Juridische spanningsvelden bij online monitoring door gemeenten

Chapter · November 2022

2 authors:

Willem Bantema
NHL Stenden University of Applied Sciences

Sipke de Vries
NHL Stenden University of Applied Sciences

Juridische spanningsvelden bij online monitoring door gemeenten

Willem Bantema & Sipke de Vries[1]

1 Inleiding

Sinds de COVID-19-crisis zijn er steeds meer voorbeelden van ordeverstoringen die via sociale media beginnen of via sociale media groot worden. Denk bijvoorbeeld aan het effect van drillraps, complottheorieën en grootschalige manifestaties die de openbare orde en veiligheid bedreigen. In verschillende rapporten wordt aangegeven dat gemeenten, om dergelijke verstoringen te voorkomen, moeten zorgen voor een goede eigen online informatiepositie, doordat deze en andere voorbeelden steeds vaker een online oorsprong hebben.[2] Minder aandacht wordt besteed aan de juridische kaders waar gemeenten mee te maken hebben en krijgen als zij hun online informatiepositie willen versterken. Onder andere de Algemene verordening gegevensbescherming (AVG), het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 10 van de Grondwet zijn daarbij relevant.

In deze bijdrage wordt zowel gekeken naar de werkwijze van gemeenten op het gebied van online aangejaagde ordeverstoringen als naar juridische kaders waarbinnen gemeenten moeten opereren en de eventuele (niet-)naleving daarvan door gemeenten. De volgende vraag staat daarbij centraal: 'In hoeverre is gemeentelijke monitoring toegestaan en welke voorbeelden van juridische spanningsvelden komen naar voren?'. Onder monitoring wordt verstaan 'het raadplegen van (open) internetbronnen waarmee het gedrag en de online uitlatingen van burgers in de gaten wordt gehouden.'[3] Openbare (internet)-bronnen kenmerken zich doordat in beginsel eenieder er toegang tot kan krijgen. Openbare bronnen staan tegenover afgeschermende bronnen, die zich kenmerken doordat er een controle plaatsvindt op wie diegene is die toegang wil

---

[1] Dr. W. Bantema en mr. S. de Vries zijn beiden werkzaam bij de onderzoeksgroep Cybersafety, NHL Stenden Hogeschool, Thorbecke Academie. Willem Bantema als lector en Sipke de Vries als docent-onderzoeker.
[2] Zie o.a. W. Bantema e.a., *Black box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk* (Politiekunde 109), Den Haag: Sdu 2021. Zie ook: S. de Vries & W. Bantema, *Online aanpak in kaart*, Leeuwarden: Onderzoeksgroep Cybersafety 2022.
[3] Deze bijdrage heeft niet tot doel om een discussie over de definitie ervan te voeren. In het onderzoek 'Black box van gemeentelijke online monitoring' ging het overwegend over het gebruik van informatie uit open bronnen.

tot een bepaalde groep of bron.[4] Denk aan het lid worden van een Facebookgroep waarvoor toestemming moet worden gevraagd en expliciet verleend.

Uit het onderzoek *Black box van gemeentelijke online monitoring* blijkt onder andere dat 95% van de gemeenten die hebben gereageerd op het verzoek van NHL Stenden Hogeschool en de Rijksuniversiteit Groningen om aan het onderzoek mee te doen, op een of andere manier actief zijn op het gebied van online monitoring.[5] Dit terwijl het onderzoek plaatsvond vóór de COVID-19-crisis en de behoefte aan online informatie waarschijnlijk daarna alleen nog maar groter is geworden. Online monitoring door gemeenten is onder een vergrootglas komen te liggen het afgelopen jaar. Dit komt onder andere door berichtgeving over het heimelijk volgen van burgers met nepaccounts door zowel het NCTV[6] alsook door het ministerie van Defensie.[7]

Op basis van het onderzoek van NHL Stenden en Rijkuniversiteit Groningen is meer inzicht verkregen in dit onderbelichte vraagstuk. In deze bijdrage zal een aantal belangrijke aandachtspunten uit dit onderzoek naar voren komen en wordt er ook aandacht besteed aan bestuurlijke reacties op het onderzoek.

2 Onderzoeksmethoden

In dit artikel wordt ingegaan op enkele juridische grondslagen van de AVG en het EVRM die relevant zijn voor de beschreven werkwijze van online monitoring door de gemeenten. Vervolgens wordt bekeken of en hoe die werkwijze kan leiden tot inbreuken op deze juridische kaders. Voor de reflectie op deze juridische kaders is het van belang om inzicht te krijgen in de gemeentelijke praktijk op het gebied van online monitoring. Dat inzicht is verkregen door een online vragenlijst die onder gemeenten is verspreid. De betreffende vragenlijst is voorgelegd aan 349 Nederlandse gemeenten waarvan een e-mailadres bekend was en uiteindelijk gebaseerd op de reacties van 196 gemeentelijke medewerkers uit 156 unieke Nederlandse gemeenten. Daarnaast wordt — waar mogelijk — gebruikgemaakt van anekdotes uit de acht interviews die zijn gehouden met gemeentelijke medewerkers.[8]

Online monitoring door gemeenten kan leiden tot een inbreuk op de persoonlijke levenssfeer van de personen die gemonitord worden. De persoonlijke levenssfeer wordt op diverse plaatsen juridisch beschermd, vandaar dat

[4] Bantema e.a. 2021, p. 16-17.
[5] Bantema e.a. 2021, p. 35.
[6] 'NCTV volgde in het geheim burgers op sociale media met nepaccounts', 10 april 2021, https://nos.nl/artikel/2376104-nctv-volgde-in-het-geheim-burgers-op-sociale-media-met-nepaccounts.
[7] 'Excuses minister Bijleveld voor informatieverzameling burgers door defensie', 26 mei 2021, https://nos.nl/artikel/2382430-excuses-minister-bijleveld-voor-informatieverzameling-burgers-door-defensie.
[8] Voor meer informatie over de methoden zie Bantema e.a. 2021, p. 19-22.

artikel 8 EVRM een aantal keer de revue passeert in deze notitie. Daarnaast komt ook de bescherming van persoonsgegevens ter sprake, het belangrijkste juridische document daarvoor is de AVG. Ook bij de AVG wordt diverse keren stilgestaan.

3 De praktijk

Een van de aspecten waarop werd ingegaan in het onderzoek betrof de doelstellingen van online monitoring. Waarom doen gemeenten aan online monitoring? De reden dat gemeenten monitoren is onder andere om de openbare orde en veiligheid in de gemeente te waarborgen. Gemeenten krijgen met het online monitoren zicht op wat er binnen de gemeente speelt. Figuur 1 geeft een indicatie van welke digitale dreigingen zich zoal voordoen binnen de onderzochte gemeenten.[9] De gemeentelijke afdelingen zien bijvoorbeeld veel onrust rondom politieke besluiten, maar ook overlast door jongeren en individuen die eerder overlast hebben veroorzaakt, maar ook oproepen tot demonstraties en manifestaties. Uit dit overzicht blijkt dat gemeenten naar tal van klassieke openbare ordevraagstukken kijken die ook een online component hebben.

Figuur 1. De meest gemonitorde categorieën van ordeverstoringen (in %, N varieert van 113-157)

[9] De figuren en tabellen in het artikel komen uit het onderzoek *Black box van gemeentelijke online monitoring*.

3.1 Juridische kennis/borging

Voordat in de volgende paragrafen de concrete werkwijzen van gemeenten en de daarbijbehorende juridische reflecties aan bod komen, wordt er eerst een stap teruggezet. Die stap is om in beeld te brengen in hoeverre bij gemeenten bekend is wat de juridische kaders rondom online monitoring zijn en wat zij doen om ervoor te zorgen dat er volgens die kaders gewerkt wordt. Wanneer die inzichten niet bekend zijn, is de kans op privacyinbreuken mogelijk groter.

Borging van kaders en/of protocollen waarbinnen de gemeente 'mag' werken dient onder andere ter bescherming van burgers en kan bijdragen aan het verminderen van rechtsongelijkheid. Ook kan een protocol het gedrag en de werkwijze van medewerkers standaardiseren.

In 2021 geeft 27% (*N* = 147) van de respondenten aan dat het juridische kader van online monitoring bij hun gemeente onduidelijk is.[10] 21% geeft aan dat het wél duidelijk is. De overige 52% is neutraal. Op de vraag of er een juridische waarborging in een protocol of beleidsdocument is, geeft 8% 'ja' aan, en 54% 'nee' (*N* = 147). De overige 38% zegt niet te weten of het mogelijk anders was. De gemeentelijke medewerkers geven dus zelf aan overwegend geen juridische kennis te hebben met betrekking tot online monitoring door hun gemeenten en ook zelden met een protocol te werken dat richting geeft aan de (juridische) werkwijze.

Een andere manier om het juridische kader binnen gemeenten te borgen is door de Functionaris Gegevensbescherming (hierna: FG) te betrekken bij de handelswijze van monitoring. Een FG is verantwoordelijk voor de toepassing en de naleving van de AVG en daardoor ook voor de monitoring van gemeenten. Sinds de invoering van de AVG zijn gemeenten, op basis van artikel 37 AVG, verplicht om een FG aan te stellen, ongeacht het type gegevens dat verwerkt wordt. Van de 147 respondenten geeft 16% aan dat dat de FG betrokken is bij het juridische kader en 37% geeft aan dat dit niet het geval is. De overige 47% geeft aan dit niet te weten of dat het anders geregeld is.[11]

Nu is gebleken dat een deel van de gemeenten nog geen (duidelijk) juridisch kader heeft en de FG in veel gemeenten niet betrokken is bij online monitoring, is de volgende stap om te kijken in hoeverre de beperkte juridische kennis rondom online monitoring problemen oplevert. Dit hangt onder andere af van de concrete werkwijzen van gemeenten en de hierop van toepassing zijnde juridische kaders.

[10] Bantema e.a. 2021, p. 55.
[11] Bantema e.a. 2021, p. 56.

3.2 Juridisch kader en spanningsveld juridische kennis/borging

Wanneer het gaat om persoonsgegevens komen er als gezegd diverse juridische kaders om de hoek kijken die stenge eisen stellen aan de verwerking van persoonsgegevens. De kaders hebben betrekking op de bescherming van een individu, eerbiediging van de persoonlijke levenssfeer en privacy. De waarborgen die daarop betrekking hebben zijn voornamelijk neergelegd in artikel 8 EVRM, artikel 10 Grondwet en de AVG.[12]

Een gebrek aan juridische borging en kennis kan een probleem zijn, doordat er met gemeentelijke online monitoring vrijwel altijd persoonsgegevens gemoeid zijn. Voor dit artikel is van belang te benoemen dat zodra er er géén sprake is van persoonsgegevens, deze genoemde juridische kaders niet van toepassing zijn. Doordat er wordt stilgestaan bij persoonsgegevens, valt alles wat niet als persoonsgegeven gezien kan worden buiten de scope van dit artikel. Een aandachtspunt is wel dat de AVG een erg ruime uitleg geeft aan het begrip 'persoonsgegeven'. Een voorbeeld hiervan is dat wanneer verwerkte gegevens niet tot een persoon herleidbaar zijn, maar dat wel het geval is als die gegevens worden aangevuld met andere openbaar beschikbare informatie, er alsnog sprake is van persoonsgegevens.

In de hiernavolgende alinea's wordt een aantal gemeentelijke werkwijzen beschreven die tot juridische spanningen kunnen leiden. Deze spanningen zijn allesbehalve uitputtend: ze zijn slechts een indicatie van de spanningen die er voor gemeenten kunnen zijn bij het online monitoren. Het betreft aandacht voor de frequentie van online monitoring en bijbehorende doelstellingen (paragraaf 4), het gebruik van monitoringstools, verwerking van persoonsgegevens, stelselmatigheid (paragraaf 5) en de herkenbaarheid van gemeenten bij het gebruik van online monitoring (paragraaf 6).

4 Achtergronden van gemeentelijke online monitoring

4.1 Inleiding

Zoals al eerder genoemd blijkt dat 95% van de gemeentelijke respondenten (*N* = 260) aangeeft dat zij of een van hun collega's in online openbare bronnen op het internet monitoren. Uit het Black box-onderzoek blijkt dat online monitoring het meeste voorkomt bij de afdeling Communicatie: zij gebruiken in de meeste gevallen een vorm van monitoring voor een Klant Contact Centrum of

[12] Het recht op eerbiediging van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens zijn ook gecodificeerd in de artikelen 7 en 8 van het Handvest van de grondrechten van de EU. Artikel 7 Handvest heeft in principe eenzelfde reikwijdte en inhoud als artikel 8 EVRM. Artikel 8 Handvest is uitgewerkt in de AVG en overige regelgeving.

Webcare.[13] Daarna volgt de afdeling Openbare Orde en Veiligheid (OOV) als de afdeling waar online monitoring het meeste voorkomt. Ruim 60% (*N* = 260) van de respondenten geeft aan dat deze afdeling doet aan online monitoring. Een belangrijke constatering voor de volgende paragrafen is dat online monitoring dus op meerdere plaatsen van de organisatie plaatsvindt.

	Hoofdoel	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

Tabel 1. Doelstellingen gericht op communicatie (in %, N = 196)

4.2 Hoofd- en nevendoel(en) van monitoring in de praktijk

Een eerste spanningsveld betreft het hoofd- en nevendoel van de online monitoring. Voor de AVG maakt het uit met welk doel er gemonitord wordt. Volgens de literatuur is de verwachting dat er binnen de gemeente globaal twee doelen zijn voor online monitoring: communicatie en de handhaving van de openbare orde, maar in de praktijk blijkt dit weerbarstiger. De afdeling Communicatie monitort vooral om te weten te komen wat er in een gemeente speelt, om de dienstverlening voor inwoners te verbeteren en om in de gaten te houden hoe de gemeente wordt gewaardeerd (zie tabel 1). Online monitoring met communicatiedoeleinden wordt door enkele respondenten uit het Black box-onderzoek gezien als een thermometer om de temperatuur binnen een gemeente te meten, om zo de status binnen een gemeente te peilen.[14]

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

Tabel 2. Doelstellingen gericht op openbare orde en veiligheid (in %, N = 196)

[13] Bantema e.a. 2021, p. 55.
[14] Bantema e.a. 2021, p. 47.

Voor de handhaving van de openbare orde zijn er ook meerdere (sub)doelen om te monitoren, zie tabel 2. Van de respondenten geeft 43% aan dat het signaleren van dreigingen een reden is om te monitoren (41% ziet dit als een nevendoel). Het onderzoeken van gesignaleerde dreigingen ziet 33% van de respondenten als een hoofddoel, terwijl 39% dit als een nevendoel ziet. We zien dus dat de doelen van de afdeling OOV om te monitoren meer door elkaar heen lopen dan dat dat bij de afdeling Communicatie het geval is. In de interviews die gehouden zijn voor het onderzoek komt vaak naar voren dat de signalering van dreigingen wordt beschreven als bijvangst: ‘Het zijn meer dingen die oppoppen dus het is niet iets waar we specifiek op monitoren.’[15] In de volgende paragraaf wordt ingegaan op de juridische relevantie van dit geconstateerde onderscheid in hoofd- en nevendoelen van online monitoring.

4.3 Hoofd- en nevendoel(en) in de AVG

We hebben gezien dat gemeentelijke afdelingen om verschillende redenen en met verschillende doelen monitoren. De rangschikking van het hoofddoel en nevendoel is van belang in de doelbepaling in de AVG. Die doelbepaling kan online monitoring rechtvaardigen. De scheiding in de tabellen tussen hoofd- en nevendoel(en) zijn dus van belang voor eventuele bijvangst en waarvoor die gebruikt wordt.

Het artikel uit de AVG dat over doelbepaling gaat is artikel 5 lid 1 onder b. Dit artikel (we zetten hier alleen de eerste helft van het artikel neer) luidt:

> *Persoonsgegevens moeten: Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt*

De eisen die de AVG aan de doelbepaling stelt zijn onder andere dat het doel dat met het observeren van online openbare bronnen wordt nagestreefd nauwkeurig omschreven moet zijn (welbepaald). Bovendien moet het doel vooraf uitdrukkelijk worden vastgelegd. Ook is tot op zekere mate transparantie hierover vereist. Het gebruik van gegevens voor een ander (neven)doel dan waarvoor zij oorspronkelijk verzameld zijn, vraagt om een specifieke wettelijke grondslag of toestemming van betrokken, dan wel gebruik voor een met het oorspronkelijke doel verenigbaar nieuw doel. Dit laatste moet bovendien goed worden gemotiveerd. Dit is dus 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 een nevendoel te gebruiken. Een term als ‘bijvangst’ kan dus overduidelijk juridische spanningen opleveren.

---

[15] Bantema e.a. 2021, p. 48.

5 Het verzamelen van online gegevens door gemeenten

5.1 Inleiding

Een tweede spanningsveld is de wijze waarop online gegevens worden verzameld. Online monitoring kan zowel handmatig als met monitoringstools. Dit is een spanningsveld doordat de wijze van monitoring een bepalende factor is voor de mate en intensiteit van monitoring. Door de opkomst van software is het mogelijk om in relatief korte tijd een ongekende hoeveelheid informatie van het internet te halen, waardoor er mogelijk steeds ingrijpender privacyinbreuken plaatsvinden.[16] In paragraaf 5.2 wordt een indicatie gegeven over de wijze waarop gemeenten monitoren. Daarna wordt in paragraaf 5.3 de AVG toegepast op de verzamelwijze. Tot slot kan de wijze van monitoring ook van invloed zijn op de stelselmatigheid van de monitoring, dit wordt in paragraaf 5.4 besproken.

5.2 Het verzamelen van online gegevens in de praktijk

Allereerst enkele cijfers die een indicatie zijn voor de mate en wijze van informatieverzameling. Uit het Black box-onderzoek volgt dat 76% van de gemeentelijke respondenten gebruik maakt van tools om in online bronnen te monitoren. De overige respondenten geven aan dit niet te weten, of niet te doen. Naast het gebruik van monitoringstools, monitort 39% (ook) handmatig online informatie. Dat kan via Google zijn, of via Facebook of Twitter, of kranten, etc.
In het verlengde van de wijze van monitoring is een tweede aandachtspunt wat er vervolgens met de verkregen gegevens wordt gedaan. Slaat men de gegevens op? Of niet? Dit proces wordt ook wel dossiervorming genoemd, wat opnieuw relevant is in de context van de gegevensverwerking en persoonsgegevens en dus de AVG. Voordat de AVG ter sprake komt volgt eerst een indicatie.

	Regelmatig + jaarlijks	Regelmatig*	Jaarlijks	Nooit	weet niet
In de gaten houden en niet opslaan	51	21	30	9	17
Automatische dossiervorming	14	5	9	46	21
Handmatige dossiervorming	33	8	25	8	19

Tabel 3. Frequentie van dossiervorming (in %, N = 162)

[16] J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen: Documentatieblad van het Ministerie van Justitie* (38) 2012, afl. 5, p. 35-49.

Iets meer dan de helft van de respondenten in het Black box-onderzoek (tabel 3) geeft aan dat online berichten niet worden opgeslagen en er daardoor geen dossier wordt opgebouwd. Verder geeft 14% van de respondenten aan gebruik te maken van automatische dossiervorming, waardoor informatie over een thema, groep of individu wordt samengevoegd. Dit kan automatisch gebeuren doordat er zoektermen worden ingevoerd in een monitoringstool. Deze informatie wordt dan automatisch opgezocht en opgeslagen. Tot slot is er volgens 33% van de respondenten sprake van handmatige dossiervorming.

Een derde aandachtspunt is wie de opdrachtgever tot de verzameling van online gegevens is. Dit is juridisch van belang voor de proportionaliteit[17] van de handeling, die in verhouding moet staan tot het publieke belang dat met de handeling wordt gediend, blijkt uit de AVG. Uit de interviews van het Black box-onderzoek blijkt dat het veelal de afdeling OOV is die een omgevingsanalyse opvraagt bij de afdeling Communicatie. Een enkele gemeente geeft aan dat de zoektermen gezamenlijk door de afdelingen OOV en Communicatie worden vastgesteld. Een andere respondent geeft aan dat dit wordt bepaald door veiligheidsadviseurs en/of de politie. Een laatste mogelijkheid komt vanuit de leveranciers van de monitoringstools. Zij leveren standaardterminologie aan. Er zijn gemeenten die alleen deze terminologie gebruiken, andere gemeenten vullen de standaardterminologie aan met eigen termen.[18]

5.3 Verzamelen en verwerken van (online) gegevens volgens de AVG

De wijze waarop er met de verkregen persoonsgegevens wordt omgegaan maakt uit voor de toepassing van de AVG. Artikel 4 van de AVG bevat alle belangrijke begrippen van de AVG en definieert deze begrippen. Doordat we het hier over de verwerking van gegevens hebben, is in dit geval vooral artikel 4 lid 2 van de AVG van belang. Artikel 4 lid 2 luidt:

> *Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals 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.*

De bepalingen uit de AVG die zien op verwerking gelden dus voor alle vormen van verwerking die in artikel 4 lid 2 AVG worden besproken. Zowel gegevens die geheel of gedeeltelijk geautomatiseerd verwerkt zijn als handmatig verwerkte gegevens die zijn opgenomen in een bestand of bedoeld zijn om in een bestand

[17] Proportionaliteit houdt in dat het doel van de verwerking van de persoonsgegevens in verhouding moet staan tot de inbreuk die op de privacy wordt gemaakt.
[18] De Vries & Bantema 2022, p. 18.

te worden opgenomen vallen onder die definitie. Wanneer er bij handmatig verwerkte gegevens géén bestand aan te pas komt, is de AVG níet van toepassing, blijkt uit artikel 4 lid 2 AVG.

Gegevensverwerking in de AVG doelt op een verwerkingshandeling die al dan niet wordt uitgevoerd met behulp van een computer of ander technologisch hulpmiddel. Wanneer de gegevens in een gestructureerde verzameling worden opgenomen, is er sprake van gegevensverwerking. Voorbeelden van verwerkingshandelingen zijn: vastleggen, ordenen, opslaan en structureren. Het verzamelen van gegevens zonder deze op te slaan valt óók onder het verwerken van gegevens. Er is kortom al heel snel sprake van verwerking van gegevens als bedoeld in de AVG.

Uit de cijfers van het Black box-onderzoek blijkt dus dat het overgrote deel van dossiervorming door gemeenten onder de AVG valt. De vraag is of gemeenten doorhebben dat dit het geval is, want het juridische kader en de betrokkenheid van een FG bleken summier in de gemeenten (zie par. 3.1).

5.4 Verwerkingsverantwoordelijke

Zoals bleek in het slot van paragraaf 5.2 is het ook van belang wie de opdrachtgever tot verzameling van de gegevens is. In de AVG wordt dit de verwerkingsverantwoordelijke genoemd. In de systematiek van de AVG zit er een verschil tussen de 'verwerker' en de verwerkingsverantwoordelijke. De verplichtingen uit de AVG zijn in principe van toepassing op de verwerkingsverantwoordelijke; degene die vaststelt welke persoonsgegevens worden verzameld, voor welk doel dit gebeurt, en op welke wijze en met welke middelen dit plaatsvindt (artikel 4 ondereel 7 AVG).[19] Wie dit is kan blijken uit een expliciete juridische bevoegdheid, maar ook uit een impliciete bevoegdheid[20] of uit de feitelijke invloed van een persoon. Belangrijk om te benoemen is dat de verwerkingsverantwoordelijke, naast dat hij verantwoordelijk is voor de naleving van de beginselen rondom de verwerking van persoonsgegevens, die naleving ook moet kunnen aantonen.[21]

5.5 Stelselmatigheid

Een derde spanningsveld rondom de wijze van online monitoring is de stelmatigheid van het monitoren. Er kunnen twee typen online monitoring worden onderscheiden: niet-stelselmatig en stelselmatig. Voor beide typen geldt dat de monitoring een beperking van artikel 8 EVRM en artikel 10 Grondwet

[19] Zie ook: B.W. Schermer, D. Hagenauw & N. Falot, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, Ministerie van Justitie en Veiligheid 2018.

[20] Denk bijvoorbeeld aan een vereniging die gegevens van haar leden registreert.

[21] Blijkt uit artikel 5 lid 1 en 2 AVG. Ter verduidelijking: bij de afdeling OOV zal het de burgemeester zijn die verwerkingsverantwoordelijke is, in veel andere gevallen kan er sprake zijn van politiegegevens, waardoor er een andere verwerkingsverantwoordelijke is.

moet kunnen rechtvaardigen,[22] de zogeheten beperkingssystematiek.[23] Daarom is voor een beperking van de waarborgen uit deze artikelen een wettelijke grondslag vereist. Er zit echter een verschil in 'zwaarte' tussen niet-stelselmatige monitoring en stelselmatige monitoring. Stelmatige monitoring wordt ook wel intensiever of ingrijpender monitoren genoemd. Er is sprake van stelselmatige monitoring als er met de monitoring een min of meer compleet beeld kan worden gekregen van bepaalde aspecten van iemands privéleven (bijvoorbeeld iemands uitgavenpatroon).[24]

Artikel 8 van het EVRM stelt meer eisen aan stelselmatige monitoring dan aan niet-stelselmatige monitoring. Stelselmatige monitoring moet een deugdelijke wettelijke grondslag hebben die meer waarborgen bevat. Zo worden eisen gesteld aan de maximale duur van de monitoring en de technische hulpmiddelen die gebruikt worden om te monitoren. De bestaande Nederlandse wetgeving bevat vooralsnog geen grondslag voor stelselmatige monitoring, terwijl voor niet-stelselmatige monitoring mogelijk artikel 172 lid 1 Gemeentewet, artikel 3 Politiewet en artikel 53a Participatiewet aanknopingspunten bieden.

Is er in de praktijk sprake van stelselmatige monitoring? Deze vraag is lastig te beantwoorden. Wanneer we kijken naar het Black box-onderzoek zien we dat er in de regel niet op personen wordt gezocht, tenzij het mensen zijn met een publieke functie zoals invloedrijke mensen uit de gemeente en opiniemakers. Dit kunnen ook mensen zijn die duidelijk naar voren komen uit een standaardanalyse, op wie dan verder is gemonitord. 'Natuurlijk ben je af en toe geïnteresseerd in iemand die iets initieert, dus dat houd je in de gaten.' Een enkele gemeente zoekt soms wél specifiek op naam, maar dat is echt een uitzondering.

Voor de beoordeling van de (oorspronkelijke) offline stelselmatigheid (van observaties) in het strafrecht zijn de plaats, duur, intensiteit, frequentie van de monitoring en het gebruik van technische hulpmiddelen relevant.[25] Echter worden de criteria om te bepalen of er sprake is van stelselmatige monitoring anders zodra het om online openbare bronnen gaat. Uit onderzoek van de Commissie-Koops[26] blijkt dat de oorspronkelijke offline criteria niet allemaal bruikbaar zijn bij online monitoring, omdat de duur en frequentie per definitie anders zijn.[27] In de regel is online monitoring geen momentopname, maar gelijk een verzameling van online uitingen over een langere periode in een relatief

---

[22] M. Buitenhuis & S. Hendriks, 'Blogreeks online monitoring deel 3: privacyaspecten', 24 november 2021, htttps://akd.eu/nl/insights/blogreeks-online-monitoring-deel-3-privacyaspecten.
[23] Zie bijv. P.P.T. Bovend'Eert e.a., *Constitutioneel recht*. Deventer: Wolters Kluwer 2021.
[24] Dit geldt óók voor het strafrecht.
[25] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27.
[26] De Commissie-Koops is ingesteld in 2017 op verzoek van het ministerie van Veiligheid en Justitie om te onderzoeken of de wettelijke regeling van het opsporingsonderzoek voldoet of aanvulling nodig heeft, o.a. door toenemende digitalisering.
[27] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018 (hierna: Commissie-Koops 2018).

korte tijd. De Commissie-Koops doet een voorstel voor een aantal criteria voor de beantwoording van de vraag of de inbreuk meer of minder waarborgen vergt. Deze criteria kunnen ook voor gemeentelijke monitoring zinvol zijn:[28]

1. *Omvang en het type gegevens*
2. *Aard van de bron*
3. *De wijze van zoeken*
4. *Het gebruiken van de gegevens*
5. *De mogelijke impact op de persoon*

Gemeenten kunnen deze strafrechtelijke criteria van de Commissie-Koops ook gebruiken om af te wegen wanneer iets stelselmatig monitoren is of niet, ze zijn echter niet uitputtend. Door aansluiting te vinden bij deze strafrechtelijke criteria wordt de consistentie van gemeentelijke monitoring vergroot, en wordt er ook voorkomen dat het voor gemeenten interessant is om 'alles maar' binnen de gemeentelijke scope te laten vallen omdat de politie op dit moment aan meer regelgeving rondom monitoring is gebonden.[29]

6 De herkenbaarheid van gemeenten bij online monitoring

6.1 Inleiding

Het laatste spanningsveld dat wordt besproken in dit artikel is de inzet van privé- en nepaccounts voor monitoringsdoeleinden. Dit spanningsveld heeft de nodige stof doen opwaaien in de media.[30] Allereerst wordt een aantal redenen voor het gebruik van privé- en nepaccounts besproken. Daarna volgt een aantal cijfers (lees: indicatie). Tot slot wordt de juridische context ervan geschetst.

6.2 Inzet van privé- en nepaccounts in de praktijk

Een reden voor gemeenten om privé- of nepaccounts in te zetten is dat het mogelijk is om meer en andere online bronnen in te zien. Ze worden bijvoorbeeld ingezet om informatie op te halen van openbare bronnen die niet door een monitoringstool worden aangeboden (denk aan Facebook of Instagram), maar ook voor bronnen die niet openbaar toegankelijk zijn, zoals besloten groepen op sociale mediakanalen. Door privé- en nepaccounts te gebruiken kan men dan alsnog toegang krijgen tot deze groepen.

[28] Commissie-Koops 2018, p. 156-168.
[29] Bantema e.a. 2021, p. 85.
[30] Zie o.a. ANP/Redactie gemeente.nu, 'Gemeenten niet op de hoogte van regels online monitoring', 18 mei 2021, https://gemeente.nu/bedrijfsvoering/privacy/gemeenten-niet-op-de-hoogte-van-regels-online-monitoring.

Uit het Black box-onderzoek komt naar voren dat 40% van de respondenten aangeeft nog nooit een privéaccount te hebben gebruikt om te monitoren. Dat geldt voor zowel het eigen account als dat van collega's. In het geval van nepaccounts is dat 67%. Redenen om geen nepaccounts te gebruiken hebben een ethische grondslag: 'we vinden dat tegenstrijdig met de open en eerlijke overheidsinstantie die we willen zijn', maar ook 'omdat er risico's aan verbonden zijn.'[31]

Toch zijn er ook medewerkers die er wel gebruik van maken. Een ander deel van de respondenten (38% privéaccounts van medewerkers, 13% nepaccounts) geeft namelijk aan soms wel op deze manier online te monitoren. Dit laat zien dat gemeenten terughoudender zijn met nepaccounts dan met privéaccounts (zie tabel 4). Slechts 1% geeft aan dat zowel privé- als nepaccounts vrijwel altijd worden ingezet. Bij een van de interviews geeft een respondent aan dat privéaccounts bijdragen aan de online informatiepositie: zo worden privéaccounts op sociale mediabronnen gebruikt om een 'sneller en beter beeld te krijgen van de situatie.' Ten aanzien van nepaccounts zegt een gemeentefunctionaris: 'Dat mag eigenlijk helemaal niet, maar we hebben wel fakeaccounts met een naam die niet bestaat, maar onder wie we opereren.'

	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

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

Per definitie leidt het gebruik van privé- en nepaccounts sneller tot een inbreuk op de privacy, maar een belangrijke kanttekening bij het gebruik van privéaccounts is dat het niet altijd een bewuste keuze is om ermee te monitoren. Gemeentelijke medewerkers kunnen met hun eigen accounts informatie voorbij zien komen die zij van belang achten voor de openbare orde en veiligheid, terwijl zij niet actief zoeken op deze informatie. Dit kan gelden voor WhatsAppgroepen, maar ook voor openbare Facebookgroepen (of zelfs gesloten) waarvoor toegang gevraagd moet worden, denk aan: 'Je bent 'plaatsnaam' als-groepen'.

6.3 Juridische context van de inzet van privé- en nepaccounts

Met het gebruik van privé- en nepaccounts kunnen gemeenten op veel platforms toegang krijgen tot gegevens over de personen die actief zijn op deze platforms. Het volgen van die personen met privé- en nepaccounts en het gebruiken van de

[31] Bantema e.a. 2021, p. 44.

informatie die deze personen delen kan leiden tot een inbreuk op de persoonlijke levenssfeer. Er zijn wel enkele omstandigheden die een rol spelen bij de bepaling en mate van de inbreuk. Zo is van belang hoe herkenbaar een account van een individuele gemeentefunctionaris of -ambtenaar is die gebruikt wordt.[32]

Daarnaast is het goed dat gemeenten zich ervan bewust zijn dat inwoners en andere personen die gemeentelijke accounts volgen dit doen omdat zij op de hoogte willen blijven van bijvoorbeeld nieuwsberichten van en uit de gemeente. Zij zullen redelijkerwijs niet of nauwelijks verwachten dat een gemeente de onderlinge connectie ook gebruikt om informatie in te winnen.

Het gebruik van nepaccounts vergroot het heimelijke karakter rondom monitoring en is een stap verder dan het gebruik van privéaccounts. Rondom de juridische kaders kunnen nog veel vragen worden gesteld en is vooralsnog veel onduidelijk. Vastgesteld kan worden dat nepaccounts per definitie een inbreuk vormen op de persoonlijke levenssfeer van degenen die geobserveerd en/of gevolgd worden. Dit geldt ook als het om open bronnen gaat.

7 Conclusie en bestuurlijke reactie

7.1 Conclusie

In deze bijdrage hebben we aandacht besteed aan de vraag of er een juridische basis is voor online monitoring door gemeenten. Deze vraag is relevant in een tijd waarin er een toename lijkt te zijn van online aangejaagde ordeverstoringen, waarbij de noodzaak voor een goede online informatiepositie verder toe lijkt te nemen.

Harde cijfers over wat gemeenten doen zijn er niet, maar op basis van het beschikbare materiaal is er wel een globaal beeld ontstaan van wat en hoe gemeenten online monitoren, met welke doelen ze dat doen en in hoeverre er rekening wordt gehouden met juridische kaders binnen de organisatie. Uit de bijdrage blijkt ook dat gemeenten de juridische kennis op dit vlak ontberen. Dit kan deels ondervangen worden door het benutten van de FG, die hoort toe te zien op de naleving van de AVG. De FG is echter in veel gevallen niet betrokken bij de online monitoring binnen gemeenten. De vraag is in hoeverre dat problematisch is en in hoeverre de werkwijzen van gemeenten tot juridische problemen kunnen leiden bij de online monitoring. Die kans is zeker aanwezig wanneer de werkwijze van gemeenten in ogenschouw wordt genomen.

Door het gebruik van monitoringstools is bijvoorbeeld de kans groter dat er sprake is van stelselmatige monitoring, ongeacht of het gaat om open of besloten bronnen. Daarnaast is gebleken dat er geen juridische grondslag is voor stelselmatige online monitoring. Indien gemeenten dat wel doen, is de kans

[32] Bantema e.a. 2021, p. 44.

groot dat er een inbreuk is op artikel 8 EVRM. Verder is het aannemelijk dat gemeenten al snel stuiten op de AVG. Wanneer zij sociale media monitoren, zijn er al snel persoonsgegevens in beeld en alleen het kijken naar persoonsgegevens (zonder zelfs op te slaan) maakt al dat er rekening met de regelgeving in de AVG dient te worden gehouden. Dit betekent bijvoorbeeld dat gemeenten verantwoording moeten afleggen aan de Autoriteit Persoonsgegevens[33] over welke gegevens zijn verzameld en hoe ze deze verwerken, zodat zij dit kunnen toetsen aan de eisen die worden gesteld in de AVG. Dit betekent ook dat gemeenten duidelijk moeten omschrijven met welke doelen (doelbepaling) ze dat doen en de FG hierbij betrekken. We zien dat de FG juist weinig wordt betrokken, terwijl we tegelijkertijd zien dat er veel persoonsgegevens worden verwerkt en er duidelijk sprake is van nevendoelen van de online monitoring (bijvangst). Gegevens die zijn verkregen voor een bepaald doel mogen voor dat nevendoel niet zonder meer gebruikt worden. Voor het gebruik van nepaccounts geldt dat er al snel sprake is van een inbreuk op de persoonlijke levensfeer in de zin van artikel 8 EVRM en wordt daarom afgeraden. Bij het gebruik van privéaccounts is vooral de herkenbaarheid van de gemeente van belang en de wijze waarop de conntectie tot stand komt. Als dat op een open en transparantie manier wordt gedaan, is het niet per se in strijd met onder andere het EVRM.

7.2 Bestuurlijke reacties op het onderzoek naar online monitoring

Na het rapport, dat breed in de media werd uitgemeten, kwamen er verschillende reacties vanuit gemeenten. *De Volkskrant* inventariseerde een aantal reacties, enkele weken na het uitkomen van het onderzoek.[34] Daarbij werd vooral ingegaan op het gebruik van nepaccounts. Meerdere gemeenten, waaronder Uithoorn en Hilversum, zijn naar aanleiding van het onderzoek gestopt met het gebruik van nepaccounts, maar destijds bleek ook dat in ieder geval negen gemeenten vasthielden aan die werkwijze. Een andere gemeente gaf aan hiermee door te gaan omdat het gebruik van nepaccounts in haar ogen niet per se ingaat tegen de regels. Tijdens een recent webinar van AKD op 24 maart 2022, dat ging over online monitoring, werd ook een stelling voorgelegd over de werkwijze van gemeenten.[35] Van 64 toehoorders die ook meewerkten aan de digitale stemming, bleek ruim de helft (55%) aan te geven door te zijn gegaan op de oude voet, terwijl ook een deel aangeeft gestopt te zijn met online monitoring (11%) of juist actief

[33] De Autoriteit Persoonsgegevens is de Nederlandse gegevensbeschermingsautoriteit en is het toezichthoudende orgaan van de AVG in Nederland.

[34] H. von Piekartz, 'Gemeenten gaan ondanks kritiek door met gebruik nepaccounts', *de Volkskrant* 3 juni 2021, https://volkskrant.nl/nieuws-achtergrond/gemeenten-gaan-ondanks-kritiek-door-met-gebruik-nepaccounts~ba11d0fe/.

[35] De gegevens van het webinar zijn niet gepubliceerd en zijn indicatief voor de reacties van gemeenten. We zien dit niet als representatief, want dat is niet vast te stellen. Het laat wel zien dat er verschillen zijn in de reactie op het onderzoek.

aan de slag is gegaan met een protocol (34%). Dat laatste sluit mooi aan bij de aanbevelingen die zijn gedaan in *Black box van gemeentelijke online monitoring*.

Er zijn ook veel gemeenteraden geweest die raadsvragen hebben gesteld. Zelfs in de Tweede Kamer zijn vragen gesteld aan de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) over het onderzoek. Uit de antwoorden op die vragen blijkt dat de minister erkent dat de verzameling van persoonsgegevens in veel gevallen van groot belang is voor de taakuitvoering van de overheid, maar dat het binnen de kaders van de wet moet plaatsvinden.[36] Naast aandacht voor bewustwording (onder andere via de Vereniging van Nederlandse Gemeenten) wordt een rijksbrede richtlijn/handreiking monitoring ontwikkeld waarin wordt aangegeven hoe departementen en uitvoeringsinstanties binnen de kaders van de AVG kunnen monitoren. Voordat deze richtlijn uitkomt, heeft Veiligheidsalliantie Noord-Holland Samen Veilig naar aanleiding van het onderzoek een werksessie georganiseerd samen met bestuursrechtadvocaten om de juridische kaders helder te krijgen en te vertalen in een handreiking. Deze handreiking is afgerond en online te raadplegen.[37]

In deze handreiking wordt een aantal aanbevelingen van Bantema e.a. verder uitgewerkt op basis van handelingen die gemeenten wel en niet moeten doen. Daarnaast wordt aangegeven welke zaken aan bod zouden moeten komen bij de uitwerking van een protocol voor online monitoring. Ondanks dat deze handreiking gemeenten helpt bij het organiseren en stroomlijnen van de werkwijze bij het online monitoring, lijken meer ingrijpende (juridische) wijzigingen onvermijdelijk als we de verouderde en niet op maat toegesneden juridische kaders naast de gemeentelijke werkwijze houden. De bestaande kaders lijken namelijk niet meer goed toepasbaar te zijn in de huidige digitale samenleving. Daarnaast kan men zich afvragen, en dat is geen juridische vraag, of gemeenten wel de aangewezen partij zijn om zo'n actieve rol bij online monitoring te spelen of dat dit toch meer een politietaak zou moeten zijn. Hoe dan ook laat deze bijdrage zien dat gebruik en ontwikkelingen in technologie tot juridische spanningen kunnen leiden.

[36] M. Maas, 'Ollongren gaat in gesprek over gemeentelijke privacy', 5 juli 2021, www.binnenlandsbestuur.nl/digitaal/minister-gaat-gesprek-over-gemeentelijke-privacy.
[37] NH Samen Veilig, Project Online Orde, *Handreiking Online Orde sessie & factsheet Black Box van gemeentelijke online monitoring*, 8 april 2022, geraadpleegd via https://nh-sv.nl/kennisbank/cyber/project-online-orde/.