 2.4 vat aan het slot van het hoofdstuk de belangrijkste inzichten samen en geeft daarmee tevens enkele essentiële handvatten voor het vervolg van de studie.

45 Het onderzoek richt zich op uitingen op social media die voor iedereen toegankelijk zijn. Accounts of platformen die zonder wachtwoorden niet toegankelijk of zichtbaar zijn, vallen dus buiten het bestek van het onderzoek. Media-platformen die uitsluitend via betaaldiensten of die zich anderszins aan het zicht van het grote publiek zijn onttrokken zoals het 'darkweb', vallen eveneens buiten de scope van dit onderzoek.

2.2 Online monitoren door de politie

2.2.1 *Intenties en doelstellingen*

Voordat wordt ingegaan op de concrete intenties en doelstellingen met betrekking tot monitoring komen eerst de redenen van de politie om zich met sociale media in het algemeen bezig te houden aan bod. Monitoring kan niet los gezien worden van de socialemediastrategie die kan worden onderverdeeld in vier aspecten.[46] Ten eerste betreft dat de zichtbaarheid. De eenheden bepalen door het gericht gebruiken van sociale media voor een groot deel zelf wat op welke wijze met het publiek wordt gedeeld en geven daarmee blijk van zichtbaarheid en toegankelijkheid voor het publiek. Ten tweede bieden sociale media de mogelijkheid om de aandacht te vestigen op de doelstellingen van de organisatie en kunnen issues langdurig worden geagendeerd. Hierdoor wint de boodschap ook aan gewicht. Ten derde is men in staat om via sociale media naar eigen inzicht te reageren op vragen en kritiek. Men geeft daarmee inzicht in de prioritering en de manier waarop men te werk gaat. Ten vierde kan men, in tegenstelling tot wat bij traditionele media mogelijk is, zelf actief een relatie opbouwen met de verschillende actoren waardoor de politie tot op zekere hoogte 'in control' is over de loop van gebeurtenissen. Dit aspect van monitoring is concreet invulling gegeven bij de politie-eenheid Zeeland-West-Brabant die het doel van online monitoring als volgt omschrijft: "Om grip te krijgen op het virtuele deel van de maatschappij is voor de politie een 'online media monitor' onmisbaar."[47] Daarbij geeft men aan dat de organisatie grip of 'control' probeert te krijgen op online berichten en snel een omgevingsbeeld wil creëren bij calamiteiten. Een andere vorm van 'control', in een meer fundamentele betekenis, komt naar voren in een betrekkelijk 'vroeg' artikel over online monitoring door overheden.[48] De auteurs daarvan onderscheiden drie verschillende doelstellingen als het gaat om monitoren, namelijk:

1. monitoren ten behoeve van handhaving;
2. monitoren om de dienstverlening te verbeteren;
3. monitoren om het publieke debat te beïnvloeden.

Het voorliggende onderzoek gaat met name in op de eerste twee genoemde doelstellingen waarbij de aandacht nu eerst uitgaat naar de eerste vorm (monitoring ten behoeve van handhaving). Afhankelijk van de fase waarin een incident zich bevindt en de aanpak wordt in dat verband, overigens zonder dit verder te expliciteren, gesproken over

46 D.T. Snively (2016). Doctoral dissertation. *Effective social media use by law enforcement agencies: A case study approach to quantifying and improving efficacy and developing agency best practices.*
47 Politie-eenheid Zeeland-West-Brabant (2015). *Online mediamonitoring tool en proces (2) Ervaringen en inzichten naar aanleiding van operationele ervaring bij de politie-eenheid Zeeland-West-Brabant.*, p. 6.
48 Zie: A.J. Meijer & D. van Berlo (2011).

'actieve' monitoring dan wel over 'passieve' monitoring.[49] De politie tracht door bijvoorbeeld het opstellen van een zogenaamde 'dreigingsmonitor' op handen zijnde verstorende activiteiten te voorkomen. Dit past ook bij de strategie van de politie bij bijvoorbeeld het voorkomen van vechtafspraken tussen supportersgroepen van voetbalclubs.[50] Voorkomen vergt relatief weinig capaciteit ten opzichte van ingrijpen op locatie en het daaropvolgende strafrechtelijke proces in de zin van opsporen en bestraffen. Daarbij neigen de ontwikkelingen bij monitoring naar 'predictive policing' namelijk het voorspellen van crimineel en normoverschrijdend gedrag door middel van grootschalige monitoring en data-analyse.[51] Predictive policing heeft in beginsel betrekking op de strafrechtelijke handhavingstaak maar de werkwijzen kunnen ook worden toegepast op vraagstukken met betrekking tot de handhaving van de openbare orde.

De politie spreekt in haar visie uit dat ze sociale media zo veel mogelijk wil inzetten om haar operationele doelstellingen te realiseren.[52] Om dit voornemen door te voeren binnen de politieorganisatie zijn negen domeinen gedefinieerd waarop voor sociale media naast de klassieke politietaken (opsporing, preventie en crisisbeheersing) ook een rol is weggelegd voor 'media watch' en 'webcare'. Bij 'media watch' richt de aandacht zich op de berichtgeving over de politie terwijl webcare zich richt op direct online communicatie met doelgroepen. Het toenemend belang van sociale media uit zich in toenemende capaciteit bij de politie voor deze taak.[53] Soms zijn het complete afdelingen[54] die volledig gericht zijn op opsporing op sociale media, in de andere gevallen betreft het individuele rechercheurs die ondersteuning bieden aan de tactische opsporing. Rechercheurs worden daarbij geselecteerd uit de reguliere opsporing op basis van kennis, interesse of technische achtergrond, of uit de informatieorganisatie op basis van kennis en ervaring in (online) informatieverzameling. Overigens worden socialemedia-analyses niet alleen ex ante toegepast, ook vindt monitoring plaats voor analyses achteraf om te reconstrueren welke feiten en omstandigheden een rol speelden bij een incident en op welke wijze daarover gecommuniceerd werd. De politie-eenheid Zeeland-West-Brabant monitort bij concrete zaken waarbij zich in potentie openbare-ordevraagstukken kunnen aandienen, zoals vermissingen, een feest van een motorclub en de aankomst van wrakstukken van de MH17. De politie-eenheid maakt ook melding van de waarde van monitoring bij woordvoering en communicatie zoals het voeren van campagnes en het meten van resultaten van de eenheid.

---

49 S. van Veen & T. van den Ende (2012). *Wat vertellen social media ons over dreigingen?* Bron: https://www.trendsinveiligheid.nl/wp-content/uploads/2018/04/tiv2017_12_wat_vertellen_ social_media_ons_over_dreigingen-1.pdf.

50 T. van Ham, L. Scholten, A. Lenders & H. Ferwerda (2017). *Vechten op afspraak. Inzicht in het fenomeen en input voor de ontwikkeling van een politiestrategie* (reeks politie en wetenschap). Den Haag: Sdu.

51 A.R. Lodder & M.B. Schuilenburg (2016). 'Politie-webcrawlers en Predictive policing.' *Computerrecht, 2016(3),* 150-154.

52 M. Oosterhoff (2016). *Opsporing op social media* (Master thesis). Heerlen: Open Universiteit.

53 In internationaal verband zie: S.D. Musteen (2013). *Social Media's Law Enforcement.*

54 Het reeds genoemde doelgroepteam en de afdeling OSINT. Zie voor uitleg de volgende paragraaf.

Wanneer de doelstellingen en intenties worden samenvat, is te zien dat de nadruk bij de politie met betrekking tot monitoring ligt op het voorkomen van grote incidenten en verstoringen, al kan geconcludeerd worden dat ook reguliere 'webcare' en algemene 'communicatiedoeleinden' tot de dagelijkse activiteiten behoren. In de praktijk zal blijken dat openbare orde- en communicatiedoeleinden in elkaar overlopen en dus zeker niet strikt van elkaar gescheiden zullen zijn. De navolgende paragrafen gaan in op de vraag wat er bekend is omtrent de instrumenten die de politie kent voor monitoring, welke werkwijze ze hanteren en tegen welke grenzen ze daarbij oplopen.

2.2.2 *Werkwijzen en instrumenten*

Nu de doelstellingen van monitoring in beeld zijn gebracht, wordt gekeken welke middelen de politie daarvoor ter beschikking staan. Dergelijke monitoringstools zijn, althans dat is de veronderstelling van de politie, door de toepassing van algoritmen en beslisregels in staat zijn om de berichten te verzamelen, te ordenen, te duiden en te presenteren voor de eindgebruiker. Veelgenoemde leveranciers van dergelijke software zijn OBI4wan[55], Coosto, HowAboutYou[56] en Buzzcapture. Dergelijke instrumenten zijn over het algemeen ontwikkeld voor commerciële en/of journalistieke doeleinden.[57] Om de inzet van deze instrumenten te kunnen plaatsen in een bestuurlijke context is het nodig om de termen 'open source intelligence' (OSINT) en 'Real Time Intelligence Centers' (RTIC's) te introduceren.

Een Belgische politiestudie duidt de achtergrond van het acroniem OSINT als volgt: "Elke dag worden we overspoeld met informatie over een grote variëteit aan onderwerpen via de zogenaamde open bronnen zoals de pers, het internet, de sociale media en zo meer. Het gebruik en de analyse van deze lawinestroom aan informatie, die nog sterk wordt aangedikt doordat miljoenen individuen persoonlijke informatie beschikbaar stellen via sociale media, wordt internationaal in de Engelstalige benaming OSINT (Open Source Intelligence) genoemd."[58] Het omvat de methoden om informatie en inlichtingen middels openbare bronnen te verzamelen. Dit hoeft niet altijd in de vorm van geschreven tekst te zijn. Ook (digitale) foto's, video- en audiofragmenten kunnen gebruikt worden voor het effectief bestrijden van criminele activiteiten, zoals fraude en oplichting, het handhaven van de openbare orde of het waarborgen van de internationale veiligheid. Belangrijk bij de ontwikkeling van socialemediamonitoring is het ontstaan van Real Time Intelligence Centers (RTIC's) binnen de politie.

55 Bij de politie-eenheid Zeeland-West-Brabant (2015) is onderzoek gedaan naar de gebruikerservaring van de monitoringstool OBI4wan.

56 HowAboutYou is overgenomen door OBI4wan. Bron: https://www.OBI4wan.com/nl/OBI4wan-howaboutyou-samen-verder/.

57 Zie o.a.: A. Mateescu, D. Brunton, A. Rosenblat, D. Patton, Z. Gold, & D. Boyd (2015). Social media surveillance and law enforcement. *Data Civil Rights, 27*, 2015-2027.

58 R. Cox. (2013). Kritisch verslag over het gebruik van inlichtingen uit open bronnen en sociale media – verslag van een studiedag van het BISC. doi: 10.13140/RG.2.1.3613.8484.

De organisatie-eenheid RTIC is een uitgebreide meldkamer waarin data uit politieregisters, andere gegevens (zoals bijvoorbeeld van de Kamer van Koophandel) en persoonsgegevens van socialemediaplatformen zoals Facebook en Twitter samenkomen. De ontwikkeling van het RTIC komt voort uit de behoefte aan actuele informatie ten behoeve van besluitvorming op straat. Daarbij hoort ook het 24/7 monitoren van de buitenwereld door het signaleren van informatie ten behoeve van de aanpak van veiligheidsproblemen.[59] Het gaat hier om relevante extra informatie uit open bronnen, die realtime wordt gekoppeld aan politiekennis en politie-informatie. De doelstellingen van de RTIC's zijn: de veiligheid van de politiefunctionarissen op straat vergroten, 'vroegsignalering', en het vergroten van de 'heterdaadkracht'. Daarbij kijkt men onder andere naar persoonsgegevens, netwerken, locaties, getuigen en beeldmateriaal.[60]

In breder verband passen OSINT en RTIC in het streven van de organisatie naar 'Informatie gestuurd politiewerk' (IGP) waarbij op operationeel, tactisch en strategisch niveau kennis met partners wordt uitgewisseld om concrete veiligheidsproblemen aan te pakken. Een voorbeeld hiervan is het zogenaamde internet Research Network (iRN,)[61] een netwerkinfrastructuur voor onderzoek en opsporing op internet. Daarbij is een systeem (iColumbo) ontwikkeld dat niet alleen gegevens uit internetbronnen zoekt, maar ook analyseert (bijvoorbeeld met objectherkenning en datamining), selecteert, ordent en overzichtelijk presenteert. Daarmee komt gemakkelijk informatie in beeld die niet zou zijn gevonden tijdens een 'handmatige' surveillance op internet (zonder gebruik van de software). Als voordelen van dergelijke systemen noemt men dat de tijdsbesparing ten opzichte van het handmatig zoeken naar de informatie op internet enorm is.[62]

Naast iColombo wordt gebruikgemaakt van zoektools zoals OBI4wan (zoals bijvoorbeeld gebruikt door de politie-eenheid Zeeland-West-Brabant) en Coosto. Daarnaast is echter ook nog sprake van handmatig zoekwerk en ook van het gebruik van meer fakeaccounts.[63, 64] Deze accounts worden gehanteerd om toegelaten te worden in bepaalde groepen en om 'vrienden' te worden met verdachten of mensen daaromheen. Om de accounts geloofwaardig te houden, wordt af en toe iets geplaatst op deze fake Facebookpagina of wordt gecommuniceerd met een andere Facebookgebruiker.[65] De meer gespecialiseerde recherche-eenheden gaan hierin veel verder. Zij gaan met hun account nadrukkelijk de interactie met hun subjecten aan. Belangrijke grenzen die daarbij in acht moeten worden genomen, zijn uiteraard dat geen sprake mag zijn van

59 M. den Hengst, T. ten Brink & J. ter Mors (2017).
60 Politie-eenheid Zeeland-West-Brabant (2015).
61 J.J. Oerlemans & B.J. Koops (2012). Surveilleren en opsporen in een internetomgeving. *Justitiële verkenningen*, 38(5), 15.
62 Politie-eenheid Gelderland-Zuid (z.d.),bron: https://www.commit-nl.nl/universities/politie-gelderland-zuid.
63 A.J. Meijer (2013). *Politie en sociale media. Van hype naar onderbouwde keuzen*. Reed Business Information.
64 De suggestie voor strafrechtgeleerden is om te beschouwen in hoeverre deze praktijken zijn geoorloofd dat deze buiten het bereik van deze studie vallen.
65 M. Oosterhoff (2016).

het (mede)plegen van strafbare feiten, infiltratie of stelselmatige informatie-inwinning. Aan het begin van het vorige decennium sprak men nog in 'ambachtelijke' termen over 'het zoeken' op Hyves en ander sociale media in termen van 'het lezen van een krant'.[66]

Omdat de traditionele analyses die vaak door de politie worden gemaakt als reactie op een gebeurtenis of een gerucht veel handwerk vergden, heeft online monitoring zich razendsnel ontwikkeld tot een grotendeels geautomatiseerd proces hetgeen nieuwe vragen oproept die in dit onderzoek aan de orde komen.[67] Een interessant zijpad dat hier slechts wordt aangestipt, is dat uit onderzoek blijkt dat externe experts, waarbij OBI4wan met name werd genoemd, veelvuldig worden betrokken bij crises omdat zij daadwerkelijke specifieke kennis in huis hebben die nodig en bruikbaar is voor het beheersen van de crisis en de communicatie daarover.[68] Wat betreft de afhankelijkheid van externe leveranciers wordt erop gewezen dat niet altijd duidelijk is wie welke informatie in beheer heeft en waarvoor die wordt gebruikt.[69]

2.2.3 *Knelpunten en dilemma's*

Deze paragraaf beschrijft knelpunten en dilemma's zoals die in de literatuurverkenning over de politiepraktijk prominent naar voren komen. Het gaat dus niet om een uitputtend overzicht en een diepgaande analyse maar om een eerste verkenning die de belangrijkste kwesties blootlegt.

De onderkende knelpunten hangen sterk af van het perspectief van de belanghebbenden. Zo wijzen enkele consultants er bijvoorbeeld op dat de politie nog te veel reactief opereert.[70] Monitoring wordt in hun ogen tegenwoordig vooral gebruikt voor rechercheWerk ter ondersteuning van de agenten op straat of voor het oplossen van misdrijven. In de toekomst, zo is de gedachte, zullen complexe algoritmes in staat zijn om complexe terreurnetwerken bloot te leggen. Critici wijzen er juist op dat vraagtekens kunnen worden gesteld bij de transparantie en doelstellingen van leveranciers van dergelijke hulpmiddelen.[71]

Wat betreft eventuele juridische grenzen wordt hier een tweetal vraagstukken aangestipt die in hoofdstuk 4 nader zullen worden uitgewerkt. Ten eerste is de vraag in hoeverre in de praktijk een onderscheid gemaakt kan worden tussen 'gesloten' bronnen enerzijds en tussen 'open' bronnen anderzijds. Gesloten bronnen kunnen in beginsel alleen met toestemming van de officier van justitie worden onderzocht maar er zijn er

66 Zie: A.J. Meijer & D. van Berlo (2011).
67 S. van Veen & T. van den Ende (2012).
68 C. van Eijk, W. Broekema & R. Torenvlied (2013). *Geen uniformen, maar specialisten. Betrokkenheid van externe experts in crisissituaties.* Leiden: Universiteit Leiden.
69 A.R. Lodder & M.B. Schuilenburg (2016).
70 S. van Veen & T. van den Ende (2012).
71 O.a.: Buro Jansen & Janssen (2017). 'Social Media Surveillance in Nederland.' *Observant,* 70.

ook verhalen bekend van politiemedewerkers die uit hoofde van handhaving gebruikmaken van niet-herleidbare 'nicknames', 'avatars' en 'fakeaccounts' waardoor het onderscheid tussen open bronnen en gesloten bronnen diffuus wordt.[72] Ten tweede wordt verwezen naar onderzoek over de veranderende bevoegdheden van de politie wat betreft het gebruik van open bronnen.[73] Hierin vormt het begrip 'stelselmatigheid' (de mate waarin een min of meer compleet beeld van (een deel van) iemands privéleven wordt verkregen) een belangrijk ijkpunt. De inzet van 'technische' hulpmiddelen, zoals het gebruik van monitoringstools als Coosto en OBI4wan, lijkt daarbij ook een bepalende factor voor de vraag in hoeverre online monitoring toelaatbaar wordt geacht. In de sfeer van het strafrecht lijkt overigens in algemene zin, vergeleken met het bestuursrecht, ruim aandacht te worden besteed aan fundamentele rechten. Deze zijn geborgd door gedetailleerde wetten[74] en regelingen voor de toepassing van 'bijzondere opsporingsbevoegdheden'. Deze gelden in het bijzonder als de inbreuk op de persoonlijke levenssfeer van de betrokkene 'meer dan gering' is. Als waarborg daarvoor geldt bijvoorbeeld de voorafgaande toestemming van een hogere autoriteit zoals een officier van justitie of een rechter-commissaris.[75] De bijzondere opsporingsbevoegdheden uit het strafrecht en de inlichtingensfeer kunnen echter niet zomaar worden overgezet naar het bestuursrecht en de bestuurlijke context waarop deze studie zich met name richt.

Naast de vraagstukken over de juridische toelaatbaarheid valt bij de politie te constateren dat de kwaliteit van de door online monitoring verkregen gegevens onderwerp van gesprek is. Gegevenskwaliteit wordt beschreven als: "De mate waarin politiegegevens voldoen aan de eisen en verwachtingen die behaald moeten worden om de intelligence op te bouwen die het dagelijkse politiewerk aanstuurt. Om deze kwaliteit te waarborgen, wordt verwezen naar drie hoofdaspecten, te weten: juistheid, doeltreffendheid en controleerbaarheid." [76] Wat betreft juistheid dient in dit verband natuurlijk gewezen te worden op de toename van 'fakenieuws' en het belang van het falsificeren van desinformatie. Daarnaast lijkt het erop dat zich ook bij de politie knelpunten kunnen voordoen bij het koppelen van gegevens en het delen met andere partijen. De vraag is bovendien of de politie in staat is de snelheid waarmee op sociale media geacteerd wordt tijdig om

72 Zie: A.J. Meijer & D. van Berlo (2011).
73 W.Ph. Stol, & L. Strikwerda (2018).
74 Aan de ene kant wil de wetgever de politie zo veel mogelijk bevoegdheden geven om haar taken te kunnen uitoefenen maar aan de andere kant dienen waarborgen omtrent privacy en rechtsbescherming te worden. ingebouwd. De Wet politiegegevens, in lijn met haar grote broer de Wet bescherming persoonsgegevens, voorziet in deze waarborgen (M. den Hengst, T. ten Brink & J. ter Mors (2017). p. 66) omdat: "De politie gegevens registreert zonder dat zij daar vooraf toestemming voor geven; Waarheidsvinding het risico met zich meebrengt dat politiegegevens onjuist of onvolledig zijn; De politie een bijzondere rol in de maatschappij heeft in de verhouding tussen overheid en burger. De wet reguleert het informatieproces, waardoor dit transparant en controleerbaar is."
75 J.J. Oerlemans & Y.E. Schuurmans (2019).
76 M. den Hengst, T. ten Brink & J. ter Mors (2017). p. 109.

te zetten in relevante informatie. Onderzoeken[77, 78] laten zien dat het gebruik van sociale media[79] sterk afhangt van met name de leeftijd en het opleidingsniveau van de gebruiker. Bepaalde groepen zullen dus vaker in zoekresultaten verschijnen hetgeen de doeltreffendheid kan beïnvloeden. Een enkele auteur[80] wijst op het bijzondere belang van vertrouwen. Zodra dit wordt beschaamd en de controleerbaarheid in het geding is, zal het publiek massaal en direct afstand doen van de zorgvuldige opgebouwde relatie met de politie.

In de loop der jaren heeft zich dus een praktijk ontwikkeld waarbij monitoring van online bronnen niet meer handmatig plaatsvindt, maar dat systemen internet doorzoeken. De opkomst van software maakt het efficiënt zoeken in de zee van informatie op internet mogelijk en brengt een ongekende hoeveelheid informatie in relatief korte tijd naar boven.[81] Echter, door het gebruik van geautomatiseerde politiesystemen worden privacy-inbreuken mogelijk steeds ingrijpender.[82] Dergelijke zorgen worden gedeeld door de politieorganisatie zelf.[83] Gegevens mogen alleen worden vastgelegd zover dat noodzakelijk is, ze moeten ter zake dienend zijn en niet 'bovenmatig'. Met andere woorden: monitoring moet voldoen aan de gebruikelijke eisen rondom proportionaliteit[84] en subsidiariteit.[85] Gesteld wordt dat de veranderingen rondom sociale media en de rol van de politie zo snel verandert dat de beleidsmakers en gezagsdragers deze nauwelijks meer kunnen bijbenen.[86] Daarbij zal ook de interne organisatie aangepast moeten worden. Nieuwe inzichten leiden tot de koppeling van systemen, collega's met andere vaardigheden en attitudes. Deze en andere organisatorische aspecten het hoofd biedend, zou dit kunnen leiden tot nieuwe bureaucratisering binnen de politie. In 2015 constateerde de Nationale Politie dat bij veel operationele politieprocessen het gebruik van sociale media nog niet opgenomen was in de werkprocessen en dat niet exact bekend was welke afdelingen zich er mee bezighielden.[87] Uit de aanbeveling bleek dat aandachtspunten lagen in de mindset en het opleidingsniveau van de medewerkers. Ook constateerde men een tekort aan gekwalificeerd personeel om de soms ingewik-

77 R. Ruddell & N. Jones (2013). 'Social media and policing: matching the message to the audience. Safer Communities. *Safer communities.*' *12* (2), 64-70

78 P. Lewis, T. Newburn, M. Taylor, C. Mcgillivray, A. Greenhill, H. Frayman & R. Proctor (2011). *Reading the riots: investigating England's summer of disorder.* London: The Guardian.

79 Dergelijke studies gaan overigens over social media gebruik door politieorganisaties in het algemeen en niet specifiek over monitoring van openbare bronnen.

80 D.T. Snively (2016).

81 Waarbij wordt opgemerkt dat niet alle socialmediaplatforms zich evengoed lenen voor monitoring. Dit hangt bijvoorbeeld af van de geboden privacy-instellingen. Zie o.a.: A. Mateescu et al. (2015).

82 Zie: J.J. Oerlemans & B.J. Koops (2012).

83 M. den Hengst, T. ten Brink & J. ter Mors (2017). p. 20.

84 De zwaarte van het in te zetten middel moet in verhouding staan tot het beoogde doel. Hierbij speelt de ernst van het 'delict' een rol.

85 Het middel wordt ingezet als een eventueel minder zwaar middel niet tot voldoende resultaat heeft geleid of zal kunnen leiden.

86 M. den Hengst, T. ten Brink & J. ter Mors (2017).

87 IM Adviesrapport Tools Informatieorganisatie (2015). Bron: https://respubca.home.xs4all.nl/pdf/ politiebesluitadviesrapportd.pdf.

kelde tools te kunnen doorgronden en optimaal in te zetten. Om de monitoring te kunnen ontwikkelen, legde men de nadruk op zowel de interne samenwerking (o.a. inkoop, ICT) als de samenwerking met de leveranciers. Ook de politie-eenheid Zeeland-West-Brabant (2015) benadrukt dat het gebruik van monitoring (tools) de nodige organisatiekundige vraagstukken blootlegt over rollen, taken en verantwoordelijkheden. Niet alleen binnen de politie maar zeker ook met de maatschappelijke partners. Daarnaast wordt melding gemaakt van een gebrek aan enthousiasme in de geledingen over online monitoring. Overigens kan geconstateerd worden dat deze organisatiekundige aspecten zich ook voordeden bij de introductie van sociale media in het algemeen en dat die ook in internationaal verband zichtbaar zijn.[88]

Uit de literatuur die in de voorgaande paragrafen aan bod kwam, zijn vanuit de politiepraktijk globaal twee doelstellingen van online monitoring te destilleren.

A. Het verbeteren van de kwaliteit van de dienstverlening. Hier gaat het in beginsel om een bijzondere vorm van 'reputatiemanagement'. In de praktijk spreekt men hierover als 'van buiten naar binnen halen' of 'temperaturen' en kan daarmee worden geschaard onder de parapluterm (bedrijfs)communicatie.
B. Het in kaart brengen van potentiële verstoringen van de openbare orde, eventuele strafbare feiten en andere ontwikkelingen die duiden op crises, kortweg: handhaving. Het zal uit de vorige paragraaf duidelijk zijn geworden dat de politie met name geïnteresseerd is in de strafbare feiten terwijl de gemeente de zorg voor handhaving van de openbare orde en veiligheid tot haar kerndoelstellingen mag rekenen.

Daarnaast is te zien dat de politie zich qua houding van reactief naar proactief ontwikkelt. De technische hulpmiddelen maken het mogelijk om steeds meer informatie in te winnen waardoor de wettelijke grenzen sluipenderwijs overschreden kunnen worden. Daarbij is het de vraag in hoeverre de politie nog daadwerkelijk 'in control' is over de verkregen informatie. Het vraagstuk van de ethiek dringt zich daardoor steeds nadrukkelijker op. Moeten we dit, op deze manier, nog wel willen? De volgende paragraaf laat zien in hoeverre gemeenten met dergelijke vraagstukken te maken hebben waarbij logischerwijs de focus meer op het vraagstuk van openbare orde komt te liggen en minder op de opsporing van strafbare feiten.

2.3 Online monitoren door gemeenten

Uit de vorige paragraaf blijkt dat op hoofdlijnen twee doelstellingen van online monitoring bij de politie te onderscheiden zijn: communicatiedoeleinden en handhaving van de openbare orde en veiligheid. In de praktijk zijn deze doelstellingen nauw aan

88 K. Bullock (2018). 'The police use of social media: Transformation or normalisation?' *Social Policy and Society, 17*(2), 245-258.

elkaar verbonden. Aan de hand van deze twee paraplubegrippen wordt nu nader ingegaan op de intenties en doelstellingen die de literatuur prijsgeeft over online monitoring bij gemeenten.

2.3.1 *Intenties en doelstellingen*

Communicatie
Binnen de publieke sector worden sociale media in het algemeen ingezet om beter in verbinding te staan met burgers, om opener en transparanter zijn en om rekenschap af te kunnen leggen over het gevoerde beleid.[89] Ten eerste zetten gemeenten online monitoring, als onderdeel van de webcarestrategie, in voor het verhogen van de kwaliteit van dienstverlening. Webcare is een structurele '(near) real time' dienstverlening van de gemeente richting haar inwoners via sociale media.[90] Het doel van webcare is ten eerste het beantwoorden van vragen en het reageren op klachten (waarmee ook de angel uit potentiële veiligheidsvraagstukken gehaald kan worden) en ten tweede het bewaken en verzorgen van de online reputatie van de gemeente. Webcare wordt in de regel uitgevoerd door het gemeentelijke 'Klant Contact Centrum' of door de 'Afdeling Communicatie'. Een van de voorlopers in Nederland is de gemeente Utrecht die al in 2012 een officieel 'Webcareteam' installeerde en daarbij een strategie op het gebied van socialemediabeleid opstelde.[91] In de gemeente Utrecht wordt gesproken over een 'conversatiemanager' als iemand die weet wat er wordt besproken en wanneer het juiste moment is om (namens de organisatie) deel te nemen aan een gesprek. Een vervolgstap is om onderwerpen die leven in de stad in kaart te brengen en te analyseren.

Een eerste ontwikkeling betreft de oprichting van zogenaamde 'Newsrooms'. Met name grote en middelgrote gemeenten werken met een fysieke plek binnen de organisatie, waar 'binnen- en buitenwereld' met elkaar in verbinding worden gebracht, het luisteren en zenden op elkaar worden afgestemd en daarmee het gesprek en de samenwerking mogelijk worden gemaakt.[92] In een dergelijke afdeling wordt continu gemonitord wat over de gemeente wordt gezegd, om daar vervolgens ook snel op te kunnen reageren. Online monitoring wordt voorts gebruikt om informatie te verzamelen over actuele kwesties binnen en buiten de gemeente. Men haalt 'buiten naar binnen' door de creatie van een omgevingsbeeld. Dat kan bijvoorbeeld gaan over de renovatie van een stationsgebied, aangekondigde demonstraties of het in de gaten houden van een groep personen die mogelijk overlast veroorzaken. Dergelijke gebeurtenissen zijn nauw verbonden aan het domein van openbare orde en veiligheid. Naast een analyse van de

89 S.M. Zavattaro (2013).
90 Zie: D. Kok (red.) (2013). *Sociale gemeenten. De kracht van nieuwe media*. Delft: Academische Uitgeverij Eburon.
91 P. Veltman (2014). *Utrecht en de ontwikkeling van Social Webcare bij de gemeente Utrecht: een kijkje achter de schermen.* Bron: https://www.marketingfacts.nl/berichten/webcare-bij-de-gemeente-utrecht-een-kijkje-achter-de-schermen.
92 Stichting Arbeidsmarkt- en opleidingsfonds gemeenten (2014). *Handelingsinstructies – Agressie Social Media en Webcare.*

traditionele media speelt berichtgeving op sociale media vanzelfsprekend een belangrijke rol. De beknopte rapportage van deze actualiteiten wordt vaak verspreid als online 'knipselkrant'. De gemeente Delft ziet het gebruik van dergelijke communicatie als een manier om duurzaam (minder oppervlakkig en langduriger) op een laagdrempelige (voor iedereen toegankelijke) wijze toegevoegde waarde te kunnen leveren.[93]

Gemeentelijke initiatieven zoals Webcare en Newsrooms zijn weliswaar niet primair bedoeld voor het domein van openbare orde en veiligheid maar kunnen wel degelijk een belangrijke invloed hebben. Webcare kan niet alleen bijdragen aan de de-escalatie van maatschappelijke spanningen maar ook bestuurders informatie geven over op handen zijnde verstoringen. Hierop wordt in de volgende alinea nader ingegaan.

Handhaving van de openbare orde en veiligheid

Bekend is dat al in 2013 een kleine meerderheid van alle gemeenten gebruikmaakt van sociale media in het algemeen ten behoeve van openbare orde en veiligheid.[94] Over de exacte intenties en werkwijze van gemeenten op het gebied van openbare orde en veiligheid en in hoeverre monitoring wordt ingezet, was echter nog weinig bekend.[95] Hier wordt aan de hand van met name de praktijk van de gemeente Amsterdam ingegaan op deze kwesties. Concreet benoemt de gemeente Amsterdam de volgende activiteiten die een raakvlak hebben met openbare orde: monitoring en crowdcontrol bij grote evenementen zoals Koningsdag, handhaving bij (illegale) evenementen, het gedrag van jongeren met betrekking tot overlast of criminaliteit op straat en het daaraan gerelateerde gedrag op sociale media.[96] Verder maakt Amsterdam bekend dat de gemeente monitoring inzet bij specifieke calamiteiten en incidenten in het bijzonder. De gemeente gebruikt hiervoor instrument Coosto. Wat betreft digitale dreigingen lezen we verder dat wanneer een dergelijke dreiging zich manifesteert de Amsterdamse openbare orde in het geding kan komen. De gemeente wil dan direct ingelicht worden om een significant incident te herkennen, goed voorbereid te zijn en te beschikken over de juiste middelen en communicatielijnen om (de gevolgen van) een crisis te beheersen.

Het aspect handhaving is overigens niet alleen zichtbaar binnen het domein van openbare orde en veiligheid maar ook in het domein van de sociale zekerheid. Er wordt, in het kader van inkomensvoorzieningen zoals de bijstand, gecontroleerd op woonplaats en bijverdiensten op sociale media en online handelsplatformen zoals Marktplaats. Op weer een geheel ander domein worden de vluchtverhalen van asielzoekers gecheckt aan de hand van tijdlijnen op bijvoorbeeld Facebook of Instagram. Op het terrein van

93 Gemeente Delft (jaartal onbekend). *Keuzehulp Social Media*, Gemeente Delft.

94 J.A. van Dijk, L. Wijngaert & S.T. Tije (2015). *Overheidsparticipatie in sociale media*. Universiteit Twente-Center for Telematics and Information Technology.

95 Onder wetenschappers ging de aandacht met name uit naar surveillance door de politie (zie bijv. J. J. Oerlemans & B.J. Koops (2012).

96 Gemeente Amsterdam (2019).

huisvesting worden maatregelen genomen ten aanzien van de illegale verhuur van woonruimte.[97]

Wanneer de beperkte informatie over gemeenten wordt samengevat, blijkt dat monitoring gebruikt wordt in een breed palet van handhavingsvraagstukken. Van fysieke dreigingen tot gedigitaliseerde criminaliteit en van openbare orde tot verhuurbeleid. Tevens is te zien dat gegevensuitwisseling een cruciaal aspect is in de werkwijze en dat deze de betrokken organisaties voor de nodige uitdagingen stelt. Het praktijkonderzoek, zie hoofdstuk 3, zal meer inzicht geven in de doelstellingen en de werkwijzen van gemeenten op het gebied van communicatie en openbare orde en veiligheid. Eerst zal nu gekeken worden welke monitoringtools door deze organisaties worden ingezet en hoe deze in de praktijk werken.

2.3.2 *Werkwijzen en instrumenten*

Monitoring blijkt steeds populairder te worden binnen de publieke sector in het algemeen en bij gemeenten in het bijzonder.[98] Met de beschikbare instrumenten kunnen online openbare bronnen gemonitord en geanalyseerd worden. Dergelijke tools worden aangeboden door verschillende bedrijven op het gebied van reputatiemanagement. Hoewel de tools aanvankelijk vooral bedoeld zijn voor communicatiedoeleinden worden de tools nu ook gebruikt in het domein van handhaving. Genoemd zijn OBI-4wan en Coosto als leveranciers van gelijkluidende tools. De tools downloaden structureel bepaalde data afkomstig van de belangrijkste sociale media zoals Twitter en Facebook en slaan deze op in hun systemen waarna zoekopdrachten worden toegepast.[99] Door de snelheid van achtereenvolgende handelingen kunnen de verwerking en presentatie bijna realtime plaatsvinden. Daarbij komt dat dergelijke tools in staat zijn links en eerder gevonden informatie te koppelen aan actuele gegevens.[100] Ze verzamelen data op continue basis, maken deze doorzoekbaar en bieden gereedschappen om gegevens te analyseren, resultaten te presenteren en te reageren op berichten.

Met een monitoringstool kan informatie van het het wereldwijde web worden afgehaald en vervolgens worden doorzocht met bepaalde zoektermen (zoals gemeente X, demonstratie Y), maar ook op lijsten van personen. Verkregen resultaten kunnen ook worden verrijkt met allerlei informatie over geografische locaties of persoonsgegevens. Daarnaast kan allerlei meta-informatie worden verkregen op basis van het aantal en de aard van het gebruik van zogenaamd hashtags.[101] Ook kan in kaart worden gebracht hoe vaak een 'post' is gezien, geliked of gedeeld. Aan de monitoringstools kunnen spe-

97 Gemeente Amsterdam (2019).
98 Zie o.a: Computable. Main Capitals OBI4wan lijft howaboutyou in. Bron: https://www.computable.nl/artikel/nieuws/overheid/6909591/250449/main-capitals-obi4wan-lijft-howaboutyou-in.html
99 Zie ook: J.J. Oerlemans & Y.E. Schuurmans (2019).
100 O.a: J. Bakker et al. (2016).
101 Symbool: #.

cifieke rechten worden toegekend. Dit voorkomt in beginsel het ontstaan van wildgroei aan het aantal medewerkers dat zendt, reageert of rapportages uitdraait. Bij een zogenaamde sentimentsanalyse[102] worden berichten gelabeld als positief of negatief (of door middel van kleurenvarianten) met als doel een snel overzicht te krijgen over de mate waarin beleidsvoornemens of de algehele waardering van de dienstverlening worden gewaardeerd.

Wat betreft de handhavingsvraagstukken heeft een van de leveranciers, te weten Coosto, in samenwerking met het WODC een verkenning uitgevoerd naar de toepasbaarheid van hun instrument voor het in kaart brengen van online dreigingen.[103] Deze zogenaamde dreigingsmonitor is in staat om de inhoud van individuele berichten te analyseren en daar geautomatiseerd een dreigingsniveau aan toe te kennen. Daarnaast bestaat de mogelijkheid om online informatie te verzamelen over de berichtgeving op sociale media omtrent specifieke incidenten zodat het bevoegd gezag deze informatie kan meenemen bij het bepalen van de aanpak.

2.3.3 *Knelpunten en dilemma's*

Nu de doelstellingen, de werkwijze en instrumenten zijn beschreven, behandelt deze paragraaf een aantal beperkingen die aan online monitoring zijn verbonden voor gemeenten. Deskundigen maken een aantal fundamentele opmerkingen met betrekking tot de wenselijkheid van monitoring.[104] Zij vragen zich af of de wereld van Twitter, Facebook en YouTube het nieuwe dorpsplein is waar iedereen, dus ook overheidsfunctionarissen, aanwezig mogen zijn en kunnen meepraten. Of is het meer een clubhuis waar alleen leden welkom zijn en anderen, en dus ook ambtenaren, niets te zoeken hebben? Voorts geven ze aan dat er nauwelijks wordt gesproken over de wenselijkheid van monitoren op internet en de vraag of overheden dit wel zouden moeten willen. Zij hebben de indruk dat monitoring algemeen geaccepteerd is en dat overheden een groot vertrouwen stellen in de validiteit van de door hen verkregen informatie al weten zij niet exact op welke wijze deze tot stand is gekomen. Ten slotte wijzen deze deskundigen erop dat pragmatisme de boventoon lijkt te voeren. Men zoekt naar tools die zo veel mogelijk kunnen en zo min mogelijk kosten. Daarbij wordt vooral vertrouwd op de ervaringen en 'best practices' van andere gemeenten.

Enkele privacyorganen hebben hun zorgen geuit over deze ontwikkelingen. Zo voert de Raad van Europa, met het oog op grondrechten zoals het recht van vrijheid van meningsuiting en de persvrijheid, met enige regelmaat onderzoeken uit naar de manier waarop overheden internet monitoren en welke wettelijke gronden zij hiervoor

102 De techniek om online sentimenten automatisch te analyseren wordt 'opinion mining' genoemd, zie: J. Bakker et al. (2016).
103 O.a.: J. Bakker et al. (2016).
104 A.J. Meijer & D. van Berlo (2011).

hanteren.[105] In de Verenigde Staten is er bescherming van de 'Civil Rights' in het algemeen en het 'First Amendment-right' die de vrijheid van meningsuiting beschermen en 'Fourth-amendment-right' die de burger zo veel mogelijk moet vrijwaren van overheidsbemoeienis.[106] Het gaat er overigens niet alleen om dat de overheid zich onthoudt van dergelijke inbreuken, maar ook dat individuele burgers worden gevrijwaard van schendingen door andere private partijen.[107]

In Nederland houdt vooral de Autoriteit Persoonsgegevens (het toezichthoudende orgaan van de AVG in Nederland, hierna: AP) de verwerking van persoonsgegevens bij overheidsinstanties zoals gemeenten in de gaten.[108] Recentelijk is door de AP advies uitgebracht over het rechtmatig verwerken van persoonsgegevens in het kader van het sociaal domein, zoals het online monitoren (van onder andere sociale media) in het kader van de bestrijding van uitkeringsfraude. In het Protocol internetonderzoek door gemeenten (2015) is besloten dat gemeenten alleen internetonderzoek mogen doen bij aantoonbare indicaties van misbruik of fraude. Preventief internetonderzoek, bijvoorbeeld bij de aanvraag van een uitkering, is niet toegestaan. Om ervoor te zorgen dat organisaties voldoen aan de toepassing en naleving van de AVG-wetgeving zijn gemeenten, sinds het van kracht worden van de AVG op 25 mei 2018, verplicht om een functionaris gegevensbescherming aan te stellen, ongeacht het type gegevens dat ze verwerken.[109]

Gesteld wordt dat openbronnenonderzoek in beginsel geen bijzonder ingrijpende manier van informatievergaring is.[110] Gegevens die op internet voor eenieder beschikbaar zijn, mogen in beginsel door ambtenaren, als daar aanleiding toe is, worden verzameld als onderdeel van hun algemene bevoegdheid, voortvloeiend uit het vigerende bestuursrecht om informatie te verzamelen. De auteurs stellen dat ook binnen het strafrecht en het 'inlichtingendomein' de nodige juridische waarborgen zijn ingebouwd ter bescherming van de grondrechten van betrokkenen terwijl deze in het bestuursrecht nog ontbreken. Het is dus onduidelijk wat er precies wél en niet mag. Risico's liggen in de sfeer van:

1. Het ontbreken van specifieke wettelijke grondslagen voor het doen van online bronnenonderzoek al lijken algemene beginselen als proportionaliteit, subsidiariteit en zorgvuldigheid de belangrijkste toetsingscriteria.

105 Raad van Europa (2017). Comparative study on blocking, filtering and take-down of illegal internet content.
106 A. Mateescu et al. (2015).
107 Schweizerische Eidgenossenschaft (2011). *Legal Basis for Social Media Report of the Federal Council in Fulfilment of the Amherd Postulate 11.3912 of 29 September 2011.*
108 Zie in het kader van de actualiteit: Argos, 29 mei 2020. Kwart van gemeenten neemt privacy niet serieus. VPRO. Bron: https://www.vpro.nl/argos/lees/nieuws/2020/kwart-van-gemeenten-neemt-privacy-niet-serieus0.html#
109 Artikel 37 van de Algemene Verordening Gegevensbescherming (AVG).
110 Zie o.a.: J.J. Oerlemans & Y.E. Schuurmans (2019).

2. Het opereren van een 'internetrecherche' buiten het gezichtsveld van belanghebbenden zoals de burger zelf en de rechterlijke macht.
3. Hiermee hangt samen de mate van transparantie en de beginselen van proportionaliteit en stelselmatigheid.[111] Als er een min of meer compleet beeld van (een deel van) iemands persoonlijk leven in kaart zal worden gebracht, zullen de rechterlijke macht en toezichthouders een strengere koers varen en mogelijk gemeenten tot de orde roepen. Een andere belangrijke open vraag is hoe de AVG monitoring normeert en onbekend is in hoeverre het vage begrip 'stelselmatigheid' leidend is.[112]

Vanuit de praktijk van de gemeente Amsterdam worden nog meer beperkingen onderkend naast de zojuist genoemde (privacy)aspecten.[113] Zo kan men op basis van open bronnen altijd maar een deel van de informatie krijgen: je weet niet wat je niet ziet en hoe waardevol de beschikbare informatie is. Een online 'oproep tot ongehoorzaamheid' kan bijvoorbeeld in werkelijkheid iets anders zijn dan het op het internet lijkt. Online informatie moet dus altijd in samenhang met de andere informatiebronnen worden gebruikt.[114] Daarnaast onderkent de gemeente Amsterdam een aantal duidelijk praktische beperkingen. De online wereld is namelijk 24/7 actief terwijl ambtenaren dat in veel mindere mate zijn. Daarnaast is online contact geen vervanging van offline contact. Betrokken instanties als jongerenwerk, politie, hulpverleners en gemeente(n) doen allemaal wel iets op sociale media, maar in beperkte mate en gefragmenteerd. Bovendien is de kwaliteit van de monitoring vaak afhankelijk van de kennis, kunde en houding van individuele professionals. Begrip van de belevingswereld van jongeren is niet vanzelfsprekend. Dergelijke zwakke punten worden niet alleen door de gemeente Amsterdam onderkend maar ook platforms wijzen op de beperkingen van open bronnen.[115] Concreet wordt gewezen op programma's als OBI4wan en Coosto die (weliswaar realtime) altijd slechts een deel van de online beschikbare informatie leveren. Ook bestaat er geen wetenschappelijke onderbouwing van de kwaliteit, nauwkeurigheid en totstandkoming van bijvoorbeeld 'sentimentsanalyses'. Ouderwets 'handwerk' blijft noodzakelijk. Vanuit gedragskundige hoek valt op dat er grote verschillen zijn in hoe ambtenaren tegen het gebruik van sociale media in het algemeen en monitoring in het bijzonder aankijken. Sommige medewerkers zijn uit angst voor wat wel en wat niet kan op sociale media erg terughoudend. Anderen zijn (over)enthousiast. Voor beide groepen wordt een belangrijke stelregel als houvast gebruikt.[116]

111 Stol, W. ph., & W. Bantema (2020). 'Stadbestuur en digitale veiligheid, een analyse van beleidsplannen.' In M. Malsch & J.W. Sap (red.), *Orde en verwarring in de stad*. Boom Criminologie.
112 Ontleend aan: J.J. Oerlemans & Y.E. Schuurmans (2019).
113 Gemeente Amsterdam (2016).
114 In onderzoek van W. Bantema, S. Westers & S.A.J. Munneke (2020) wordt door crisiscommunicatie-experts aangegeven dat bestuurders nooit genoegen moeten nemen met uitsluitend een online sentimentenanalyse voor het duiden van een crisis of de dreiging die ervan een online situatie uitgaat. Onder andere omdat soms veel mensen buiten de gemeente bijdragen aan een beeld dat soms op straat niet wordt herkend (inmenging online op sociale media).
115 Waaronder: Buro Jansen & Janssen (2017).
116 Zie bijvoorbeeld: J.A. van Dijk et al. (2015).

Vanuit ethisch perspectief kunnen vraagtekens bij gemeentelijk gebruik van online openbare bronnen worden gezet: "Het openbaar toegankelijke karakter van informatie kan geen rechtvaardiging kan zijn voor ongebreidelde verspreiding en opslag."[117] Omdat online informatie uit de context kan worden gehaald en een eigen leven kan leiden. Informatie wordt gedeeld met een bepaalde functie in een bepaalde context, ook online. Een patiënt vertelt een huisarts bijvoorbeeld over zijn of haar aandoening op hoop van genezing, en niet voor commerciële doeleinden. Privacy wordt gezien als het recht om in een wereld te leven waar de informatie vloeit volgens onze gelegitimeerde verwachtingen, gedefinieerd als contextuele integriteit.[118] Zodra informatie anders gebruikt wordt, is de context verloren gegaan en moet privacy opnieuw beoordeeld worden. Daaruit volgt de vraag: ligt het, in deze context, in de lijn der verwachting dat inwoners door de gemeente online in de gaten gehouden worden?

Of er sprake is van een privacyschending is afhankelijk van de mate van inbreuk op de persoonlijke levenssfeer door monitoring. Voor gemeenten is dit dus de mate van online monitoring van (groepen) personen, specifiek heimelijke monitoring. In de offline wereld vindt een schending van de privacy plaats op een specifiek moment en een specifieke plaats, zoals een persoon die ongewenst foto's maakt vanuit de bosjes. Deze zogenoemde lokale privacy is makkelijk vast te stellen en te handhaven op die plaats, op dat tijdstip. Digitalisering heeft geleid tot een verschuiving van de lokale privacy naar informationele privacy.[119] Informatie over een persoon is langere tijd en op meerdere plekken (online) te bekijken en kan in een andere context worden geplaatst. Als de gemaakte foto's vanuit de bosjes online worden gezet, kunnen deze jarenlang en op meerdere locaties telkens weer de privacy schenden. Dit zorgt ervoor dat informationele privacyschending moeilijker te duiden en te handhaven is. De grens van deze informationele privacyschending is afhankelijk van de inbreuk op de persoonlijke levenssfeer.

Verder valt het op dat het moeilijk kan zijn om de informatie die door monitoringtools wordt verkregen juist te interpreteren. Online berichten hebben doorgaans een gebrek aan context, specifieke sociale signalen, figuurlijke tekst en offline dynamiek. Daarnaast geeft bijvoorbeeld de gemeente Amsterdam aan dat haar inwoners wekelijks in contact komen met onjuiste data en informatie, die veelal verspreid worden via socialemediaplatformen als Facebook, Twitter en Instagram. Om de informatie sneller te analyseren, bieden monitoringstools een sentimentanalyse. Bedrijven als Coosto en OBI4wan presenteren de sentimentanalyse doorgaans als een wetenschappelijke methode. Er bestaat echter geen wetenschappelijke onderbouwing van de kwaliteit, nauwkeurigheid en totstandkoming van de analyses.[120]

117 M.J. Becker (2015). *Ethiek van de digitale media*. Amsterdam: Boom. p. 91.
118 Nissenbaum in M.J. Becker (2015).
119 M.J. Becker (2015).
120 o.a.: Buro Jansen & Janssen (2017).

Wat betreft organisatorische aspecten wijst de gemeente Amsterdam op een gebrek aan gekwalificeerd personeel, het ontbreken van mogelijkheden tot investeringen en problemen met betrekking tot de uitwisseling tussen bijvoorbeeld wetenschappers, bedrijfsleven en overheid.[121] De gemeente stelt zich voorts de vraag wat de impact van het digitaliseren is op de onderlinge samenhang en verhoudingen tussen de verschillende gemeentelijke diensten. Digitalisering strekt zich immers uit over alle domeinen en kan niet vanuit een portefeuille of directie vanuit de gemeente worden bepaald. Over het thema openbare orde en veiligheid vermeldt de gemeente Amsterdam dat veiligheidsregio's zoekende zijn naar hun rol bij digitale verstoringen.

2.4 Afsluiting

De politie monitort openbare bronnen met als doel om grote incidenten en verstoringen te voorkomen en om de dienstverlening van de politie te verbeteren. De toegepaste instrumenten passen binnen grotere kaders zoals OSINT en RTIC's en zijn onderdeel van de dagelijkse praktijk. De politie heeft zich qua houding van reactief naar proactief ontwikkeld. De technische hulpmiddelen maken het mogelijk om steeds meer informatie in te winnen waardoor de wettelijke grenzen (met name het vraagstuk van stelselmatigheid wint aan urgentie) sluipenderwijs overschreden kunnen worden. Daarbij wint de vraag in hoeverre de politie nog daadwerkelijk 'in control' is over de verkregen informatie aan urgentie.

Wat betreft gemeenten is te zien dat 'webcare' en 'communicatie' van oorsprong de voornaamste drijfveren waren om tot monitoring over te gaan en dat er nu sprake is van een verschuiving naar handhavingsvraagstukken in het algemeen en het domein van openbare orde en veiligheid in het bijzonder. Samengevat kunnen de beperkingen onderverdeeld worden in drie verschillende componenten. Ten eerste is aandacht voor de organisatorische issues omtrent de betrouwbaarheid van de informatie en de beschikbaarheid van de juiste middelen. Deze zijn te vatten onder de noemer 'kunnen'. Ten tweede komen juridische grenzen die voortvloeien uit de AVG en het EVRM, maar ook aspecten van proportionaliteit en stelselmatigheid naar voren die gelabeld kunnen worden als 'mogen'. Ten derde is te zien dat er ethische vraagstukken te onderkennen zijn die te vatten zijn onder het kopje 'willen'. Dit onderzoek beoogt een aantal mogelijke spanningsvelden bij online monitoring door gemeenten verder bloot te leggen. Deze spanningsvelden zijn dus terug te voeren op de techniek (kunnen), ethiek (willen) en het recht (mogen) en uiten zich onder meer in de volgende vragen: als het technisch en organisatorisch geregeld kan worden, kan het monitoren dan ook in juridisch opzicht door de beugel? Als het monitoren in juridische zin geoorloofd is, moeten we het dan ook per se willen? Als het juridisch mag, kunnen gemeenten daar dan ook in technisch en organisatorisch opzicht handen en voeten aan geven? Als bepaalde

121 Gemeente Amsterdam (2019).

informatie nodig blijkt te zijn, wordt deze dan op een wijze verkregen die het minste inbreuk maakt op de privacy van betrokkenen?

Het volgende hoofdstuk, het empirische hart van deze studie, gaat in op de praktijk van online monitoring bij gemeenten. Er wordt ten eerste aandacht besteed aan de mate waarin en de wijze waarop gemeenten monitoren. Ten tweede worden de intenties en doelstellingen die daaraan gekoppeld zijn belicht en ten derde is er aandacht voor de knelpunten en dilemma's die gemeenten in de dagelijks praktijk ervaren.

3. De gemeentelijke praktijk van online monitoring

3.1 Inleiding

Uit hoofdstuk 2 blijkt dat de literatuur over online monitoring zich grotendeels richt op de politiepraktijk. Dit hoofdstuk richt zich daarom op de gemeentelijke praktijk van online monitoring. De gepresenteerde resultaten zijn gebaseerd op een online vragenlijst en interviews met gemeentelijke ambtenaren die werkzaam zijn bij de afdeling OOV of de afdeling Communicatie. Daarnaast wordt soms ter illustratie verwezen naar toelichtingen van respondenten op antwoorden die ze in de vragenlijst hebben gegeven (open velden).

In dit hoofdstuk worden twee onderzoeksvragen beantwoord: (1) In hoeverre en op welke wijze monitoren gemeenten online en met welke intenties en doelstellingen doen zij dat? en (2) Welke knelpunten en dilemma's ervaren gemeenten op dit moment bij het online monitoren? Logischerwijs volgt daaruit dat hoofdstuk 3 is opgedeeld in twee samenhangende delen. Waar in het eerste deel van het hoofdstuk een beschrijving van de gemeentelijke praktijk van online monitoring centraal staat, gaat het tweede deel over de reflectie van gemeenten (medewerkers) op hun eigen praktijk en werkwijze van online monitoring.

In het eerste deel van dit hoofdstuk wordt aandacht besteed aan de mate waarin online monitoring plaatsvindt binnen gemeenten en aan de afdelingen waar het plaatsvindt (paragraaf 3.2). Daarna staat vooral de werkwijze bij gemeentelijke online monitoring centraal (paragraaf 3.3). Naast aandacht voor de online signalen waar gemeenten zich op richten, is er ook aandacht voor de rol van techniek bij online monitoring, de verwerking van informatie, het gebruik van omgevingsanalyses en informatiedeling naar aanleiding van online monitoring. Het eerste deel van het hoofdstuk sluit af met een beschouwing over de gemeentelijke doelstellingen van online monitoring (paragraaf 3.4). Het is voor de bepaling van juridische grenzen en het juridische kader (hoofdstuk 4) van belang om inzicht te verkrijgen in wat gemeenten doen aan online monitoring en met welke doelstellingen ze dat doen.

In het tweede deel van dit hoofdstuk staat de reflectie van gemeenten op hun eigen werkwijze rondom online monitoring centraal. Daarbij is achtereenvolgens aandacht

voor de technische (paragraaf 3.5), organisatorische knelpunten (paragraaf 3.6), juridische grenzen (paragraaf 3.7) en ethische opvattingen over online monitoring (paragraaf 3.8). Het hoofdstuk eindigt met enkele afsluitende opmerkingen (paragraaf 3.9).

3.2 De mate van online monitoring

Voordat wordt ingegaan op concrete werkwijzen bij het online monitoren, zal eerst de omvang van de gemeentelijke monitoring in kaart gebracht worden. Uit de vragenlijst blijkt dat 95% (*N*=260) van de gemeentelijke respondenten aangeeft dat zij of hun collega's online openbare bronnen op internet monitoren. Dertien respondenten (5%) geven aan geen gebruik te maken van online monitoring binnen hun eigen gemeente.[122] In de toelichting op hun antwoorden noemen deze respondenten tijdsgebrek, capaciteitsgebrek, kennistekort of een gebrek aan noodzaak als redenen om niet online te monitoren. De op de vragenlijst gebaseerde resultaten die hierna volgen, zijn gebaseerd op de gemeenten die wél aan online monitoring doen. Het aantal respondenten dat genoemd wordt in de resultaten zal lager zijn dan 260 omdat een deel van de respondenten de vragenlijst niet volledig heeft ingevuld (zie hoofdstuk 1). Het aantal (onderliggende) respondenten per vraag varieert tussen 140 en 196. Geënquêteerden worden in het vervolg van dit hoofdstuk respondenten genoemd. Waar mogelijk worden interviewcitaten gebruikt die aanvullend of illustratief zijn voor de resultaten uit de vragenlijst.

Uit het literatuuronderzoek blijkt dat er binnen gemeenten verschillende afdelingen zich bezighouden met online monitoring, maar een landelijk en cijfermatig overzicht is niet voorhanden. In eerste instantie is gekozen voor een breder perspectief dan alleen dat van de openbare orde en veiligheid. Naar aanleiding van de literatuur en enkele verkennende interviews met gemeenten zijn verschillende afdelingen waar online monitoring plaatsvindt opgenomen in de vragenlijst. Het betreft de afdelingen: Communicatie, Webcare, Newsroom, OOV en Onderzoek. Uit de vragenlijst[123] blijkt dat online monitoring het meeste voorkomt bij de afdeling Communicatie (89%). Deze afdeling gebruikt online monitoring in 49 procent van de gevallen voor de dienstverlening in de vorm van een Klant Contact Centrum[124] of Webcare.

Webcare is gericht op online dienstverlening. Er wordt gereageerd op klachten en vragen van inwoners worden beantwoord. Webcare kan uitgevoerd worden door gebruik te maken van een monitoringstool. In de tool komen berichten binnen die gestuurd zijn via WhatsApp, de telefoon, e-mail en sociale media zoals Twitter en Facebook. Vragen kunnen gericht worden aan de gemeente door hen te taggen (@gemeente x). Op deze manier kan iedereen met een socialemedia-account een vraag stellen aan de

122 Deze niet online monitorende respondenten geven aan niet structureel te monitoren, maar raadplegen wel publiek toegankelijke bronnen op incidentele basis als daar een aanleiding voor is (*N* = 4).
123 Totale *N* bij deze vraag is 196.
124 In het vervolg is dit afgekort als KCC.

gemeente. Het is dus niet nodig om een online connectie te hebben met de gemeente, zoals het lid zijn van hun Facebookgroep, de gemeente te volgen op Twitter of een connectie te hebben op LinkedIn. Bij één van de geïnterviewde gemeentelijke medewerkers vertegenwoordigt het KCC verschillende afdelingen, namelijk burgerzaken, vergunningen, openbare ruimte en afval (G2). Inwoners kunnen met hun vragen terecht bij deze afdelingen.

Na de afdeling Communicatie werd de afdeling OOV het vaakst genoemd in relatie tot online monitoring. Volgens zestig procent van de respondenten maakt de gemeentelijke afdeling OOV gebruik van online monitoring. Daarnaast geeft veertien procent van de respondenten aan een Newsroom in hun gemeente te hebben. In interviews wordt beschreven dat de Newsroom signaleert wat er buiten speelt en hierop reageert. Overeenkomstig de literatuur, wordt in een interview beschreven dat ze in een Newsroom werken van 'buiten naar binnen' en van 'binnen naar buiten' (G2). Online monitoring vindt dus plaats op verschillende plekken in de gemeentelijke organisatie, maar het perspectief van online monitoring ten behoeve van de openbare orde en veiligheid zal centraal staan in dit hoofdstuk.

Monitoring volgens medewerkers van de afdeling OOV en Communicatie
Er zijn verschillen in hoe medewerkers van de afdeling OOV en Communicatie aankijken tegen de organisatie van monitoring in hun gemeente. Volgens medewerkers Communicatie vindt monitoring vaker plaats binnen de afdeling Communicatie (98%) dan volgens medewerkers van de afdeling OOV (79%). De laatste groep geeft overigens ook vaker aan het niet te weten (19% versus 0%). Datzelfde geldt voor Webcare. Medewerkers van de afdeling Communicatie geven vaker dan medewerkers van de afdeling OOV aan dat monitoring plaatsvindt bij de afdeling Webcare (64% versus 29%). Ook hier geldt dat medewerkers van de afdeling OOV het vaker niet weten (46% versus 3%).

Tot slot geldt (omgekeerd) dat medewerkers van de afdeling OOV vaker aangeven (80%) dat monitoring binnen hun afdeling plaatsvindt dan medewerkers van de afdeling Communicatie (32%). Medewerkers van de afdeling Communicatie geven juist vaker aan het niet te weten (35% versus 1%). Deze verschillen laten zien dat 'de gemeente' niet bestaat en dat verschillende medewerkers allicht niet altijd goed zicht hebben over wat er op het gebied van monitoring bij andere afdelingen wordt gedaan.

3.3 De werkwijze van online monitoring ten behoeve van de openbare orde en veiligheid

3.3.1 *Monitoren van online signalen*

Naar welke online signalen van mogelijke openbare-ordeverstoringen kijken gemeenten? Op basis van literatuuronderzoek en verkennende interviews is een lijst van der-

tien mogelijke openbare-ordeverstoringen tot stand gekomen die gemeenten willen voorkomen met online monitoring. Die voorbeelden zijn vervolgens in de vragenlijst aan een grotere groep gemeentelijke medewerkers voorgelegd. De mogelijke verstoringen zijn gecategoriseerd in 'polarisatie' (tussen inwoners, op thema), 'overlast' (door groepen, door individuen die al vaker ophef hebben veroorzaakt), 'oproepen' (tot demonstraties, tot illegale evenementen, tot hooliganisme), 'onrust' (rond politieke besluiten, rond asielzoekerscentra, rond teruggekeerde zedendelinquenten), 'bedreiging van gezagsdragers' en het 'verspreiden van nepnieuws'.

Om een beeld te schetsen van de frequentie waarin online signalen van eerdergenoemde categorieën voorkomen, is respondenten gevraagd hoe vaak zij online berichten over mogelijke verstoringen hebben gesignaleerd. Bijna alle respondenten geven aan dat hun gemeente gebruikmaakt van online signalen over mogelijke ordeverstoringen (86%). Het grootste deel daarvan geeft aan dergelijke signalen één keer in het jaar of zelfs minder waar te nemen in hun gemeente (73%) en enkelen maandelijks (9%) of wekelijks (4%). Een klein deel van de respondenten weet het niet (9%) of geeft aan nog nooit een online signaal van een mogelijke ordeverstoring te hebben waargenomen (4%). Er is een onderscheid gemaakt tussen de meest voorkomende en de minst voorkomende categorieën van online signalen over mogelijke ordeverstoringen.[125]

Meest online gemonitorde categorieën van ordeverstoringen
De meest gemonitorde berichten betreffen 'onrust rondom politieke besluiten', 'overlast' (door groepen en individuen), 'oproepen' (tot demonstraties en illegale evenementen), 'polarisatie op thema en tussen inwoners' (zie figuur 1). De percentages variëren van 91 procent (onrust rond politieke besluiten) tot 80 procent (polarisatie tussen inwoners).

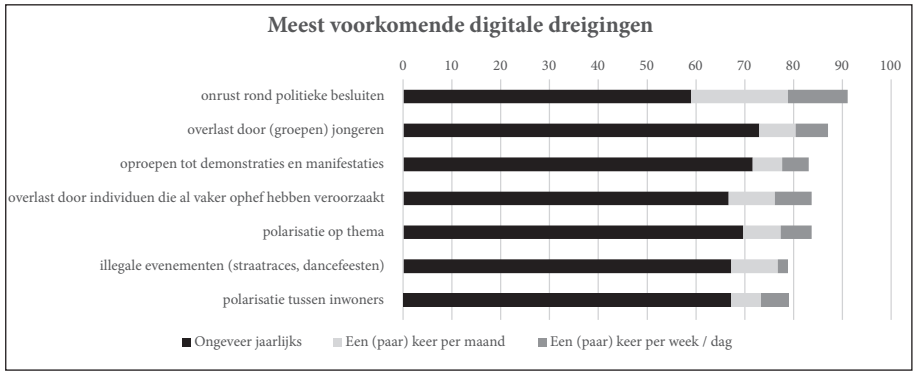
De categorie 'onrust rond politieke besluiten' komt, zoals gezegd, naar voren als het thema dat online het meest gemonitord wordt door gemeenten. Uit interviews komt naar voren dat de communicatieafdeling berichtgeving rondom een politiek besluit in de gaten houdt om te zien 'hoe deze landt' (G2, G4).[126] Eén gemeente had bijvoorbeeld een sluitingsbevel van coffeeshops opgeheven en via Webcare geconstateerd dat daarop kalm is gereageerd door inwoners (G4). Een andere gemeente monitorde op overlast van bouwprojecten of wegwerkzaamheden (G1). Mogelijke onrust rondom politieke besluiten wordt dus regelmatig online waargenomen door gemeenten.

Een tweede categorie die relatief veel online wordt waargenomen, is 'overlast door (groepen) jongeren' (87%). In een van de interviews wordt gesproken over een groep jongeren die overlast veroorzaken in een winkelcentrum (G5). Het betrof een groep die door het winkelcentrum aan het fietsen was op hun achterwiel (ook wel 'wheelies

125 Deze resultaten zijn gebaseerd op *N*=162.
126 Vrijheid van meningsuiting en proportionaliteit kunnen daar een rol spelen (juridische grenzen).

maken' genoemd) en daardoor een mogelijk gevaar voor de openbare orde zouden kunnen vormen. Gemeentemedewerkers uit het veiligheidsteam hebben vervolgens samen met communicatiemedewerkers deze groep jongeren in kaart gebracht door hun berichten op sociale media te volgen. De gemeentelijke afdeling Communicatie nam vervolgens contact op met team buurttoezicht om de informatie te verifiëren. Daarna heeft de burgemeester een informatieve brief geschreven aan de ouders en de jongeren waarin verzocht werd het ongewenste gedrag te beëindigen.

Figuur 1. De meest gemonitorde categorieën van ordeverstoringen (in %, *N* varieert van 113-156)



De derde categorie die het vaakste voorkomt, betreft 'oproepen tot demonstraties en manifestaties', zoals de demonstratie van de blokkeerfriezen op de A7 (83%), maar ook 'overlast door groepen jongeren' (87%).

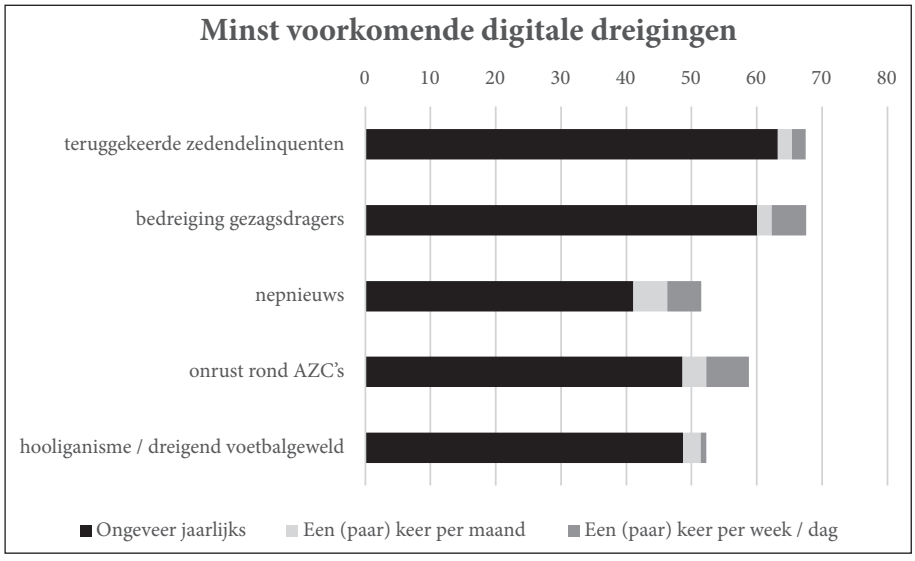
Minst online gemonitorde categorieën van ordeverstoringen
De minst gemonitorde online berichten hebben betrekking op 'teruggekeerde zedendelinquenten' in de gemeente, 'bedreigingen richting gezagsdragers', 'nepnieuws', 'onrust rond asielzoekerscentra' en 'hooliganisme' (zie figuur 2). De genoemde percentages variëren tussen 68 (terugkeer zedendelinquenten en bedreigingen van gezagsdragers) en 52 (hooliganisme of dreigend voetbalgerelateerd geweld en nepnieuws).

'Onrust door de komst van asielzoekerscentra' is door 59 procent van de respondenten online waargenomen binnen de gemeente. Een geïnterviewde vertelt dat een aantal jaren geleden onrust op sociale media werd geconstateerd rondom de komst van een asielzoekerscentrum. Dit leidde er onder andere toe dat er een grote demonstratie werd georganiseerd ten tijde van een gemeenteraadsvergadering. *"Als je je uitsluitend zou richten op de sociale media zou je denken, dit gaat niet goed"*, aldus de burgemeester (G5). De burgemeester koos ervoor om tijdens de demonstratie met de groep in ge-

sprek te gaan. Dit bleek te werken. Als gevolg hiervan werden er vooral positieve berichten over de gemeente geplaatst op sociale media.

Zoals eerder genoemd, wordt door 52 procent van de respondenten aangegeven dat binnen hun gemeente online berichten worden gevolgd binnen de categorie 'hooliganisme of dreigend voetbalgeweld', zoals discriminatie en online oproepen tot geweld. Eén geïnterviewde geeft aan dat hun gemeente bij naderende risicowedstrijden online monitort (G1). In het verleden hebben bepaalde mensen zich zo negatief uitgelaten aangaande een risicowedstrijd dat ze op de grens van strafbare discriminatie zaten. Anderen hebben vechtpartijen aangekondigd tijdens de wedstrijd.

Figuur 2. De minst gemonitorde categorieën van ordeverstoringen (in %, *N* varieert van 113-138)



Samenvattend hebben de meeste respondenten binnen hun gemeente online signalen waargenomen die wijzen op mogelijke ordeverstoringen, maar die berichten of signalen worden overwegend hooguit één keer per jaar waargenomen. Dat geldt voor de genoemde categorieën van zowel figuur 1 als figuur 2.

Gemonitorde ordeverstoringen volgens medewerkers van de afdeling OOV en Communicatie
Er zijn enkele verschillen tussen de medewerkers van de afdeling OOV en Communicatie als het gaat om het 'signaleren van hooliganisme', ' terugkeer zedendelinquenten', 'onrust rondom politieke besluiten' en 'illegale feesten en evenementen'. Hooliganisme wordt door medewerkers OOV in 60 procent van de gevallen ongeveer jaarlijks waar-

genomen, door medewerkers Communicatie is dat 36 procent.[127] Voor het signaleren van onrust rond zedendelinquenten is een soortgelijk resultaat te zien. Medewerkers OOV geven vaker aan onrust rond zedendelinquenten ongeveer jaarlijks te zien (73%) dan medewerkers Communicatie (50%).[128] Online signalen van onrust rondom politieke besluiten wordt vaker maandelijks (29%) en wekelijks (15%) waargenomen bij de afdeling Communicatie, dan het maandelijks (11%) en wekelijks (8%) bij de afdeling Communicatie wordt waargenomen.[129] Tot slot worden door medewerkers van de afdeling OOV vaker maandelijks online signalen van illegale feesten waargenomen (17%), dan medewerkers van de afdeling Communicatie (3%).[130]

3.3.2 *Het gebruik van technologie bij monitoren*

Uit de literatuur blijkt dat gemeenten voor het online monitoren gebruikmaken van technische hulpmiddelen, zoals een monitoringstool en/of handmatig online te zoeken in openbare bronnen (zie hoofdstuk 2). Uit de vragenlijst blijkt dat in de praktijk 75 procent van de respondenten een monitoringstool gebruikt. Het grootste deel van de respondenten gebruikt de monitoringstool OBI4wan (52%) of Coosto (13%) en deel geeft aan gebruik te maken van andere tools (10%). Alternatieve zoekmachines[131] die gebruikt worden zijn TweetDeck[132], Copernic, Meltwater en Hootsuite. De overige respondenten wisten niet of er een monitoringstool wordt gebruikt (22%) of gebruikten geen tool (3%).[133] Maar er wordt ook handmatig naar informatie gezocht online. Een groot deel van de respondenten geeft aan (ook) handmatig, zonder monitoringstool, te zoeken in online informatie (39%). In de toelichting van de vragenlijst worden veelgebruikte websites voor deze handmatige zoekslag genoemd: Google, Google Alerts, sociale media (Facebook en Twitter), de Kamer van Koophandel, online media en (regionale) kranten. Ook wordt duidelijk dat respondenten bijvoorbeeld handmatig monitoren binnen besloten Facebookgroepen waar ze lid van zijn.

Medewerkers van de afdelingen OOV en Communicatie hebben wel een andere perceptie van het gebruik van monitoringstools binnen hun gemeente. Vrijwel alle medewerkers van Communicatie (99%) geven aan dat hun gemeente monitoringstools gebruikt, tegenover 51 procent van de medewerkers OOV.[134, 135]

---

127 Percentages van OOV (*N*=58) en Communicatie (*N*=55).
128 Percentages van OOV (*N*=73) en Communicatie (*N*=64).
129 Percentages van OOV (*N*=74) en Communicatie (*N*=80).
130 Percentages van OOV (*N*=72) en Communicatie (*N*=72).
131 Deze zoeken in hun eigen index en tonen het online resultaat, de monitoringstools blijven daarentegen binnen hun eigen kopie van het internet.
132 Tweetdeck monitort alleen berichten op Twitter, aldus een geïnterviewde (G7).
133 Enkele respondenten geven bij de toelichting aan handmatig in openbare bronnen op internet te zoeken, zoals nieuwssites en Drimble.
134 Alle benoemde verschillen zijn statistisch significant ($p<.01$).
135 Het betreft een vergelijking tussen 104 medewerkers Communicatie en 90 medewerkers OOV.

3.3.3 *De verwerking van informatie*

Gemeenten kunnen online berichten in de gaten houden en ervoor kiezen om deze op te slaan of niet. Dit is relevant in verband met de eisen die de AVG stelt aan gegevensverwerking en het opslaan van persoonsgegevens. Monitoringtools bieden de mogelijkheid om dossiers aan te maken op specifieke zoektermen.[136] Deze automatisering is eveneens relevant voor het juridisch kader en daarom is aan respondenten gevraagd of zij online berichten opslaan en zo ja, of dit proces geautomatiseerd verloopt.

Iets minder dan de helft van de respondenten gaf aan dat online berichten niet worden opgeslagen en er geen dossier wordt opgebouwd naar aanleiding van de online monitoring (48%, zie tabel 2).[137] Bij online monitoring kan gedacht worden aan het in de gaten houden van de verkiezingen (thema), demonstratie van Kick Out Zwarte Piet (groep volgen) of een reeds bekende voetbalhooligan (individu volgen). Eén geïnterviewde gaf aan dat de accounts van de gemeente een paar keer per dag in de gaten worden gehouden (G7). Tevens voegt deze geïnterviewde toe dat er geen verslag van de resultaten van die handelingen wordt gemaakt en dat over het algemeen, die informatie niet wordt verspreid.

Tabel 2. Frequentie van dossiervorming (in %; *N*=162)

	Regelmatig + jaarlijks	Regelmatig*	Jaarlijks	Nooit	Weet niet
In de gaten houden en niet opslaan	48	18	30	9	17
Automatische dossiervorming	14	5	9	46	21
Handmatige dossiervorming	33	8	25	27	19

**NB: regelmatig is maandelijks, wekelijks en dagelijks samengenomen*[138]

Van de respondenten geeft 14 procent aan gebruik te maken van *automatische dossiervorming* om informatie over een thema, groep of individu samen te voegen (zie tabel 2). Door zoektermen te includeren in de standaard zoekopdracht van de monitoringstool wordt automatisch informatie opgezocht en opgeslagen.

De andere variant is het handmatig in de gaten houden van bronnen en opslaan van online informatie. Eerder in dit hoofdstuk is vastgesteld dat respondenten handmatig zoeken door gebruik te maken van websites (zoals Google of sociale media) in plaats van de monitoringstool. Ongeveer een derde van de respondenten slaat de bronnen van deze handmatig zoektocht ook op (33%, zie tabel 2), ook wel omgevingsanalyse

136 In principe is alles al opgeslagen/overgenomen binnen de tool, maar gemeenten kunnen daarbinnen wel gerichte zoektermen aandragen.
137 Voor deze drie items zijn er geen verschillen tussen Communicatie en OOV gevonden.
138 Er is een restpercentage van de categorie 'minder vaak dan jaarlijks' die niet is opgenomen in de tabel.

genoemd. [139] Respondenten maken een dergelijk dossier relatief gezien niet vaak (25% jaarlijks). Eén geïnterviewde vertelt alleen te zoeken op specifieke termen naar aanleiding van aanvragen van crisiscommunicatie of de veiligheidsadviseur, over bijvoorbeeld evenementen (G3).

Deze frequentie van dossiervorming komt overeen met de bevinding uit de literatuur dat gemeenten regelmatig een actualiteitenoverzicht maken. Ook de geïnterviewde gemeentelijke medewerkers geven aan dagelijks een overzicht te maken van de sentimenten die spelen in de gemeente (G1 t/m G7).[140]

3.3.4 *Omgevingsanalyse bij een concrete dreiging*

Uit de verkennende interviews blijkt dat gemeenten een omgevingsanalyse maken om meer te weten te komen over specifiek thema, groep of individu. Deze omgevingsanalyse is ontwikkeld binnen de communicatieafdeling om in het geval van een crisis te voorzien in de crisiscommunicatie (zie hoofdstuk 2). Tegenwoordig wordt het door meer gemeenten gebruikt om een actualiteitenoverzicht te maken (de zogenaamde tamtam). De vragenlijst is ingezet om vast te stellen of gemeenten ook gebruikmaken van een online omgevingsanalyse bij een concrete dreiging van openbare-ordeverstoringen.

Bijna alle respondenten geven aan dat hun gemeente inderdaad een omgevingsanalyse maakt bij een concrete dreiging van de openbare orde en veiligheid (84%, zie tabel 3). Bijna de helft van de respondenten geeft aan soms een omgevingsanalyse te maken (41%) en een kwart van de respondenten geeft aan altijd (25%) of vaak (18%) een omgevingsanalyse te maken. *"Kennis is macht dus hoe beter je lokaal weet wat er speelt en wie de spelers zijn, hoe beter je kunt anticiperen en reageren […] online monitoring is daar een vanzelfsprekend onderdeel van in deze moderne tijd",* aldus een respondent in de toelichting.

Tabel 3. Maken van een omgevingsanalyse na concrete dreiging (in %, *N*=158)

Bij een concrete dreiging van de openbare orde wordt …	Ja*	Altijd	Vaak	Soms	Nooit	Weet niet
een omgevingsanalyse gemaakt	84	25	18	41	8	8

**Antwoorden altijd, vaak en soms samengenomen*

139 Uit meerdere interviews komt naar voren dat omgevingsanalisten dagelijks worden ingezet om een tamtam / knipselkrant te maken van sentimenten in de gemeente (G1, G2, G3, G4). Als omgevingsanalist wordt een standaard query gebruikt die wordt aangevuld met extra zoektermen (specifieke query) die op dat moment relevant zijn voor de tamtam (bijv. boerenprotest) (G2). Opiniemakers (zoals politie en invloedrijke inwoners van de gemeente) en een bevolkingsbeeld worden in de tamtam meegenomen (G4).

140 Er zijn geen verschillen tussen medewerkers OOV en Communicatie als het gaat om dossiervorming.

Uit toelichting op de antwoorden uit de vragenlijst blijkt dat een omgevingsanalyse vooral wordt gebruikt op thema's, zoals het in kaart brengen van reacties op gevoelige politieke besluiten. Ook worden omgevingsanalyses gemaakt over bijvoorbeeld een sinterklaasintocht, toename van inbraken of het veiligheidsgevoel binnen de gemeente.

Wie de opdracht tot een omgevingsanalyse of specifieke zoektermen geeft, verschilt per gemeente. Dit is juridisch van belang voor de proportionaliteit van de handeling die in verhouding moet staan tot het publieke belang dat met de handeling wordt gediend. Op basis van de interviews lijkt de afdeling OOV veelal een omgevingsanalyse op te vragen bij de afdeling Communicatie (G1, G2, G3). Eén gemeente geeft aan dat de zoektermen door medewerkers van de afdeling Communicatie en OOV samen bepaald worden (G2). Een andere geïnterviewde geeft aan dat zoektermen worden bepaald door de veiligheidsadviseurs of de politie (G1). De betreffende gemeente blijkt onder andere honderd woorden voor geweld of daaraan gerelateerde zoektermen te gebruiken in hun zoektermen. Voorbeelden zijn: 'messen', 'pijn', 'bloed', 'gemeen' of 'bel de politie'.

Er wordt hierna in dit hoofdstuk extra aandacht besteed aan het online monitoren van groepen en personen en het gebruik van privé- en nepaccounts, omdat in deze acties potentieel een schending van de privacywetgeving schuilt. Daarom wordt beschreven wat in de interviews naar voren is gekomen over het online monitoren van groepen en personen en wordt ingegaan op het gebruik van prive- en nepaccounts door gemeenten.

Gemeentelijk monitoren van groepen en personen

Door sommige gemeenten worden groepen of individuen gemonitord met een omgevingsanalyse. Een respondent licht in de vragenlijst toe: "*Incidenteel checken we het internet bij geprioriteerde personen en/of groepen.*" In de meeste interviews wordt aangegeven dat bij de gemeentelijke monitoring in de regel niet op namen wordt gezocht, maar er worden wel enkele uitzonderingen gemaakt (G2, G3, G4). Er wordt in de regel niet op personen gezocht, tenzij het mensen zijn met een publieke functie (G2), zoals opiniemakers en invloedrijke personen uit de gemeente (G4) of als personen duidelijk naar voren komen in de standaardanalyse en op die manier bij de analyse horen (G3)[141]. Een uitzondering is bijvoorbeeld een omgevingsanalyse over specifieke liquidaties gekoppeld aan een rechtszaak. In deze analyse werd een dagelijks rapport opgeleverd van de locaties van verstuurde berichten over de liquidaties (een 'heat map') (G2, G8).[142] *"Natuurlijk ben je af en toe geïnteresseerd in iemand die iets initieert, dus dat houd je in de gaten."* (G1). Eén gemeente geeft aan soms wel specifiek op naam te zoeken: *"ja, op sociale media zeker. Het is allemaal openbaar, wat ze er zelf op plaatsen*" (G5). Eén geïnterviewde geeft aan niet te monitoren op specifieke personen (G7).

141 Zie voetnoot 140.

142 Er zijn twee respondenten die aangeven gebruik te maken van open source intelligence van Fox-IT en gebruik maken van de webcrawler die Web-IQ aanbiedt

Inzet privé- en nepaccounts

Uit de literatuur blijkt dat de politie gebruikmaakt van nepaccounts binnen sociale media. Met nepaccounts is het mogelijk om meer en andere online bronnen in te zien. Dit kunnen openbare bronnen zijn die niet in de monitoringstool worden aangeboden maar wel voor eenieder dezelfde informatie opleveren en publiek toegankelijk zijn (Facebook, Instagram), of bronnen die niet openbaar zijn, zoals een besloten Facebookgroep of afgeschermde accounts. Privé- en nepaccounts verschaffen toegang tot deze, anders onbereikbare, informatie. Het gebruik van deze accounts en monitoring van afgeschermde bronnen hebben een grotere kans om in privacyschendingen te resulteren. Uit de verkennende interviews zijn aanwijzingen naar voren gekomen die erop wijzen dat ook gemeentelijke medewerkers dergelijke accounts gebruiken voor online monitoring. Om het gemeentelijke gebruik van privé- en nepaccounts in de volle breedte van gemeenten in kaart te brengen, zijn vragen hierover opgenomen in de vragenlijst.

Bijna de helft van de respondenten geeft aan dat zij of hun collega's voor de online monitoring nooit gebruikmaakt van privéaccounts (40%) en twee derde (67%) geeft aan nooit gebruik te maken van nepaccounts. Met deze accounts ontstaat er toegang tot informatie over concrete online dreigingen voor de openbare orde en veiligheid die soms niet bereikt wordt met monitoringstools (zie tabel 4). Sommige gemeenten lijken er bewust voor te kiezen om geen gebruik te maken van deze accounts. Een van de respondenten geeft aan "*absoluut geen nepaccounts of privéaccounts van medewerkers te gebruiken om facebookprofielen te bekijken. Dit in verband met risico's.*" Een andere respondent geeft aan geen nepaccounts te gebruiken vanwege de ethische aspecten, *"omdat we dat tegenstrijdig vinden met de open en eerlijke overheidsinstantie die we willen zijn."* Dezelfde respondent geeft aan dat binnen zijn gemeente wel privéaccounts van medewerkers gebruikt worden bij online monitoring.

Tabel 4. Gebruik van privéaccounts/nepaccounts na signalering van concrete dreigingen (in %, *N*=158)

Bij een concrete dreiging van de openbare orde…	Ja*	Altijd	Vaak	Soms	Nooit	Weet niet
gebruik privéaccounts van medewerkers	38	1	5	32	40	22
gebruik nepaccounts	13	1	1	11	67	20

**Antwoorden altijd, vaak en soms zijn samengenomen.*

Ruim één derde van de respondenten blijkt wel eens een privéaccount (sociale media) van medewerkers te gebruiken om een beter online beeld te krijgen van een concrete dreiging (38%), en een veel kleiner deel (6%) blijkt dat altijd tot vaak te doen (zie tabel 4). *"Je haalt sowieso alles binnen wat openbaar is, maar als ik mijn account toevoeg, dan zoekt hij [red. de monitoringstool] ook in mijn bronnen*" (G1). Door gebruik te maken van privéaccounts kunnen dus meer bronnen bekeken worden. Deze privéaccounts worden

veelal alleen gebruikt om te monitoren en niet om boodschappen te verspreiden of vragen te stellen. *"Soms heb je een merkwaardige kennisgeving, en dan denk je, ik googel de naam. […] Dan kan ik bevestigen dat ik ergens geen goed gevoel over heb"* (G2). Gemeenten *"gebruiken de monitoring accounts (of WhatsAppberichten) van collega's die bij Communicatie werken."* Ook bij de afdeling OOV worden via privéaccounts op sociale media bronnen geraadpleegd om een *"sneller en beter beeld te krijgen van de situatie"*.

Het gebruik van privéaccounts hoeft niet bewust ingezet te worden om te monitoren (bewust met eigen account iemand opzoeken). Medewerkers kunnen op hun privé- of persoonlijke socialemedia-accounts informatie voorbij zien komen die ze van belang achten voor de openbare orde en veiligheid, terwijl ze niet actief zoeken naar deze informatie. Eén geïnterviewde vertelt dat ze weleens op de Facebookpagina van haar wijk 'iets' tegenkomt en dit tijdens haar werk opzoekt (G2).

Slechts enkele respondenten geven in de vragenlijst aan dat de gemeente nepaccounts gebruikt om op sociale media een beter beeld te krijgen van over een concrete dreiging (13%; 12% soms en 1% vaak, zie tabel 4). "*Dat mag eigenlijk helemaal niet, maar we hebben wel fakeaccounts met een naam die niet bestaat, maar onder wie we opereren*" (G1). Een korte toelichting op het gebruik van nepaccounts wordt gegeven in box 1.

Box 1. Toelichting uit een interview over monitoring in besloten facebookgroepen

"Wij halen niet op van groepen […] als we dat al willen weten dan kijken we gewoon op Facebook zelf bijvoorbeeld" (G3). Het handmatig opzoeken van Facebookgroepen kan wel. "Ik kan me herinneren bijvoorbeeld bij de vluchtelingencrisis dan word je gewoon zelf als persoon met een soort fakeaccount, lid van zo'n groep om te kijken wat daar speelt. Maar met de tool kan het niet" (G3).

3.3.5 *Informatiedeling bij concrete dreigingen*

Er is in kaart gebracht hoe gemeenten monitoren, signaleren en analyseren. De laatste stap is het delen van informatie binnen en buiten de gemeente. Deze stap wordt ook onderscheiden met een schuin oog naar het juridische kader (zie hoofdstuk 4). Met name persoonlijke informatie is onder strikt toezicht toegestaan en het delen van (persoonlijke) informatie kan dus een vorm van privacyschending zijn. Daarom wordt in deze paragraaf beschreven hoe gemeenten informatie delen binnen en buiten de gemeente.

Informatievergaring bij politie
Gemeenten hebben samen met de politie de taak om de openbare orde en veiligheid te handhaven (zie hoofdstuk 1). De politie heeft mogelijk andere informatie en kennis en door de politie te vragen kan de gemeente mogelijk aan nieuwe informatie komen. De

politie is dan ook logischerwijs de 'go to'-partner om samen informatie over openbare-ordedreigingen te duiden en dat wordt bevestigd in de vragenlijst.

De meeste respondenten hebben ooit online informatie bij de politie opgevraagd over een concrete dreiging van de openbare orde (61%, zie tabel 5). Het grootste deel (37%) geeft aan 'soms' informatie over een dreiging en een minderheid geeft aan 'vaak' (13%) of 'altijd' (11%) informatie bij de politie op te vragen.

Tabel 5. Handelingen na signalering van concrete dreiging (in %, *N*=158)

Bij een concrete dreiging van de openbare orde…	Ja*	Altijd	Vaak	Soms	Nooit	Weet niet
wordt online informatie over de dreiging opgevraagd bij de politie	61	11	13	37	17	22

**Antwoorden altijd, vaak en soms samengenomen*

Uit de toelichting in de vragenlijst blijkt dat gemeentelijke medewerkers contact zoeken met de politie om aanvullende informatie te verzamelen, informatie te controleren, een dreiging te monitoren of een omgevingsanalyse te maken. Bij het interpreteren van deze resultaten moet rekening gehouden worden met het feit dat een concrete dreiging niet vaak voorkomt. Drie respondenten geven aan nog geen concrete dreiging te hebben meegemaakt en daarom onbekend zijn met de mogelijkheden om bronnen te benutten om informatie te verzamelen.

In interviews wordt aangegeven dat de politie wordt ingeschakeld zodra informatie op persoonsniveau nodig is of als er sprake is van een strafrechtelijke overtreding (G2, G3). Online informatie opzoeken op persoonsniveau vinden deze geïnterviewden geen taak voor de gemeente, maar voor de politie. Als voorbeeld wordt genoemd *"een jongen van veertien met een laag IQ die dreigde om de hele boel kort en klein te slaan en iedereen dood te maken met zijn kalasjnikov. De politie gaat dan na wie het is en de informatie te duiden. Deze zaak was voor de politie."* (G2).

Geïnterviewden van de gemeenten geven tevens aan dat de politie *"vanwege hun opsporingsbevoegdheid […] meer data verzamelen"* (G2). De politie ontkracht deze stelling in hun interview. De afdeling OOV en de politie hebben in hun ogen niet veel vrijheid om online te monitoren. Als zij informatie in het kader van de openbare orde en veiligheid willen ophalen van internet, dan is er snel sprake van stelselmatige monitoring en is toestemming van de officier van justitie nodig (G10). Voor meer informatie over monitoring bij de politie, zie box 2.

Box 2. Online monitoring bij politie ten behoeve van de openbare orde en veiligheid

De landelijke projectleiders sociale media geven in het interview aan dat de Nationale Politie binnen meerdere afdelingen op verschillende wijzen gebruikmaakt van de monitoringstool (G10). De afdeling Communicatie monitort op sentimenten zoals politiek gevoelige vragen en het imago van de politie. Samen met de afdeling Webcare houden ze ook de socialemediakanalen van de politie in de gaten. De projectleiders geven tevens aan dat de politie nog enkele andere query's draait, maar expliciet geen open zoekvragen uitvoert in afspraak met het reputatiemanagementbedrijf.

Informatiedeling door de gemeente

In de vragenlijst is respondenten voorgelegd of ze online informatie over gesignaleerde online dreigingen van de openbare orde en veiligheid doorsturen binnen de gemeente, politie en/of naar andere partijen.

Tabel 6. Frequentie van doorsturen van gesignaleerde dreigingen (in %, *N*=162)

	Ja*	Regelmatig**	Jaarlijks	Nooit	Weet niet
Doorgestuurd binnen de gemeente	56	15	41	8	9
Doorgestuurd naar de politie	40	8	32	17	17
Doorgestuurd naar andere partijen	26	4	22	30	23

**Bij dit antwoord zijn regelmatig en jaarlijks samengenomen.*
***Bij dit antwoord zijn maandelijks, wekelijks en dagelijks samengenomen.*[143]

De meeste respondenten geven aan informatie over gesignaleerde mogelijke online dreigingen door te sturen binnen de gemeente (56%) en een kleiner deel naar de politie (40%) en een nog kleiner deel doet dat ook richting andere partijen, zoals de veiligheidsregio (26%, zie tabel 6). De frequentie waarin informatie over online dreigingen wordt doorgestuurd, is in de regel hooguit één keer per jaar.

Informatiedeling volgens medewerkers van de afdeling OOV en Communicatie

Uit de vergelijking tussen medewerkers van de afdeling Communicatie en OOV blijkt dat medewerkers OOV vaker regelmatig informatie doorsturen naar de politie (15%) dan medewerkers van de afdeling Communicatie (1%). Dat geldt ook voor het doorsturen op jaarlijkse basis (45% versus 19%). Het 'nooit' doorsturen van informatie aan de politie komt vaker voor bij medewerkers van de afdeling Communicatie (24% versus 10%). Het doorsturen van informatie naar andere partijen komt eveneens vaker

143 Er is een restpercentage van de categorie 'minder vaak dan jaarlijks' die niet is opgenomen in de tabel.

jaarlijks voor bij medewerkers van de afdeling OOV (29% versus 15%) en juist vaker nooit bij medewerkers van de afdeling Communicatie (38% versus 21%).[144]

3.4 Doelen van gemeentelijk monitoren

3.4.1 *Communicatiedoelen van online monitoring*

Aan het begin van dit hoofdstuk kwam naar voren dat de monitoring overwegend plaatsvindt binnen de gemeentelijke afdelingen Communicatie en OOV. Op basis van de literatuur is de verwachting dat globaal twee doelen onderscheiden kunnen worden voor online monitoring: communicatie en handhaving van de openbare orde en veiligheid. Uit de verkennende interviews is gebleken dat de praktijk weerbarstiger is en dat het ideaaltypische onderscheid in doelen niet correspondeert met de praktijk. Zo levert informatie die naar voren komt bij de communicatieafdeling, bij werkzaamheden rondom de dienstverlening, soms informatie op die van belang is voor het doel van openbare orde en veiligheid en handhaving. In de verkennende interviews (voorafgaand) komt het geregeld voor dat informatie die met een specifiek doel is verzameld ook bruikbaar blijkt te zijn voor een ander doel. De doelstellingen zijn dus met elkaar verweven.

Op basis van deze inzichten is in de vragenlijst bij alle specifieke doelstellingen een onderscheid gemaakt tussen hoofd- en nevendoelen. De meeste gemeenten monitoren met het oog op communicatiedoeleinden. Dit brede doel is opgedeeld in drie specifieke doelstellingen die hierna worden besproken (zie tabel 7).

Tabel 7. Doelstellingen voor online monitoring gericht op communicatie (in %, *N*=196)

	Hoofddoel	Nevendoel	Geen doel	Weet niet	Totaal %/n
Weten wat er speelt in de gemeente	79	15	1	5	100/196
Dienstverlening verbeteren voor inwoners	59	21	10	10	100/196
In de gaten houden hoe de gemeente wordt gewaardeerd	33	41	14	11	100/196

'Weten wat er speelt in de gemeenten' is een van de meest genoemde doelstellingen van online monitoring gericht op communicatie (79% als hoofddoel; 15% als nevendoel, zie tabel 7). In de interviews wordt gesproken over het 'buiten naar binnen halen' (G4, G2). In deze analogie raadplegen gemeenten (binnen) online bronnen om actualiteiten in kaart te brengen en te kijken hoe inwoners daarop reageren (buiten) (G4). Er wordt door meerdere geïnterviewden een vergelijking gemaakt met een 'thermometer' of 'temperaturen' (G3, G4, G7). Met deze digitale thermometer, ofwel het raadplegen van

144 Percentages op basis van twee groepen van *N*=80.

online openbare bronnen, wordt gekeken wat de status is van de gemeente. *"Als organisatie moet je gewoon weten wat er allemaal speelt in een stad"* (G2).

Een meerderheid onderschrijft de specifieke gemeentelijke communicatiedoelstelling om de dienstverlening richting inwoners te verbeteren (59% als hoofddoel; 21% als nevendoel, zie tabel 7). Vragen worden met behulp van online vergaarde informatie (online) gesignaleerd en beantwoord. Dit kunnen heel praktische vragen zijn over openingstijden (G1), of over de openbare veiligheid, zoals 'waarom is deze demonstratie?' (G3). Door een klein deel van de respondenten wordt monitoring ingezet om in de gaten te houden hoe de gemeente wordt gewaardeerd (33% als hoofddoel; 41% als nevendoel, zie tabel 7). Het doel is om *"gewoon even in de gaten te houden van wat leeft er en hoe er over [naam gemeente] wordt gesproken"* (G6).

Monitoringsdoelen voor communicatie volgens medewerkers van de afdeling OOV en Communicatie
Er zijn verschillen in de perceptie van doelen tussen medewerkers OOV en Communicatie. Belangrijkste verschil is dat medewerkers van de afdeling Communicatie de genoemde communicatiedoelen van monitoring vaker onderstrepen dan hun collega's van de afdeling OOV – die juist vaker aangeven niet te weten wat de communicatiedoelen zijn.

Medewerkers van de afdeling Communicatie geven in vergelijking met medewerkers OOV vaker aan dat 'weten wat er speelt' een hoofddoel is (93% versus 61%), door medewerkers OOV wordt dat juist vaker als een nevendoel gezien (25% versus 7%). Het verbeteren van dienstverlening wordt eveneens vaker door medewerkers Communicatie gezien als een hoofddoel (80% versus 34%) en vaker door medewerkers OOV als een nevendoel (26% versus 17%). Medewerkers OOV geven ook vaker aan het verbeteren van dienstverlening niet als een monitoringsdoel te zien (19% versus 2%) en geven ook vaker aan het niet te weten (21% versus 1%). Tot slot wordt het 'in de gaten houden van de gemeentelijke waardering' vaker door medewerkers Communicatie als een hoofddoel gezien in vergelijking met medewerkers OOV (45% versus 18%) en vaker door medewerkers OOV als 'geen doel' gezien (23 versus 8%). Ook geven medewerkers OOV hier vaker dan medewerkers van de afdeling Communicatie aan het niet te weten (24% versus 1%).[145]

3.4.2 *Openbare orde en veiligheidsdoelen van online monitoring*

Eerder is vastgesteld dat gemeenten niet alleen online monitoren voor communicatiedoeleinden maar dat ze dat ook doen in het kader van de openbare orde en veiligheid. Naar aanleiding van de literatuur en interviews vooraf is in de vragenlijst het brede doel 'online monitoren in het kader van de openbare orde en veiligheid' opgedeeld in

145 Gebaseerd op totale groepen van medewerkers Communicatie (*N*=104) en OOV (*N*=89).

specifieke doelstellingen, te weten: het signaleren, onderzoeken en handhaven van openbare-ordedreigingen. Tot slot is gevraagd of gemeenten online monitoren in openbare bronnen om strafbare feiten op te sporen.

Het signaleren van dreigingen is voor de bijna de helft van de respondenten een reden om te monitoren (43% als hoofddoel; 41% als nevendoel, zie tabel 8). In meerdere interviews wordt deze signalering van dreigingen beschreven als 'bijvangst' (G1, G3, G4, G7). *"Het zijn meer dingen die oppoppen dus het is niet iets waar we specifiek op monitoren"* (G3).

Tabel 8. Doelstellingen van online monitoring gericht op de openbare orde en veiligheid (in %, *N*=196)

	Hoofddoel	Nevendoel	Geen doel	Weet niet	Totaal %/n
Signalering van dreigingen in OOV	43	41	9	7	100/196
Onderzoeken van gesignaleerde dreigingen in OOV	33	39	18	11	100/196
Handhaving van dreigingen in de OOV	26	41	22	11	100/196
Opsporen van strafbare feiten	9	25	53	13	100/196

Het onderzoeken van gesignaleerde dreigingen wordt ook door de meeste respondenten onderschreven als monitoringsdoel (33% als hoofddoel; 39% als nevendoel, zie tabel 8). Op het moment dat een mogelijke openbare-ordeverstoring is vastgesteld, zoals een oproep tot een demonstratie, kunnen online bronnen gebruikt worden om de actualiteiten in kaart te brengen. Sociale media, andere online media en fora bevatten recente informatie om een gesignaleerde dreiging in te schatten en acties te ondernemen. Een van de respondenten geeft in de toelichting aan alleen casusgericht te onderzoeken. Als een onderwerp speelt, kan aan crisiscommunicatiemedewerkers worden gevraagd om een omgevingsanalyse te maken (G3).

De handhaving van mogelijke dreigingen wordt ook zowel als hoofd- en nevendoel gezien (26% als hoofddoel; 41% als nevendoel, zie tabel 8). In de toelichting van de vragenlijst beschrijft een respondent dat openbare bronnen nodig zijn om de wettelijke taak van openbare-ordehandhaving uit te voeren. Ruim een vijfde van de respondenten vindt ordehandhaving geen doel van online monitoring (22%). In box 3 wordt een toelichting gegeven door respondenten en geïnterviewden op het doel om online te monitoren in het kader van de openbare orde en veiligheid.

Box 3. Quotes uit de vragenlijst over het doel om online te monitoren in het kader van de openbare orde en veiligheid.

- *We hebben open bronnen nodig om in het kader van uitvoering van onze wettelijke taak de openbare orde te handhaven.*
- *Het hoofddoel van de online monitoring is de dienstverlening aan onze burgers, maar het wordt ook gebruikt om te signaleren wat er in onze gemeenten leeft. Bij dreigingen die worden geconstateerd worden wij (afdeling OOV) door Webcare/Communicatie geattendeerd op de dreiging en kunnen wij zelf acties gaan ondernemen. Of een aanvullend verzoek doen aan Webcare om strikter op een bepaald onderdeel te monitoren. Wij ontvangen vervolgens ook de monitoringsrapportages.*
- *Via sociale media proberen we snel te achterhalen wat er speelt en wat eventueel de maatschappelijke impact is.*

Tot slot geeft 9 procent aan de opsporing van stafbare feiten als een hoofddoel te zien van monitoring ten behoeve van de openbare orde en veiligheid, 24 procent ziet het als een nevendoel en de meeste respondenten (53%) geven aan dat het geen doel is van de monitoring.

Monitoringsdoelen voor OOV volgens medewerkers van de afdeling OOV en Communicatie

Ook bij deze op openbare orde en veiligheid gerichte doelen zijn er verschillen tussen typen medewerkers. Belangrijkste verschil is dat medewerkers van de afdeling OOV de genoemde openbare orde en veiligheidsdoelen van monitoring vaker onderstrepen dan hun collega's van de afdeling OOV – die juist vaker aangeven niet te weten wat de specifieke doelen zijn.

Zo wordt het signaleren van online dreigingen door medewerkers OOV vaker als een hoofddoel gezien (57%) in vergelijking met medewerkers van de afdeling Communicatie (31%). Medewerkers Communicatie zien het vaker als een nevendoel (50%) dan medewerkers OOV (30%). Het verder onderzoeken van gesignaleerde dreigingen wordt eveneens vaker als doel gezien door medewerkers OOV (53%) in vergelijking met medewerkers van de afdeling Communicatie (16%). Medewerkers Communicatie zien het vaker als een nevendoel (44% versus 30%) en als geen doel (25% versus 10%). Wanneer het gaat om het handhaven van gesignaleerde dreigingen blijken medewerkers OOV dit ook vaker als een hoofddoel te zien (46%) dan medewerkers Communicatie (10%). Medewerkers Communicatie geven vaker aan het niet als een monitoringsdoel te zien (31% versus 11%) of het niet te weten (15% versus 6%). Tot slot zijn er ook verschillen tussen medewerkers als het gaat om het opsporen van strafbare feiten als monitoringsdoel. Medewerkers OOV blijken dit vaker als een hoofddoel te zien (17%) dan medewerkers Communicatie (3%). Ook wordt door medewerkers OOV het vaker als nevendoel aangemerkt (38% versus 13%). Medewerkers Communicatie ge-

ven vaker aan het niet als een doel te zien (66% versus 37%) of het niet te weten (18% versus 8%).[146]

3.5 Technische knelpunten van online monitoring ('kunnen')

3.5.1 *Bruikbaarheid en meerwaarde van online informatie*

De resultaten in dit hoofdstuk roepen vragen op over organisatorische, technische, juridische en ethische aspecten van online monitoring. In het laatste deel van dit hoofdstuk zullen de reflectie, de opvattingen en ervaren knelpunten en dilemma's van gemeenten bij online monitoring, centraal staan. Bij technische knelpunten gaat het onder andere over de vraag of met behulp van monitoringstools doelstellingen behaald kunnen worden ('kunnen'). Er is onder andere aandacht voor de bruikbaarheid van de verzamelde informatie. Naast de hoeveelheid informatie (kwantiteit) wordt er ook gereflecteerd op de kwaliteit van de verzamelde informatie.

Uit de literatuur blijkt dat de bruikbaarheid en kwantiteit van online informatie die de monitoringstool opleveren niet voldoen aan de wensen van de organisatie. Er wordt onder andere geschreven over incomplete informatie (onvoldoende bronnen en content) en een beperkte bruikbaarheid van informatie. Of deze technische knelpunten in de gemeentelijke praktijk ook worden ervaren, wordt in het huidige onderzoek getoetst. Immers, uit de vragenlijst blijkt dat monitoringstools door 75 procent van de respondenten gebruikt wordt. Uit de verkennende interviews komt naar voren dat de tool niet altijd bruikbare informatie geeft (offline contacten geven een beter beeld), dat er veel besproken wordt in privé (niet openbare) groepen en dat er geen wetenschappelijke onderbouwing is voor de sentimentanalyse. Om in kaart te brengen of deze ervaren knelpunten gedeeld worden door een grote groep gemeentemedewerkers zijn in de vragenlijst verschillende stellingen over deze onderwerpen voorgelegd en is tevens gevraagd om toelichting op de antwoorden te geven (open veld). Achtereenvolgens worden de resultaten van de vragenlijst en de toelichting hierop in de vragenlijst en de interviews behandeld.

Gemeenten zijn niet uitgesproken over de ervaringen van monitoren. De helft van de respondenten geeft aan dat de monitoringstool van de gemeente in hun ogen geschikt is om bruikbare informatie te verzamelen om de gestelde doelen te behalen (56% eens, zie tabel 9). Slechts een paar respondenten geven expliciet aan dat de monitoringstool geen bruikbare informatie verzamelt (8% oneens) of zorgt voor te veel irrelevante informatie (13% eens). Daarnaast geven de meeste respondenten aan dat de monitoringstool over het algemeen voldoende informatie oplevert om de gestelde doelen te behalen (44% eens). Tegelijkertijd geeft een deel van de respondenten aan dat de monitoringstool in hun ogen onvoldoende content biedt (22% eens). Kortom, responden-

146 Gebaseerd op totale groepen van medewerkers Communicatie (*N*=104) en OOV (*N*=89).

ten zouden graag toegang hebben tot meer informatie. De sentimentanalyse wordt door een kwart van de respondenten als een nuttige tool gezien om de online berichten mee te categoriseren (26% eens). Een kanttekening is dat de meeste respondenten geen uitgesproken mening hierover hebben. Hierna wordt duiding gegeven aan deze percentages over technische knelpunten, eerst aan de hand van de toelichting in de vragenlijst en daarna aan de hand van interviews. Deze duiding wordt eerst geschetst voor de bruikbaarheid van informatie, daarna over (on)voldoende informatie en tot slot over de sentimentanalyse.

Tabel 9. Technische knelpunten bij gebruik van de monitoringstool (in %, *N*=140-142) [147]

	Eens	Oneens	Neutraal
Bruikbare informatie	56	8	18
Irrelevante informatie	13	40	27
Voldoende informatie	44	13	24
Onvoldoende content	22	32	25
Sentimentanalyse is nuttig	26	13	29

Uit de toelichting op de antwoorden in de vragenlijst komt naar voren dat informatie als bruikbaar wordt gezien mits deze in de juiste context geplaatst wordt en samen wordt genomen met andere informatiebronnen. Er wordt onder andere aangegeven dat een nadere duiding in de vorm van bijvoorbeeld een omgevingsanalyse nodig is om online informatie bruikbaar te maken voor bestuurders, politie en collega's van de afdeling OOV. Volgens meerdere respondenten is online informatie een onderdeel van de beeldvorming en wordt deze vaak samengenomen met andere informatiebronnen zoals persoonlijke contacten en mondelinge informatie en politiecijfers. Andere beschikbare informatie is nodig om de informatie te duiden of beter in kaart te brengen en volgens een van de respondenten is de monitoringstool daarin aanvullend. Respondenten die de informatie niet of minder bruikbaar vinden, lichten toe: "Je kunt niet alleen op basis van online informatie handelen." "De informatie die de monitoringstool oplevert, zal moeten worden vergeleken met andere beschikbare informatie om deze informatie te kunnen duiden en op waarde te kunnen schatten." "Het is wat mij betreft zaak om je niet blind te staren op de resultaten die de monitoringstool oplevert."

In de toelichting wordt door respondenten beschreven dat online content beperkt wordt aangeboden: "Sommige openbare pagina's kunnen we wel via ons eigen Facebookaccount bereiken en raadplegen, maar die inhoud vinden we niet altijd terug in de monitoringstool. Dat is jammer." Een andere respondent voegt toe: "Een technisch probleem is dat het lastig is om het platform Facebook goed te laden en dat dit het

147 Het resterende percentage (restcategorie) betreft 'weet niet' en varieert van 18 tot 32 procent per antwoordcategorie.

nummer één platform is waar de meeste input vandaan gehaald kan worden." Daarnaast verschuift de informatie van potentiële digitale dreigingen van openbare platformen (onder andere Facebook) naar andere niet-openbare platformen zoals WhatsApp. "We zien dat tegenwoordig veel potentiële overlastgevers onder de radar werken", waardoor niet alle relevante informatie in de monitoringstool naar voren komt.

In interviews wordt dieper ingegaan op de technische knelpunten. Over de kwantiteit van de bronnen zeggen gemeentelijke medewerkers het volgende: "De analyse beperkt zich tot bijna alleen Twitter en de pagina's die je al kent. Als er een nieuwe openbare Facebookpagina is, (die kan leiden tot bijvoorbeeld snelle mobilisatie) selecteert de tool die niet. Afnemers van de tool kunnen bij Coosto wel aanvragen om een bepaalde Facebookpagina ook te volgen, maar het duurt even voordat deze pagina in de tool te zien is. Het acuut achterhalen van een evenement wordt lastig op deze manier" (G3). Tegelijkertijd geven de geïnterviewden ook aan dat berichtgeving op sociale media steeds vaker niet zichtbaar is doordat die zich verplaatst naar gesloten bronnen of groepen (G1, G3). Ze geven aan dat jongeren niet meer op Facebook actief zijn maar zich verplaatsen naar Instagram, YouTube, WhatsApp en Snapchat en vallen daarmee buiten het bereik van Coosto en OBI4wan (alleen YouTube wordt beperkt aangeboden). Daarom wordt een beperkt deel binnengehaald, waardoor de jongere generatie ontbreekt. "Wat je krijgt aan resultaten is echt een fractie." Deze geïnterviewden geven aan dat ze zich dan "ook heel erg bewust [zijn] van het feit dat je dus maar een beperkt deel ziet, […] alleen de openbare bronnen". Een online gebeurtenis hoeft namelijk niets in de offline wereld te betekenen, maar geeft wel een beeld van het online sentiment (G3). Dezelfde geïnterviewde geeft ook aan dat dit een extra informatiestroom is die als nuttig wordt omschreven. De informatie uit de 'offline' wereld blijft voor deze specifieke gemeente het meest waardevol. "Je mist veel als je niet op straat bent en niet in de wijken zit. Als je niet op de juiste plekken bent op bepaalde momenten met letterlijk ogen, oren of camera's dan mis je veel meer", dan online niet aanwezig te zijn (G3). Online informatie is dus bruikbaar, maar vooral in combinatie met andere bronnen.

De laatste aanvulling en toelichting op tabel 9 gaat over de sentimentanalyse. Ter herinnering, een kwart van de respondenten geeft aan de sentimentanalyse nuttig te vinden (zie tabel 9). In de toelichting op de antwoorden in de vragenlijst wordt aangegeven waar men kritisch over is. Een van de respondenten geeft bijvoorbeeld aan dat de sentimentanalyse niet nuttig is omdat de toon in berichten op meerdere manieren geïnterpreteerd kan worden, een beeld dat ook in de interviews naar voren kwam. Een andere respondent geeft aan dat een "verdieping in de aard en inhoud van de reacties evenals een belangrijke discussie altijd nodig is om goed te kunnen duiden".

In interviews is ook aandacht voor het gebruik van de sentimentanalyse. Geïnterviewden geven aan de sentimentanalyse niet of beperkt te gebruiken, omdat deze in hun ogen niet accuraat is (G1, G3). Een geïnterviewde geeft het voorbeeld van een woord wat op meerdere manieren te interpreteren is: "de bom" (G1). De 'bom' zal negatief in

de sentimentanalyse naar voren komen, omdat het wordt geassocieerd met een ontploffend wapen. Het kan echter ook in straattaal een positieve beschrijving van iets zijn ('de bom zijn') en daarmee is de sentimentanalyse niet accuraat. Samenvattend, meer dan de helft van de respondenten heeft geen uitgesproken mening over technische knelpunten. Er wordt wel degelijk meerwaarde ervaren van de informatie, die wordt verkregen door online monitoring maar men is zich er ook van bewust dat slechts een deel van de online informatie zichtbaar is voor gemeenten.

Technische knelpunten monitoringstools en verschillen tussen OOV en Communicatie
Er zijn tot slot verschillen als het gaat om medewerkers van de afdeling OOV en Communicatie. Het belangrijkste verschil is dat medewerkers Communicatie positiever zijn over het gebruik van monitoringstools, maar ook dat medewerkers van de afdeling OOV het moeilijk vinden om er een oordeel over te vellen en vaker aangeven het niet te weten.

Medewerkers Communicatie, vergeleken met medewerkers OOV, vinden de informatie die de monitoringstools oplevert vaker bruikbaar (73% versus 36%) en geven minder vaak aan het niet te weten (3% versus 36%). Medewerkers Communicatie vinden ook vaker dat de tool voldoende informatie oplevert (62% versus 39%) en geven minder vaak aan het niet te weten (1% versus 39%). Medewerkers Communicatie zijn het ook vaker oneens met de stelling dat de tool onvoldoende content oplevert (44% versus 18%). Ook hier geven de medewerkers OOV vaker aan het niet te weten (43% versus 4%). Tot slot lijken medewerkers van de afdeling Communicatie wél kritischer dan medewerkers OOV over het nut van de sentimentenanalyse. 23 procent van de medewerkers Communicatie is het oneens met de stelling dat de sentimentenanalyse nuttig is, tegenover 2 procent van de medewerkers OOV. Wederom blijkt dat medewerkers OOV vaker 'weet niet' noteren (55%) dan medewerkers van de afdeling Communicatie (12%).[148]

3.6 Organisatorische knelpunten van online monitoring ('kunnen')

3.6.1 *Organisatorische randvoorwaarden*

De mogelijkheden voor een organisatie zoals de gemeente om online te kunnen monitoren, worden niet alleen bepaald door technische mogelijkheden en knelpunten (deel 1 van het 'kunnen'), maar ook door organisatorische mogelijkheden (deel 2 van het 'kunnen'). Technische hulpmiddelen kunnen het werk voor gemeenteambtenaren gemakkelijker maken, ook bij online monitoring, maar zonder een duidelijke duiding van die informatie is het moeilijk om de informatie te gebruiken of te vertalen in een concrete handeling. Dit vraagt mogelijk veel manuren en specifieke kennis. Is er genoeg capaciteit en beschikken de medewerkers over voldoende kennis en kunde om hun doelen te behalen? Ter herinnering, eerder is duidelijk geworden dat gemeenten online monitoring gebruiken met als doel om hun informatiepositie te versterken en

148 Gebaseerd op totale groepen van medewerkers Communicatie (*N*=74-75) en OOV (*N*=66-67).

deels voor de handhaving van de openbare orde en veiligheid. Ook bleek de samenwerking met de politie belangrijk te zijn voor gemeenten. Daarom zijn in de vragenlijst drie stellingen aan de respondenten voorgelegd over mogelijke organisatorische knelpunten: de capaciteit, kennis en kunde van medewerkers en de informatie-uitwisseling met de politie. Deze worden verder uitgewerkt in deze paragraaf.

De eerste stelling over organisatorische knelpunten is: 'Binnen de gemeente is er over het algemeen voldoende capaciteit om de doelstellingen van online monitoring te behalen'. Met die stelling is 39% het oneens (onvoldoende capaciteit) en 26% het eens (zie tabel 10). Een groot deel van de respondenten geeft dus aan dat hun gemeente onvoldoende capaciteit heeft om de doelstellingen te behalen. Uit de toelichting van respondenten op de stellingen blijkt dat tijd wordt genoemd als een serieus knelpunt bij de online monitoring. 'Online monitoring kost veel tijd en die hebben we vaak niet. Op het moment dat er wel iets gesignaleerd wordt, dan moet er actie genomen worden en dat kost ook capaciteit. Dus vaak is het een keuze of je er tijd voor hebt of niet.' Er is geen toelichting gegeven door de respondenten die het eens zijn met deze stelling.

Tabel 10. Organisatorische knelpunten bij online monitoring (in %, *N*=152)

	Eens	Oneens	Neutraal
De gemeente heeft voldoende capaciteit	26	39	35
Medewerkers hebben voldoende kennis en kunde	39	27	34
Gemeente is tevreden over informatie-uitwisseling met de politie*	43	8	49

* **Medewerkers van de afdeling OOV zijn vaker tevreden over de informatie-uitwisseling met de politie (58%) dan medewerkers van de afdeling Communicatie (26%).**

De tweede stelling over organisatorische knelpunten is: 'Binnen de gemeente hebben de medewerkers over het algemeen *voldoende kennis en kunde* om de doelstellingen van online monitoring te behalen.' Vier op de tien respondentenzijn het eens met deze stelling (39%) en een kwart van de respondenten is het daarmee oneens (zie tabel 10). Het grootste deel van de respondenten geeft dus aan dat gemeentelijke medewerkers voldoende kennis en kunde hebben om online monitoring doelen te behalen. Een respondent licht toe: "We beschikken over voldoende getrainde mensen met goede tools om online monitoring mogelijk te maken". Er is geen toelichting gegeven door respondenten die het oneens zijn met de stelling en er lijkt veel variatie te zijn in de opvattingen van respondenten.

De derde stelling gaat over de samenwerking met de politie, een belangrijke partner in de signalering van digitale dreigingen en duiding van informatie. De stelling is: 'Mijn gemeente is tevreden met de uitwisseling tussen gemeente en politie van informatie over openbare orde en veiligheid die is verkregen via online monitoring.' Bijna de helft van de respondenten geeft aan tevreden te zijn over de uitwisseling van informatie over

openbare orde en veiligheid tussen gemeente en politie (43%) en een klein aantal is het oneens met deze stelling en is ontevreden (8%, zie tabel 10). In de toelichting op de antwoorden in de vragenlijst beschrijft een respondent dat de politie de gemeente niet ziet als een volwaardige partner en er vermoedelijk een gebrek aan vertrouwen is. In de toelichting van de vragenlijst komt verder naar voren dat niet alleen gemeenten met capaciteitsproblemen lijken te kampen: "De samenwerking met de politie is prima, maar staat enorm onder druk door de capaciteitsproblemen bij de politie." Een andere respondent beaamt het capaciteitsprobleem bij de politie en geeft aan dat dit ervoor zorgt dat de informatie die ze van de politie krijgen hierdoor vaak 'te kort door de bocht is'.

Kortom, gemeenten zijn verdeeld over de aanwezige organisatorische randvoorwaarden. De meeste respondenten geven aan dat de medewerkers over voldoende kennis en kunde beschikken, maar dat de organisatie onvoldoende capaciteit heeft om de doelen te behalen. De meeste respondenten zijn tevreden over de informatie-uitwisseling met de politie. Ook bij deze stellingen geeft een derde tot de helft van de respondenten geen expliciete mening (neutraal), waardoor bovenstaande resultaten slechts een indicatie geven voor de praktijk.

3.7 Juridische grenzen en verantwoordelijkheid ('mogen')

Gedrag van mensen wordt door veel factoren bepaald en het recht is daar één van. In hoofdstuk 4 komen verschillende juridische grenzen naar voren zoals het recht op de privacy, recht op vrijheid van meningsuiting en de persvrijheid. Men mag verwachten dat overheden zorgvuldig omgaan met de rechten van inwoners. Voordat het juridische kader voor gemeentelijke online monitoring wordt gepresenteerd in hoofdstuk 4, worden enkele opvattingen van gemeentelijke medewerkers gepresenteerd die verband houden met mogelijke juridische grenzen.

3.7.1 *Werken met het juridische kader*

Het juridische kader van online monitoring bij gemeenten is een grijs gebied. Dat was en is ook een van de drijfveren van het huidige onderzoek. Aan de respondenten is gevraagd of voor hen wél duidelijk is onder welk juridisch kader zij online monitoring handen en voeten kunnen geven en of zijn conform dat kader werken.

Een kwart van de respondenten geeft expliciet aan dat het juridische kader voor hen niet duidelijk is (27%) en ongeveer een vijfde gaf aan dat het juridisch kader wel duidelijk is (21%). Tegelijkertijd gaf bijna de helft van de respondenten aan wél te werken volgens het juridische kader (46%, zie tabel 11). Dat is een bijzondere tegenstelling. Een communicatiemedewerker geeft in de toelichting op de vragenlijst aan dat er geen juridische kennis aanwezig is bij het team: 'De indruk is dat het niet nodig is omdat we analyses niet extern verspreiden (tenzij in crisissituaties) en het gaat om openbaar toe-

gankelijke en beschikbare informatie.' Een andere respondent geeft in een toelichting op de vragenlijst aan dat het gebruik van openbaar toegankelijke bronnen valt onder de vrijheid van meningsuiting en burger- en overheidsparticipatie en benadrukt dat de informatie vrijwillig door mensen met de gemeente wordt gedeeld.

Tabel 11. Juridische knelpunten bij online monitoring (in %, *N*=147)

	Eens	Oneens	Neutraal
Juridisch kader is duidelijk	21	27	52
Werken volgens juridisch kader	46	4	50

In de interviews wordt gereflecteerd op de juridische kaders waar de gemeente mee werkt en welke juridische grenzen zij zien bij de online monitoring door gemeenten. Een medewerker beschrijft: "Sinds de AVG mogen wij niet meer zoekopdrachten maken die uitsluitend gericht zijn op één persoon. Het is nog wel mogelijk om op persoon te zoeken in de monitoringstool, maar het wordt streng afgeraden in verband met de AVG" (G3).[149] Volgens deze geïnterviewde mag een zoekopdracht op de persoon niet opgeslagen worden, maar is het wel mogelijk om elke dag dezelfde zoekopdracht uit te voeren zonder deze gegevens op te slaan, maar "het komt zelden voor eigenlijk dat je specifiek van één persoon iets wilt weten". In een ander interview wordt aangegeven dat gemeentelijke medewerkers die woonachtig zijn in de dezelfde gemeente niet weten of ze mensen op sociale media mogen toevoegen. Met als reden, dat "als ik hem/haar toevoeg, dan weet diegene die mij geaccepteerd heeft niet dat ik hem op de monitoringstool kan zien". Een andere geïnterviewde geeft aan: "Als iemand zich op internet met naam en al manifesteert of met gegevens die tot hem herleidbaar zijn dan geeft hij eigenlijk zelf een stukje van zijn privacy op. Dus daar mag je naar kijken. Maar op het moment dat een gemeente dat in verschillende media doet en een langere tijd alles wat die betreffende persoon op sociale media doet volgt of verzamelt, dan ontstaat een bewerking van de persoonsgegevens en dan gaat het onder de AVG vallen" (G2). Dit veronderstelt enige kennis van het begrip 'een meer dan geringe inbreuk' van online monitoring. Volgens dezelfde gemeente valt Newsroom monitoring niet onder de AVG, "omdat er geen persoonsgegevens worden verzameld of bewerkt. Bewerking is de centrale term in de AVG, dat doet de Newsroom niet". "Als er een naam in de rapportages staat dan is het een naam die al in de openbaarheid is, van iemand die zijn privacy heeft prijsgegeven." "Als dat bericht binnen de organisatie wordt doorgestuurd, dan speelt de AVG niet. Die gaat wel spelen op het moment dat je iemand vaker in beeld krijgt. Wij hebben natuurlijk bevoegdheden om die gegevens te verzamelen, in artikel 6 van de AVG staan de doelen waarvoor persoonsgegevens verzameld mogen worden" (G2).

149 Facebook voorkomt actief (bijvoorbeeld) dat de overheid meeleest ('law enforcement').

3.7.2 *Waarborging van het juridisch kader*

Eerder is vastgesteld dat het voor medewerkers niet duidelijk is wat het juridisch kader is waarbinnen online monitoring plaatsvindt. Met de vragenlijst is uitgezocht of, en op welke manier, een juridisch kader is gewaarborgd in de organisatie. Hier zijn verschillende manieren voor, zoals i) een handelingsprotocol en, ii) betrokkenheid van een functionaris gegevensbescherming. Een vastgelegd handelingsprotocol of beleidsdocument, opgesteld met inachtneming van de wet- en regelgeving, kan het gedrag van medewerkers standaardiseren en tegelijkertijd de rechtsongelijkheid van onderzochte subjecten minimaliseren. Daarom is gevraagd of de gemeente werkt met een vastgelegd handelingsprotocol of beleidsdocument.

De meerderheid van de respondenten geeft aan geen protocol of beleid te hebben voor online monitoring binnen de gemeente (54% nee) en ruim een derde heeft hier geen kennis van (38%; zie tabel 12). Slechts 8% van de respondenten geeft aan wel op de hoogte te zijn van een vastgelegd protocol of beleidsdocument voor gemeentelijke online monitoring. In de toelichting op de vragenlijst wordt aangegeven dat gemeenten werken volgens richtlijnen in plaats van een protocol of werken volgens het protocol van de veiligheidsregio. Uit een van de interviews komt die onduidelijkheid naar voren: “Het is een beetje schimmig en ook onduidelijk wat wel en niet mag” (G3). De betreffende medewerker van een gemeente geeft aan dat collega’s elkaar wel trainen, maar dat er geen vast protocol aanwezig is om ervoor te zorgen dat alle gemeentelijke medewerkers zich houden aan het juridische kader. Dezelfde geïnterviewde geeft ook aan dat de prioriteit niet hoog ligt: “Maar het heeft voor ons ook niet heel erg veel belang” (G3).

Tabel 12. Waarborging juridisch kader bij online monitoring bij gemeenten (in %, *N*=147)

	Ja	Nee	Weet niet/ anders
Vastgelegd protocol of beleidsdocument	8	54	38
Betrokkenheid functionaris gegevensbescherming	16	37	47

Een tweede manier om het juridische kader te waarborgen binnen de gemeente is door de Functionaris Gegevensbescherming te betrekken bij de handelwijze van monitoring (onafhankelijk of deze handelwijze op papier is beschreven).[150] Een Functionaris Gegevensbescherming (ook wel FG of privacyfunctionaris genoemd) is verantwoordelijk voor de toepassing en naleving van de AVG, dus ook bij monitoring van gemeenten. Gemeenten zijn sinds het van kracht worden van de AVG (25 mei 2018) verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken.

Bijna de helft van de respondenten geeft aan niet te weten of een FG betrokken is bij het vaststellen wat wel en niet mag bij online monitoren (47%, zie tabel 12) en ruim een

150 Er kan ook nog gedacht worden aan een privacyfunctionaris binnen gemeenten.

derde geeft aan dat er geen FG betrokken is (37%). Slechts zestien procent van de respondenten geeft aan dat de FG wel betrokken is geweest. Een mogelijke verklaring voor deze resultaten is dat een deel van de gemeenten eerder met online monitoring zijn begonnen dan de inwerkingtreding van de AVG (25 mei 2018). Een respondent verklaart in de toelichting op een van zijn antwoorden in de vragenlijst dat 'voor de AVG de nadruk op privacy minder groot was'. Een andere respondent licht toe dat zijn/haar gemeente zes jaar geleden met online monitoring is begonnen en er toen minder aandacht was voor juridische aspecten. Een andere respondent bevestigt dit en schreef: *'Na intrede van de AVG is dit meer op het netvlies gekomen*'. Toentertijd was bij het inrichten van de tool een FG of protocol nog niet aanwezig. Meerdere respondenten geven aan dat een beleidsplan nog geschreven moet worden. Kortom, er is dus zelden een protocol dat beschrijft hoe gemeentelijke medewerkers juridisch gezien wel en niet mogen handelen. Tevens is bij de meeste gemeenten geen Functionaris Gegevensbescherming betrokken bij dit handelingskader, ondanks dat dit een verplichting van de wet is.

Verschillen in waarborging juridische kaders door OOV en Communicatie
Er zijn op dit vlak ook verschillen tussen gemeentelijke medewerkers waargenomen. Medewerkers van de afdeling Communicatie geven vaker aan een protocol te gebruiken (15%) dan medewerkers van de afdeling OOV (1%), maar geven eveneens vaker aan het niet te gebruiken (67% versus 42%). Dat komt doordat medewerkers van de afdeling OOV vaker aangeven het niet te weten (54% versus 14%).[151] Daarnaast wordt vaker door medewerkers Communicatie aangegeven dat er geen FG betrokken is bij de monitoring (54% versus 19%) en geven medewerkers van de afdeling OOV vaker aan dat ze het niet weten (62% versus 24%).

3.7.3 *Juridische verantwoordelijkheid*

In de vragenlijst is aan de respondenten voorgelegd wie zij juridisch verantwoordelijk achten voor gemeentelijke online monitoring. De reden voor deze vraag is dat tijdens een verkennend interview werd aangegeven dat het reputatiemanagementbedrijf verantwoordelijk is. Dit is van belang omdat, volgens deze geïnterviewde, de gemeente daarmee juridisch mag handelen binnen de mogelijkheden van de monitoringstool. Daarom is gevraagd wie respondenten juridisch verantwoordelijk vinden: de gemeente als organisatie, gemeentemedewerkers of het reputatiemanagementbedrijf.

De meeste respondenten geven aan dat de gemeentelijke organisatie uiteindelijk juridisch verantwoordelijk is voor gemeentelijke online monitoring (55% eens). Een kleiner deel geeft aan dat de individuele gemeentelijke medewerkers (27% eens) of het reputatiemanagementbedrijf (16% eens) dat de monitoringstool levert, juridisch verantwoordelijk zijn (zie tabel 13).

151 Gebaseerd op totale groepen van medewerkers Communicatie (*N*=72) en OOV (*N*=74).

Tabel 13. Juridische knelpunten bij online monitoring (in %, *N*=147)[152]

	Eens	Oneens	Neutraal
De Gemeentelijke organisatie is verantwoordelijk	55	3	42
Gemeentemedewerkers zijn verantwoordelijk	27	25	48
Reputatiemanagementbedrijf is verantwoordelijk	16	34	50

Een van de geïnterviewde medewerkers is van mening dat het reputatiemanagementbedrijf juridisch verantwoordelijk is, want de AVG bepaalt wat het bedrijf wel en niet met de monitoringstool aan zou mogen bieden (G3). *"De leverancier van de monitoringstool die zorgt ervoor dat het juridisch binnen de grenzen werkt, zodat wij (de gemeente) ons daar niet druk om hoeven te maken. Als wij het hier op onze eigen servers hadden draaien dan zouden we er al veel minder van doen mee hebben dan nu. Maar het draait over hun servers heen dus zij hebben de opslag. Daarom zijn zij ook medeverwerkers. Het is hun verantwoordelijkheid."* Omdat de leverancier de dataopslag regelt is deze verantwoordelijk volgens de AVG, aldus deze geïnterviewde. Zolang de leverancier handelt conform de wet, dan doet de gemeente dit ook.[153]

3.8 Ethische opvattingen ('willen')

3.8.1 *Dilemma's van verantwoording en transparantie*

In deze subparagraaf wordt in kaart gebracht wat de (ethische) opvattingen van gemeentelijke medewerkers over online monitoring in het algemeen zijn wat ze vinden over de mate waarin hun gemeente transparant is over de werkwijze rondom online monitoring.

Bijna drie kwart van de respondenten geeft aan de online monitoring bij hun gemeente over het algemeen als ethisch verantwoord te zien (72%) en slechts 5 procent vindt van niet (zie tabel 14). Enkele respondenten lichten in de vragenlijst toe waarom het in hun ogen ethisch verantwoord is om online monitoring in zetten voor de openbare orde en veiligheid (*N*=3). "*Als mensen zich vrij uitlaten over controversiële onderwerpen in de media met een duidelijk doel van een verstoring van de openbare orde, dan zien wij geen enkel probleem hen te volgen,*" aldus een respondent.

Tabel 14. Ethische opvattingen over online monitoring (in %, *N*=140)[154]

	Eens	Oneens	Neutraal
Monitoring algemeen	72	5	23
Open en transparant over online monitoring	38	11	51

152 Er zijn op dit vlak geen verschillen tussen medewerkers van de afdeling OOV en Communicatie.
153 De juridische duiding hiervan is te vinden in hoofdstuk 4.
154 Er zijn op dit vlak geen verschillen tussen medewerkers van de afdeling OOV en Communicatie.

Naast aandacht voor de ethische opvattingen over online monitoring in het algemeen is ook gekeken naar de mate waarin medewerkers van gemeenten vinden dat hun organisatie open en transparant naar hun inwoners is over de online monitoring.

Ruim één derde geeft aan dat hun gemeente transparant is in online monitoring (38%) en een klein deel vindt hun gemeente niet transparant (11%, zie tabel 14). In de vragenlijst licht een van de respondenten toe waarom de gemeente in zijn ogen transparant is: "*We hebben een privacyprotocol dat voor iedereen opvraagbaar is, en via Wob-verzoeken is andere informatie boven water te krijgen.*" Een andere respondent (interview) vult aan: *"Als we het doen, dan doen we het volgens de regels, dan vind ik dat ethisch verantwoord.*"

3.8.2 *Ethische opvatting over monitoren van groepen en (publieke) personen*

Met het oog op de privacy is het ingrijpender wanneer individuen gevolgd worden dan wanneer de online monitoring gericht is op groepen. Wanneer een persoon gevolgd wordt, kan het juridisch uitmaken of er sprake is van een 'publiek' persoon of van een 'onbekend' persoon. Voor publieke personen is de kans op een privacy-inbreuk van online monitoring waarschijnlijk kleiner dan voor een 'onbekend' persoon. Aan respondenten is gevraagd of ze gemeentelijk online observeren van groepen (publiek/onbekend) ethisch verantwoord vinden.

Uit de vragenlijst komt naar voren dat meer dan de helft van de respondenten het monitoren van groepen ethisch verantwoord vindt (61%) en dat een klein aantal respondenten het als onethisch ziet (4%, zie tabel 15). Een van de respondenten licht dat als volgt toe in de vragenlijst: "*Het doel moet de middelen heiligen. Lukraak observeren zonder dat je als gemeente een reden/doel hebt, is ethisch niet verantwoord. Op het moment dat jij groepen of individuen hebt die geobserveerd moeten worden in het belang van de openbare orde en veiligheid is dit ethisch verantwoord.*"

Tabel 15. Is het online monitoren door gemeenten ethisch verantwoord? (in %, *N*=140)

	Eens	Oneens	Neutraal
Monitoring van groepen	61	4	35
Monitoring van publieke personen	60	7	33
Monitoring van 'onbekende' personen	34	22	44

Het online monitoren van 'publieke' personen (die in de media naar voren komen) wordt door de meerderheid van de respondenten ook als ethisch verantwoord gezien (60%). Slechts 7% is het hiermee oneens (zie tabel 15). De meeste respondenten vinden dus dat het online volgen van groepen en 'publieke' personen ethisch verantwoord is, maar is dat ook zo voor personen die niet in de media naar voren zijn gekomen?

Eén derde van de respondenten geeft aan het ethisch verantwoord te vinden om 'onbekende' personen (die niet in de media naar voren komen) online te observeren door de gemeente (34%, zie tabel 15). Eén op de vijf respondenten vindt het niet ethisch verantwoord (22%). Het volgen van 'onbekende' personen (22%) wordt dus relatief vaker als onethisch beschouwd dan het volgen van 'publieke' personen (7%).

Respondenten geven bij de toelichting op de antwoorden in de vragenlijst aan dat online monitoring ethisch verantwoord is zolang het om openbare bronnen gaat. De betreffende persoon kiest er immers zelf voor om informatie op een openbaar platform te publiceren, zo redeneren zij. *"Mensen die actief zijn op openbare online platforms weten dat anderen dit kunnen zien en hierop kunnen reageren. Daarom is het ethisch verantwoord. Dat is het hele doel van sociale media. Als je dat niet wil, moet je acteren in een besloten groep (dat meet de monitoringstool niet)."* Deze respondenten geven aan online monitoring dus ethisch verantwoord te vinden, zolang het openbare bronnen zijn. *"We monitoren waartoe we toegang hebben. Wij hebben geen toegang tot afgeschermde accounts en dat moet zo blijven."* Sterker nog, twee respondenten geven aan dat inwoners van de gemeente verwachten dat ze hun sociale media volgen. *"Burgers verwachten dat de overheid naar hen luistert. Online monitoring is een manier om dat te doen."* Een geïnterviewde geeft aan het eens te zijn met dit standpunt en stelt dat burgers rekening houden met het feit dat de gemeente hun berichten leest: *"Ze weten ook van, we moeten hier niet te veel dingen gaan delen want er luisteren ook andere mensen mee"* (G2).

Daarnaast wordt beargumenteerd dat online monitoring ethisch verantwoord is zolang gehandeld wordt volgens de geldende wet- en regelgeving. *"Signalen die worden opgevangen of personen die naar voren komen worden vervolgens altijd behandeld volgens geldende wet- en regelgeving. Online monitoring wordt niet ingezet om meningen te onderdrukken, maar juist om ze te kennen en om ze zodoende een plek te kunnen geven in het maatschappelijk debat."* Een andere respondent legt uit dat de monitoringstool alleen openbare bronnen toegankelijk maakt: *"Dus in die zin kunnen wij het juridisch naar mijn mening niet fout doen."*

3.8.3 *Ethische opvattingen over gebruik van privéaccounts*

De laatste 'ethische stelling' gaat over het gebruik van privéaccounts. Ruim een derde van de gemeentelijke medewerkers geeft aan het gebruik van privéaccounts niet ethisch verantwoord te vinden (36%) en ook bijna een derde van de respondenten geeft aan het gebruik van privéaccounts in bepaalde gevallen wel ethisch verantwoord te vinden (28%, zie tabel 16). *"Het gebruik van privéaccounts is alleen verantwoord indien de informatie met betrekking tot een mogelijke dreiging van de openbare orde op geen enkele andere manier te verkrijgen is. Veelal is dit via de politie wel mogelijk, dus niet noodzakelijk,"* aldus een respondent.

Tabel 16. Is het monitoren met privéaccounts door gemeenten ethisch verantwoord? (in %, *N*=140)

	Eens	Oneens	Neutraal
Monitoring met privéaccounts	28	36	36

Kortom, de meeste respondenten vinden het ethisch verantwoord dat gemeenten online monitoren (in algemene zin) en ook het volgen van groepen en 'publieke' individuen wordt als niet bezwaarlijk gezien. Wanneer het gaat om onbekende personen (niet publieke personen) of het gebruik van nepaccounts zijn gemeentelijke medewerkers meer verdeeld in hun opvattingen.[155]

3.9 Afsluiting

In dit empirische hoofdstuk is meer inzicht verkregen in de black box van gemeentelijke monitoring door aandacht te besteden aan werkwijzen, doelstellingen en ervaren knelpunten in de gemeentelijke praktijk van monitoring.

Uit dit hoofdstuk komt naar voren dat online monitoring gemeengoed is geworden onder bijna alle geraadpleegde gemeenten en dat vooral de afdelingen Communicatie en OOV zich hiermee bezighouden. Een belangrijk aspect van het laatstgenoemde betreft het voorkomen van openbare-ordeverstoringen door gebruik te maken van online signalen. De meeste van die online signalen worden hooguit één keer per jaar waargenomen. Alleen online onrust rondom politieke besluiten wordt met enige regelmaat online gesignaleerd door gemeenten.

Uit dit hoofdstuk werd ook duidelijk hoe gemeenten het online monitoren handen en voeten geven in de praktijk. De meeste gemeenten maken gebruik van technische hulpmiddelen, zogenaamde 'monitoringstools', maar zoeken ook geregeld informatie handmatig op. Op het moment dat een digitale dreiging is gesignaleerd, wordt de samenwerking binnen en buiten de gemeente opgezocht. Overeenkomstig met de literatuur blijkt dat de politie een natuurlijke samenwerkingspartner is bij het handhaven van de openbare orde en veiligheid. Dit zien we terug in de informatie-uitwisseling tussen deze partijen. Ook met andere relevante partijen wordt samenwerking gezocht en informatie uitgewisseld. Om de digitale dreiging beter in kaart te brengen, wordt in de praktijk vaak een omgevingsanalyse gemaakt. Hierbij wordt ook specifiek gezocht op een groep personen of individu en bij uitzondering gebruikgemaakt van de privéaccounts van medewerkers. Dit leidt ertoe dat gemeenten inzicht hebben in meer (en gesloten) bronnen. In een enkel geval worden zelfs nepaccounts gebruikt door de gemeente.

155 Er zijn geen verschillen gevonden tussen medewerkers OOV en Communicatie bij de vragen over ethische aspecten van monitoring.

Waarom doen gemeenten aan online monitoring? Deze vraag over doelstellingen is van belang met het oog op de proportionaliteit. Zoals gezegd doen vooral de afdelingen Communicatie en OOV aan online monitoring binnen gemeenten. De doelen van online monitoring verschillen in theorie van elkaar maar lopen in de praktijk door elkaar heen. De Communicatieafdeling ziet bijvoorbeeld openbare-ordedreigingen als 'bijvangst' in de continue monitoring of maakt een omgevingsanalyse van een specifiek thema, groep of individu. Online monitoring wordt vooral ingezet met het doel om de informatiepositie van de gemeenten te versterken en secundair om de openbare orde en veiligheid te handhaven.

De resultaten in dit hoofdstuk roepen vragen op over organisatorische, technische, juridische en ethische aspecten van online monitoring. In het laatste deel van dit hoofdstuk stonden reflecties vanuit gemeenten op hun eigen werkwijze centraal en was aandacht voor ervaren knelpunten en dilemma's bij online monitoring. Daaruit blijkt dat gemeentelijke medewerkers weinig knelpunten zien of ervaren als het gaat om online monitoring, ongeacht of het gaat om technische, organisatorische of ethische aspecten ervan en dat ze niet weten waar de juridische grenzen liggen. Zo zijn de gemeentelijke medewerkers overwegend tevreden over de resultaten die online monitoring oplevert in relatie tot de doelstellingen en vinden ze de aanwezige kennis over online monitoring binnen de gemeente van voldoende niveau. Men is daarnaast wel kritisch over de aanwezige capaciteit om de online monitoring goed uit te kunnen voeren. Ook blijkt dat het juridisch kader voor online monitoring door gemeenten vaak niet bekend is en dat juridische aspecten in de gekozen werkwijze geen (expliciete) grote rol spelen. De gemeentelijke organisatie wordt daarentegen door haar medewerkers wel als eindverantwoordelijk gezien voor de naleving van een juridisch kader en de juridische grenzen.

Daar waar een deel van de medewerkers wel aangeeft de regels te kennen, is de borging daarvan alsnog een punt van zorg, mede doordat in dit hoofdstuk naar voren komt dat bij de meeste gemeenten geen Functionaris Gegevensbescherming betrokken is bij de online monitoring. Tot slot wordt online monitoring over het algemeen gezien als een weinig bezwaarlijke activiteit en is privacy van inwoners onderbelicht. Desalniettemin maakt het grootste deel van de medewerkers geen gebruik van nepaccounts of privéaccounts bij online monitoring en toch vindt een derde het ethisch verantwoord om privéaccounts te gebruiken bij hun taakuitvoering.

Nu duidelijk is wat gemeenten doen en hoe ze reflecteren op hun eigen werkwijze bij online monitoring wordt in het volgende hoofdstuk het juridische kader beschreven waarbinnen gemeenten zich kunnen bewegen bij online monitoring en wordt er gereflecteerd op een deel van de empirische uitkomsten die in dit hoofdstuk naar voren zijn gekomen.

4. Het juridisch kader voor de monitoring van online openbare bronnen

4.1 Inleiding

In hoofdstuk 3 is aan de hand van empirisch onderzoek inzicht gegeven in monitoring van gemeenten van online openbare bronnen en de knelpunten die zij daarin ervaren. Gemeenten gebruiken monitoringstools om hun informatiepositie te verbeteren, voeren handmatige zoekopdrachten uit of verrichten omgevingsanalyses. Dit hoofdstuk sluit daarop aan, door het juridisch kader te schetsen dat op deze handelingen van toepassing is en een algemene beoordeling te geven van de rechtmatigheid van deze monitoring.[156] De deelvraag die in dit hoofdstuk wordt beantwoord is: aan welke juridische grenzen zijn gemeenten gebonden wat betreft online monitoren?

Dit hoofdstuk richt zich nadrukkelijk op het gebruik van openbare bronnen. Ter herinnering, gelet op de definitie die in paragraaf 1.3 is opgenomen, wordt een open bron omschreven als een bron waartoe 'in beginsel eenieder toegang kan verkrijgen en dat voor zover toegang gebonden is aan een account, het verkrijgen van een account een (semi-)geautomatiseerd proces is waarbij niet bepaalde groepen worden uitgesloten van registratie'. Dat betekent dat zodra er enige vorm van selectie plaatsvindt in de toegang tot die informatie – iemand wordt wel of niet geaccepteerd als connectie, of voor de toegang tot een Facebookgroep moet het aspirant-lid enige vragen over zijn of haar belangstelling voor het onderwerp beantwoorden – de betreffende bron geen open bron is. In hoofdstuk 3 is ook besproken dat gemeenten in sommige gevallen gebruikmaken van privéaccounts of nepaccounts (zie 3.3.4). Die accounts worden gebruikt om niet-open bronnen te ontsluiten. Ook gemeentelijke accounts worden hiervoor gebruikt. In paragraaf 4.3.1 wordt kort ingegaan op het gebruik van gemeentelijke accounts, privéaccounts en nepaccounts voor het benaderen van niet-openbare bronnen.

De gedachte dat informatie die in openbare bronnen is terug te vinden vanwege dat openbare karakter zonder beperking door gemeentebesturen kan worden gebruikt, is onjuist. Ook voor het raadplegen en gebruiken van informatie uit openbare bronnen gelden regels. De achterliggende gedachte is hier dat dergelijke monitoring door ge-

156 Wij bedanken Janey Huibers voor de ondersteuning bij het schrijven van dit juridische hoofdstuk.

meenten inbreuk kan maken op de persoonlijke levenssfeer. Die persoonlijke levenssfeer wordt op verschillende plaatsen juridisch beschermd, vandaar dat meerdere juridische kaders in dit hoofdstuk de revue passeren. Voor zover het specifiek gaat om de bescherming van persoonsgegevens is de Algemene Verordening Gegevensbescherming (AVG) het belangrijkste juridische document. De aandachtspunten en eisen die op basis van de AVG door gemeenten in acht moeten worden genomen bij de online monitoring van openbare bronnen, wordt geschetst in paragraaf 4.2. De AVG kan worden gezien als een verordening waarin het recht op privacy specifiek voor persoonsgegevens wordt geoperationaliseerd.

Het recht op privacy is een onderdeel van het recht op eerbiediging van de persoonlijke levenssfeer. Dat recht is onder andere gecodificeerd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 10 van de Grondwet. Hoewel die twee artikelen hetzelfde recht codificeren, stellen ze verschillende eisen aan de beperking van deze rechten. In paragraaf 4.3 en paragraaf 4.4 wordt besproken onder welke omstandigheden de monitoring in overeenstemming is met de eisen die artikel 8 EVRM en artikel 10 Grondwet daaraan stellen. De monitoring moet dus met ieder van deze kaders in overeenstemming zijn. Het recht op eerbiediging van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens zijn ook opgenomen in artikelen 7 en 8 van het Handvest van de grondrechten van de EU (Handvest). Voor artikel 7 Handvest geldt dat het in principe dezelfde reikwijdte en inhoud heeft als artikel 8 EVRM.[157] Artikel 8 Handvest is uitgewerkt in de AVG en overige regelgeving.[158] Daarom is dit hoofdstuk gericht op de uitwerking die dataprivacy heeft gekregen in de AVG, op artikel 8 EVRM en artikel 10 Grondwet. In paragraaf 4.5 volgt een afsluitende beschouwing.

4.2 Algemene verordening gegevensbescherming

Sinds 25 mei 2018 is in Nederland de Algemene Verordening Gegevensbescherming van kracht geworden. Deze EU-verordening regelt, zoals uit de naam al blijkt, de bescherming van persoonsgegevens van burgers. Voordien was dit onderwerp geregeld in een Europese richtlijn en in Nederland uitgewerkt in de Wet bescherming persoonsgegevens (Wbp). Met de inwerkingtreding van de AVG is deze wet komen te vervallen en is het persoonsbeschermingsrecht in de hele EU gelijkgetrokken. Wel kent de AVG op onderdelen nog enige (nationale) uitvoeringswetgeving, die in Nederland vorm heeft gekregen in de Uitvoeringswet AVG (UAVG).

Om te kunnen vaststellen of het door gemeenten monitoren van online openbare bronnen in overeenstemming is met de AVG, dient een aantal stappen te worden doorlopen. In de eerste plaats moet het uiteraard gaan om gedragingen die vallen onder het

157 Toelichting bij artikel 7 Handvest. Zie tevens: J. Gerards, R. Nehmelman & M. Vetzo (2018). *Algoritmes en grondrechten*, Utrecht. p. 36.
158 Toelichting bij artikel 8 Handvest.

toepassingsbereik van de AVG, om zaken dus waar de AVG op ziet. Centraal in de AVG staat de *verwerking* van *persoonsgegevens*. Vastgesteld moet dus allereerst worden of sprake is van een *persoonsgegeven* als bedoeld in de AVG en of sprake is van *verwerking* daarvan. Beide zijn juridische begrippen met een eigen definitie. Is geen sprake van persoonsgegevens of van verwerking, dan stelt de AVG aan de gedragingen in kwestie verder geen eisen of voorwaarden.

Er moet sprake zijn van verwerking van persoonsgegevens, wil de AVG van toepassing kunnen zijn, maar niet alle verwerkingen van persoonsgegevens vallen binnen het toepassingsbereik van de AVG. Soms gelden voor de verwerking van persoonsgegevens met betrekking tot specifieke onderwerpen eigen, uitputtende regels. Dan is niet de AVG van toepassing maar andere regelgeving. Een belangrijke categorie in dit verband is de verwerking van persoonsgegevens door de politie (politiegegevens). Daarop is in Nederland niet de AVG van toepassing, maar de Wet politiegegevens.[159] Omdat de openbare-ordehandhaving in Nederlands deels tot de taak van de politie behoort, is dit een belangrijk aandachtspunt waarop hierna in paragraaf 4.2.1 nader wordt ingegaan.

Nadat is vastgesteld dat op een bepaalde gedraging de AVG van toepassing is, zal als tweede stap moet worden vastgesteld of die gedraging in kwestie (het online observeren dus) ook voldoet aan de eisen die in de AVG worden gesteld. Met andere woorden: als tweede stap zal de rechtmatigheid van de verwerking in het licht van de AVG moeten worden nagegaan. Allereerst eist de AVG daartoe dat voor de verwerking van gegevens een *deugdelijke grondslag* bestaat. Van de zes mogelijke grondslagen die in de AVG worden genoemd,[160] is er een van bijzonder belang voor dit onderzoek: de grondslag dat de verwerking van persoonsgegevens gebeurt door een persoon of organisatie die belast is met een publieke taak die bij wet is vastgelegd. Gekeken moet daarbij ook worden naar het doel van de gegevensverwerking. In de tweede plaats eist de AVG dan dat de verwerking van persoonsgegevens voor die wettelijke taak ook *noodzakelijk* is. In dat verband wordt gekeken naar de beginselen van *proportionaliteit* en *subsidiariteit*. Is aan deze eisen voldaan, dan is de gegevensverwerking rechtmatig (en dus toegestaan). Is daaraan niet voldaan, dan is de gegevensverwerking onrechtmatig (en dus niet toegestaan). Deze elementen worden nu stap voor stap bij langsgelopen.

4.2.1 *Toepassingsbereik AVG*

De AVG is alleen van toepassing als sprake is van de verwerking van persoonsgegevens en op die verwerking geen specifieke andere, uitputtende regels van toepassing zijn (dat wil zeggen: de gegevens moeten vallen binnen de materiële werkingssfeer van de AVG). Zowel het begrip 'persoonsgegeven' als het begrip 'verwerking' wordt in de

159 Deze is in overeenstemming gebracht met EU-richtlijn 2016/680 die op deze categorie gegevens ziet.
160 Artikel 6, eerste lid, AVG.

praktijk ruim uitgelegd. Hetzelfde geldt voor de materiële werkingssfeer. Er mag dus niet te snel worden aangenomen dat de AVG niet van toepassing is.

Onder persoonsgegevens wordt volgens de definitie van artikel 4 onder 1 AVG verstaan: 'Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.' Het moet gaan om natuurlijke personen; organisaties vallen buiten het bereik van de AVG.

Een natuurlijk persoon is *geïdentificeerd* als deze uniek van alle andere personen binnen een groep te onderscheiden is.[161] Iemand is *identificeerbaar* als deze persoon nog niet geïdentificeerd is, maar dit zonder onevenredige inspanning wel mogelijk is.[162] Voor de identificatie wordt gebruikgemaakt van zogeheten identificatoren, zoals (de combinatie van) iemands naam en adres of geboortedatum. Andere, minder directe, identificatoren zijn bijvoorbeeld iemands uiterlijke kenmerken, en zaken als beroep, inkomen of opleiding. Door deze gegevens onderling te koppelen of te combineren met andere gegevens is veelal identificatie mogelijk. Gegevens die niet tot een persoon herleidbaar zijn, kunnen niet als persoonsgegevens worden aangemerkt. Dat geldt volgens de Britse Information Commissioner's Office bijvoorbeeld voor veelvoorkomende namen als 'John Smith'. Omdat er veel personen zijn met die naam is die naam op zichzelf niet altijd een persoonsgegeven. Dat wordt het pas als het gecombineerd wordt met een andere gegevens, zoals een adres, een werkplek of telefoonnummer.[163]

Er bestaan ook online identificatoren, zoals IP-adressen, aliassen, *nicknames* en ID's van mobiele apparaten (inclusief telefoonnummers). Ook deze kunnen, al dan niet in onderlinge samenhang, als (identificerend) persoonsgegeven worden aangemerkt omdat zij identificatie mogelijk maken.[164] Ook als de naam van een persoon onbekend is, kan dus van persoonsgegevens sprake zijn. Als er een koppeling kan worden gemaakt van de bepaalde gegevens met de identificerende gegevens van een individu, gelden ook die gegevens als een persoonsgegeven. Volgens het College Bescherming Persoonsgegevens (CBP; thans de Autoriteit Persoonsgegevens ('AP')) geldt dat zelfs voor dynamische IP-adressen die worden verwerkt in combinatie met datum en tijd: 'Het maakt geen verschil dat een verantwoordelijke het IP-adres niet zal gebruiken om een persoon mee te identificeren. Het feit dat de mogelijkheid bestaat bij de verantwoordelijke of bij een derde om dit te doen, is voldoende.'[165]

---

161 Handleiding AVG, p. 24 te vinden via de website van de Autoriteit Persoonsgegevens (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf).

162 Handleiding AVG, p. 24. Zie in dit verband ABRvS 10 juni 2009, ECLI:NL:RVS:2009:BI7267, r.o. 2.4.2.

163 Information Commissioner's Office (2012), *Determining what is personal data*, P. 7, bron: Ico.org.uk.

164 A. Murray (2019). *Information Technology Law. The Law & Society, Oxford:* Oxford University Press p. 573.

165 H.R. Kranenborg & L.F.M. Verhey (2018). *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief (Mastermonografieën staats- en bestuursrecht*), Deventer: Wolters Kluwer, p. 109. Zie in dit verband ook *HvJ EU* 19 oktober 2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779. Voorts, alweer wat ouder: College bescherming persoonsgegevens, 'CBP Richtsnoeren: Publicatie van persoonsgegevens op internet', december 2007, p. 10, Autoriteitpersoonsgegevens.nl.

Met andere woorden, ook als iemand niet direct geïdentificeerd kan worden op basis van bijvoorbeeld diens naam, zal het gemeentebestuur bij online observatie moeten nagaan of op basis van de wel bekende combinatie van gegevens iemand identificeerbaar is. Is dat het geval, dan is sprake van persoonsgegevens als bedoeld in de AVG. Het hoeft daarbij overigens niet alleen te gaan om gegevens waar het gemeentebestuur al zelf over beschikt. Ook een combinatie met bijvoorbeeld via internet beschikbare openbare gegevens, kan leiden tot identificatie, en dus tot de kwalificatie als persoonsgegeven.[166] Om te bepalen of een natuurlijke persoon identificeerbaar is, moet volgens overweging 26 van de AVG rekening worden gehouden met middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van, en de tijd die benodigd is voor identificatie, waarbij de beschikbare technologie op het tijdstip van verwerking en verdere technologische ontwikkelingen in acht moeten worden genomen.[167]

De AVG is niet van toepassing op anonieme gegevens, omdat individuele mensen daarmee niet te identificeren zijn.[168] De AVG is daarentegen wel van toepassing op gepseudonimiseerde gegevens. Bij gepseudonimiseerde gegevens worden gegevens over personen verwerkt zonder dat daarbij duidelijk wordt om welke personen het gaat. Met aanvullende bronnen kunnen die personen alsnog worden geïdentificeerd. Dat is bijvoorbeeld het geval als personen in een gepseudonimiseerde lijst een nummer hebben gekregen en elders de nummering van de betreffende personen met foto's van deze mensen is opgeslagen.

In de praktijk komen geanonimiseerde gegevens niet vaak voor, omdat gegevens vaak alsnog (indirect) herleidbaar zijn tot een individu. Een voorbeeld is het publiceren van foto's van dieven met behulp van een camerabewakingssysteem. De gezichten van de dieven worden onherkenbaar gemaakt, maar er bestaat nog steeds de mogelijkheid dat deze dieven worden herkend door bijvoorbeeld vrienden of familie, omdat hun figuur, kapsel en kleding nog steeds herkenbaar zijn.[169] Anonieme gegevens worden vooral gebruikt voor statistische doelen of onderzoeksdoeleinden.[170] Bij wijze van tussencon-

166 Handleiding AVG, p. 25.
167 Overweging 26 AVG.
168 Mits deze anonieme gegevens ook niet door middel van een andere beschikbare database te de-anonimiseren zijn.
169 Article 29 Data Protection Working Party (2016). *Opinion 4/2007 on the concept of personal data*, 20 juni 2016, 01248/07/EN/WP 136, p. 21.
170 Het is niet uitgesloten dat de systemen die gebruikt worden om geautomatiseerd gegevens uit openbare online bronnen te verzamelen, vervolgens geanonimiseerd ter beschikking worden gesteld aan gebruikers. Hoewel de werkingssfeer van de AVG ruim is, is een aantal specifieke verwerkingen uitgesloten van de AVG. Voor die van de AVG uitgesloten verwerkingen gelden veelal andere, specifieke regels.

clusie kan dus worden vastgesteld dat berichten van burgers op internet gewoonlijk persoonsgegevens zullen zijn, en dat het gebruik van *nicknames* daaraan niet af doet.

Artikel 4 onder 2 AVG geeft de volgende definitie van verwerking: 'Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés.' De definitie benoemt in een niet-uitputtende opsomming wat als verwerkingshandelingen kunnen worden aangemerkt. Dat zijn het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Op grond van deze ruime definitie is dus ook het verzamelen van persoonsgegevens zonder deze op te slaan al een verwerking. Hetzelfde geldt voor de exploitant van een zoekmachine die gegevens verzamelt en die via zijn indexeringsprogramma's opvraagt, vastlegt en ordent, op zijn servers bewaart en verstrekt aan en ter beschikking stelt van zijn gebruikers in de vorm van resultatenlijsten van hun zoekopdrachten.[171] Het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, is ook als een 'geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens' aan te merken.[172] Er is al met al snel sprake van verwerking van gegevens als bedoeld in de AVG.

Artikel 2, eerste lid, van de AVG bepaalt, dat de AVG (alleen) van toepassing is als de gegevensverwerking geheel of gedeeltelijk *geautomatiseerd* is of als de handmatig verwerkte gegevens zijn opgenomen in een *bestand* of bedoeld zijn om in een bestand te worden opgenomen. Met andere woorden, als de gegevensverwerking niet geheel of gedeeltelijk geautomatiseerd is, dan moeten de handmatig verwerkte gegevens in een bestand zijn opgenomen of bedoeld zijn om daarin te worden opgenomen, anders is de AVG alsnog niet van toepassing. Aan artikel 2, eerste lid, AVG is voldaan op het moment dat een verwerkingshandeling (het verwerken, vastleggen, ordenen enzovoort) wordt uitgevoerd met behulp van een computer of andere technologisch hulpmiddel, of als de gegevens in een gestructureerde (digitale of fysieke) verzameling worden opgenomen. Het Hof van Justitie van de Europese Unie (HvJ EU) heeft geoordeeld dat persoonsgegevens die verzameld zijn voor een van-huis-tot-huisverkondiging ook onder het begrip 'bestand' vallen wanneer deze gegevens, zoals de namen, adressen en eventuele andere informatie over de personen die zijn bezocht, zijn gestructureerd. Wanneer de persoonsgegevens zijn gestructureerd, moeten deze gestructureerde gegevens ook gemakkelijk zijn terug te vinden voor later gebruik.[173] Bij het vereiste 'gestruc-

171 HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain SL*), r.o. 28.
172 HvJ EU 6 november 2003, C-101/01, ECLI:EU:C:2003:596 (*Bodil Lindqvist*), r.o. 27.
173 HvJ EU 10 juli 2018, C-25/17, ECLI:EU:C:2018:551 (*Tietosuojavaltuutettu*), r.o. 62.

tureerd geheel' moet de gegevensverwerking of de verzameling een onderlinge samenhang vertonen op grond van meer dan één kenmerk.[174] Het verzamelen van tot personen herleidbare informatie op internet is dus te beschouwen als verwerking van persoonsgegevens in de zin van de AVG.

In de systematiek van de AVG speelt ook het begrip 'verwerkingsverantwoordelijke' een belangrijke rol. Er bestaat verschil tussen de 'verwerkingsverantwoordelijke' en de 'verwerker'. De verplichtingen uit de AVG zijn in principe van toepassing op de verwerkingsverantwoordelijke. Dit is de 'natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'.[175] De verwerkingsverantwoordelijke is met andere woorden degene die vaststelt welke persoonsgegevens worden verzameld, voor welk doel dit gebeurt, en op welke wijze en met welke middelen dit plaatsvindt.[176] Het antwoord op de vraag wie verwerkingsverantwoordelijke is, kan volgen uit een expliciete juridische bevoegdheid daartoe,[177] maar kan ook blijken uit een impliciete bevoegdheid[178] of uit de feitelijke invloed van een bepaalde persoon.[179] De verwerkingsverantwoordelijke is niet alleen verantwoordelijk voor de naleving van de beginselen inzake verwerking van persoonsgegevens, maar moet die naleving ook kunnen aantonen (verantwoordingsplicht), aldus artikel 5, eerste en tweede lid AVG. In het licht van de taak tot handhaving van de openbare orde zal, waar het om de verwerking van persoonsgegevens onder de AVG gaat, de burgemeester de verwerkingsverantwoordelijke zijn. In veel gevallen kan hier echter ook sprake zijn van politiegegevens. In dat geval geldt een ander verwerkingsregime (en een andere verwerkingsverantwoordelijke), op grond van de Wet politiegegevens.

Materiële werkingssfeer en Wet politiegegevens

Hoewel de werkingssfeer van de AVG zeer ruim is, zijn bepaalde categorieën verwerkingen van de AVG uitgesloten. Voor deze verwerkingen gelden veelal specifieke eigen regels. Deze uitzonderingen zijn opgesomd in artikel 2, tweede lid, van de AVG. In het kader van dit onderzoek is vooral de in onderdeel d van dit artikel genoemde categorie van belang. Onderdeel d verklaart dat de AVG niet van toepassing is op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

174 Rb. Midden-Nederland 25 juli 2018, ECLI:NL:RBMNE:2018:3624, r.o. 4.12.
175 Artikel 4 onderdeel 7 AVG.
176 Handleiding AVG, p. 32.
177 Een voorbeeld is gegevensverwerking door de Belastingdienst, zie Handleiding AVG, p. 32.
178 Bijvoorbeeld een vereniging die gegevens van de leden registreert, of een werkgever die persoonsgegevens van zijn werknemer vastlegt, zie Handleiding AVG, p. 32.
179 Zie Handleiding AVG, p. 32.

Voor deze categorie verwerkingen van persoonsgegevens zijn de regels neergelegd in Richtlijn (EU) 2016/680. De uitwerking daarvan heeft plaatsgevonden in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).[180] Deze wetten kennen eigen regels omtrent de rechtmatigheid van de verwerking van persoonsgegevens, eigen verwerkingsverantwoordelijken, en veelal beperktere mogelijkheden tot het onderling uitwisselen van informatie tussen overheidsorganen. Voorbeelden van bevoegde autoriteiten voor wie deze bijzondere wetgeving geldt, zijn de politie, de Koninklijke Marechaussee, de rijksrecherche, de bijzondere opsporingsdiensten, officieren van justitie, strafrechters, het College van procureurs-generaal en de minister van Justitie en Veiligheid.[181]

De afbakening tussen de AVG en de Wet politiegegevens is hier bijzonder complex. Artikel 1 van de Wet politiegegevens omschrijft het begrip politiegegeven als 'elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012 (…)' (met uitzondering van twee hier niet ter zake doende situaties). Artikel 3 van de Politiewet bepaalt dat de politie tot taak heeft om in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Die daadwerkelijke handhaving van de rechtsorde kan, zo blijkt uit de artikelen 11 en 12 Politiewet 2012, worden onderscheiden in de handhaving van de openbare orde en de strafrechtelijke handhaving van de rechtsorde. Treedt de politie op ter handhaving van de openbare orde, dan staat zij onder het gezag van de burgemeester (artikel 11 Politiewet). Op grond van artikel 11, tweede lid Politiewet 2012 kan de burgemeester de betrokken ambtenaren van de politie de nodige aanwijzingen geven voor de vervulling van de in het eerste lid bedoelde taken. Hoewel het gezag over de politie dus bij de burgemeester berust voor zover de openbare-ordetaak in het geding is, zegt dat niet iets over de verantwoordelijkheid voor de omgang met persoonsgegevens. De leiding over de politieorganisatie ligt namelijk bij de korpschef. Artikel 27, eerste lid, van de Politiewet 2012 bepaalt dat de korpschef met de leiding en het beheer van de politie is belast. De korpschef is dan ook, als de politietaak in het geding is (en de Wet politiegegevens van toepassing) aangewezen als verwerkingsverantwoordelijke voor die gegevens. De regering overwoog bij de totstandkoming van de gewijzigde Wet politiegegevens – in reactie op kritische vragen van de Autoriteit Persoonsgegevens – op dit punt: "Voor wat betreft het onderscheid tussen beheer en gezag kan voorts worden opgemerkt dat de organisatorische inbedding van de gegevensverwerkingsverantwoordelijke bij het beheer van de politie – of van een bijzondere opsporingsdienst – voor de hand ligt omdat de rol van de verwerkingsverantwoordelijke betrekking heeft op de beschikbaarstelling van de middelen voor een adequate gegevensverwerking. Dit raakt aan de bedrijfsvoering van de

180 Zie voor meer informatie *Kamerstukken II* 2017/18, 34 889, 3.
181 *Kamerstukken II* 2017/18, 34 889, 3, p. 7-10.

betreffende opsporingsdienst. Daarbij ligt de nadruk meer op de middelen dan op het doel van de verwerking."[182]

Tegelijkertijd moet worden vastgesteld dat de burgemeester een eigen wettelijke grondslag heeft voor zijn taak op het terrein van de handhaving van de openbare orde, en dat hij op dat terrein ook, los van de eventuele inzet van de politie, over eigen bevoegdheden beschikt. Artikel 172, eerste lid, van de Gemeentewet bepaalt dat de burgemeester belast is met de handhaving van de openbare orde. Dit is de eigen grondslag voor deze taakopdracht. Het tweede lid voegt daaraan toe dat hij bevoegd is overtreding van wettelijke voorschriften die betrekking hebben op de openbare orde te beletten of te beëindigen, en dat hij zich daarbij bedient van de onder zijn gezag staande politie. Dit is echter slechts een deelaspect van de zorg voor de openbare orde. Artikel 172 lid 3 Gemeentewet, bijvoorbeeld, kent de burgemeester een eigen (lichte) bevelsbevoegdheid toe die hij, bij verstoring van de openbare orde, of ernstige vrees voor het ontstaan daarvan kan inzetten. Het betreft hier niet zozeer feitelijk handelen als wel het in het leven roepen van nieuwe rechtsgevolgen voor bepaalde burgers, en de bevoegdheid kan dan in beginsel ook zonder inzet van de politie worden uitgeoefend. De Gemeentewet bevat verder nog vele andere juridische bevoegdheden die de burgemeester op eigen titel kan inzetten ter handhaving van de openbare orde. Voor zover bij de (voorbereiding van de) uitoefening van die bevoegdheden persoonsgegevens worden verwerkt, is dus geen sprake van uitvoering van de politietaak, maar uitvoering van een eigen op de Gemeentewet gebaseerde taak van de burgemeester ter handhaving van de openbare orde. Is dat het geval, dan is de AVG gewoon van toepassing. De in artikel 2, tweede lid, onderdeel d genoemde uitzondering doet zich dan niet voor.

Problematisch is het dat in de praktijk deze zaken eenvoudig verweven kunnen raken. Dat leidt tot juridische onzekerheid omtrent de vraag welk rechtsregime van toepassing is, of beide rechtsregimes kunnen samenlopen, of de burgemeester door 'slim handelen' kan kiezen voor het ene dan wel het andere verwerkingsregime enzovoort. Dergelijke vragen zijn, ook gelet op de relatief recente inwerkingtreding van de AVG, in de jurisprudentie nog niet of nauwelijks aan de orde geweest, laat staan opgehelderd. Voor de online observatie in het kader van de handhaving van de openbare orde betekent een en ander dat als daarbij niet de politie (of bijzonder opsporingsambtenaren) is betrokken, maar 'gewone' gemeentelijke ambtenaren, de AVG het toepasselijke rechtsregime is. Is echter sprake van politiegegevens, omdat de politie bij de observatie een rol heeft gespeeld, dan geldt de Wet politiegegevens en is de korpschef in het kader van deze wet de bevoegde autoriteit en verwerkingsverantwoordelijke. Voor de inhoudelijke normstelling maakt dat uit. Bij uitwisseling van gegevens tussen de gemeentelijke dienst en de politie zou het dan dus ook kunnen uitmaken wie welke gegevens aan wie verstrekt; dat is met het oog op de rechtszekerheid en het legaliteitsbeginsel een onge-

182 *Kamerstukken II* 2017/18, 34 889, 3, p. 24; Autoriteit Persoonsgegevens, *Verzoek om advies ten aanzien van wetsvoorstel inzake implementatie van Richtlijn (EU) 2016/680*, 7 april 2017, Z2017-01571, p. 12.

wenste uitkomst waarvoor tot op heden geen duidelijke oplossing bestaat.[183] In het navolgende laten we de specifieke regeling van de Wet politiegegevens buiten beschouwing en richten wij ons op de AVG.

4.2.2 *Voorwaarden voor rechtmatige verwerking van persoonsgegevens*

Nadat is vastgesteld dat aan alle voorwaarden voor toepasselijkheid van de AVG is voldaan,[184] komt vervolgens de vraag aan de orde of de concrete gegevensverwerking (de online monitoring) in overeenstemming met de regels uit deze verordening geschiedt. Artikel 5 van de AVG geeft op dit punt een aantal algemene beginselen die moeten worden nageleefd. Volgens het eerste lid van dit artikel moeten persoonsgegevens:

1. worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is ('rechtmatigheid, behoorlijkheid en transparantie');
2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (…) ('doelbinding');
3. toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking');
4. juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ('juistheid');
5. worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (…) ('opslagbeperking');
6. door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ('integriteit en vertrouwelijkheid').

Allereerst de als tweede genoemde eis: de gegevensverwerking dient met het oog op een specifiek doel plaats te vinden (doelbinding). Deze doelen dienen bovendien uitdrukkelijk te zijn vastgelegd. Het is mogelijk persoonsgegevens voor meerdere doelen tegelijk te verwerken, maar dan moeten die verschillende doelen in principe elk wel-

183 Vergelijkbare discussies hebben zich in het verleden ook voorgedaan bij bijvoorbeeld het verzamelen door private ondernemingen van gegevens (bijvoorbeeld passagiersgegevens van luchtvaartmaatschappijen), die vervolgens ook aan de politie moesten worden verstrekt. Zie daarover o.a. H.R. Kranenborg & L.F.M. Verhey (2018). *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief*: Deventer: Wolters Kluwer, p. 114-118 en 121.

184 Zie over de wettelijke grondslag voor gemeentelijke bestuursorganen om inbreuk te mogen maken op het recht op privacy zoals beschermd door artikel 10 Gw hierna, paragraaf 5.4.

overwogen zijn bepaald en vastgelegd. Zijn deze doelen niet afgebakend en vastgelegd, dan is de verwerking van persoonsgegevens onrechtmatig. Vereist is dus dat, voorafgaand aan de verwerking van persoonsgegevens, vastgelegd moet worden door de verwerkingsverantwoordelijke waarvoor de persoonsgegevens nodig zijn. Een algemene omschrijving als 'ze kunnen in de toekomst nog wel eens van pas komen', is onvoldoende welbepaald.[185] Tegelijkertijd bestaat wel een zekere flexibiliteit bij de vastlegging van deze doelen. Belangrijk is vooral dat een zekere materiële omschrijving wordt gegeven van het doel waarvoor de gegevens worden verwerkt.

Artikel 5 AVG eist niet alleen dat het doel *welbepaald* en *uitdrukkelijk omschreven* is, maar ook dat het *gerechtvaardigd* is. Dit laatste betekent dat het doel moet aansluiten bij een van de grondslagen die in artikel 6 van de AVG worden genoemd.

De verwerking van persoonsgegevens is alleen rechtmatig indien en voor zover aan ten minste een van de in artikel 6, eerste lid, AVG genoemde voorwaarden is voldaan. Het betreft hier een zestal grondslagen die de verwerking van persoonsgegevens kunnen rechtvaardigen. Voor observaties van online openbare bronnen is de vijfde grondslag het meest relevant. Deze grondslag gaat over de situatie dat de verwerking 'noodzakelijk [is] voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen'. Volgens artikel 6, derde lid, AVG moet deze grondslag worden vastgesteld bij Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Grondslag vijf is dus geen zelfstandige rechtsgrondslag, maar gekoppeld aan een bepaling van nationaal of EU-recht. In het geval van observatie van online openbare bronnen met het oog op de handhaving van de openbare orde, zou die grondslag in artikel 172 Gemeentewet gevonden kunnen worden. Vereist is wel dat vastgesteld is wie deze taak uitvoert of aan wie het openbaar gezag is opgedragen (in casu: de burgemeester).[186] In de nationale bepalingen zouden specifieke begrippen kunnen worden opgenomen die de eisen van de AVG verder operationaliseren, bijvoorbeeld door nader te specificeren welke gegevens worden verwerkt, wie daarbij betrokken zijn, welk doel de verwerking precies dient, hoelang gegevens worden bewaard en hoe de gegevens mogen worden verwerkt. Artikel 6, derde lid AVG eist dat de regeling beantwoordt aan een doelstelling van algemeen belang en evenredig is aan het nagestreefde doel. Daarop doelt ook overweging 41, waarin tevens wordt verwezen naar de eisen die het EHRM stelt aan de kwaliteit van een wettelijke regeling.

Het is niet uitgesloten dat het gemeentebestuur persoonsgegevens wil verwerken voor een ander doel dan waarvoor zij aanvankelijk zijn verzameld. Volgens artikel 6, vierde lid AVG jo. overweging 50 AVG is dat toegestaan in drie situaties:

185 Handleiding AVG, p. 35.
186 Handleiding AVG, p. 39.

Het mag allereerst als er sprake is van een *verenigbaar doel*.[187] Om vast te stellen of het nieuwe doel verenigbaar is met het oorspronkelijke doel moet naar een aantal elementen worden gekeken. Allereerst naar het verband tussen beide doelen: hoe dichter zij bij elkaar liggen, hoe sneller sprake zal zijn van verenigbare doelen. In de tweede plaats moet worden gekeken naar de context waarin de persoonsgegevens zijn verzameld. Belangrijk daarbij zijn de verwachtingen die de betrokkene mocht hebben ten aanzien van het verdere gebruik van de verzamelde persoonsgegevens. Ook de aard van de persoonsgegevens is een relevant element. Betreft het gevoelige persoonsgegevens dan zullen deze veel minder snel voor een ander doel mogen worden gebruikt. In de vierde plaats spelen de mogelijke gevolgen voor de betrokkenen van verdere verwerking een rol. En als vijfde relevant element kan het al dan niet bestaan van passende waarborgen worden genoemd, zoals de mogelijkheid de persoonsgegevens te pseudonimiseren of te versleutelen voor het nieuwe gebruik. Hoe groter de waarborgen, hoe eerder sprake zal zijn van een verenigbaar doel.

1. De betrokkene heeft toestemming gegeven voor de verdere verwerking. Dat kan dus ook het geval zijn als het nieuwe doel niet met het oorspronkelijke doel verenigbaar is.
2. Op basis van een Unierechtelijke of lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de doelstellingen genoemd in artikel 23, eerste lid AVG (algemeen belang). Te denken valt aan de, voor gemeenten niet meteen heel vaak voorkomende, geval dat een verplichting voor de verwerkingsverantwoordelijke bestaat gegevens aan een overheidsorgaan (een rechter, een onafhankelijke toezichthouder, een onderzoeks- of enquêtecommissie enzovoort) te verstrekken.

Van deze gronden lijkt de eerste, voor de gemeentelijke praktijk van het observeren van online openbare bronnen met het oog op de handhaving van de openbare orde, het meest relevant te zijn. Dat betekent dat acht moet worden geslagen op de hiervoor beschreven elementen. Denkbaar is dat, voor zover het oude en het nieuwe doel beide uitwerkingen zijn van de taak de openbare orde te handhaven, daarin een aanwijzing kan worden gevonden dat de beide doelen niet al te ver uit elkaar liggen en een zekere verwantschap vertonen. Echter zal ook dan moeten worden gekeken naar de overige genoemde elementen. In box 1 volgt een korte juridische reflectie op de in hoofdstuk 3 waargenomen informatie-uitwisseling bij informatie die soms voor andere doelen is verzameld dan waarvoor die uiteindelijk wordt gebruikt.

187 B.W. Schermer, D. Hagenauw, & N. Falot (2018) *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, Ministerie van Justitie en Veiligheid, p. 35.

Box 1. Juridische reflectie op empirische gegevens over doelstellingen en informatie-uitwisseling.

In de praktijk van de gemeentelijke observatie van online openbare bronnen kan het voorkomen dat informatie die bijvoorbeeld door een afdeling Webcare of Communicatie is verzameld met het oog op een goede gemeentelijke dienstverlening, wordt doorgegeven aan de afdeling die verantwoordelijk is voor het monitoren van dreigende aantasting en van de gemeentelijke openbare orde. In zo'n situatie is sprake van verwerking van persoonsgegevens voor een ander doel dan waarvoor zij werden verzameld. Dan zullen in het concrete geval dus de hiervoor onder punt 1 genoemde elementen moeten worden langsgelopen om vast te stellen of sprake is van verwerking met een verenigbaar doel. Uiteraard helpt het daarbij als expliciet ook die gegevensverwerking in het kader van de handhaving van de openbare orde duidelijk is geëxpliciteerd. Duidelijke normen op dit punt op basis van recente jurisprudentie zijn er (nog) niet.

Vereist is ten slotte dat de gegevensverwerking ook noodzakelijk is voor de taak die in het algemeen belang of voor de uitoefening van het openbaar gezag wordt verricht.[188] Deze noodzakelijkheidseis volgt rechtstreeks uit de tekst van de grondslagen genoemd in artikel 6 AVG. 'Noodzakelijk' betekent dat de verwerking een doelgerichte en evenredige manier moet zijn om het doel te bereiken.[189] De noodzakelijkheid van de verwerking moet worden getoetst aan de beginselen van *proportionaliteit* en *subsidiariteit* (zie daarover ook de volgende paragraaf). Het proportionaliteitsbeginsel houdt in dat het doel van de verwerking van de persoonsgegevens in verhouding moet staan tot de inbreuk die op de privacy wordt gemaakt. Het subsidiariteitsbeginsel houdt in dat steeds de minst ingrijpende weg moet worden bewandeld om het gestelde doel te bereiken. Als er een andere redelijke en minder ingrijpende manier is om hetzelfde resultaat te bereiken, bijvoorbeeld zonder de verwerking van persoonsgegevens, dan moet daarvoor gekozen worden.

Toezicht op de naleving: functionaris voor de gegevensbescherming
Het toezicht op de naleving van de AVG berust bij de Autoriteit Persoonsgegevens (AP). Dat is echter niet de enige toezichthouder. In de praktijk kent de AVG een belangrijke rol toe aan een interne toezichthouder, de *Functionaris Gegevensbescherming* (FG). Overheidsinstanties zijn verplicht een FG aan te stellen (artikel 37 AVG). Binnen de gemeente heeft de FG een onafhankelijke positie.

Artikel 38, eerste lid, AVG bepaalt dat de verwerkingsverantwoordelijke en de verwerker ervoor moeten zorgen dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden. De FG heeft niet alleen tot taak

188 'Public task', *Information Commissioner's Office*, bron: Ico.org.uk en H.R. Kranenborg & L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief (Mastermonografieën staats- en bestuursrecht*), Deventer: Wolters Kluwer 2018, p. 154.
189 Ibid.

te informeren en adviseren over zaken met betrekking tot de verwerking van persoonsgegevens, maar ook de taak toe te zien op de naleving van de AVG.

Als de gegevensverwerking een hoog privacyrisico oplevert voor diegenen van wie de persoonsgegevens verwerkt worden, verplicht de AVG bovendien tot een *gegevensbeschermingseffectbeoordeling* of Data Privacy Impact Assessment (DPIA of PIA). Daarmee kunnen vooraf de privacyrisico's van een gegevensverwerking in kaart worden gebracht.

4.2.3 *Conclusie: AVG en observatie van online openbare bronnen*

Wat betekent het voorgaande nu voor de praktijk van het observeren van online openbare bronnen ten behoeve van de handhaving van de openbare orde?

a) Een eerste belangrijke vaststelling is dat het feit dat het gaat om gegevens uit openbare bronnen, niet afdoet aan de verplichtingen uit de AVG. Gemeentebesturen hebben dus ook bij het gebruik van gegevens uit openbare bronnen de verplichting na te gaan of de in de AVG gestelde regels van toepassing zijn, en zo ja, of daaraan in het concrete geval wordt gedaan.
b) In het verlengde daarvan ontslaat ook het gebruik van geautomatiseerde systemen als OBI4wan enzovoort gemeentebesturen niet van de verplichting zelfstandig na te gaan of aan de wettelijke eisen wordt voldaan.
c) Het toepassingsbereik van de AVG is ruim; er is al snel sprake van het verwerken van gegevens in de zin van de AVG, zelfs als die gegevens niet verder worden opgeslagen of doorgegeven, terwijl ook het begrip persoonsgegevens ruim moet worden uitgelegd. Ook als het gegevens betreft die niet al tot concrete personen herleidbaar zijn, dient het bestuursorgaan na te gaan of door koppeling van gegevens alsnog een natuurlijk persoon te identificeren is. Is dat het geval dan is toch sprake van persoonsgegevens in de zin van de AVG. Daarvan zal al snel het geval zijn. Op dit punt wordt van gemeentebesturen voor zover verder nodig ook een actieve onderzoekshouding verwacht.
d) Het pseudonimiseren doet niet af aan de kwalificatie als persoonsgegeven in de zin van de AVG. Op grond van het uitgangspunt van *privacy by design* dient pseudonimiseren evenals het minimaliseren van het gebruik van persoonsgegevens het uitgangspunt te zijn. Als tot anonimisering kan worden overgegaan en het achterliggende doel daarmee kan worden bereikt, dient die weg te worden bewandeld. Verwerking van persoonsgegevens lijkt dan niet noodzakelijk voor het bereiken van het gestelde doel.
e) Bijzondere aandacht vraagt de relatie tot de politie wanneer deze betrokken is bij gegevensverwerking ter handhaving van de openbare orde. Betrokkenheid van de politie bij deze openbare-ordetaak van de burgemeester bepaalt of het rechtsregime van de AVG van toepassing is dan wel dat van de Wet politiegegevens. De inhoudelijke normstelling van beide regelingen is niet hetzelfde. Met name waar het om

onderlinge gegevensuitwisseling gaat, dient zeer zorgvuldig naar de toepasselijke wettelijke regels te worden gekeken. Voor zover de politie niet betrokken is (wat vaak het geval zal zijn), is de AVG van toepassing; het gemeentebestuur is dan verwerkingsverantwoordelijke.

f) Artikel 6, eerste lid, grondslag 5 AVG biedt in combinatie met artikel 172 Gemeentewet (of een andere specifieke openbare-ordebepaling in de Gemeentewet) een wettelijke grondslag voor observatie van online openbare bronnen ter handhaving van de openbare orde. Wel dient die grondslag is samenhang te worden beschouwd met het beoogde doel van de online observatie.
g) Het doel dat met het oberveren van online openbare bronnen wordt nagestreefd, dient nauwkeurig omschreven te zijn ('welbepaald') en vooraf uitdrukkelijk te worden vastgelegd. Tot op zekere hoogte is transparantie op dit punt een vereiste, al valt uit de jurisprudentie niet precies af te leiden hoever deze verplichting in concrete gevallen reikt.
h) Het gebruik van gegevens voor een ander doel dan waarvoor zij verzameld zijn, vraagt hetzij een specifieke wettelijke grondslag of toestemming van betrokkenen, dan wel gebruik voor een met het oorspronkelijke doel verenigbaar nieuw doel. Daarbij moet worden gemotiveerd waarom het nieuwe doel met het oorspronkelijke doel verenigbaar is. Dit is van belang wanneer gegevens voor een ander hoofddoel dan de handhaving van de openbare orde zijn verzameld, maar de inhoud ervan reden geeft ze wel voor dat nevendoel te gebruiken.
i) Verwerking van persoonsgegevens is onrechtmatig als het gestelde doel ook op andere wijze, dus zonder dat van verwerking sprake is, kan worden bereikt. De mate waarin inbreuk wordt gemaakt op de bescherming van persoonsgegevens en de privacy, dient in overeenstemming te zijn met het belang dat die inbreuk dient.
j) Het is verplicht de functionaris gegevensbescherming te betrekken bij de gemeentelijke observatie van online openbare bronnen. Ook kan een Data Privacy Impact Assessment (PIA) verplicht zijn als de verwerking van persoonsgegevens een hoog privacyrisico oplevert.

4.3 Artikel 8 EVRM

Of de monitoring van online openbare bronnen in overeenstemming is met de eerbiediging van de persoonlijke levenssfeer kan worden beoordeeld aan de hand van artikel 8 EVRM en artikel 10 Grondwet. Beide artikelen beschermen het recht op eerbiediging van de persoonlijke levenssfeer, maar de wijze waarop zij dat doen, verschilt.

Het Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden, kortweg EVRM, is een verdrag dat na de Tweede Wereldoorlog tot stand kwam in het kader van de Raad van Europa. Nederland is partij bij dat verdrag. Het verdrag codificeert een aantal belangrijke mensenrechten. Juridische geschillen daarover worden in laatste instantie beslecht door het Europees Hof voor de Rechten van de Mens (EHRM) in Straatsburg. De bepalingen uit het EVRM kunnen in Nederland door burgers bij de

nationale rechter worden ingeroepen en Nederlandse wetgeving dient in overeenstemming te zijn met deze verdragsbepalingen. In de praktijk is de jurisprudentie van het EHRM van groot belang: in die jurisprudentie zijn tal van nadere rechtsnormen ontwikkeld die ter bescherming van de genoemde grondrechten door nationale overheden in acht moeten worden genomen.

De beoordeling aan de hand van artikel 8 EVRM vindt plaats in paragraaf 4.3.1 en geschiedt in een aantal stappen. De eerste stap is te bepalen of sprake is van een gedraging die inbreuk maakt op artikel 8 EVRM. Als dat niet het geval is, valt de gedraging buiten de reikwijdte van artikel 8 EVRM en is die daarmee dus ook niet in strijd. Als wel sprake is van een inbreuk, kan die inbreuk wellicht gerechtvaardigd worden. Of dat het geval is, hangt af van het bestaan van een grondslag voor die gedraging die bij wet is voorzien, het doel van de gedraging, en van de beoordeling van de gedraging als 'noodzakelijk' in een democratische samenleving' (paragraaf 4.3.2 en 4.3.3). In paragraaf 4.4 wordt vervolgens besproken of de monitoring van online openbare bronnen in overeenstemming is met artikel 10 Grondwet.

4.3.1 *Reikwijdte en inbreuk: onder welke omstandigheden kan het monitoren van openbare bronnen een inmenging vormen in de persoonlijke levenssfeer?*

Er kan geen sprake zijn van een inbreuk op de persoonlijke levenssfeer als het gaat om monitoring die volledig geanonimiseerd geschiedt. Het kan bijvoorbeeld gaan om openbare online bronnen die worden verwerkt zonder dat daarbij foto's van gezichten, online aliassen of adres- of precieze locatiegegevens worden verwerkt. Technologische hulpmiddelen die berichtgeving op sociale media geanonimiseerd kunnen verwerken en waarvan de output is ontdaan van tot personen herleidbare informatie, maken dan ook geen inbreuk op de persoonlijke levenssfeer. Ook het opslaan van die informatie levert dan geen problemen op met artikel 8 EVRM. In zoverre geldt voor de verhouding van monitoring in online openbare bronnen tot artikel 8 EVRM dus hetzelfde als in relatie tot de AVG: geen van beide kaders is van toepassing op anonieme, dus niet tot personen herleidbare gegevens.

Als wel sprake is van tot personen herleidbare informatie, moet worden beoordeeld of de monitoring inbreuk maakt op (of: een inmenging vormt in) het recht op eerbiediging van de persoonlijke levenssfeer. Er is jurisprudentie van het EHRM over observatiemethoden en de persoonlijke levenssfeer die aanknopingspunten biedt voor de beantwoording van de vraag of monitoring een inbreuk maakt op de persoonlijke levenssfeer en of die inbreuk kan worden gerechtvaardigd. De meeste jurisprudentie van het EHRM gaat echter niet over *online* openbare bronnen, maar over het offline publieke domein. Er is voor gekozen om een vertaling te maken van de factoren naar monitoring van online openbare bronnen en denken dat de jurisprudentie bruikbare inzichten oplevert in de bescherming die artikel 8 EVRM biedt tegen inbreuken die

online worden gemaakt op de persoonlijke levenssfeer.[190] Tegelijkertijd kan constateert worden dat die vertaalslag allerlei principiële vragen oproept. Die principiële vragen zijn niet alleen van juridische aard. Bijvoorbeeld: in hoeverre verschillen gedragingen of uitingen van mensen in de offline openbare ruimte van gedragingen en uitingen in online openbare bronnen? Meer specifiek: kun je zeggen dat uitingen in de offline openbare orde onvermijdelijk zijn, al was het voor woon-werkverkeer, het onderhouden van sociale contacten en recreatie, terwijl aan uitingen in online openbare bronnen een duidelijker keuze van de betrokkene ten grondslag ligt? Of is dat irrelevant, omdat ook online aanwezigheid steeds meer bij het normaal maatschappelijk leven hoort?

Naar vaste jurisprudentie kan aan de omstandigheid dat een uiting in het openbaar is gedaan, niet de conclusie worden verbonden dat geen sprake is van een inbreuk.[191] Daaraan ligt de gedachte ten grondslag dat artikel 8 EVRM mede het recht omvat een identiteit te hebben, zich persoonlijk te ontwikkelen en relaties met anderen aan te gaan. Er is daarom 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'.[192] Daarop kan met monitoring in de openbare ruimte onder omstandigheden inbreuk worden gemaakt.

In welke gevallen monitoring inbreuk maakt op de persoonlijke levenssfeer, hangt af van meerdere factoren. Die factoren worden in onderlinge samenhang door het EHRM beoordeeld. Uit jurisprudentie van het EHRM blijkt dat dit de belangrijkste factoren zijn:

1. Welke verwachtingen mag een burger in de gegeven omstandigheden redelijkerwijs hebben van zijn of haar privacy?
2. Worden online uitlatingen bekeken, of gekopieerd en opgeslagen?
3. Als gegevens worden gekopieerd of opgeslagen, hoelang worden de gegevens bewaard?
4. Waarvoor worden de gegevens gebruikt? Welke gevolgen heeft de verwerking van de gegevens voor de betrokkene?
5. Wordt een compilatie gemaakt van gegevens over een specifiek individu?
6. Worden gegevens gedeeld met de media of het algemene publiek?

De eerste factor gaat over de verwachtingen die een burger redelijkerwijs mag hebben van zijn of haar privacy. De impact van deze factor kan worden gerelativeerd: deze verwachtingen zijn niet zonder meer beslissend voor de vraag of sprake is van een inbreuk. In jurisprudentie wordt het voorbeeld gegeven van iemand die over straat loopt. Over het algemeen kan iemand in het openbaar redelijkerwijs weinig privacy verwach-

190 Zie bijvoorbeeld ook Koops et al. (2018) en Oerlemans (2017) die ons hierin zijn voorgegaan.
191 Bijvoorbeeld: EHRM 12 januari 2010, 4158/05 (*Gillan en Quinton t. VK*), rov. 61; EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 43; EHRM 28 januari 2003, 44647/98 (*Peck t. VK*), rov. 57; EHRM 25 september 2001, 44787/98 (*P.G. en J.H. t. VK*), rov. 56.
192 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 43.

ten te genieten. 's Nachts, in een verlaten straat kan iemand mogelijk al wat meer privacy verwachten.[193] Die persoon weet dat hij of zij op dat moment zichtbaar is voor iedereen die daar op dat moment ook is, onder wie eventuele politieagenten of gemeentelijke ambtenaren. Daarmee acht het EHRM vergelijkbaar dat een beveiliger (of een politieagent of een gemeentelijk ambtenaar) via een gesloten camerasysteem mee kan kijken. Het via een gesloten systeem meekijken op schermen leidt dus volgens het EHRM niet tot een inmenging.[194] Volgens ons zal dat ook gelden voor het realtime meekijken met berichten op sociale media, zoals gebeurt tijdens evenementen. Medewerkers van de gemeente, vaak van de afdeling Communicatie, volgen de berichtgeving en kunnen het aan andere medewerkers doorgeven als meerdere berichten erop wijzen dat (bijvoorbeeld) stromen bezoekers omgeleid moeten worden of fietsenstallingen niet goed te vinden zijn. We gaan er daarbij van uit dat geen tot personen herleidbare gegevens worden opgeslagen. Iets lastiger ligt het al bij berichtgeving op openbare sociale media. Het ligt voor de hand om in beginsel aan te nemen dat wie een bericht plaatst op openbare sociale media of deelneemt aan een discussie op een openbaar forum, geacht mag worden zich ervan bewust te zijn dat zijn of haar bijdrage door een onbegrensde groep mensen te bekijken is, in de meeste gevallen ook nog lange tijd na het posten van het bericht. Sterker: het kan zelfs iemands *bedoeling* zijn om de uiting onder de aandacht van een onbegrensd breed publiek te brengen.

Een gedetailleerder blik op de verwachte privacy laat echter zien dat de situatie ingewikkelder kan zijn. Met welk doel heeft iemand een uiting gedaan? Gaat de uiting alleen over die betrokkene zelf of ook over anderen, bijvoorbeeld doordat een foto wordt gedeeld waarop ook andere mensen staan en, als dat zo is, is niet ook hun verwachting van privacy relevant? Als iemand kon verwachten dat 'eenieder' kan meekijken, kon diegene dan ook verwachten dat ook bestuursorganen belangstelling hebben voor die informatie, en die misschien zelfs wel kopiëren en bewaren? Daarnaast speelt voor wat betreft de monitoring door de gemeente volgens ons ook hier een rol in hoeverre de gemeente naar burgers open is over die monitoring. De veelheid van factoren die invloed kunnen hebben op de verwachtingen die iemand redelijkerwijs kan hebben van zijn of haar privacy maken van deze eerste factor een lastige factor om algemene en heldere lijnen te trekken over wat wel en niet is toegestaan.

Volgens jurisprudentie van het EHRM 'kan? dient?' alsnog sprake zijn van een inbreuk als er opnames worden gemaakt, vooral gelet op 'the systematic or permanent nature of the record'.[195] In de lijst hiervoor is dat de tweede factor die moet worden betrokken

193 EHRM 28 januari 2003, 44647/98 (*Peck t. VK*), rov. 62.

194 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 44, welke uitspraak ging over gps-tracking van een auto voor een periode van drie maanden; EHRM 28 januari 2003, 44647/98 (*Peck t. VK*), rov. 59; EHRM 25 september 2001, 44787/98, (*P.G. en J.H. t. VK*), rov. 57. Zie ook: EHRM 17 juli 2003, 63737/00 (*Perry t. VK*), rov. 38.

195 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 44, welke uitspraak ging over gps-tracking van een auto voor een periode van drie maanden; EHRM 28 januari 2003, 44647/98 (*Peck t. VK*), rov. 59; EHRM 25 september 2001, 44787/98, (*P.G. en J.H. t. VK*), rov. 57.

bij de beantwoording van de vraag of monitoring in een concreet geval een inbreuk kan vormen op het privéleven in de zin van artikel 8 EVRM. In het voornoemde voorbeeld van een gesloten camerasysteem, waarbij de camera's gericht zijn op een openbare plaats zoals een winkelstraat, betekent dat dat de opslag van het beeldmateriaal alsnog kan leiden tot een inbreuk. In de woorden van het EHRM: 'Public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities.'[196] Dat geldt temeer waar het informatie betreft die betrekking heeft op iemands verleden.[197] Voor online monitoring is dat relevant. Het bevestigt dat als informatie niet alleen wordt bekeken, maar als ook dossiers worden opgebouwd, eerder sprake is van een inbreuk. Vanuit dat oogpunt is het positief dat een kwart van de gemeenten van uitingen in online openbare bronnen geen kopieën opslaat.[198] Voor zover al informatie wordt opgeslagen, is het op grond van het derde criterium ook relevant hoelang die informatie wordt bewaard. Een complicatie bij deze factoren is dat weinig bekend is over hoe de tools die gemeenten gebruiken bij online monitoring, *precies* werken. Uit hoofdstuk 3 blijkt dat veel gemeenten gebruikmaken van de diensten van private partijen. Die private partij kan door middel van *crawlen* gegevens verzamelen, opslaan, verwerken tot de output die aan een gemeente ter beschikking wordt gesteld. Als de gemeente die output niet bewaart, is dat vanuit privacyoogpunt positief, maar laat dat onverlet dat ook die private partijen inbreuk kunnen maken op de persoonlijke levenssfeer.

Ook de aard van de verzamelde gegevens heeft invloed op de vraag of sprake is van een inbreuk. Zo heeft het EHRM onderkend dat het volgen van een persoon door een gps-tracker op een auto minder ingrijpend is dan veel andere surveillancemethoden, omdat het minder gegevens oplevert. Andere surveillancemethoden, zoals met camera's en telefoontaps, kunnen meer van iemands gedragingen, opvattingen en gevoelens prijsgeven.[199] In die zaak was er echter toch sprake van een inbreuk. Onder verwijzing naar de periode waarover gegevens waren verzameld (drie maanden) en het gebruik van de gegevens (opgeslagen in het dossier over de betrokkene om een beeld van diens bewegingen te krijgen, nader onderzoek op de plekken die hij had bezocht en gebruik van de gegevens in de strafrechtelijke procedure tegen de betrokkene) heeft het EHRM alsnog geconcludeerd dat sprake was van een inbreuk.[200] Verder wordt geschreven tekst bijvoorbeeld als minder ingrijpend beschouwd dan foto's van (herkenbare) personen, en worden foto's van (herkenbare) personen weer als minder ingrijpend gezien dan videomateriaal.[201] Over foto's heeft het EHRM wel gezegd dat iemand beeltenis 'one of the chief attributes [is] of his or her personality, as it reveals the person's unique

196 EHRM 4 mei 2000, 28341/95 (*Rotaru t. Roemenië*), rov. 43. Zie ook EHRM 17 juli 2003, 63737/00 (*Perry t. VK*), rov. 41.
197 EHRM 4 mei 2000, 28341/95 (*Rotaru t. Roemenië*), rov. 43.
198 Zie paragraaf 3.5.2.
199 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 52.
200 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 51.
201 EHRM 7 februari 2012, 40660/08 en 60641/08 (*Von Hannover t. Duitsland (nr. 2)*), rov. 96.

characteristics and distinguishes the person from his or her peers'.[202] Dat betekent niet dat *iedere* foto of video waarop iemand herkenbaar in beeld is, zonder meer een inbreuk op de persoonlijke levenssfeer vormt. Het maakt uit waarvoor het beeldmateriaal wordt gebruikt. Het EHRM heeft bijvoorbeeld weleens geoordeeld dat het maken van foto's door de politie tijdens een demonstratie geen inmenging vormde, omdat de foto's alleen werden gemaakt om de politie te ondersteunen bij het managen van de betreffende demonstratie. De foto's zijn dus niet gebruikt om demonstranten te identificeren.[203] Als dat wel het geval was geweest, of als de foto's met de media zouden worden gedeeld, zou dat waarschijnlijk anders zijn.[204] Hetzelfde geldt als informatie openbaar wordt op een wijze die niet door de betrokken burger kon worden voorzien.[205] Voor monitoring in online openbare bronnen is die jurisprudentie ook relevant. In paragraaf 3.4 zijn de doelstellingen van online monitoring besproken. Monitoring kan het algemene doel hebben de informatiepositie van de gemeente te verbeteren, te 'weten wat er speelt', of zijn gericht op het bewaken van de openbare orde. Binnen de monitoring met het oog op de openbare orde verschilt de mate waarin de monitoring is gericht op individuele personen of groepen personen. Dat kan het genuanceerde verschil zijn tussen het volgen van de uitlatingen van individuele leden van een actiegroep tegen Zwarte Piet, met het oog op de aanstaande Sinterklaasintocht, of het inwinnen van informatie over hoe het algemene publiek zich zoal over Zwarte Piet uitlaat, met het oog op diezelfde intocht. Bij deze laatste categorie is minder snel sprake van een inbreuk, vooral niet zolang het bestuursorgaan de gegevens niet gebruikt om betrokken personen te identificeren (of anderszins belangstelling heeft voor deze specifieke personen) en de gegevens niet deelt met derden. In het eerste geval hebben individuele personen de aandacht van de gemeente. Een inbreuk zal snel aan de orde zijn als het een gemeenteambtenaar opvalt dat in online discussies steeds dezelfde naam naar voren komt. De ambtenaar kan dan belangstelling krijgen voor die persoon en doorklikken naar het profiel van die persoon. Als vuistregel kan worden aangenomen dat, zodra de monitoring zich richt op individuele personen, er sprake is van een inbreuk op het privéleven van de betrokkene.[206] Daarbij maakt het uit of de betrokkene gezien kan worden als een 'public figure'.[207] Oorspronkelijk werd met dit begrip vooral gedoeld op politici, maar inmiddels is in jurisprudentie aanvaard dat ook journalisten, bekende academici, acteurs en muzikanten en media-persoonlijkheden publieke figuren kunnen zijn.[208] Dat het EHRM in de loop der tijd steeds meer personen als 'publiek

202 EHRM 7 februari 2012, 59320/00 (*Von Hannover t. Duitsland (no.2)*), rov. 96.
203 EHRM 26 januari 1995, 15225/89 (*Friedl t. Oostenrijk*). Vgl. EHRM 17 juli 2003, 63737/00 (*Perry t. VK*), rov. 41.
204 Zie bijvoorbeeld de in EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 47 genoemde voorbeelden.
205 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 47; EHRM 28 januari 2003, 44647/98 (*Peck t. VK*), rov. 60-63.
206 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 46.
207 EHRM 7 februari 2012, 40660/08 en 60641/08 (*Von Hannover t. Duitsland (nr. 2)*), rov. 95.
208 Hughes, K. (2019). The Public Figure Doctrine and the Right to Privacy, *Cambridge Law Journal*, march 2019, p. 73-78.

figuur' heeft aangemerkt, heeft geleid tot enige onduidelijkheid over en (daardoor) onvoorspelbaarheid van dat begrip.[209] Het volgen van een publiek figuur zal betekenen dat met het volgen minder snel sprake is van een inbreuk en (vooral) dat aan een eventuele inbreuk minder gewicht wordt toegekend. Aan deze jurisprudentie kunnen argumenten worden ontleend om (bijvoorbeeld) de uitlatingen van de voorzitter van een actiegroep te volgen op socialemedia-accounts, waarop die voorzitter zich nadrukkelijk als zodanig afficheert, en dat minder snel als inbreuk te zien of die inbreuk eerder gerechtvaardigd te achten. In box 2 volgt een korte juridische reflectie op gemeentelijke webcare en de voorzienbaarheid ervan.

Box 2. Juridische reflectie op webcare en voorzienbaarheid.

Uit paragraaf 3.2 blijkt dat bijna de helft van de gemeenten als service aan bewoners en bezoekers webcare aanbiedt. Als iemand in een openbaar bericht een vraag stelt aan de gemeente door de gemeente te taggen ('Wanneer is er weer koopzondag, @gemeente_Assen?'), reageert de gemeente daarop. Burgers die de gemeente op deze openbare manier benaderen, verwachten dat de gemeente, of anders een andere twittergebruiker, zal reageren op de vraag. Bij deze manier van communiceren met burgers is in beginsel geen sprake van een inbreuk op de persoonlijke levenssfeer. Dat kan anders zijn als de gemeente pogingen doet om een beeld te krijgen van de twitteraar, bijvoorbeeld door in andere bronnen gegevens over die persoon te zoeken.

4.3.2 *Tussenconclusie*

Mag wat openbaar is vrijelijk door de gemeente gebruikt worden? Nee: monitoring kan ook tot een inbreuk op artikel 8 EVRM leiden als die zich tot openbare bronnen beperkt. Als helemaal niet wordt gewerkt met tot personen herleidbare informatie, kan een inbreuk op het privéleven niet aan de orde zijn. Voor zover binnen een gemeente wordt gemonitord met het oogmerk meer te weten te komen over 'wat er speelt', zonder dat dit per se over de openbare orde gaat, liggen er dus kansen om dat op een 'EHRM-proof' manier te doen door gebruik te maken van anonimiserende technologieën. Ook als wel gegevens worden verwerkt waarin tot personen herleidbare gegevens zijn opgenomen, hoeft dat niet zonder meer te betekenen dat sprake is van een inbreuk. Naar onze inschatting zal een rechter waarschijnlijk oordelen dat geen sprake is van een inbreuk als van de monitoring geen verslagen worden opgeslagen, als binnen de gemeente geen belangstelling bestaat voor individuele personen (bijvoorbeeld: er worden geen pogingen ondernomen om eventuele aliassen te achterhalen, of om bijdragen van één persoon op verschillende platformen aan elkaar te verbinden, of om groepen in kaart te brengen), en de gegevens worden niet met derden gedeeld, ook niet met de politie.

209 Hughes, K. (2019).

De op specifieke personen gerichte monitoring is, gelet op artikel 8 EVRM, potentieel het meest problematisch. Het volgen van een specifieke persoon zal in de meeste gevallen een inbreuk vormen, evenals het ondernemen van een poging om een sociaal netwerk rond een persoon, locatie of onderwerp in kaart te brengen. Dat is het duidelijkst als die gegevens ook worden opgeslagen of gedeeld, maar geldt ook als dat niet wordt gedaan. Als (mogelijk) sprake is van een inbreuk is daarmee nog niet gezegd dat het verzamelen van gegevens onrechtmatig is. Een inbreuk kan worden gerechtvaardigd indien die voldoet aan de eisen die artikel 8 EVRM aan een beperking stelt.

4.3.3 *Bestaat voor de monitoring een adequate wettelijke grondslag?*

Voor de gevallen waarin de monitoring (mogelijk) inbreuk maakt op de persoonlijke levenssfeer, is de vervolgstap of die inbreuk gerechtvaardigd kan worden. Een inbreuk op artikel 8 EVRM kan worden gerechtvaardigd als die voldoet aan drie eisen. De eerste eis is dat de inmenging bij wet moet zijn voorzien. In deze paragraaf staat die eis centraal. In paragraaf 4.3.3 worden de andere twee vereisten besproken.

In enquêtes en interviews hebben meerdere respondenten en geïnterviewden gesproken over de 'stelselmatigheid' van de monitoring. Dat gaat over deze tussenstap. Als sprake is van 'stelselmatige' monitoring, worden hogere eisen gesteld aan de wettelijke grondslag van de monitoring. Om iets te kunnen zeggen over de eisen aan monitoring van online openbare bronnen stelt, is ten eerste de jurisprudentie van het EHRM zelf van belang, en ten tweede de jurisprudentie van de nationale rechter waarin die jurisprudentie van het EHRM naar het Nederlandse bestuurs- en strafrecht is vertaald.

Het EHRM toetst de toegankelijkheid en voorzienbaarheid van wetgeving. Als de inmenging een grondslag heeft in wet- of regelgeving is de toegankelijkheid daarvan in orde als publicatie in het *Staatsblad* of de *Staatscourant* heeft plaatsgevonden. In het kader van de voorzienbaarheid worden meer materiële eisen aan de wetgeving gesteld. De wettelijke regeling moet voldoende duidelijk zijn om burgers een adequate indicatie te geven van de voorwaarden waaronder en omstandigheden waarin autoriteiten bevoegd zijn om die surveillancemethoden in te zetten. De voorzienbaarheid vereist in de context van 'covert measures of surveillance' niet dat een burger moet kunnen voorspellen wanneer het waarschijnlijk is dat hij of zij onderworpen zal worden aan surveillancemethoden en daarop zijn of haar gedrag kan aanpassen.[210] Heldere en gedetailleerde regels over surveillancemethoden kunnen over het algemeen onontbeerlijk ('essential') worden geacht, temeer omdat de technologieën die in dat kader gebruikt worden steeds verfijnder (en effectiever) worden.[211]

---

210 EHRM 13 september 2018, 58170/13 e.a. (*Big Brother Watch e.a. t. VK*), rov. 306 (in afwachting uitspraak Grand Chamber, laatstelijk gecontroleerd 30 november 2020). Zie ook: EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 61; EHRM 2 augustus 1984, 8691/79 (*Malone t. VK*), rov. 67.

211 O.a.: EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 61; EHRM 16 februari 2000, 27798/95, (*Amann t. Zwitserland*), rov. 56.

In uitspraken van het EHRM over heimelijke surveillancemethoden in het kader van een strafrechtelijk onderzoek zijn criteria ontwikkeld waaraan de wet- of regelgeving moet voldoen.[212] Het EHRM heeft deze criteria ook toegepast in casus over de onderschepping van communicatie in het kader van de nationale veiligheid, waaronder in gevallen waarin het ging om 'bulk interception' aan de hand van trefwoorden.[213] Volgens het EHRM brengt het heimelijke karakter van de handelingen een risico met zich mee dat een stelsel, dat is bedoeld om de nationale veiligheid te beschermen, een democratie kan ondermijnen of zelfs vernietigen, terwijl de bedoeling is die te beschermen. Daarom zijn ook waarborgen tegen misbruik belangrijk en beoordeelt het EHRM ook of bij aanvang van, tijdens of na afloop van de surveillance 'review and supervision' van de surveillance plaatsvindt, en of die wordt uitgeoefend door een rechterlijke instantie.[214] De criteria die zijn geformuleerd in uitspraken die gaan over het onderscheppen van *vertrouwelijke* informatie, gelden *niet* onverkort voor openbare bronnen. Monitoring in openbare bronnen zal in het algemeen geacht worden een minder ingrijpende inbreuk te maken op de persoonlijke levenssfeer dan het onderscheppen van vertrouwelijke informatie.[215] Niettemin onderzoekt het EHRM ook in die gevallen of er adequate en effectieve waarborgen tegen misbruik bestaan. Daarbij slaat het EHRM acht op alle omstandigheden van de zaak, waaronder de aard, reikwijdte en duur van de maatregel, de grondslag die nodig is om de maatregel in te zetten, de autoriteiten die de inzet toestaan, uitvoeren en daarop toezicht houden, en de aard van de 'remedy' die nationaal recht biedt.[216]

De eisen die worden gesteld aan de wettelijke grondslag voor een inbreuk van een grondrecht, hangen dus af van de ernst van de inbreuk. Dat is door de Centrale Raad van Beroep (CRvB) nader geoperationaliseerd. Met die jurisprudentie heeft de bestuursrechter aangesloten bij de strafrechtelijke jurisprudentie die er al over dit onderwerp was.[217] In een uitspraak van 15 maart 2016 heeft de CRvB overwogen dat de toenemende technische verfijning en intensivering van opsporingsmethoden en -technieken een meer concreet omschreven legitimatie verlangen voor inmengingen in het fundamentele recht op bescherming van privéleven.[218] Monitoring die gezien kan worden als 'stelselmatig', zoals in de regel bij het inzetten van een peilbaken of heimelijk geplaatste camera het geval is, vindt geen adequate grondslag in de algemene bevoegdheid om in het kader van de sociale zekerheid de juistheid en volledigheid van verstrekte gegevens te controleren. In het

212 EHRM 13 september 2018, 58170/13 e.a. (*Big Brother Watch e.a. t. VK*), rov. 307. Zie bijvoorbeeld ook EHRM 29 juni 2006, 54934/00 (*Weber en Saravia t. Duitsland*), rov. 93; EHRM 16 februari 2000, 27798/95, (*Amann t. Zwitserland*), rov. 57-62; EHRM 24 april 1990 11801/85 (*Kruslin t. Frankrijk*), rov. 33-36. Vgl. EHRM 19 juni 2018, 35252/08 (Centrum för Rättvisa t. Zweden) (in afwachting uitspraak Grand Chamber, laatstelijk gecontroleerd 30 november 2020).

213 EHRM 13 september 2018, 58170/13 e.a. (*Big Brother Watch e.a. t. VK*), rov. 307. Zie ook EHRM 1 juli 2008, 58243/00 (*Liberty t. VK*), rov. 63.

214 EHRM 13 september 2018, 58170/13 e.a., (*Big Brother Watch e.a. t. VK*), rov. 308-309. Zie ook EHRM 21 juni 2011, 30194/09 (*Shimovolos t. Rusland*), rov. 68; EHRM 2 augustus 1984, 8691/79 (*Malone t. VK*).

215 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 66.

216 EHRM 2 september 2010, 35623/05 (*Uzun t. Duitsland*), rov. 66 jo. 63.

217 Zie ook Annotatie Stijnen in Gst. 2016/86 bij CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947.

218 CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947, rov. 4.5.5.

artikel is (bijvoorbeeld) onvoldoende bepaald onder welke omstandigheden en gedurende welke periode een technisch hulpmiddel mag worden gebruikt, en is daardoor voor de betrokkene onvoldoende voorzienbaar.[219] Een dergelijke grondslag biedt de toezichtstitel uit de Awb evenmin.[220] De waarborgen die in dat soort situaties volgens artikel 8 EVRM van een wettelijke grondslag mogen worden verwacht, staan bijvoorbeeld wel in artikel 126g en 126o Sv.[221] Voor waarnemingen die volgens het CRvB minder 'intensief' zijn en dus een beperkter inbreuk op artikel 8 EVRM opleveren, kan in de zelfstandige onderzoeksbevoegdheid van artikel 53a Participatiewet een afdoende grondslag worden gevonden.[222] In dat geval hoeft aan de monitoring geen voorafgaand feit, grond of vermoeden of voorafgaande reden ten grondslag te liggen.[223]

Wanneer is dan sprake van monitoring die als 'stelselmatig' kan worden gezien? Dat wordt, net als in het strafrecht, gedefinieerd als met de monitoring een min of meer compleet beeld kan worden verkregen van bepaalde aspecten van iemands privéleven. Een dergelijk 'aspect van het privéleven' is bijvoorbeeld iemands uitgavenpatroon. Voor de stelselmatigheid zijn de plaats, de duur, de intensiteit en de frequentie van de monitoring en het gebruik van technische hulpmiddelen relevant.

Hulpmiddelen die niet méér doen dan de zintuiglijke waarneming versterken, zoals een verrekijker, betekenen niet zonder meer dat de monitoring een stelselmatig karakter heeft. Hulpmiddelen kunnen leiden tot het oordeel dat de monitoring een stelselmatig karakter heeft als zij de zintuiglijke waarneming in grote mate en frequentie versterken, zoals het geval kan zijn als een telescoopkijker wordt gebruikt. Daarentegen maakt het gebruik van een technisch hulpmiddel dat signalen registreert, zoals een video-opname of gps-tracker, de monitoring in beginsel stelselmatig. Dat geldt ook als het technisch hulpmiddel alleen kortdurend wordt gebruikt, bijvoorbeeld door maar een paar foto's of video's te maken. De reden: 'Zo'n registratie maakt immers een exacte en volledige weergave van het waargenomene op willekeurig welk moment mogelijk.'[224]

Wat betekenen deze criteria voor de monitoring van online openbare bronnen? De Commissie-Koops heeft er in het kader van het moderniseringstraject van het Wetboek van Strafvordering op gewezen dat deze criteria niet allemaal bruikbaar zijn voor het bepalen wanneer sprake is van stelselmatig monitoren van online openbare bron-

219 CRvB 13 september 2016, ECLI:NL:CRVB:2016:3479, m.nt. in AB 2017/47, *Gst.* 2017/33 en USZ 2016/373 (camera); CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947, m.nt. AB 2016/329, *Gst*. 2016/86 en USZ 2016/165 (peilbaken).

220 Idem. Zie tevens Oerlemans & Schuurmans 2019.

221 CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947, rov. 4.5.5.

222 CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947, rov. 4.6.1. Zie ook: CRvB 19 maart 2019, ECLI:NL:CRvB:2019:978, rov. 4.2-4.3; CRvB 18 juli 2019, ECLI:NL:CRVB:2019:2360, rov. 4.4, USZ 2019/269 m.nt. Nacinovic; CRvB 22 januari 2019, ECLI:NL:CRVB:338, rov. 4.3. Zie over strafrecht bijvoorbeeld: AG Hofstee, ECLI:NL:PHR:2015:1029, 12 en 13 bij HR 7 juli 2015, ECLI:NL:HR:2015:1815.

223 CRvB 14 april 2015, ECLI:NL:CRVB:2015:1231, rov. 4.2, USZ 2015/198, m.nt. M. van den Brink & A. Terlouw. Voorts: CRvB 22 januari 2019, ECLI:NL:CRVB:2019:338, rov. 4.2.

224 Par. 4, Commentaar op artikel 126g WvSv, T&C Wetboek van Strafvordering.

nen. Bij de stelselmatigheid van monitoring wordt van oudsher nadrukkelijk naar de frequentie en duur van de monitoring gekeken. Die factoren zijn voor online monitoring minder bruikbaar, omdat de monitoring in dat geval (in de regel) geen momentopnames zijn maar er online uitingen over een langere periode kunnen worden verzameld.[225] Ook is het lastig van tevoren in abstracto te bepalen welke inbreuk de monitoring kan maken. De Commissie-Koops doet een voorzet voor de ontwikkeling van een andere benadering voor de beantwoording van de vraag of de inbreuk meer of minder waarborgen vergt. Volgens de Commissie kan acht worden geslagen op de omvang en het type gegevens, de aard van de bron, de wijze van zoeken en het gebruik van gegevens en de mogelijke impact op de persoon.[226] Ook voor monitoring door gemeentelijke organen kunnen deze criteria zinvol zijn om stelselmatige van niet-stelselmatige inbreuken te onderscheiden. Aansluiten bij de strafrechtelijke benadering zou de consistentie ten goede komen maar zou ook voorkomen dat het gunstig wordt monitoring zo veel mogelijk binnen een gemeente te laten plaatsvinden omdat de politie aan strengere normen is gebonden.

Oerlemans en Schuurmans hebben in 2019 geconcludeerd dat er weinig jurisprudentie van de bestuursrechter is over de rechtmatigheid van openbare-bronnenonderzoek.[227] Een specifieke grondslag voor de meer ingrijpende varianten van monitoring (stelselmatige monitoring) door gemeenten in online openbare-bronnengegevens, is in wetgeving in formele zin niet te vinden. Voor zover de monitoring is gericht op het bewaken van de openbare orde zou als potentiële grondslag gedacht kunnen worden aan artikel 172, eerste lid Gemeentewet. Gelet op het algemene karakter van dat artikel en het ontbreken van waarborgen voor de gemonitorde persoon, is het niet mogelijk om stelselmatige monitoring op dat artikel te baseren. Artikel 3:2 Awb bevat de plicht voor het bestuursorgaan om ter voorbereiding van een besluit de nodige kennis omtrent de relevante feiten en de af te wegen belangen te vergaren. Deze onderzoeksplicht gaat echter niet gepaard met onderzoeksbevoegdheden, zoals een bevoegdheid onderzoek te doen in openbare online bronnen. Zelfs de toezichtstitel uit de Awb, met een standaardset aan maatregelen voor het houden van toezicht, bevat niet de bevoegdheid om stelselmatige observaties uit te voeren.

Voor niet-stelselmatige monitoring is discussie mogelijk over de vraag of een eventuele inbreuk wel gerechtvaardigd kan worden door eerdergenoemde artikelen. In het licht van artikel 8 EVRM zou artikel 172, eerste lid voor de niet-stelselmatige monitoring nog wel een adequate grondslag kunnen zijn, net zoals artikel 53a Participatiewet en artikel 3 Politiewet dat kunnen zijn. Het is echter de vraag of ook artikel 10 Grondwet met die grondslag genoegen neemt. Zie daarover par. 4.4.

225 Zie hierover ook Stol & Strikwerda (2018) en Oerlemans (2017).
226 Zie Commissie-Koops et al. (2018). p. 156-168.
227 Oerlemans & Schuurmans (2019).

4.3.4 *Tussenconclusie*

Als geconstateerd wordt dat monitoring een inbreuk vormt op het recht op eerbiediging van de persoonlijke levenssfeer kan die inbreuk worden gerechtvaardigd als die voldoet aan een aantal cumulatieve criteria. Het eerste criterium is het criterium dat in deze paragraaf centraal staat: de inbreuk moet bij wet zijn voorzien. In het kader van dat criterium wordt (ook) onderzocht of de wettelijke regeling voor de monitoring adequate en effectieve waarborgen biedt tegen misbruik. In dit geval ontbreekt een uitdrukkelijke wettelijke grondslag voor de monitoring van online openbare bronnen. Er is mist een regeling in wet- of regelgeving die duidelijk maakt wat gemeentelijke organen mogen monitoren, onder welke voorwaarden en met welke waarborgen dat is omkleed. Bij niet-stelselmatige monitoring kan die grondslag wellicht worden ingelezen in artikel 172, eerste lid Gemeentewet. Dat geldt echter niet voor *stelselmatige* monitoring. Aan die ingrijpender inbreuken op de persoonlijke levenssfeer worden op artikel 8 EVRM strenge kwaliteitseisen gesteld. Daaraan voldoet artikel 172, eerste lid Gemeentewet niet.

Stel, de gemeenteraad overweegt in de algemene plaatselijke verordening (APV) een uitgebreide regeling op te nemen over online monitoring. Zou die regeling alsnog in een wettelijke grondslag in de zin van artikel 8 EVRM kunnen voorzien, zodat inbreuk door wel en niet-stelselmatig monitoren gelden als zijnde bij wet voorzien? Dat kan, maar dat laat onverlet dat ook artikel 10 Grondwet eisen stelt aan de wettelijke grondslag van een beperking van het recht op eerbiediging van de persoonlijke levenssfeer. Anders dan artikel 8 EVRM, dat veel materiële ofwel inhoudelijke eisen stelt aan de wettelijke grondslag, stelt artikel 10 Grondwet meer formele eisen aan de grondslag. Zie daarover par. 4.4.

Een inbreuk op een grondrecht kan gerechtvaardigd zijn als die inbreuk voldoet aan drie criteria, waarvan de eerste het bestaan is van een adequate wettelijke grondslag. In de volgende paragraaf worden de twee andere criteria besproken.

4.3.5 *Voor de volledigheid: de overige twee criteria voor rechtvaardiging van een inbreuk*

Het legitieme doel
Een inmenging op artikel 8 EVRM moet in de tweede plaats een van de in het tweede lid van dat artikel opgesomde belangen dienen. De opsomming is dus uitputtend, maar uit jurisprudentie blijkt dat de reikwijdte van de belangen zo ruim wordt uitgelegd dat het EHRM zelden concludeert dat een legitiem doel ontbreekt.[228] Ook het EHRM heeft

228 J. Gerards (2019). *General Principles of the European Convention on Human Rights*, Cambridge: Cambridge University Press, p. 220 en B. Rainey, E. Wicks & C. Ovey, *Jacobs, White & Ovey* (2017). *The European Convention on Human Rights*, Oxford: Oxford University Press.

overwogen dat het in de meeste uitspraken 'beknopt' is over het legitiem doel.[229] De verwerende staat moet aantonen dat de inmenging een legitiem doel nastreefde.[230]

Doelen die bij de monitoring in dit onderzoek het meest voor de hand liggen, zijn de openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten en de bescherming van de rechten en vrijheden van anderen. Volgens ons ligt 'nationale veiligheid' als legitiem doel minder voor de hand. Dit doel is gewoonlijk alleen aan de orde in situaties waarin de veiligheid van de staat en de democratische constitutionele orde onder druk lijken te staan als gevolg van bedreigingen van binnen en buiten.[231] Of, gelet op die doelen, de inbreuk *evenredig* is, wordt eerst beoordeeld in het kader van het volgende rechtvaardigingsvereiste, de noodzakelijkheid in een democratische samenleving.

Noodzakelijkheid in een democratische samenleving

Een inmenging in het recht op eerbiediging van de persoonlijke levenssfeer moet ten slotte ook noodzakelijk zijn in een democratische samenleving. Dit vereiste komt neer op een evenredigheidstoets. Het handelen van de verwerende lidstaat moet een reactie zijn geweest op een dringende maatschappelijke behoefte en de inmenging die dat met zich brengt mag niet groter zijn dan nodig is om in die dringende maatschappelijke behoefte te voorzien. Het EHRM zal onderzoeken of, gelet op de zaak als geheel, de aangevoerde redenen om ze te rechtvaardigen relevant en toereikend waren en of de maatregelen evenredig waren aan de nagestreefde legitieme doelstellingen.[232] In het kader van die beoordeling zal het EHRM onder andere acht slaan op de achtergrondomstandigheden, het recht in kwestie en de aard van de betrokken inbreuk. Verdragsstaten hebben een zekere beoordelingsmarge (*margin of appreciation*) bij de beoordeling van de noodzaak van een inmenging, aangezien zij in een betere positie zijn om de maatschappelijke behoefte vast te stellen. Toch is het uiteindelijk aan het EHRM om te bepalen of zowel het doel als de noodzaak van een bepaalde schending van rechten onder een of meer uitzonderingen van algemeen belang verenigbaar is met het EVRM.[233]

De beoordeling van de noodzakelijkheid van de inbreuk in een democratische samenleving is een casuïstische. Bij de beoordeling zal in de eerste plaats een rol spelen hoe groot de inbreuk is die is gemaakt op de persoonlijke levenssfeer. Daarbij zullen dezelfde factoren een rol spelen als die zijn besproken in paragraaf 4.3.1. Daartegenover staan de belangen met het oog waarop de inbreuk is gemaakt. Daarbij zal een rol spelen hoe concreet de aanwijzingen voor (de vrees voor) verstoringen van de openbare orde

229 EHRM 1 juli 2014, 43835/11 (*S.A.S. t. Frankrijk*), rov. 114.
230 EHRM 23 februari 2016, 11138/10 (*Mozer v. the Republic of Moldova and Russia*), rov. 194.
231 S. Greer, (1997). *The exceptions to Articles 8 to 11 of the European Convention on Human Rights,* bron: www.echr.coe.int.
232 Gerards (2019). p. 230-250 en Rainey et al. (2017). p. 359.
233 Gerards (2019). p. 170-171, 250 en Greer (1997). p. 16.

waren. En hoe ernstig was de verstoring van de openbare orde of leek die destijds te zijn? Indien sprake was een acute en ernstige crisissituatie zal aan de belangen die pleiten voor de inbreuk meer gewicht worden toegekend. Daarbij zal ook een rol spelen in hoeverre er aanwijzingen waren dat de bewuste monitoring bij het bewaken of herstellen van de openbare orde behulpzaam zou zijn, en of hetzelfde doel op een minder ingrijpende wijze kon worden bereikt.

4.4 Artikel 10 Grondwet

Het recht op eerbiediging van de persoonlijke levenssfeer is gecodificeerd in artikel 10 tot en met 13 van de Grondwet. Artikel 10 Grondwet is van die vier artikelen het meest veelomvattend. Het eerste lid van dat artikel bepaalt dat eenieder, 'behoudens bij of krachtens de wet te stellen beperkingen', recht heeft op eerbiediging van de persoonlijke levenssfeer. De reikwijdte van deze bepaling is erg breed. Een uitputtende omschrijving van hetgeen onder het bereik van dit artikel valt wilde de grondwetgever niet geven. Wel is de volgende toelichting gegeven op de betekenis van het recht op eerbiediging van de persoonlijke levenssfeer:

> *'De termen "persoonlijke levenssfeer" en "privacy" wekken de indruk een gebied aan te duiden waarbinnen elk individu vrij is en geen inmenging van anderen behoeft te dulden. Bij de vraag naar de begrenzing van dit gebied denkt men gewoonlijk eerst aan het huis waarin iemand leeft. (…) Met deze ruimtelijke begrenzing is het gebied van de privacy niet volledig aangeduid. Bepaalde vormen van communicatie, zoals het telefoongesprek en de briefwisseling, plegen tot de privésfeer te worden gerekend en genieten eveneens een zekere rechtsbescherming. Ook het buiten een woning gevoerde vertrouwelijke gesprek mag worden gerekend tot de privésfeer van de gesprekspartners, evenals sommige gewoonten, gedragingen, contacten, abonnementen, lidmaatschappen en bepaalde aspecten van het gezinsleven. Hoewel het ruimtelijke aspect een grote betekenis heeft, is privacy derhalve toch niet iets dat alleen ruimtelijk te begrenzen valt.'*[234]

Hoewel in dit citaat wordt onderkend dat het recht op eerbiediging van de persoonlijke levenssfeer zich niet beperkt tot de beslotenheid van de eigen woning, wordt niet ondubbelzinnig aangegeven of de persoonlijke levenssfeer zich ook kan uitstrekken tot de openbaarheid. Dat dit wel het geval is, wordt aangenomen sinds 1987.[235] Die uitleg past bij de brede benadering van de persoonlijke levenssfeer als de reeks van situaties waarin iemand 'onbevangen zichzelf wil zijn'.[236] Uitingen gedaan in online openbare bronnen kunnen daar ook onder vallen. Monitoring van online openbare bronnen kunnen aldus een inbreuk maken op dat recht. Het is mogelijk dat de rechter bij de beoordeling van de vraag of daarvan sprake is aansluiting zoekt bij de criteria die daarvoor in het

234 *Kamerstukken II* 1975/76, 13872, 3, p. 40.
235 Hoge Raad 9 januari 1987, *AB* 1987/231, m.nt. Van der Burg en *NJ* 1987/928, m.nt. Van der Alkema (*Edamse bijstandsontvanger*).
236 *Kamerstukken II* 1975/76, 13872, 3, p. 40.

kader van de beoordeling van artikel 8 EVRM worden gehanteerd. In algemene zin is echter niet op voorhand aan te geven in hoeverre het monitoren van gedragingen van burgers onder de reikwijdte van artikel 10 zal vallen: daarover is te weinig (met deze casus vergelijkbare) jurisprudentie verschenen.

Net als bij artikel 8 EVRM het geval is, zijn ook op artikel 10 Grondwet beperkingen mogelijk. Een inbreuk op of inmenging in het recht van artikel 10 betekent daarom niet zonder meer dat ook van een schending sprake is. Die inbreuk of inmenging kan gerechtvaardigd zijn, mits die voldoet aan de voorwaarde dat die beperking een grondslag vindt 'bij of krachtens' de wet. Veel eisen stelt artikel 10 Grondwet dus niet aan een beperking van grondrechten. De beperkingssystematiek stelt, vergeleken met artikel 8 EVRM, zelfs behoorlijk marginale eisen aan een beperking van dit grondrecht. In dit geval vormt de bepaling echter wel een aanvulling op het regime van het laatstgenoemde artikel. Waar artikel 8 EVRM het vereiste dat een beperking bij wet moet zijn voorzien sterk materieel uitlegt, wordt aan het vereiste van artikel 10 Grondwet, dat de grondslag voor de beperking moet zijn gegeven 'bij of krachtens', een sterk formele uitleg gegeven. Dat de grondslag voor de beperking moet zijn gegeven 'bij of krachtens' de wet wil zeggen dat niet alleen de wetgever in formele zin het grondrecht mag beperken, maar dat deze bevoegdheid ook kan worden gedelegeerd. Gelet op de leer van de bijzondere beperkingen is het uitgangspunt dat een wettelijke grondslag ertoe moet strekken het grondrecht te beperken. De wettelijke grondslag moet dus zo specifiek zijn dat daarmee is beoogd het grondrecht te beperken.[237] Ten aanzien van monitoring van online openbare bronnen ontbreken specifieke wettelijke regelingen. Er ontbreekt wetgeving in formele zin met een grondslag die is geschreven voor de monitoring van online openbare bronnen. Artikel 172, eerste lid Gemeentewet kan ook niet als zodanig worden gezien. Dat een voldoende specifieke grondslag voor de beperking van artikel 10 Grondwet ontbreekt, kan niet worden hersteld door een regeling over observaties in een APV.[238]

Dit betekent dat er voor de monitoring van online openbare bronnen geen wettelijke grondslag lijkt te zijn die voldoet aan de eisen die artikel 10 Grondwet daaraan stelt. Het ontbreken van een wettelijke grondslag is vanuit juridisch oogpunt problematisch. Daarbij passen twee kanttekeningen. Ten eerste wijzen we op voorgaande constatering dat er nog onduidelijkheid bestaat over in hoeverre monitoring van online openbare bronnen met het oog op de bescherming van de openbare orde valt onder de reikwijdte van artikel 10 Grondwet. Als de reikwijdte van artikel 10 Grondwet op dit punt beperkter zou worden uitgelegd dan bijvoorbeeld bij artikel 8 EVRM het geval is, zou monitoring in sommige gevallen buiten de reikwijdte van artikel 10 Grondwet kunnen

237 Gerards, J., R. Nehmelman & M. Vetzo (2018). *Algoritmes en grondrechten*, Utrecht Gerards, J., R. Nehmelman, R. & M. Vetzo, M. (2018). Algoritmes en grondrechten, Utrecht, p. 37; Nieuwenhuis, A.J, M. den Heijer & A.W. Hins (2017). *Hoofdstukken Grondrechten*, Nijmegen: Ars Aequi Libri, p. 137-138.

238 Met name: ABRvS 28 augustus 1995, AB 1996/204, m.nt. Rogier (*Drugspand Venlo*). Zie tevens ABRvS 6 juni 2000, *Gst.* 2000-7124-3. Hoge Raad 19 maart 1996, NJ 1997/86 (*Observatie in verhoorfase*). Zie tevens RvS, *Voorlichting over grondwettelijke aspecten van (voor)genomen crisismaatregelen*, 25 mei 2020, par. 4.c.

vallen. Van een inbreuk is dan geen sprake, zodat ook niet wordt toegekomen aan de discussie over de wettelijke grondslag. Datzelfde geldt als zou worden geconstateerd dat de redelijke uitleg van het grondrecht met zich brengt dat monitoring in een concreet geval buiten de reikwijdte van het grondrecht valt.[239] Ten tweede is er wel een (beperkte) mogelijkheid om in uitzonderlijke ('concrete, acute en levensbedreigende') situaties 'gedurende korte tijd op grond van de noodbevels- en noodverordeningsbevoegdheden een inbreuk te maken op de uitoefening van grondwettelijke grondrechten'. In veruit de meeste gevallen van monitoring zoals bedoeld in dit onderzoek zal van een dergelijke situatie geen sprake zijn.[240]

In box 3 staat een korte juridische reflectie op het gebruik van gemeentelijke persoonsgebonden- en nepaccounts.

Box 3. Juridische reflectie op het gebruik van persoonsgebonden-en nepaccounts.

Gemeentelijke accounts, persoonsgebonden accounts en nepaccounts

Uit paragraaf 3.3.4 blijkt dat sommige gemeenten bij online observaties ook gebruikmaken van accounts op social media. Het kan gaan om gemeentelijke accounts, persoonsgebonden accounts en nepaccounts. Op veel platforms heeft dat echter tot gevolg dat de gemeente ook toegang krijgt tot gegevens over die personen en hetgeen ze delen op hun accounts. Ook het volgen en gebruiken van die informatie kunnen tot een inbreuk op de persoonlijke levenssfeer leiden.

Of er sprake is van een inbreuk en de ernst van de inbreuk hangt meestal af van de omstandigheden van het geval. Zo is voor het gebruik van accounts van personen relevant of het gaat om accounts die herkenbaar zijn als accounts van aan de gemeente verbonden functionarissen of ambtenaren ('Wethouder X') of dat dit minder herkenbaar is. **Gemeentelijke accounts** worden gevolgd door inwoners, bezoekers en andere inwoners die een band met de gemeente hebben. Ze volgen de gemeente met de bedoeling om van nieuwsberichten over de gemeente op de hoogte te blijven. De volgers van de gemeenten zullen redelijkerwijs niet of nauwelijks verwachten dat de gemeente de onderlinge connectie ook gebruikt om informatie in te winnen.

Wel kan worden vastgesteld of **nepaccounts** inbreuk vormen op de persoonlijke levenssfeer van de geobserveerde personen, ook als het uitsluitend wordt gebruikt om onderzoek te doen in open bronnen. Met het inzetten van deze (verhullende) wijze van het monitoren van online gedraging moet volgens ons terughoudend worden omgegaan.

239 Zie bijvoorbeeld RvS, *Voorlichting over grondwettelijke aspecten van (voor)genomen crisismaatregelen*, 25 mei 2020, par. 4.a en 7.b; Kortmann e.a. (2016). *Constitutioneel recht*, Deventer: Wolters Kluwer, p. 382-383.

240 RvS, *Voorlichting over grondwettelijke aspecten van (voor)genomen crisismaatregelen*, 25 mei 2020, par. 7.b.

4.5 Afsluiting

Ook monitoring van online openbare bronnen kan een inbreuk maken op het recht op privacy, zoals uitgewerkt in de AVG, en op artikel 8 EVRM en artikel 10 Grondwet.

Uit paragraaf 3.4 blijkt dat veel monitoring geschiedt met de bedoeling te 'weten wat er speelt' of 'hoe er over de gemeente gepraat wordt'. Op voorhand lijkt dit type monitoring mogelijk ook te kunnen worden verricht zonder persoonsgegevens te verwerken. Het doel van de monitoring kan voldoende gediend worden zonder precies te weten wie welke uitlating heeft gepost of van welk IP-adres. Als monitoring zoals deze inderdaad volledig geanonimiseerd zouden kunnen geschieden, scheelt dat veel juridische complicaties. Als er geen sprake is van de verwerking van tot personen herleidbare gegevens, zijn de AVG, artikel 8 EVRM en artikel 10 Grondwet niet op de monitoring van toepassing. Daarbij is wel een aandachtspunt dat de AVG een erg ruime uitleg geeft aan het begrip 'persoonsgegeven'. Ook als de verwerkte gegevens niet tot personen herleidbaar zijn, maar dat wel het geval is als die gegevens worden aangevuld met openbaar beschikbare informatie, is sprake van persoonsgegevens.

Het is onduidelijk in hoeverre die monitoring op dit moment al geanonimiseerd geschiedt of zou kunnen geschieden. Niet alleen is te weinig informatie beschikbaar over de werkwijzen van gemeenten, maar er is ook nog niet veel informatie over hoe de tools van commerciële aanbieders die gemeenten gebruiken bij de monitoring precies werken. Onduidelijk is bijvoorbeeld in hoeverre die aanbieders gegevens van internet kopiëren en opslaan. Niettemin blijkt uit paragraaf 3.3.2 dat 75 procent van de gemeenten een monitoringstool gebruikt.

In veel gevallen zullen bij de monitoring wel persoonsgegevens worden verwerkt of zal gebruik worden gemaakt van tot personen herleidbare informatie. Dat betekent dat de monitoring moet voldoen aan de eisen die de AVG daaraan stelt en aan de eisen die artikel 8 EVRM en artikel 10 Grondwet stellen aan gerechtvaardigde inbreuken op (of: inmengingen in) het recht op eerbiediging op de persoonlijke levenssfeer. Het is niet mogelijk om voor alle typen blijkens hoofdstuk 3 voorkomende monitoring op voorhand te zeggen in hoeverre de bestuurlijke praktijk voldoet aan de eisen van de AVG, artikel 8 EVRM en artikel 10 Grondwet. Wel signaleren we een aantal knelpunten.

De eerste twee aandachtspunten hebben te maken met de wettelijke grondslag voor monitoring. Voor zover de monitoring is bedoeld de openbare orde te bewaken, kan die een grondslag vinden in artikel 172, eerste lid Gemeentewet. Op grond van dat artikel heeft de burgemeester de bevoegdheid de openbare orde te bewaken. Een eerste knelpunt betreft de onduidelijkheden in de verhouding tussen de AVG en de Wet politiegegevens. Monitoring die op grond van artikel 172, eerste lid Gemeentewet wordt verricht, moet voldoen aan de eisen van de AVG. Dat geldt niet voor gegevens die (heel kort gezegd) betrekking hebben op strafrechtelijke vervolging of waar de politie an-

derszins bij is betrokken, want dan is de Wet politiegegevens in beeld. In de praktijk kunnen zich hier, vanwege de onderlinge verwevenheid, niettemin lastige vragen voordoen. Dat het bewaken van de openbare orde en opsporing van strafbare feiten dicht tegen elkaar aanliggen, blijkt ook uit de enquête, als besproken in paragraaf 3.4.2 waarin 25 procent van de respondenten aangeeft dat het opsporen van strafbare feiten een nevendoel of zelfs hoofddoel (9%) van de monitoring is.

Artikel 8 EVRM stelt aan 'stelselmatige' (lees: intensiever of ingrijpender) monitoring strenge eisen. Stelselmatige monitoring vergt een wettelijke grondslag die meer waarborgen bevat, zoals een bepaling over de maximale duur van de monitoring en de technische hulpmiddelen die mogen worden gebruikt. Artikel 172, eerste lid Gemeentewet schiet tekort als wettelijke grondslag voor stelselmatige monitoring.

Wat betekent dat voor de monitoring door gemeenten? De criteria aan de hand waarvan beoordeeld moet worden of monitoring 'stelselmatig' is, zijn ontwikkeld voor offline monitoring en zijn niet zonder meer geschikt voor online monitoring. Dat geldt bijvoorbeeld voor de nadruk die offline wordt gelegd op de frequentie en de duur van de monitoring. De Commissie-Koops heeft in het kader van de modernisering van het Wetboek van Strafvordering een voorstel gedaan om het begrip 'stelselmatigheid' in de context van online monitoring te operationaliseren. Hoewel dat voorstel ging over het strafrecht is het te overwegen het voorstel van de Commissie-Koops ook te gebruiken om monitoring binnen de gemeenten te kwalificeren.

Uit paragraaf 3.3.4 blijkt dat gemeenten groepen volgen, bijvoorbeeld om een sociaal netwerk in kaart te brengen. In die paragraaf is het voorbeeld gegeven van een gemeente die door online monitoring een netwerk van hangjongeren in kaart heeft willen brengen. Uit paragraaf 4.3.2 volgt volgens ons dat dergelijke op de persoon gerichte monitoring al snel als 'stelselmatig' moet worden gezien. Omdat artikel 172, eerste lid Gemeentewet geen adequate grondslag biedt voor dit soort monitoring en een betere wettelijke grondslag ontbreekt, is er voor dit type monitoring nu geen wettelijke grondslag.

Zou een APV dat gat kunnen dichten? Ofwel: kan een gemeenteraad het gebrek aan een adequate wettelijke grondslag voor monitoring wegnemen door daarover een en ander te regelen in de APV? Artikel 8 EVRM lijkt wel genoegen te kunnen nemen met een APV in plaats van een wet in formele zin om in een wettelijke grondslag te voorzien, maar artikel 10 Grondwet doet dat niet. Artikel 10 Grondwet vereist dat een beperking van het recht op eerbiediging van de persoonlijke levenssfeer 'bij of krachtens' de wet moet zijn voorzien. Artikel 172, eerste lid Gemeentewet beoogt geen beperking van artikel 10 Grondwet toe te staan en kan dan ook niet als een dergelijke grondslag fungeren. Er ontbreekt dus een wettelijke grondslag voor monitoring die als inbreuk op artikel 10 Grondwet moet worden gezien. Een APV kan dat gat niet opvullen omdat aan een bepaling in de APV over online monitoring geen specifieke? grondslag in een wet in formele zin ten grondslag zou liggen.

Het vereiste dat een inbreuk op een grondrecht een wettelijke grondslag moet hebben, wordt gesteld om de kenbaarheid, de voorzienbaarheid en voorspelbaarheid van overheidshandelen voor burgers te stimuleren. In dat licht is het opvallend dat van alle gemeenten die aangeven gebruik te maken van methodes voor online monitoring, geen enkele gemeente heeft geprobeerd om aan de gebrekkige voorzienbaarheid daarvan door het ontbreken van een daarop toegespitst wettelijk kader tegemoet te komen door – bijvoorbeeld op de eigen site – transparant te zijn over wat de gemeente online doet en welke vuistregels die daarvoor zelf hanteert.

Een derde aandachtspunt is de doelbinding van de monitoring. De AVG eist dat verwerking van persoonsgegevens plaatsvindt met het oog op een specifiek doel. Ook artikel 8 EVRM veronderstelt dat een inbreuk op de persoonlijke levenssfeer wordt gemaakt met een specifiek doel in gedachten. In het verlengde daarvan is een vierde aandachtspunt dat voor de rechtmatigheid van monitoring essentieel is dat de monitoring noodzakelijk is om dat doel te bereiken. De monitoring moet (in EHRM-termen) een reactie zijn geweest op een dringende maatschappelijke behoefte en de inmenging die dat met zich brengt mag niet groter zijn dan nodig is om in die dringende maatschappelijke behoefte te voorzien. Het EVRM maar ook de AVG verlangt dus van de gemeente dat die reflecteert op de redenen voor de monitoring in relatie tot de inbreuk die de monitoring maakt op de privacy van de betrokkenen. Dat betekent dat bijvoorbeeld relevant is hoe concreet de aanwijzingen voor (de vrees voor) verstoringen van de openbare orde waren, hoe ernstig de verstoring van de openbare orde was of destijds leek te zijn, en welke rol de monitoring in dat kader speelde. Aan die vragen moeten gemeenten voor en tijdens het online monitoren ook aandacht besteden.

Gelet op bovenstaande knelpunten zou het goed zijn meer aandacht te hebben voor de juridische implicaties van de monitoring, ook als die monitoring alleen betrekking heeft op openbare online bronnen. Het ligt voor de hand te beginnen met het, samen met de Functionaris Gegevensbescherming, opstellen van een intern protocol voor online monitoring. Een protocol zorgt voor helderheid over de implicaties van het juridisch kader voor de praktijk (vgl. paragraaf 3.7.2) en geeft aan wat binnen de gemeente de gebruikelijke werkwijze voor monitoring is.

Ter afsluiting, in dit hoofdstuk zijn een aantal knelpunten gesignaleerd voor de rechtmatigheid van online monitoring. Tegelijkertijd is te zien dat binnen gemeenten wordt gemonitord om redenen die, gelet op de juridische positie van de burgemeester en de maatschappelijke positie van de gemeente, volstrekt begrijpelijk zijn. Veel van de juridische eisen worden (misschien wel op basis van intuïtie of ethische opvattingen) nageleefd, zoals het niet bijhouden van dossiers, terughoudend zijn in 'doorklikken' op profielen en dat de meeste gemeenten aangeven geen gebruik te maken van privéaccounts en nepaccounts.

5. Het wankele fundament onder een stevige monitoringspraktijk

5.1 Inleiding

Dit hoofdstuk vat de belangrijkste aspecten van dit onderzoek naar gemeentelijke monitoring van openbare bronnen samen en bekijkt de bevindingen in samenhang. Die bevindingen zijn gebaseerd op literatuuronderzoek naar online monitoring bij politie en gemeenten, op basis van interviews (N=10) en een vragenlijst die gericht was aan medewerkers Communicatie en OOV. De beschreven resultaten zijn gebaseerd op 196 respondenten uit maximaal 156 gemeenten (45% unieke gemeenten). De gemeentelijke 'afdelingen' Communicatie (53%) en OOV (45%) zijn in een vergelijkbare mate vertegenwoordigd in dit onderzoek. Daarnaast zijn de resultaten gebaseerd op juridisch bronnenonderzoek naar de eisen die de AVG en artikel 8 EVRM stellen aan online monitoring door gemeenten.

Allereerst gaan we in paragraaf 5.2 in op de ratio achter deze nieuwe beleidspraktijk en belichten we de belangrijkste gemeentelijke doelstellingen en voordelen van monitoring. Zo blijkt dat monitoring appelleert aan de behoefte om 'in control' te zijn. Uit de onuitputtelijke hoeveelheid bronnen en de talloze vertakkingen en verbindingen die het wereldwijde web biedt, kunnen gemeenten door slimme zoekfuncties bijzonder nuttige informatie halen over mogelijke verstoringen van de openbare orde. Het fundament waarop deze wijdverbreide beleidspraktijk is gebouwd, zo leert paragraaf 5.3, is echter dun. Er vallen bijvoorbeeld verschillen te constateren tussen gemeenten over de mate waarin en de wijze waarop zij monitoren. Naast wezenlijke vragen over bijvoorbeeld het juridische kader en mogelijke gevolgen voor rechtsongelijkheid die dit onderzoek oproepen, zijn er ook veel vragen van praktische aard over bijvoorbeeld de afhankelijkheid van externe leveranciers en de wijze waarop verkregen informatie wordt geïnterpreteerd. Wat dat betreft, staat deze relatief nieuwe beleidspraktijk nog in de kinderschoenen. In dit hoofdstuk wordt de hoofdvraag uit dit onderzoek, te weten: in hoeverre geeft de huidige gemeentelijke praktijk wat betreft online monitoring van open bronnen in het domein van openbare orde en veiligheid reden tot heroverweging? kort beantwoord. Aanbevelingen van beleidsmatige en onderzoekstechnische aard zijn te vinden in paragraaf 5.4 respectievelijk paragraaf 5.5. Het hoofdstuk, en daarmee ook deze studie als geheel, sluit af met het verstrekken van een beknopte reflectie op dit onderzoek in paragraaf 5.6.

5.2 Gemeenten: De ratio achter de beleidspraktijk van online monitoren

De eerste subparagraaf geeft een overzicht van de mate waarin en de manier waarop gemeenten online monitoring in hun dagelijkse praktijk hebben opgenomen. Vervolgens wordt aan de hand van de doelstellingen en de beschikbare hulpmiddelen inzicht gegeven in de ratio die hieraan ten grondslag ligt zoals de (gerechtvaardigde) maatschappelijke en organisatorische belangen waarbij ook de beschikbaarheid van allerlei technische hulpmiddelen een rol kan spelen.

5.2.1 *De wijdverbreide praktijk van online monitoring*

Voordat ingegaan wordt op de gemeentelijke monitoringspraktijk wordt stilgestaan bij de inzichten die het (literatuur)onderzoek naar dergelijke werkwijzen bij de politie heeft opgeleverd. Dit deel laat zien dat de praktijk van online monitoring bij de politie primair gericht is op het voorkomen van grote incidenten en verstoringen, al kan ook geconcludeerd worden dat 'Webcare' en 'communicatiedoeleinden' tot de dagelijkse activiteiten behoren. De toegepaste instrumenten passen binnen grotere kaders zoals OSINT en RTIC's en zijn onderdeel van de dagelijkse praktijk. De politie heeft zich qua houding van terughoudend naar proactief ontwikkeld op dit terrein. De technische hulpmiddelen stellen de politieorganisaties in staat om steeds meer en sneller informatie in te winnen. Deze inzichten worden meegenomen bij de interpretatie van de inzichten over Nederlandse gemeenten die dit onderzoek biedt.

Uit het empirische deel van deze studie blijkt dat bijna alle onderzochte Nederlandse gemeenten (95%), openbare bronnen monitoren. Zowel grote als kleine gemeenten, in stedelijk en landelijk gebied, maken hiervan gebruik. Binnen gemeenten zijn verschillende afdelingen betrokken bij online monitoring. Vooral communicatie-experts en medewerkers die betrokken zijn bij de dienstverlening, maar ook medewerkers die zich richten op het domein van de openbare orde en veiligheid houden zich bezig met online monitoring. Gemeenten die hebben aangegeven niet actief zijn met online monitoring, dragen vooral redenen van praktische aard aan. Gesteld kan dus worden dat monitoring van online openbare bronnen een algemeen geaccepteerd verschijnsel lijkt te zijn binnen gemeenten. De volgende subparagraaf laat zien welke concrete doelstellingen men bij de online monitoring voor ogen heeft.

5.2.2 *Doelstellingen van gemeenten*

Het literatuuronderzoek naar monitoring door gemeenten maakte duidelijk dat 'Webcare' en 'communicatie' van oorsprong de voornaamste drijfveren waren om tot online monitoring over te gaan en dat er sinds een aantal jaren sprake is van een verschuiving naar handhavingsvraagstukken en het domein van openbare orde en veiligheid.

De empirische resultaten laten zien dat gemeenten door monitoring inzicht krijgen in de mate waarin de dienstverlening door de inwoners wordt gewaardeerd en op wat er zich 'buiten' het gemeentehuis afspeelt. Men spreekt hierover in termen van 'temperaturen' en 'van buiten naar binnen halen'. Uit de cijfers, de toelichtingen en de interviews blijkt dat het belang van monitoren toeneemt naarmate de maatschappelijke vraagstukken groter en urgenter zijn. Gemeenten houden graag de vinger aan de pols om de mogelijkheid te creëren om zo snel mogelijk bij eventuele 'brandjes' te kunnen zijn. Uit het empirische deel blijkt dat volgens gemeentelijke medewerkers online monitoring overwegend plaatsvindt binnen het domein van openbare orde en veiligheid (60%) en in nog grotere mate bij het domein van communicatie en dienstverlening (89%). In de praktijk blijkt er sprake te zijn van een zekere mate van overlap tussen deze gemeentelijke toepassingsgebieden.

Een overkoepelend thema dat zowel in de literatuur, in de vragenlijst als in de interviews naar voren komt, is dat gemeenten monitoring gebruiken om zelf 'in control' te zijn, al wordt het zelden zo expliciet benoemd. Men stuurt de verwachtingen omtrent de uitvoering van werkzaamheden, wil graag positief bekendstaan en streeft ernaar op een breed terrein de inwoners te vrijwaren van verstoringen van de openbare orde en/of strafbare feiten. Het lijkt erop dat online monitoring op een relatief eenvoudige en effectieve wijze het gevoel van 'in control zijn' kan voeden. De navolgende subparagraaf schetst de middelen die gemeenten ter beschikking staan.

5.2.3 *De middelen*

Het is begrijpelijk dat gemeenten informatie van online openbare bronnen gebruiken om zich van een van hun kerntaken te kwijten. Met openbare en voor iedereen toegankelijke gegevens van internetbronnen zoals Facebook en Twitter zijn gemeenten in staat (of menen dat te zijn) om zich een beeld te vormen van allerlei gevoelens van (on)tevredenheid van de inwoners. Dit kan variëren van individuele klachten over de verlichting in een nieuwe fietstunnel tot oproepen tot hooliganisme van grote protestgroepen. De informatiekanalen zijn relatief nieuw en aan verandering onderhevig (van Hyves naar Facebook naar TikTok) maar gemeenten zijn in staat gebleken om zich snel aan te passen aan deze nieuwe realiteit. Daarbij maken bestaande maar ook nieuwe technieken het gemakkelijker om informatie te delen met ketenpartners zoals politie en justitie. De wens en ambitie om steeds meer integraal en opgavegericht te werken, versterkt deze tendens. Niet onvermeld mag blijven dat gemeenten over het algemeen gebruikmaken van relatief laagdrempelig instrumentarium of monitoringstools zoals Coosto en OBI4wan. Door gebruik van technische hulpmiddelen kan in relatief korte tijd veel informatie worden verzameld over thema's, maar ook van groepen of personen. Als gevolg hiervan wordt de kans op onder andere privacy-inbreuken groter.

Kortom: online monitoring voorziet duidelijk in een behoefte van gemeenten. In de dagelijkse werkpraktijk ervaren gemeenten weinig drempels om er voortvarend mee

aan de slag te gaan. Grote hoeveelheden data kunnen immers relatief gemakkelijk in informatie worden omgezet die vervolgens ook nog eens snel en in brede kring gedeeld kan worden. Toch blijken uit deze studie de nodige haken en ogen te zitten aan deze nieuwe beleidspraktijk. Dergelijke overwegingen worden belicht in de volgende paragraaf.

5.3 De kwaliteit van het fundament

De vorige paragraaf liet zien dat dat gemeenten een manier hebben gevonden om op relatief eenvoudige wijze data te genereren om aan hun maatschappelijke taken invulling te geven. Deze paragraaf laat zien dat de huidige werkwijze niet zonder risico's is, waarvan we op hoofdlijnen drie met elkaar samenhangende risico's benoemen. Het eerste risico betreft de constatering dat er verschillen in werkwijzen lijken te ontstaan binnen het Nederlandse bestel, het tweede gevaar vloeit voort uit onduidelijkheid omtrent de juridische grondslagen en regelingen terwijl het derde gevaar de constatering betreft dat er nog weinig inzicht is in de werkzaamheid van online monitoring.

5.3.1 *Het ontstaan van verschillen*

Het overgrote deel van de gemeenten heeft aangegeven zich op de een of andere manier met online monitoring van openbare bronnen bezig te houden. Daarbij zien we grote verschillen tussen de doelstellingen en de frequenties waarmee afzonderlijke gemeenten dergelijke onderzoeken uitvoeren. Dit onderzoek laat zien dat het overgrote deel van de gemeenten online monitoring inzet voor communicatiedoeleinden en dat er binnen het domein van openbare orde en veiligheid grote verschillen zijn te constateren tussen gemeenten. Zo zien we grote verschillen in de frequentie waarop gemeenten bepaalde openbare-ordedreigingen online waarnemen. Overlast door jongeren bijvoorbeeld wordt bij sommige gemeenten veel nauwgezetter en frequenter gemonitord dan bij andere gemeenten, terwijl onduidelijk is welke afwegingen daaraan ten grondslag liggen en welke effecten vanuit alternatieve bronnen te verwachten zijn. Ditzelfde geldt bijvoorbeeld voor de bedreigingen ten aanzien van gezagsdragers. Daarnaast brengt deze studie een grote diversiteit aan methoden van monitoring aan het licht. Sommige gemeenten zoeken min of meer handmatig waardoor resultaten sterk afhankelijk zijn van de technische en beoordelingscapaciteiten en willekeur van de medewerker in kwestie. Andere gemeenten hanteren monitoringstools waarbij het de vraag is of men deze technische hulpmiddelen voldoende doorgrondt en de gevolgen in het kader van de bescherming van persoonsgegevens erkent. De nuance die hierbij past, is natuurlijk dat het concept openbare orde per definitie niet overal op dezelfde wijze kan worden ingevuld. Deze is immers sterk afhankelijk van de context en de houding van de gezagsdragers.

We zien kortom dat er tussen gemeenten verschillen zijn ontstaan tussen de mate waarin zij monitoren en de doelen die zij daarmee beogen. Daarnaast zijn er grote verschillen te zien in de wijze waarop men monitort en de tools die men hanteert. Om-

dat ten slotte sterk uit lijkt te maken wie het instrument hanteert, is het de verwachting dat de tweets van een inwoner uit bijvoorbeeld de gemeente Midden-Groningen heel anders worden geïnterpreteerd dan een gelijkluidend Facebookbericht van, laten we zeggen, een Rotterdammer. Daarnaast wordt er volgens respondenten in beperkte mate (8%) gebruikgemaakt van een handelingsprotocol ter ondersteuning van de juridische mogelijkheden en grenzen van online monitoring. Ook dat gegeven draagt niet bij aan een uniforme en systematische werkwijze.

5.3.2 *Juridisch drijfzand*

Binnen gemeenten wordt gemonitord om redenen die volstrekt begrijpelijk zijn, gelet op de juridische positie van de burgemeester en de maatschappelijke positie van de gemeente. Veel van de juridische eisen lijken in de praktijk nageleefd. Dat is niet vanwege kennis van een concreet juridisch kader. Want maar 21% van de medewerkers vindt het juridisch kader duidelijk. Toch lijken intuïtief of op basis van ethische overwegingen veel zaken goed te gaan. Zo worden er volgens respondenten in beperkte mate dossiers bijgehouden, zijn medewerkers terughoudend in het 'doorklikken' op profielen en geven ze aan dat ze voor online monitoring nooit (40%) of beperkt gebruikmaken van privéaccounts (38%) en nooit (67%) of beperkt gebruikmaken van nepaccounts (13%). Toch worden in dit onderzoek een aantal juridische knelpunten gesignaleerd, ook als ervan wordt uitgaan dat in de monitoring uitsluitend openbare bronnen worden betrokken.

Een eerste knelpunt gaat over onduidelijkheden in de verhouding tussen de AVG en de Wet politiegegevens. Monitoring die op grond van artikel 172, eerste lid Gemeentewet wordt verricht, moet voldoen aan de eisen van de AVG. Dat geldt niet voor gegevens die betrekking hebben op strafrechtelijke vervolging. Het onderscheid tussen beide typen monitoring is niet altijd duidelijk te trekken. Uit de enquête blijkt dat het bewaken van de openbare orde en opsporing van strafbare feiten ook in de praktijk dicht tegen elkaar aanliggen. Zo wordt bijvoorbeeld het opsporen van strafbare feiten door 25 procent van de gemeentelijke medewerkers als nevendoel genoemd van monitoring ten behoeve van de openbare orde en veiligheid.

Ten tweede ontbreekt voor in ieder geval de ingrijpende ('stelselmatige') observaties een deugdelijke wettelijke grondslag. In een dergelijke grondslag kan niet bij APV worden voorzien: daarvoor moet in een wet in een formele zin een grondslag bestaan.

Ten derde moet in dit kader aandacht worden gevraagd voor de doelbinding van de monitoring. De AVG en het EVRM verlangen dat de gemeente reflecteert op de redenen voor de monitoring in relatie tot de inbreuk die de monitoring maakt op de privacy van de betrokkenen. Het is bijvoorbeeld relevant hoe concreet de aanwijzingen voor (de vrees voor) verstoringen van de openbare orde zijn, hoe ernstig de verstoring van de openbare orde is of lijkt te zijn, en welke rol de monitoring in dat kader speelt. Aan

die vragen moeten gemeenten voor en tijdens het online monitoren aandacht besteden. Daarin speelt de Functionaris Gegevensbescherming een belangrijke rol. Punt van zorg is dat maar een op de zes gemeentelijke medewerkers aangeeft dat een Functionaris Gegevensbescherming betrokken is bij de online monitoring door de gemeente (16%). In paragraaf 5.4.1 wordt daar op teruggekomen.

5.3.3 *Gebrekkig zicht op werkzaamheid*

De studie heeft een inkijk gegeven in de online monitoring door gemeenten. We weten wie zich ermee bezighouden en met welke redenen. We weten ook welke instrumenten worden ingezet maar we weten nauwelijks hoe deze instrumenten werken. Zo is niet duidelijk welke bronnen en berichten wel en welke niet door de diverse zoekmachines worden geselecteerd. Daarnaast is er blijkens deze studie sprake van een gebrek aan kennis bij gemeentelijke organisaties en ontbreekt het hen aan de tijd om deze nieuwe werkwijzen goed te doorgronden en eigen te maken. Gemeenten die daarbij geautomatiseerd monitoren via diverse softwarepakketten zijn sterk afhankelijk van leveranciers in wier handen de kennis en kunde liggen ten aanzien van de te doorzoeken bronnen, de achterliggende codes ten aanzien van het zoekproces en de selectie en presentatie van de zoekresultaten. Niet alleen dat proces is een black box maar dit geldt ook ten aanzien van de uitkomsten en effecten van online monitoring. Onbekend is in hoeverre mogelijke verstoringen van de openbare orde waargenomen en voorkomen worden en of ditzelfde resultaat dan ook met andere minder verstrekkende middelen bereikt had kunnen worden. Het beeld ontstaat van: "We hebben de mensen, we hebben de middelen, het lijkt te werken, en dus gebruiken we het." Mogelijk zijn gemeenten daarnaast bevreesd voor het missen van online signalen zoals ooit in Haren is gebeurd bij Project X.

Hoe wordt er binnen gemeenten aangekeken tegen de werkzaamheid van online monitoring? Gemeentelijke medewerkers zijn overwegend tevreden over de resultaten die online monitoring oplevert in relatie tot de doelstellingen die zij voor ogen hebben. Ruim de helft van de gemeentelijke medewerkers (56%) geeft aan de informatie als bruikbaar te zien, mits deze in de juiste context wordt geplaatst en wordt vergeleken met informatie uit andere bronnen, bijvoorbeeld politiegegevens of mondelinge toelichtingen. Over de sentimentanalyse zijn de medewerkers kritischer. Ongeveer een kwart van de respondenten ervaart deze optie binnen de monitoringstool als nuttig (24%). Dat heeft onder andere te maken met de accuratesse van de analyse, doordat woorden vaak een andere betekenis hebben in een bepaalde context. Niet zozeer de hoeveelheid informatie, maar vooral de interpretatie van gegevens wordt als een belangrijk knelpunt gezien. Gemeentelijke medewerkers lijken zich bewust van het feit dat de informatie die ze zien slechts een fractie is van de totale (online) informatie. Onder andere gesloten groepen op sociale media zijn niet toegankelijk voor gemeenten en daarmee bevindt veel informatie zich onder de radar. Daarnaast zijn voldoende capaciteit (26% eens) en voldoende kennis en kunde bij medewerkers (39%) mogelijkerwijs knelpunten voor het doelbereik van online monitoring door gemeenten.

Online monitoring door gemeenten is wijdverspreid en algemeen geaccepteerd maar doelstellingen, de aanwezigheid van kaders, middelen, doelgroepen en het gebruik van protocollen loopt sterk uiteen.

5.4 Heroverwegingen en aanbevelingen voor de beleidspraktijk

Op basis van dit onderzoek worden, oplopend van concreet naar abstract, drie (aan elkaar verwante) aanbevelingen gedaan voor de beleidspraktijk. De eerste aanbeveling richt zich op het vastleggen van de huidige beleidspraktijk en het inschatten van de risico's daarvan. De tweede richt zich op de aandacht voor transparantie en ethiek binnen de gemeentelijke organisatiecultuur. Een derde punt snijdt een meer fundamenteel vraagstuk over de inrichting van het Nederlands staatsbestel aan.

5.4.1 *Inventariseer de juridische risico's van de gemeentelijke praktijk*

De eerste aanbeveling voor gemeenten is om hun monitoringspraktijk en de daarbij behorende risico's nauwgezet in kaart te brengen. We hebben immers – op een hoger waarnemingsniveau – gezien dat gemeenten er zeer uiteenlopende doelstellingen, middelen en werkwijzen op nahouden. De eerste aanbeveling luidt dan ook om te inventariseren op welke wijze gegevens worden verzameld, vastgelegd en bewerkt. Ook is het van belang in beeld te brengen in hoeverre en op welke wijze een Functionaris Gegevensbescherming is betrokken en welke kennis men heeft van de werking van ingezette instrumenten voor online monitoring.

Het is primair aan de Functionaris Gegevensbescherming om te beoordelen in hoeverre monitoring in die gemeente in overeenstemming is met (met name) de AVG, artikel 8 EVRM en artikel 10 Grondwet. Vervolgens is het aan te bevelen vast te leggen wat er onder welke omstandigheden mag worden gemonitord en onder welke voorwaarden, wat er niet kan, en welke interne procedure er in geval van twijfel kan worden gevolgd. Kortom: leg de huidige en de gewenste praktijken goed vast in processen en/of in protocollen en start eventueel een verbetertraject ter mitigatie van de onderkende risico's.

5.4.2 *Kalibreer het morele kompas*

De tweede aanbeveling is om de nodige waarborgen aan te brengen ten aanzien van transparantie en privacy. Het wordt vanuit de kennis van deze studie zinvol geacht om de cultuur ten aanzien van gemeentelijke monitoringspraktijken regelmatig bespreekbaar te maken en daarmee een vast onderdeel van de bestuurlijke agenda te maken. Daar waar mens en machine in potentie diep kunnen ingrijpen op de persoonlijke levenssfeer en in de grondrechten, zijn het niet alleen de juridische kaders die de waarborgen zullen vormen. De 'wijsheid' van het individu en de 'bedrijfscultuur' zullen dan in hoge mate bepalen wat wel en wat niet wenselijk is en hoe er in de praktijk wordt gehandeld. Nog lastiger te beïnvloeden maar evenzeer relevant is de maatschappelijk

context waarin dergelijk overheidshandelen plaatsvindt. De demonstraties in Amsterdam tegen racisme en politiegeweld van pinkstermaandag 2020 maakten duidelijk dat de gemeente Amsterdam over onvoldoende informatie beschikte om het aantal deelnemers goed in te kunnen schatten. De reflex zal – onder druk van de publieke opinie – waarschijnlijk zijn om internet meer en beter te monitoren. Aan te bevelen is dergelijke reflexen te leren beheersen door in een vroegtijdig stadium na te gaan welke ethische en morele aspecten mee zouden moeten worden gewogen en met inwoners in gesprek te gaan over hun verwachtingen. Het is aan te bevelen daar met elkaar over te spreken binnen organisatie want ethische overwegingen kunnen alleen in relatie met anderen daadwerkelijke betekenis krijgen.

Naast omgang van gemeenten met online monitoring is het ook aan te bevelen de werkwijzen ten aanzien van online monitoring en gegevensverwerking duidelijker te communiceren aan inwoners van gemeenten die weten wat ze wel en niet monitoren. Dat zou bijvoorbeeld gedaan kunnen worden door te communiceren over doelstellingen van monitoring (expliciet) en door aan te geven hoe de gemeente werkt en welke vuistregels daarbij gehanteerd worden.

5.4.3 *Verstrek handreikingen voor het delen van 'good practices'*

Deze studie laat een grote diversiteit aan werkwijzen, middelen en doelstellingen zien op het gebied van gemeentelijk monitoren. Enerzijds is dit logisch vanwege de heersende gedachte dat men op lokaal niveau het beste kan inschatten hoe men dient op te treden bij bedreigingen van de openbare orde. De vraag is echter of gemeenten niet steeds zelf het wiel opnieuw uitvinden en of zij genoeg van elkaar leren. Dat leren geldt ook voor de (lastige) interpretatie van online signalen. Dit zou mogelijk kunnen pleiten voor een grotere rol door, hetzij van 'bovenaf' door het ministerie van BZK, hetzij van 'binnenuit' en van 'onderop' door de VNG-handreikingen voor het delen van 'best practices' te verstrekken. Wellicht kiest men dan voor een vorm van harmonisering ten aanzien van de doelen, de softwarepakketten, de trainingen omtrent de vaardigheden en de juridische kaders. Handhaving van de openbare orde is mede door de opkomst van internet immers niet meer voorbehouden aan de autoriteit waar de fysieke gebeurtenis plaatsvindt maar dient steeds meer als een netwerkvraagstuk te worden aangepakt. Vanuit dit onderzoek zullen we dus niet pleiten niet voor een 'one size fits all'-benadering maar wel voor meer coördinatie, uitwisseling en samenwerking. Daarbij is het onverminderd van belang dat gemeenten in het algemeen en burgemeesters in het bijzonder maatwerkoplossingen kunnen bieden die recht doen aan de karakteristieken van de lokale situatie en de eigen opvattingen ten aanzien van het gewenste niveau van openbare orde. Efficiëntie kan echter wel een aanvullend criterium zijn, want het vermoeden bestaat dat er door politie en gemeenten veel dubbel werk wordt verricht.

5.5 Aanbevelingen voor verder onderzoek

Wat betreft de aanbevelingen voor verder onderzoek zijn twee hoofdlijnen te onderscheiden, te weten: verdieping en verbreding.

5.5.1 *Verdieping*

De gehanteerde werkwijze in dit onderzoek bracht, onder andere door triangulatie, een betrouwbaar en valide beeld op in de breedte van een groot aantal aspecten van online monitoring. Toch is het vanuit onderzoeksperspectief raadzaam om meer diepgaande kennis van de ingezette middelen en processen te vergaren, de black box kan immers verder geopend worden. Hierbij kan men denken aan een participatieve monitoring waarbij de onderzoeker meewerkt in de dagelijkse praktijk van online monitoring of het bijhouden van een logboek door medewerkers. Een andere optie kan zijn om via de analyse van werkprocessen, dus op een groter detailniveau, verder inzicht te krijgen in de dagelijkse praktijk van online monitoring. Daarbij ligt het voor de hand om de samenwerking tussen actoren in de veiligheidsketen te beschouwen: welke informatie wordt wanneer gedeeld, met welke doel en welke risico's zitten daaraan vast? Daarbij is het relevant om de ontwikkelingen binnen de politie en gemeenten goed te volgen. Denk bijvoorbeeld aan nieuwe toepassingen, zoals het gebruik van scanauto's door gemeenten. De juridische risicokaart waar deze studie een aanzet toe geeft, zou daarbij verder ontwikkeld en getest kunnen worden. Online monitoring is immers geen statisch gegeven maar is continu onderhevig aan nieuwe ontwikkelingen en voortschrijdend inzicht.

Daarnaast is aan te bevelen meer onderzoek te doen naar de duiding van online signalen. Uit dit onderzoek en uit recente andere onderzoeken blijkt dat het heel moeilijk is om online signalen te kunnen begrijpen en vertalen in concrete en passende interventies.[241] Een complicerende factor is dat het steeds vaker moeilijk blijkt, ook juridisch gezien, om te achterhalen wie er achter bepaalde online handelingen zit. Meer inzicht in de beweegredenen van online handelingen van inwoners en de relatie tussen hun online en offline gedrag kan meerwaarde hebben voor de online monitoring van gemeenten (en andere partijen) en tevens bijdragen aan het inzetten van effectieve interventies voor de openbare orde en veiligheid.

5.5.2 *Verbreding*

Tot nu toe zijn de (literatuur)studies vooral gericht geweest op monitoring bij politie en nu dus ook bij Nederlandse gemeenten. Het lijkt aannemelijk dat ook in andere publieke domeinen op een of andere wijze monitoring van openbare bronnen plaatsvindt. Te denken valt aan handhavingsvraagstukken en veiligheidsrisico's in het kader van de

241 Zie onder andere: A. Boin, K. Nooy & P. van der Velden (2020).

COVID-19-uitbraak, onderwijs, milieuvraagstukken en ook vraagstukken op het gebied van sociale zekerheid en fraudepreventie. Om een breed beeld van monitoring door andere overheidsorganen en in het bijzonder door ambtenaren met bijzondere opsporingsbevoegdheden (boa's) te verkrijgen, kan een dergelijke overzichtsstudie worden uitgevoerd. Daarbij kan wederom de nadruk wordt gelegd op de juridische, de ethische en de organisatorische risico's, maar ook op mogelijkheden voor innovatieve handhaving en het bieden van handelingsperspectief. Daarnaast kan gedacht worden aan ontwikkelingen bij de basisteams en digitale wijkagenten bij het signaleren van online dreigingen en de kennisuitwisseling met andere partijen, waaronder de gemeente. Tot slot kan verbreding plaatsvinden door een vergelijkende studie uit te voeren naar de monitoringspraktijken in andere landen. Daarbij ligt het voor de hand om te starten met onze buurlanden vanwege grensoverschrijdende vraagstukken op het gebied van openbare orde en veiligheid.

5.6 Reflectie

Tot slot van deze studie kijken we heel kort terug op twee – ogenschijnlijk tegenstrijdige – ervaringen. Dit betreft enerzijds de moeite die respondenten hadden om een 'uitgesproken' oordeel te vellen over (deel)aspecten van online monitoring en anderzijds de grote bereidwilligheid om actief te participeren in het onderzoek.

Hoewel de vragenlijsten meerdere malen zijn getest op potentiële respondenten valt uit de respons op de vragenlijsten op te maken dat een significant deel van de respondenten vragen over bijvoorbeeld de transparantie van online monitoring, het juridisch kader en de kennis en kunde van het personeel de bewuste vragen met 'neutraal' heeft beantwoord. Het hoog percentage 'neutrale' antwoorden kan mogelijk geduid worden door nuance en wisselende omstandigheden (context) waardoor een eenduidig antwoord lastig is, maar kan tevens wijzen op de moeite die respondenten hebben om een uitgesproken mening te geven. Dat is goed mogelijk, want ook de categorie 'weet niet' komt veel voor in het onderzoek. Dit kan enerzijds verklaard wordt door een gebrek aan kennis (en bewustzijn) over bepaalde regelgeving, werkwijzen en handelingen bij online monitoring, maar anderzijds ook doordat het onderzoek is gebaseerd op medewerkers van zowel de gemeentelijke afdelingen Communicatie als OOV. Een gevolg is dat zij geregeld aangeven niet te weten of en met welke doelstellingen er gemonitord wordt bij de afdeling waar men niet werkzaam is en soms anders aankijken tegen de monitoring binnen de gemeente. Dit resultaat laat zien dat 'de gemeente' niet bestaat, maar ook dat afdelingen soms niet van elkaar weten hoe men precies werkt. Waarschijnlijk is er dus ook intern winst te halen in de afstemming over de werkwijzen rondom monitoring binnen gemeenten. Daarnaast zegt de deelname van een medewerker OOV of Communicatie, wat verschilt per gemeente, mogelijk iets over hoe gemeenten werken.

De belangstelling en bereidwilligheid van het werkveld om bij te dragen aan het onderzoek hebben geleid tot een hoge respons op de vragenlijst (45% van unieke gemeenten). De gemeentelijke medewerkers die zijn aangeschreven, zijn ruimschoots bereid gebleken om deel te nemen aan interviews en tijdens de gesprekken heeft men zich open en transparant geuit over ervaren dilemma's. Uit een recent ander onderzoek blijkt die openheid over online monitoring richting de inwoners van gemeenten in zijn geheel niet naar voren te komen. Uit een steekproef onder 27 willekeurig geselecteerde gemeenten blijkt dat, in ieder geval als het gaat om beleid, geen van de gemeenten aandacht besteden aan online monitoring ten behoeve van de openbare orde en veiligheid.[242] Inwoners zouden op zijn minst een inschatting moeten kunnen maken van de mate en wijze van online monitoring van gemeenten en van de doelstellingen waarmee dit plaatsvindt. Die transparantie zou de juridische problemen niet direct oplossen, maar zorgt er wel voor dat er maatschappelijke discussie over het thema kan plaatsvinden en werkt mogelijk stimulerend voor het vertrouwen dat inwoners hebben in hun lokale overheid.

Het onderwerp leefde ten tijde van het onderzoek en is door de gevolgen van COVID-19 nog meer onder de aandacht gekomen. Met de recente manifestaties op de Dam en het Malieveld in gedachten en de verspreiding van desinformatie en complottheorieën, is het aannemelijk dat de belangstelling voor online monitoring nog zal verder toenemen. Wat betreft gemeenten is het van groot belang dat de black box van online monitoring verder wordt geopend en dat techniek, ethiek en recht blijvend met elkaar in balans worden gehouden. Een goed fundament is daarom essentieel voor een duurzame gemeentelijke monitoringspraktijk.

242 W.Ph. Stol & W. Bantema (2020).

Literatuurlijst

Baarda, B. (2009). Dit is onderzoek. Handleiding voor kwantitatief en kwalitatief onderzoek. Groningen: Uitgeverij Noordhoff.

Bakker, J., H. Tops, D. Nonahal & F. Willemsen (2016). Toepassing Social Media Data-Analytics voor het Ministerie van Veiligheid en Justitie. Toelichting, beschrijving en aanbevelingen. Coosto.

Bantema, W., S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.ph. Stol (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld* (reeks politie en wetenschap). Den Haag: Sdu.

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

Becker, M.J. (2015). *Ethiek van de digitale media*. Amsterdam: Boom.

Boin, A., K. Nooy & P. van der Velden (2020). Een verkeerde afslag: een analyse van de 1 juni demonstratie in Amsterdam.

Bullock, K. (2018). 'The police use of social media: Transformation or normalisation?' *Social Policy and Society, 17*(2), 245-258.

Buro Jansen & Janssen (2017). 'Social Media Surveillance in Nederland.' *Observant,* 70.

Criado, J.I., F. Rojas-Martín & J.R. Gil-García (2017). 'Enacting social media success in local public administrations.' *International Journal of Public Sector Management, 30* (1), 31-47.

Data Protection Working Party (2016). *Opinion 4/2007 on the concept of personal data*, 20 juni 2016, 01248/07/EN/WP 136, p. 21. Article 29.

Dijk, J.A. van, L. Wijngaert & S.T. Tije (2015). *Overheidsparticipatie in sociale media.* Universiteit Twente-Center for Telematics and Information Technology.

Eijk, C. van, W. Broekema, & R. Torenvlied (2013). Geen uniformen, maar specialisten. Betrokkenheid van externe experts in crisissituaties. Leiden: Universiteit Leiden.

Frankwatching (2018). *Newsrooms bij gemeenten: de 4 grootste misverstanden*. Bron: https://www.frankwatching.com/archive/2018/12/11/newsrooms-bij-gemeenten-de-4-grootste-misverstanden/.

Gemeente Amsterdam (2016). *Verkenning Social Media en Jeugd en Veiligheid*. Bron: https://static.nrc.nl/2018/hangjongeren-privacy/1116uitlegstuk.pdf.

Gemeente Amsterdam (2019). *Agenda Digitale Veiligheid van de gemeente Amsterdam*. Bron: https://amsterdamlogistics.nl/wp-content/uploads/2019/11/agenda_digitale_veilig-heid_amsterdam.pdf.

Gemeente Delft (jaartal onbekend). *Keuzehulp Social Media*, Gemeente Delft.

Gerards, J., (2019). *General Principles of the European Convention on Human Rights*, Cambridge: Cambridge University Press.

Gerards, J., R. Nehmelman & M. Vetzo (2018). *Algoritmes en grondrechten*, Utrecht.

Greer, S., (1997). The exceptions to Articles 8 to 11 of the European Convention on Human Rights, bron: www.echr.coe.int.

Ham, T. van, L. Scholten, A. Lenders & H. Ferwerda (2017). *Vechten op afspraak. Inzicht in het fenomeen en input voor de ontwikkeling van een politiestrategie* (reeks politie en wetenschap). Den Haag: Sdu.

Hengst, M. den, T. ten Brink & J. ter Mors (2017). *Informatiegestuurd politiewerk in de praktijk*. Deventer: Vakmedianet.

Hughes, K. (2019). 'The Public Figure Doctrine and the Right to Privacy', *Cambridge Law Journal*, March 2019, p. 73-78.

IJzendoorn, M.H. van (1988). 'De navolgbaarheid van kwalitatief onderzoek I: methodologische uitgangspunten.' *Nederlands Tijdschrift voor Opvoeding, Vorming en Onderwijs, 4*(5), 280-288.

IM Adviesrapport Tools Informatieorganisatie (2015). Bron: https://respubca.home.xs4all.nl/pdf/ politiebesluitadviesrapportd.pdf.

Information Commissioner's Office (2012). *Determining what is personal data*, bron: Ico.org.uk.

Johannink, R.H., I. Gorissen & N.K. van As (2013). 'Sociale media: factor van invloed op onrustsituaties?' *Politiekunde, 52*.

Jong, M.A.D.W. de, W. van der. Woude, W.S. Zorg, J.L.W. Broeksteeg, R. Nehmelman, I.U. Tappeiner, & H.R.B.M. Kummeling (2017). *Orde in de openbare orde. Een onderzoek naar verbetering van de toepasbaarheid en inzichtelijkheid van het openbare-orderecht*.

Kok, D., (red) (2013). *Sociale gemeenten. De kracht van nieuwe media*. Delft: Academische Uitgeverij Eburon.

Koops, E.J., R.J. Verbeek, B.W. Schermer, M.J. Grapperhaus, A. Kuijer, D. Ven-Laheij, … & M. Viersma (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving.*

Kortmann, C.A.J.M., P.P.T. Bovend'Eert, J.L.W. Broeksteeg, C.N.J. Kortmann & B.P. Vermeulen (2016). *Constitutioneel recht*, Deventer: Wolters Kluwer, p. 382-383.

Kranenborg, H.R. & L.F.M. Verhey (2018). De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief (Mastermonografieën staats- en bestuursrecht), Deventer: Wolters Kluwer, p. 109.

Lewis, P., T. Newburn, M. Taylor, C. Mcgillivray, A. Greenhill, H. Frayman & R. Proctor (2011). *Reading the riots: investigating England's summer of disorder.* London: The Guardian.

Lodder, A.R. & M.B. Schuilenburg (2016). 'Politie-webcrawlers en Predictive policing.' *Computerrecht, 2016(3),* 150-154.

Mateescu, A., D. Brunton, A. Rosenblat, D. Patton, Z. Gold & D. Boyd (2015). 'Social media surveillance and law enforcement.' *Data Civil Rights, 27*, 2015-2027.

Meijer, A.J. (2013). Politie en sociale media. Van hype naar onderbouwde keuzen. Reed Business Information.

Meijer, A.J. & D. van Berlo (2011). 'Big Brother of gesprekspartner? Monitoren van communicatie van burgers via social media.' *Bestuurswetenschappen, 6*, 90-98.

Murray, A.D. (2016). *The legal challenges of social media*. In: Gillies Lorna and Mangan, David, (Eds.) Mapping the rule of law for the internet. Edward Elgar Publishing, UK.

Murray, A. (2019). Information Technology Law. The Law & Society, Oxford: Oxford University Press.

Musteen, S.D. (2013). Social Media's Law Enforcement.

Nieuwenhuis, A.J, M. den Heijer & A.W. Hins (2017). *Hoofdstukken Grondrechten*, Nijmegen: Ars Aequi Libri, p. 137-138.

Oerlemans, J.J. (2018). 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk.' *Platform Modernisering Strafvordering.*

Oerlemans, J.J. & B.J. Koops (2012). 'Surveilleren en opsporen in een internetomgeving.' *Justitiële verkenningen, 38*(5), 15.

Oerlemans, J.J. & Y.E. Schuurmans (2019). 'Internetonderzoek door bestuursorganen.' *Nederlands Juristenblad, 94* (20), 1458-1466.

Oosterhoff, M. (2016). *Opsporing op social media* (Master thesis). Heerlen: Open Universiteit.

Politie-eenheid Zeeland-West-Brabant (2015). Online mediamonitoring tool en proces (2) Ervaringen en inzichten naar aanleiding van operationele ervaring bij de politie-eenheid Zeeland-West-Brabant.

Politiestudies (2013). Bron: https://www.researchgate.net/publication/304807161_Kritisch_verslag_ over_het_gebruik_van_inlichtingen_uit_open_bronnen_en_sociale_media_-verslag_van_een_ studiedag_van_het_BISC_december_2013, p.2

Raad van Europa (2017). Comparative study on blocking, filtering en and take-down of illegal internet content.

Rainey, B., E. Wicks & C. Ovey, *Jacobs, White & Ovey (*2017). *The European Convention on Human Rights*, Oxford: Oxford University Press

Rizza, C., Â. G. Pereira & P. Curvelo (2014). '"Do-it-yourself justice": considerations of social media use in a crisis situation: the case of the 2011 Vancouver riots.' *International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 6*(4), 42-59.

Ruddell, R., & N. Jones (2013). 'Social media and policing: matching the message to the audience. Safer Communities.' *Safer communities. 12* (2), 64-70.

RvS, Voorlichting over grondwettelijke aspecten van (voor)genomen crisismaatregelen, 25 mei 2020, par. 4.a en 7.b.

Schermer, B.W., D. Hagenauw & N. Falot (2018) Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming, Ministerie van Justitie en Veiligheid.

Schweizerische Eidgenossenschaft (2011). Legal Basis for Social Media Report of the Federal Council in Fulfilment of the Amherd Postulate 11.3912 of 29 September 2011.

Snively, D.T. (2016). Doctoral dissertation. Effective social media use by law enforcement agencies: A case study approach to quantifying and improving efficacy and developing agency best practices.

Stichting Arbeidsmarkt- en opleidingsfonds gemeenten (2014). *Handelingsinstructies – Agressie Social Media en Webcare.*

Stol, W.ph. & W. Bantema (2020). *Stadbestuur en digitale veiligheid, een analyse van beleidsplannen.* In M. Malsch en J.W. Sap (red.), Orde en verwarring in de stad. Boom Criminologie

Stol, W.ph., & L. Strikwerda (2018). Online vergaren van informatie voor opsporingsonderzoek. *Tijdschrift voor Veiligheid, (17)* 1-2, 8-22.

Thiel, S. V. van (2007). *Inleiding Bestuurskundig onderzoek.* Bussum: Uitgeverij Coutinho.

Veen, S. van & T. van den Ende (2012). *Wat vertellen social media ons over dreigingen?* Bron: https://www.trendsinveiligheid.nl/wp-content/uploads/2018/04/ tiv2017_12_ wat_vertellen_social_media_ons_over_dreigingen-1.pdf.

Veltman, P. (2014). *Utrecht en de ontwikkeling van Social Webcare bij de gemeente Utrecht: een kijkje achter de schermen.* Bron: https://www.marketingfacts.nl/berichten/ webcare-bij-de-gemeente-utrecht-een-kijkje-achter-de-schermen.

Yang, M. (2013). The collision of social media and social unrest: Why shutting down social media is the wrong response. *Northwestern Journal of Technology and Intellectual Property, 11* (7), 708-728.

Zavattaro, S.M. (2013). Social media in public administration's future: A response to Farazmand. *Administration & Society, 45* (2), 242-255.

Zee, F. van der (2004). Kennisverwerving in de empirische wetenschappen. De methodologie van wetenschappelijk onderzoek. Groningen: BMOOO.

Bijlage I. **Interviewprotocol gemeenten**

Introductie

Wie zijn wij en wat gaan we doen?
Allereerst bedankt dat u mee wilt werken met ons onderzoek. De Onderzoeksgroep Cybersafety (NHL Stenden Hogeschool en de Politieacademie) voert onderzoek uit naar monitoring in cyberspace door gemeenten, in verband met ordehandhaving. Door op werkbezoek te gaan bij de gemeente willen we inventariseren welke mogelijkheden en beperkingen er zijn bij het monitoren in cyberspace. Aan de hand van deze informatie kunnen we in kaart brengen of en op welke manier monitoring ingezet kan worden door gemeenten ter versterking van openbare orde en veiligheid. Wij voeren dit onderzoek uit in opdracht van het programma Politie en Wetenschap en in samenwerking met de RUG.

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

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

Verloop
Tijdens dit werkbezoek willen we graag de werkzaamheden van uw team observeren. Daarnaast willen we u vragen stellen over 1) digitale dreigingen van de openbare orde en veiligheid, 2) online monitoring, 3) knelpunten die u en uw team mogelijk ervaren en 4) de rolverdeling van de gemeente, de politie en het OM in het online monitoren en handelen naar deze digitale dreigingen.

Introductievragen

1. Wat is uw functie? *(indien nodig)*
2. Kunt u meer vertellen over uw werkzaamheden?

Digitale dreigingen

We willen eerst graag enkele vragen stellen over digitale dreigingen die een risico vormen voor de openbare orde en veiligheid. Met digitale dreigingen bedoelen we alle dreigende openbare-ordeverstoringen waarbij gedragingen in cyberspace het startpunt zijn of een katalysator.

3. In hoeverre heeft u in uw werk/uw gemeente te maken met digitale dreigingen die een risico vormen voor de openbare orde en veiligheid (OOV)? *[aanpassen per respondent]*
   a) Welke dreigingen zijn voorgekomen in uw vakgebied?
   b) Heeft u online dreigingen gezien grote feesten (Project X)?
   c) Heeft u online oproepen van demonstraties (gele hesjes/blokkeerfriezen/hooligans)?
   d) Heeft u te maken gehad met treitervloggers?
   e) Heeft u te maken gehad met online dreigingen gericht tegen de politie? (Mitch Hendriquez, uitlokkende filmpjes online van veroordeelden/verdachten)?
   f) Reacties op birdbox challenge?
   g) Terugkeer zedendelinquenten?
   h) Treitervloggers (Ismael Ilgun)
   i) Terugkeer zedendelinquenten
   j) Reacties op film (birdbox challenge)
   k) Gevolgen van een app (pokemon app)
   l) Ruzie tussen burgers online
   m) Sexting
   n) Polarisatie (Facebookgroep opgericht door ouders tegen een schoolbezoek aan moskee, WhatsApp buurtgroep waarin bewoners jacht maken op Polen)
4. Wat zijn volgens u mogelijke gevolgen van deze digitale dreigingen?
   a) Welke digitale dreiging is het grootst voor de OOV?
   b) Welke digitale dreiging is het minst groot voor de OOV?

Online monitoren

De volgende vragen gaan over online monitoring.

5. In hoeverre heeft u in uw werk te maken met online monitoring van digitale dreigingen van de OOV? *Zoals: (benoem enkele dreigingen van vraag 3)*
6. Op welke wijze wordt online gemonitord?
   a) Is de monitoring georganiseerd of ongeorganiseerd (toevallige signalen)?
   b) Is de monitoring constant of incidenteel?
   c) Gebruikt u een protocol voor het online monitoren van digitale dreigingen van de OOV? Zo ja, is deze in overleg met de politie opgesteld?
      i) Is er een overall socialemediabeleid?

d) Welk programma wordt gebruikt?
   i) Gebruiken deze open bronnen of ook gesloten bronnen?
e) Welke afdeling? Hoeveel mensen zijn aan het online monitoren?
   i) Zijn er trainingen om online te monitoren? Indien nee, vindt u dat men opgeleid zou moeten zijn?
f) Is monitoring/ observering door gemeente te vergelijken met digitaal fouilleren (ST)?
g) In hoeverre werkt u bij het monitoren samen met andere partijen?
   i) Politie ?
   ii) OM ?
   iii) Sociale media?
   iv) Andere partijen ?

7. In hoeverre constateert u digitale dreigingen met monitoring?
8. Wat zijn vervolgstappen na detectie van digitale dreigingen?
9. Reageert u/uw team op een gedetecteerde digitale dreiging? Zo ja,
   a) Hoe vaak reageert u/uw team op deze digitale dreigingen?
   b) Wanneer reageert u/uw team wel of niet?
   c) Op welke manier reageert u/uw team op deze digitale dreigingen?
   d) In hoeverre heeft deze reactie effect?
10. Met welke doelstelling is uw team aan het online monitoren?
11. Wordt deze doelstelling gehaald?

Knelpunten

De volgende vragen gaan over de mogelijke knelpunten in online monitoring. Dit zal gaan over de juridische, organisatorische, technische en ethische aspecten van monitoring.

12. Wat is de **wettelijke** grondslag van monitoring binnen de gemeente? Welke wetsartikelen zijn dit?
    a) Voldoen deze huidige bevoegdheden?
    b) Welke voorwaarden stellen die bevoegdheden?
    c) Is deze wettelijke grondslag vastgelegd in een protocol? Zo ja, wordt daarmee gewerkt?
    d) In hoeverre ervaart uw team juridische grenzen in de monitoring?
    e) In hoeverre ervaart uw team juridische knelpunten in de monitoring?
    f) Wat is nodig om knelpunten in monitoring te verhelpen?
13. In hoeverre ervaart uw team **organisatorische** grenzen in de monitoring?
    a) In hoeverre ervaart uw team organisatorische knelpunten in de monitoring?
       i) Organisatorisch binnen de gemeente?
       ii) In de samenwerking met politie?
       iii) In de samenwerking met het OM?
    b) Wat is nodig om organisatorische knelpunten in monitoring te verhelpen?
       i) Organisatorisch binnen de gemeente?
       ii) In de samenwerking met politie?
       iii) In de samenwerking met het OM?

14. In hoeverre ervaart uw team **technische** grenzen in de monitoring?
    a) In hoeverre ervaart uw team technische knelpunten in de monitoring?
    b) Wat is nodig om technische knelpunten in monitoring te verhelpen?
15. In hoeverre ervaart uw team **ethische** grenzen in de monitoring?
    a) In hoeverre ervaart uw team ethische knelpunten in de monitoring?
    b) Wat is nodig om ethische knelpunten in monitoring te verhelpen?

Rolverdeling

De volgende vragen gaan over de rolverdeling van de politie, de gemeente en het OM in het handelen naar digitale dreigingen in het kader van OOV.

16. Wat is volgens u de rol van **gemeenten** in online monitoren van digitale dreigingen in het kader van OOV?
    a) Wat zou volgens u de rol van gemeenten moeten zijn?
17. Wat is volgens u de rol van de **politie** in het algemeen in online monitoren van digitale dreigingen in het kader van OOV?
    a) Wat zou de rol van de politie in het algemeen moeten zijn?
18. Wat is volgens u de rol van het **Openbaar Ministerie** in online monitoren van digitale dreigingen in het kader van OOV?
    a) Wat zou volgens u de rol van het OM moeten zijn?
19. Kan de gemeente een rol vervullen in het online monitoren om politiewerk aan te vullen in het **kader van OOV**?
    a) Op welke wijze?
    b) Zijn hier knelpunten aan verbonden? En hoe kan op deze knelpunten worden ingespeeld?
        i) Juridisch?
        ii) Technisch?
        iii) Organisatorisch?
20. Wie zouden nog meer een rol kunnen of moeten spelen in online monitoren van digitale dreigingen in het kader van OOV?
21. Kan de gemeente een rol vervullen in het online monitoren om politiewerk aan te vullen in het **kader van de opsporing**?
    a) Op welke wijze?
    b) Zijn hier knelpunten aan verbonden? En hoe kan op deze knelpunten worden ingespeeld?
        i) Juridisch?
        ii) Technisch?
        iii) Organisatorisch?
22. Wie zouden nog meer een rol kunnen of moeten spelen in online monitoren van digitale dreigingen in het kader de opsporing?

Afsluitende vragen en afronding

23. Is er volgens u een onderwerp of gedachte niet aan de orde gekomen dat/die u nog graag zou willen delen?

Respondent bedanken, opname eindigen en vervolgprocedure toelichten
Respondent nogmaals mededelen dat de uitwerking van het interview binnen twee weken gestuurd wordt en respondent daar commentaar op kan geven.

Bijlage 2. **Vragenlijst**

Welkom bij deze vragenlijst. We willen in kaart brengen of en op welke manier gemeenten openbare bronnen op internet (zoals Facebook, Instagram, blogs) raadplegen, gericht op het handhaven van de openbare orde en veiligheid (OOV). Het raadplegen van online openbare bronnen noemen we in deze vragenlijst online monitoring. De vragenlijst bestaat uit zeven blokken: algemene vragen, werkwijze bij online monitoring in het kader van de OOV en vraagstukken over de techniek, juridische kaders, organisatie en ethiek.
Het invullen van de vragenlijst duurt ongeveer 15-20 minuten. De vragen zijn bedoeld voor vertegenwoordigers van afdelingen binnen de gemeente die in hun werk te maken hebben met online monitoring (bijv. werkzaam als beleidsmedewerkers/adviseurs bij de afdeling communicatie of OOV). Meerdere mensen binnen de gemeente kunnen dus deze vragenlijst invullen. Alle gegevens worden anoniem verwerkt.
Het onderzoek wordt uitgevoerd door de Onderzoeksgroep Cybersafety (NHL Stenden Hogeschool) in samenwerking met de Rijksuniversiteit Groningen en in opdracht van Politie en Wetenschap.

Algemene vragen

1. In welk vakgebied bent u werkzaam? (meerdere antwoorden zijn mogelijk)
   - ☐ Communicatie
   - ☐ Openbare Orde en Veiligheid
   - ☐ Anders, namelijk…

2. Hoeveel inwoners heeft uw gemeente?
   - ☐ < 15.000 inwoners
   - ☐ 15.000-30.000 inwoners
   - ☐ 30.000-60.000 inwoners
   - ☐ 60.000-100.000 inwoners
   - ☐ 100.000-200.000 inwoners
   - ☐ 200.000 inwoners

3. In hoeverre heeft uw gemeente een stedelijk of plattelands karakter?

1	2	3	4	5
Stedelijk		Gemengd		Plattelands

Vragen over werkwijzen bij online monitoring

De volgende vragen gaan over de werkwijze bij online monitoring. Met online monitoren wordt het bekijken en/of in de gaten houden en/of opslaan van publiek toegankelijke bronnen op internet bedoeld. Deze bronnen zijn beschikbaar zonder in te hoeven loggen op een website. Voorbeelden zijn openbare socialemedia-accounts (Webcare), nieuwsartikelen en reguliere websites zoals www.politie.nl.

4. Worden er binnen de gemeenteorganisatie publiek toegankelijke bronnen op internet geraadpleegd (hierna: online monitoring)?
   - ☐ Ja
   - ☐ Nee (R: q4a)

4a. Kunt u toelichten waarom de gemeente geen gebruikmaakt van publiek toegankelijke bronnen op internet?

Bedankt voor uw medewerking. De vragenlijst stopt hier

5. Welke monitoringstool gebruikt uw gemeente voor online monitoring ?
   - ☐ Coosto
   - ☐ OBI4wan
   - ☐ Buzzcapture
   - ☐ HowAboutYou
   - ☐ Anders, namelijk… *(niet verplicht invulveld)*
   - ☐ Weet ik niet

6. De vorige vraag ging over het gebruik van een tool voor online monitoring. Gebruikt uw gemeente ook nog **andere methoden** voor online monitoring?
   - ☐ Ja, namelijk… (verplicht invulveld)
   - ☐ Nee
   - ☐ Weet ik niet

7. Welke afdeling houdt zich bezig met online monitoring binnen de gemeente? (meerdere antwoorden mogelijk)

	Ja	Nee	Weet ik niet	Niet van toepassing
Afdeling Communicatie				
Webcare/Dienstverlening/Klant Contact Centrum				
Newsroom				
Afdeling Openbare Orde en Veiligheid				
Afdeling Onderzoek				
Andere afdeling, namelijk *(invulveld)*				

8. Met welk **doel** wordt online geobserveerd binnen uw afdeling van de gemeente?

	Hoofddoel	Nevendoel	Geen doel	Weet ik niet
Dienstverlening verbeteren naar de inwoners van de gemeente				
Weten wat er speelt in de gemeente				
In de gaten houden hoe de gemeente wordt gewaardeerd				
Signalering van dreigingen in openbare orde en veiligheid				
Onderzoeken van gesignaleerde dreigingen in openbare orde en veiligheid				
Handhaving van dreigingen in de openbare orde en veiligheid				
Bijdragen aan opsporing van strafbare feiten				
Anders, namelijk (*invulveld*)				

9. Kunt u een toelichting geven op (een van) uw antwoorden over werkwijze bij online monitoring?

Vragen over werkwijzen bij het online monitoren van openbare orde en veiligheid
De volgende vragen gaan over de werkwijze bij online monitoring van publiek toegankelijke bronnen specifiek gericht op openbare orde en veiligheid.

10. Hoe vaak worden in uw gemeente online berichten geobserveerd over een mogelijke verstoring van de OOV door … ?

	Nooit	Minder vaak dan jaarlijks	Een (paar) keer per jaar	Een (paar) keer per maand	Een (paar) keer per week	Een (paar) keer per dag	Niet van toepassing
hooliganisme/dreigend voetbalgeweld							
bedreiging gezagsdragers							
polarisatie tussen inwoners							
polarisatie op thema							
overlast door (groepen) jongeren							
overlast door individuen die al vaker ophef hebben veroorzaakt							
oproepen tot demonstraties en manifestaties							

	Nooit	Minder vaak dan jaarlijks	Een (paar) keer per jaar	Een (paar) keer per maand	Een (paar) keer per week	Een (paar) keer per dag	Niet van toepassing
teruggekeerde zedendelinquenten							
ondermijnende activiteiten							
nepnieuws							
onrust rond politieke besluiten							
onrust rond AZC's							
illegale evenementen (straatraces, dancefeesten)							
anders, namelijk *(niet verplicht invulveld)*							

11. Hoe vaak worden in uw gemeente online berichten over een mogelijke verstoring van de OOV …?

	Nooit	Minder vaak dan jaarlijks	Een (paar) keer per jaar	Een (paar) keer per maand	Een (paar) keer per week	Een (paar) keer per dag	Weet ik niet
gesignaleerd	R: q12 overslaan						
in de gaten gehouden, maar niet opgeslagen							
automatisch in de gaten gehouden en opgeslagen (dossiervorming)							
handmatig in de gaten gehouden en opgeslagen (dossiervorming)							
doorgestuurd binnen de gemeente							
doorgestuurd naar de politie							
doorgestuurd naar andere partijen							

12. Op welke wijze worden dreigingen op de openbare orde en veiligheid online **gesignaleerd?** Meerdere antwoorden mogelijk
    - ☐ Door signalen die naar voren komen bij de reguliere monitoring, waar niet specifiek wordt gezocht naar OOV thema's (bijvangst)
    - ☐ Door signalen die naar voren komen bij de reguliere monitoring, inclusief OOV thema's
    - ☐ Door een specifieke zoekopdracht over een specifiek OOV thema, buiten reguliere monitoring om
    - ☐ Anders, namelijk… (*niet verplicht invulveld)*

13.

Bij een concrete dreiging van de openbare orde…	Nooit	Soms	Vaak	Altijd	Weet ik niet
wordt online informatie over de dreiging opgevraagd bij de politie					
wordt online informatie verzameld over de dreiging binnen de gemeentelijke organisatie (omgevingsanalyse)					
gebruikt de gemeente nepaccounts op sociale media om een beter beeld te krijgen					
gebruikt de gemeente privéaccounts van medewerkers op sociale media om een beter online beeld te krijgen					

14. Kunt u een toelichting geven op (een van) uw antwoorden over **werkwijzen bij het online monitoren van OOV?**

Techniek

In hoeverre bent u het oneens/eens met de volgende stellingen?

15. De monitoringstool van de gemeente is geschikt om **bruikbare** informatie te verzamelen om gestelde doelen te behalen.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

16. De monitoringstool van de gemeente is geschikt om **voldoende** informatie te verzamelen om gestelde doelen te behalen.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

17. De monitoringstool van de gemeente zorgt voor te veel **irrelevante** informatie.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

18. De monitoringstool van de gemeente biedt **onvoldoende content** (beperkt aantal sociale media platformen/berichten/websites).

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

19. De sentimentanalyse (labelen van berichten positief/negatief/neutraal) van de **monitoringstool is nuttig**.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

20. Wilt u (een van) uw antwoorden over techniek toelichten?

21. Hoe wordt de bruikbaarheid van de verkregen informatie beoordeeld in uw gemeente? Denk hierbij aan het valideren en het duiden van de informatie.

Organisatie

In hoeverre bent u het oneens/eens met de volgende stellingen?

22. Binnen de gemeente hebben de medewerkers over het algemeen **voldoende kennis en kunde** om de doelstellingen van online monitoring te behalen.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

23. Binnen de gemeente is er over het algemeen **voldoende capaciteit** om de doelstellingen van online monitoring te behalen.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

24. Mijn gemeente is tevreden met de uitwisseling tussen gemeente en politie van informatie over OOV die is verkregen via online monitoring.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

25. Wilt u (een van) uw antwoorden over de organisatie toelichten?

Juridische kaders

In hoeverre bent u het oneens/eens met de volgende stellingen?

26. Voor medewerkers die betrokken zijn bij online monitoring binnen de gemeente is het **duidelijk welke juridische kaders** gelden.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

27. Medewerkers die betrokken zijn bij online monitoring binnen de gemeente **werken volgens de juridische kaders en wet- en regelgeving**

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

28. De **gemeente is verantwoordelijk** bij het overtreden van juridische grenzen door gemeentelijk gebruik van de monitoringstool

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

29. **Medewerkers van de gemeente zijn verantwoordelijk** bij het overtreden van juridische grenzen door gemeentelijk gebruik van de monitoringstool

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

30. Het bedrijf die de **monitoringstool levert is verantwoordelijk** bij het overtreden van juridische grenzen door gemeentelijk gebruik van de monitoringstool

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

31. De gemeente is bij online monitoring aan minder wettelijke restricties gebonden dan de politie, omdat het bij de gemeente gaat om openbare orde en veiligheid (en niet om opsporing).

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

32. Het behalen van de doelstellingen van het online monitoren wordt **belemmerd door juridische kaders**.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

33. Vindt het online monitoren plaats op basis van een **vastgelegd protocol of beleidsdocument?**
    - ☐ Ja
    - ☐ Nee
    - ☐ Weet ik niet
    - ☐ Anders, namelijk (*niet verplicht invulveld)*

34. Is de **Functionaris Gegevensbescherming of privacyfunctionaris betrokken** (geweest) bij de vormgeving van de wijze waarop online wordt geobserveerd?
    - ☐ Ja
    - ☐ Nee
    - ☐ Weet ik niet
    - ☐ Anders, namelijk (*niet verplicht invulveld)*

35. Wilt u (een van) uw antwoorden over juridische kaders toelichten?

Ethisch

In hoeverre bent u het oneens/eens met de volgende stellingen?

36. Gemeentelijk online monitoren is ethisch verantwoord.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

37. Gemeentelijk online monitoren **van individuen die in de media naar voren komen** is ethisch verantwoord.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

38. Gemeentelijk online monitoren **van individuen die niet in de media naar voren komen** is ethisch verantwoord.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

39. Gemeentelijk online monitoren **van groepen personen in de gemeente** is ethisch verantwoord.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

40. Gemeentelijk online monitoren **met privéaccounts is in bepaalde gevallen** ethisch verantwoord.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

41. De gemeente is **open en transparant** over de wijze waarop zij online informatie verzamelt.

Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
1	2	3	4	5

42. Wilt u (een van) uw antwoorden over ethiek toelichten?

Afsluiting

Dit is het einde van de vragenlijst. We hebben nog twee afsluitende vragen.

43. Voor welke gemeente bent u werkzaam? *Alle gegevens van de vragenlijst worden anoniem verwerkt

*Niet verplicht

44. Mogen we u benaderen voor een vervolginterview? Het telefonische vervolginterview zal gepland worden in de eerste maanden van 2020 en zal ongeveer dertig minuten duren.
    - ☐ Liever niet
    - ☐ Ja, dat mag (R: q42a)

Op welk telefoonnummer of e-mailadres kunnen we u bereiken?
Telefoonnummer/e-mail:

Hartelijk bedankt voor uw medewerking!

Leden Redactieraad Programma Politie & Wetenschap

Uitgaven in de reeks Politiekunde

1. ***Criminaliteit in de virtuele ruimte***
   P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/ TNO-FEL, Den Haag, 2002
2. ***Cameratoezicht. Goed bekeken?***
   I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2002
3. ***De 10 stappen van Publiek-Private Samenwerking (PPS)***
   J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002
4. ***De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding***
   C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn, 2003
5. ***Cameratoezicht. De menselijke factor***
   A.Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg, 2003
6. ***Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlist-methodiek***
   H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem, 2004 (vierde druk 2006)
7. ***Hooligans in beeld.Van informatie naar aanpak***
   H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005
8. ***Richtlijnen auditieve confrontatie***
   J.H. Kerstholt, A.G. van Amelsfoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/NFI, Den Haag, 2005
9. ***Niet verschenen***
10. ***De opsporingsfunctie binnen de gebiedsgebonden politiezorg***
    O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006
11. ***Inzoomen en uitzoomen op Zaandam***
    I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

12. ***Aansprakelijkheidsmanagement politie. Beschrijving, analyse en handreiking***
E.R. Muller, J.E.M. Polak, C.J.J.M. Stoker m.m.v. M.L. Diepenhorst & S.H.E. Janssen, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag/ Faculteit der Rechtsgeleerdheid Universiteit Leiden, 2006

13. ***Cold cases – een hot issue***
I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem, 2006

14. ***Adrenaline en reflectie. Hoe leren politiemensen op de werkplek?***
A. Beerepoot & G. Walraven e.a., DSP-groep BV, Amsterdam/Walraven onderzoek en advies, 2007

15. ***Tussen aangifte en zaak. Een referentiekader voor het aangifteproces***
W. Landman, L.A.J. Schoenmakers & F. van der Laan, Twynstra Gudde, adviseurs en managers, Amersfoort, 2007

16. ***Baat bij de politie. Een onderzoek naar de opbrengsten voor burgers van het optreden van de politie***
M. Goderie & B. Tierolf, m.m.v. H. Boutellier & F. Dekker, Verwey-Jonker Instituut, Utrecht, 2008

17. ***Hoeveel wordt het vandaag? Een studie naar de kans op voetbalgeweld en het veiligheidsbeleid bij voetbalwedstrijden***
E.J. van der Torre, R.F.J. Spaaij & E.D. Cachet, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2008

18. ***Overbelast? De administratieve belasting van politiemensen bij de afhandeling van jeugdzaken***
G. Brummelkamp & M. Linssen, EIM, Zoetermeer, 2008

19. ***Geografische daderprofilering. Een inventarisatie van randvoorwaarden en succesfactoren***
G. te Brake & A. Eikelboom, TNO Defensie en Veiligheid, Soesterberg, 2008

20. ***Solosurveillance. Kosten en baten***
S.H. Esselink, J. Broekhuizen & F.M.H.M. Driessen, Bureau Driessen, 2009

21. ***Onderzoek naar de mogelijke meerwaarde van AWARE voor de politie. Ervaringen met een nieuwe aanpak van belaging door ex-partners***
M.Y. Bruinsma, J. van Haaf, R. Römkens & L. Balogh, IVA Beleidsonderzoek en Advies, i.s.m. INTERVICT/Universiteit van Tilburg, 2008

22. ***Gebiedsscan criminaliteit en overlast. Een methodiekbeschrijving***
B. Beke, E. Klein Hofmeijer & P. Versteegh, Bureau Beke, Arnhem, 2008

23. ***Informatiemanagement binnen de politie. Van praktijk tot normatief kader***
V. Bekkers, M. Thaens, G. van Straten & P. Siep; m.m.v. A. Dijkshoorn, Center for Public Innovation, Erasmus Universiteit Rotterdam, 2009

24. ***Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept***
H.B Ferwerda, E.J van der Torre & V. van Bolhuis, Bureau Beke, Arnhem/ COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

25. ***Rellen om te rellen. Een studie naar grootschalige openbare-ordeverstoringen en notoire ordeverstoorders***
I. van Leiden, N. Arts & H.B. Ferwerda, Bureau Beke, Arnhem, 2009

26a. ***Verbinden van politie- en veiligheidszorg. Politie en partners over signaleren & adviseren***
W. Landman, P. van Beers & F. van der Laan, Twynstra Gudde, Amersfoort, 2009

26b. ***Politiepolitiek. Een empirisch onderzoek naar politiële signalering & advisering***
E.J.A. Bervoets, E.J. van der Torre & J. Dobbelaar m.m.v. N. Koeman, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

27. ***De politie aan zet: de aanpak van veelplegers in Deventer***
I. Bakker & M. Krommendijk, IPIT, Enschede, 2009

28. ***Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland***
O.M.J. Adang (redactie), S.E. Bierman, K. Jagernath-Vermeulen, A. Melsen, M.C.J. Nogarede & W.A.J. van Oorschot, Politieacademie, Apeldoorn, 2009

29. ***Rellen in Ondiep. Ontstaan en afhandeling van grootschalige ordeverstoring in een Utrechtse achterstandswijk***
G.J.M. van den Brink, M.Y. Bruinsma (redactie), L.J. de Graaf, M.J. van Hulst, M.P.C.M. Jochoms, M. van de Klomp, S.R.F. Mali, H. Quint, M. Siesling, G.H. Vogel, Politieacademie, Apeldoorn, 2010

30. ***Burgerparticipatie in de opsporing. Een onderzoek naar aard, werkwijzen en opbrengsten***
A. Cornelissens & H. Ferwerda (redactie), met medewerking van I. van Leiden, N. Arts & T. van Ham, Bureau Beke, Arnhem, 2010

31. ***Poortwachters van de politie. Meldkamers in dagelijks perspectief***
J. Kuppens, E.J.A. Bervoets & H. Ferwerda, Bureau Beke, Arnhem & COT, Den Haag, 2010

32. ***Het integriteitsbeleid van de Nederlandse politie: wat er is en wat ertoe doet***
M.H.M. van Tankeren, Onderzoeksgroep Integriteit van Bestuur, Vrije Universiteit Amsterdam, 2010

33. ***Civiele politie op vredesmissie. Uitzendervaringen van Nederlandse politie - functionarissen***
H. Sollie, Universiteit Twente, Enschede, 2010

34. ***Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?***
M.L. Koemans, Universteit Leiden, 2010

35. ***Het districtelijk opsporingsproces; de black box geopend***
R.M. Kouwenhoven, R.J. Morée &. P. van Beers, Twynstra Gudde, Amersfoort, 2010

36. ***Balanceren tussen alert maken en onrust voorkomen. Publiekscommunicatie over seriële schokkende incidenten (casestudy Lelystad)***
A.J.E. van Hoek, m.m.v. P.F. van Soomeren, M.D. Abraham & J. de Kleuver, DSP-groep, Amsterdam, 2011

37. ***Sturing van blauw. Een onderzoek naar operationele sturing in de basispolitiezorg***
W. Landman, m.m.v. M. Malipaard, Twynstra Gudde, Amersfoort, 2011

38. ***Onder het oppervlak. Een onderzoek naar ontwikkelingen en (a)select optreden rond preventief fouilleren***
J. Kuppens, B. Bremmers, E. van den Brink, K. Ammerlaan & H.B. Ferwerda, m.m.v. E.J. van der Torre, Bureau Beke, Arnhem/COT, Den Haag, 2011

39. ***Naar eigen inzicht? Een onderzoek naar beoordelingsruimte van en grenzen aan de identiteitscontrole***
J. Kuppens, B. Bremmers, K. Ammerlaan & E. van den Brink, Bureau Beke, Arnhem/COT, Den Haag, 2011

40. ***Toezicht op zedendelinquenten door de politie in samenwerking met de reclassering***
H.G. van de Bunt, N.L. Holvast & J. Plaisier, Erasmus Universiteit, Rotterdam/ Impact R&D, Amsterdam, 2012

41. ***Daders over cameratoezicht***
H.G.A. van Schijndel, A. Schreijenberg, G.H.J. Homburg & S. Dekkers, Regioplan Beleidsonderzoek, Amsterdam, 2012

42. ***Aanspreken op straat. Het werk van de straatcoach in al zijn verschijnings - vormen***
L. Loef, K. Schaafsma & N. Hilhorst, DSP-groep, Amsterdam, 2012

43. ***De organisatie van de opsporing van cybercrime door de Nederlandse politie***
N. Struiksma, C.N.J. de Vey Mestdagh & H.B. Winter, Pro Facto, Groningen/ Kees de Vey Mestdagh, Groningen, 2012

44. ***Politie in de netwerksamenleving. De opbrengst van de politiële netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg***
I. Helsloot, J. Groenendaal & E.C. Warners, Crisislab, Renswoude, 2012

45. ***Tegenspraak in de opsporing. Verslag van een onderzoek***
R. Salet & J.B. Terpstra, Radboud Universiteit Nijmegen, 2012

46. ***Tunnelvisie op tunnelvisie? Een verkennend en experimenteel onderzoek naar de besluitvorming door VKL-teams met betrekking tot het onderkennen van tunnelvisie en andere procesaspecten***
I. Helsloot, J. Groenendaal & B. van 't Padje, Crisislab, Renswoude, 2012

47. ***M.-waarde. Een onderzoek naar de bijdrage van Meld Misdaad Anoniem aan de politionele opsporing***
M.C. van Kuik, S. Boes, N. Kop, M. den Hengst-Bruggeling, T. van Ham & H. Ferwerda, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2012

48. ***Seriebrandstichters. Een verkennend onderzoek naar daderkenmerken en delictpatronen***
Y. Schoenmakers, A. van Wijk & T. van Ham, Bureau Beke, Arnhem, 2012

49. ***Van wie is de straat? Methodiek en lessen voor de politie om ongrijpbare veiligheidsfenomenen grijpbaar te maken – op basis van vijf praktijkcasus***
H. Ferwerda, T. van Ham, B. Bremmers, K. Tijhof & M. Grotens, Bureau Beke, Arnhem, 2013

50. ***Recherchesamenwerking in de Euregio Maas-Rijn. Knooppunten, knelpunten en kansen***
H. Nelen, M. Peters & M. Vanderhallen, Politieacademie, Apeldoorn/ Universiteit Maastricht, 2013

51. ***De operationele politiebriefing onderzocht. Een onderzoek naar de effectiviteit van de operationele politiebriefing***
A. Scholtens, J. Groenendaal & I. Helsloot, Crisislab, Renswoude 2013

51a. ***De operationele politiebriefing onderzocht (2). Een actie(vervolg)onderzoek om tot een effectievere politiebriefing te komen***
A. Scholtens, Crisislab, Renswoude 2015

52. ***Sociale media: factor van invloed op onrustsituaties?***
R.H. Johannink, I. Gorissen & N.K. van As, Politieacademie Apeldoorn/ VDMMP, Houten, 2013

53. ***De terugkeer van zedendelinquenten in de wijk***
C.E. Huls & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen/Centrum voor Openbare Orde en Veiligheid, Groningen, 2013

54. ***Van meld- naar aantoonplicht. Een onderzoek naar een systeem van digitale surveillance***
C. Veen & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen, 2013

55. ***Heterdaadkracht in twee Haagse pilotgebieden***
B. van Dijk, J.B. Terpstra & P. Hulshof, Politieacademie, Apeldoorn/DSPgroep, Amsterdam, 2013

56. ***Inzet op Maat. Onderzoek naar kenmerken en mogelijkheden van duurzame inzetbaarheid van oudere medewerkers***
H. de Blouw, I.R. Kolkhuis Tanke & C.C. Sprenger, Politieacademie, Apeldoorn, 2013

57. ***Interventies in de opsporing. Impulsen in kwaliteit en effectiviteit van het opsporingsproces***
R.M. Kouwenhoven, R.J. Morée & P. van Beers, Twynstra Gudde, Amersfoort, 2013

58. ***De plaats delict in beeld. Fotografie in de dagelijkse en gesimuleerde praktijk***
G. Vanderveen & J. Roosma, Instituut voor Strafrecht & Criminologie, Universiteit Leiden, 2013

59. ***Jeugdgroepen van toen. Een casusonderzoek naar de leden van drie criminele jeugdgroepen uit het einde van de vorige eeuw***
H. Ferwerda, B. Beke & E. Bervoets, Bureau Beke, Arnhem/Beke Advies, Arnhem/LokaleZaken, Rotterdam, 2013

60. ***Tussen hei en hoofdbureau. Leiderschapsontwikkeling bij de politie***
W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2013

61. ***Gemeentelijk blauw. Het dagelijks werk van gemeentelijke handhavers in beeld***
E. Bervoets, J. Bik & M. de Groot, LokaleZaken, Rotterdam, 2013

62. ***Excessief geweld op en om de voetbalvelden. Praktijkonderzoek naar omvang, ernst en aanpak van 'voetbalgeweld'***
P. Duijvestijn, B. van Dijk, P. van Egmond, M. de Groot, D. van Sommeren & A. Verwest, DSP-groep, Amsterdam, 2013

63. ***Beeld van gezag bij de politie. Maatschappelijke verbeelding en de impact van gezagsbeelden op burgers***
H. de Mare, B. Mali, M. Bleecke & G. van den Brink, m.m.v. Motivaction, Tilburg University, Stichting IVMV, Leiden, 2014

64. ***Informatiegestuurde dienders. Informatiesturing tussen theorie en praktijk***
A. van Sluis, P. Siep, V. Bekkers, m.m.v. M. Thaens & G. Straten, Center for Public Innovation, Erasmus Universiteit, Rotterdam, 2014

65. ***Hard op weg. Onderzoek aanpak verkeersveelplegers***
B. Bieleman, M. Boendermaker, R. Mennes & J. Snippe, Intraval, Groningen/ Rotterdam, 2014

66. ***Tussen hulp en hype. De inzet van opsporingsberichtgeving in ontvoeringszaken***
Y.M.M. Schoenmakers, J.V.O.R. Doekhie & J.C. Knotter, Yvette Schoenmakers Onderzoek en advies, Weesp, 2014

67. ***Nachtdienst bij de politie en verkeersveiligheid. Onderzoek naar ervaringen van politieagenten met verkeersonveiligheid in woon-werkverkeer na de nachtdienst***
P. Boekhoorn, BBSO, Nijmegen, 2014

68. ***Buit van woninginbraak. Onderzoek onder inbrekers en helers***
J. Snippe, M. Sijtstra, R. Mennes & B. Bieleman, Intraval, Groningen/ Rotterdam, 2014

69. ***Privaat blauw. Portiers, evenementbeveiligers en voetbalstewards op risicovolle locaties en tijdens risicovolle momenten***
E. Bervoets & S. Eijgenraam, LokaleZaken, Rotterdam, 2014

70. ***Met grof geschut. Reconstructie van een moordonderzoek binnen de criminele woonwagenwereld***
I. van Leiden, B. Bremmers & H. Ferwerda, Bureau Beke, Arnhem, 2014

71. ***Met fluwelen handschoenen? Politie en de omgang met verwarde personen in Amsterdam***
J. Kuppens, T. Appelman, T. van Ham & A. van Wijk, Bureau Beke, Arnhem, 2015

72a. ***Vermisten op de kaart. Aard en omvang van langdurige vermissingen***
I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2015

73. ***Van intel tot operatie. De impact van veiligheidsanalisten bij de aanpak van misdaad***
M. den Hengst, M. Bruinsma, Y. Schoenmakers, W. Niepce, Bureau Bruinsma, Tilburg, 2015

74. ***De bestuurlijke rapportage. Gezamenlijke inspanning in de aanpak van (georganiseerde) criminaliteit en overlast***
I. Gorissen, m.m.v. R.H. Johannink, PBLQ, Den Haag, 2015

75. ***De aangifte van delicten bij de multichannelstrategie van de politie***
P. Boekhoorn & J. Tolsma, Bureau Boekhoorn/Radboud Universiteit, Nijmegen, 2016

76. ***Die pakken we toch niet op? Afstemming tussen politie en Openbaar Ministerie in zaken van veelvoorkomende aangiftecriminaliteit***
R. Kouwenhoven & L. Kleijer-Kool, Twynstra Gudde, Amersfoort, 2016

77. ***Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie***
A. Scholtens, M. den Hengst & R. Waterreus, Crisislab, Renswoude/ Politieacademie, Apeldoorn, 2016

78. ***Hoe lang kun je 'schijt hebben'? Dertien desisters uit criminele jeugdgroepen aan het woord***
C.E. Hoogeveen, A.E. van Burik & B.J. de Jong, m.m.v. E.M. Klooster, Bureau Alpha, 's-Hertogenbosch/VanMontfoort, Woerden, 2016

79. ***Onbenutte kansen. Een onderzoek naar het gebruik van restinformatie in de opsporing***
A. van Wijk & L. Scholten, m.m.v. B. Bremmers, Bureau Beke, Arnhem, 2016

80. ***Verbale leugendetectie-wizards***
G. Bogaard & E.H. Meijer, Maastricht University, Maastricht, 2016

81. ***Mensenhandel in de prostitutie opsporen zonder aangifte? Een vervolgonderzoek om de doorzettingsmacht van de politie te verduidelijken***
M. Goderie, m.m.v. R. Kool, Goderie Onderzoek, Klarenbeek, 2016

82. ***De onvindbaren. Op zoek naar voortvluchtige veroordeelden in Nederland***
Y. Schoenmakers, I. de Groot, J. van Zanten, A. van Rooyen & J. Baars, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2017

83. ***Elke dump is een plaats delict. Dumping en lozing van synthetisch drugsafval: verschijningsvormen en politieaanpak***
Y. Schoenmakers, S. Mehlbaum, M. Everartz & C. Poelarends, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2016

83A. ***De Intelligence Paradox. Lessen uit de integrale pilot Analyse Synthetische Drugs in Oost-Nederland***
Y. Schoenmakers, S. Mehlbaum, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2019

84. ***Naar handhaafbare noodbevelen en noodverordeningen. Een analyse van het gemeentelijke noodrecht***
A.J. Wierenga, C. Post & J. Koornstra, Rijksuniversiteit Groningen, Centrum voor Openbare Orde en Veiligheid, 2016

85. ***Vermisten op het spoor. Rechercheren naar langdurige vermissingen***
I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

86. ***De aard van het beestje. Kenmerken en achtergronden van dierenmishandelaars***
A. van Wijk & M. Hardeman, Bureau Beke, Arnhem, 2017

87. ***Modus operandi van de recherche. De rechercheprakijk in moord- en verkrachtingszaken***
A. van Wijk, I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

88. ***Over grenzen in de sport. De rol van de politie in de aanpak van seksueel grensoverschrijdend gedrag in de sport in samenwerking met relevante partners***
A. van Wijk, M. Hardeman, L. Scholten & M. Olfers, Vrije Universiteit Amsterdam, Bureau Beke, Arnhem, 2017

89. ***Defensiehulp. Legergroene bijstand aan de politie bij handhaving van de rechtsorde***
E. Bervoets, m.m.v. S. Eijgenraam, T. Dijkhuizen & J. van de Werken, Bureau Bervoets, Amersfoort, 2017

90. ***Tussen onder en boven. Productie en distributie van softdrugs in Noord- Nederland***
J. Snippe, R. Mennes, M. Sijtstra & B. Bieleman, Intraval, Groningen/Rotterdam, 2017

91. ***Vechten op afspraak. Inzicht in het fenomeen en input voor de ontwikkeling van een politiestrategie***
T. van Ham, L. Scholten, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem, 2018

92. ***Notoire straten. Over de lokale inbedding van georganiseerde criminaliteit***
S. Mehlbaum, Y. Schoenmakers & J. van Zanten, Mehlbaum Onderzoek, Amsterdam, 2018

92A. ***De wortel en de stok. Praktijklessen uit een gebiedsgerichte probleemaanpak van ondermijning***
S. Mehlbaum, Y. Schoenmakers, Mehlbaum Onderzoek, Amsterdam, 2019

93. ***Ondermijning door criminele 'weldoeners'***
M. Bruinsma, R. Ceulen & T. Spapens, m.m.v. C. Deij, Tilburg University, Tilburg/Bureau Bruinsma, Tilburg, 2018

94. ***Kiezen voor politie. Een onderzoek onder mbo-studenten met een migratie - achtergrond in het veiligheidsdomein***
S. de Winter-Koçak, E. Klooster & M. Day, m.m.v. S. Mehlbaum, M. van Vugt & K. Leschonski, Verwey-Jonker Instituut, Utrecht, 2018

95. ***Doe-het-zelf-surveillance. Een onderzoek naar de werking en effecten van WhatsApp-buurtgroepen***
S. Mehlbaum & R. van Steden, m.m.v. M. van Dijk, Vrije Universiteit Amsterdam, Mehlbaum Onderzoek, Amsterdam, 2018

96. ***Een klacht is een gratis advies***
G. Jacobs, T. Hak, G. Vanderveen, M. Flory, T. Thuis, S. Valkeman & M. Franken, Erasmus Universiteit, Rotterdam, 2018

97. ***Voortgezet crimineel handelen tijdens detentie: je gaat het pas zien als je het doorhebt***
A. Verwest, W. Buysse, P. van Egmond, D. Hofstra, DSP-groep, Amsterdam, 2019

98. ***Zorg voor kinderen bij aanhouding van ouders; Best practices uit binnen- en buitenland***
J. Reef, N. Ormskerk, Universiteit Leiden, 2019

99. ***Aankoopfraude uit het buitenland***
J. Jansen, S. Westers, S. Twickler, W. Stol, NHL Stenden Hogeschool / Politieacademie

100. ***Grijs vakmanschap? Taakgerelateerd ongeoorloofd handelen binnen de politie***
R. Chr. van Halderen (diss. Avans Hogeschool), 2019

101. ***Niet meer doen! Een onderzoek naar de INDIGO-afdoening***
A. van Wijk, S. Dickie, J. van Esseveldt, Bureau Beke, Arnhem, 2019

102 ***De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging***
P. Boekhoorn, BBSO, Nijmegen, 2020

103 ***In- en doorstroom van nieuwkomers in beeld. Opgetekende lessen uit acht casussen rond de opvang van asielzoekers in Nederland.***
J. Kuppens, Bureau Beke, Arnhem 2020

104 ***De lading van vuurwapens. Een onderzoek naar de impact van illegale vuurwapens in Nederland.***
H. Ferwerda, J. Wolsink en I. van Leiden, Bureau Beke, Arnhem 2020

105 ***Q-teams. De politie onderweg naar toekomstbestendige opsporing en vervolging?***
P. van Egmond, A. Swami-Persaud, A. Verwest, DSP-groep, Amsterdam 2020

106 ***Onderwereld boven water? Zoektocht naar georganiseerde criminaliteit in de Noordelijke zeehavens***
N. Struiksma, C. Boxum, S.J. Hollenberg, N.O.M. Woestenburg, Pro Facto, Groningen 2020

107 ***Benutten van digitale sporen***
R. Zuurveen, W. Ph. Stol, Onderzoeksgroep Cybersafety. NHL Stenden en CyberScienceCenter 2020

108 ***Kansen en knelpunten binnen de financiële opsporing***
L.N. de Swart, G.P.J.M op 't Hoog, B.M.J Slot, A. Winkel. Ecorys 2021