ONLINE GEGEVENSGARING IN EEN WOELIGE SAMENLEVING

Spanningen bij politiewerk op het web

De politie maakt in haar werk in toenemende mate gebruik van gegevens op het wereldwijde web. Dit doet zij voor verschillende doeleinden. In hoofdlijnen is hierbij een onderscheid te maken tussen intelligence en bewijs.

Het online vergaren van gegevens ten behoeve van intelligence wordt OSINT genoemd: *open source intelligence*. Het online vergaren van gegevens ten behoeve van bewijs wordt internetrechercheren genoemd. OSINT heeft een niet-strafvorderlijk karakter en moet plaatsvinden op basis van de algemene taakstelling, die is opgenomen in artikel 3 van de Politiewet. Internetrechercheren heeft een strafvorderlijk karakter en vindt plaats binnen het kader van het Wetboek van Strafvordering. Dit artikel gaat over OSINT. De eerste paragrafen zijn inleidend en daarna volgen de vijf spanningen die centraal staan in dit artikel.

Intelligence is geanalyseerde informatie en kennis op grond waarvan beslissingen over de uitvoering van de politietaak worden genomen (Kop & Klerks,(2009). Korter gezegd: *information designed for action* (Duijn, 2011). In het intelligenceproces worden informatie- of intelligenceposities opgebouwd[1] over veiligheidsthema's. Voor het opbouwen van deze posities worden uiteenlopende gegevensbronnen benut. Een van die bronnen bestaat uit online gegevens. Het gaat daarnaast om bronnen waar de politie al langer gebruik van maakt, waaronder gegevens die worden verzameld in het straatwerk, in de opsporing en via het runnen van informanten. De bijdrage die online beschikbare gegevens leveren aan de intelligencepositie, is onder andere afhankelijk van de aard van het veiligheidsthema (Landman & Groothuis, 2022). In dit artikel zoom ik vooral in op het gebruik van OSINT voor het opbouwen van een intelligencepositie op het gebied van maatschappelijke onrust, omdat 1) dit een actueel thema is waarbij OSINT een belangrijke rol speelt, en 2) zich bij dit thema volop spanningen rond het gebruik van OSINT voordoen.

1 Onder opbouwen schaar ik ook het onderhouden van de intelligencepositie.

Over de auteur
Wouter Landman PhD begeleidt veranderprocessen en verricht onderzoek. Actuele thema's zijn: technologie & politiewerk, innovatie en ontwikkeling van politieteams. www.bureaulandman.nl

Tekst: Wouter Landman

Maatschappelijke onrust als veiligheidsthema

In de Veiligheidsagenda 2023-2026 is maatschappelijke onrust omschreven als "collectieve gedragingen in situaties die voortkomen uit een gevoel van angst, onzekerheid, onvrede of miskenning" (Ministerie van Veiligheid en Justitie, 2022). Er zijn verschillende vormen van maatschappelijke onrust, uiteenlopend van vreedzame en kleinschalige demonstraties tot radicale(re), stafbare en grootschalige acties. Er is tegenwoordig sprake van een breed scala aan maatschappelijke thema's die collectief ongenoegen in grote groepen in de samenleving veroorzaken (Bekkers et al., 2023). Hierdoor is de Nederlandse samenleving in 'woelig vaarwater' terechtgekomen (Eysink Smeets, 2022). Dit vaarwater wordt gekenmerkt door spanningen tussen bevolkingsgroepen en verzet tegen de overheid.

Het internet in het algemeen en socialemediaplatformen in het bijzonder spelen een belangrijke rol bij maatschappelijke onrust: het is het domein waar burgers zich onder andere uiten, verbinden en organiseren met gelijkgestemden en waar zij (des)informatie tot zich nemen die van invloed is op het ervaren ongenoegen (Bekkers et al., 2023; Beugelsdijk, 2021; Fukuyama, 2019). Deze rol van sociale media bij maatschappelijke onrust impliceert dat het voor de politie een belangrijk domein is voor het vergaren van gegevens over dit veiligheidsthema. Sinds de avondklokrellen in januari 2021 – toen de samenleving (opnieuw) te maken kreeg met grootschalige, online aangejaagde openbare ordeverstoringen – zijn de investeringen van de politie in OSINT dan ook toegenomen (Landman & Groothuis 2022).

Inzet van OSINT

Online verzamelde gegevens worden gebruikt voor het *monitoren* van trends & ontwikkelen en het *identificeren* van groepen en personen op het gebied van maatschappelijke onrust. OSINT-activiteiten worden vooral uitgevoerd door specialisten binnen de intelligenceorganisatie van de politie en in toenemende mate ook door digitaal-wijkagenten in de basisteams

> Het internet en socialemediaplatformen spelen een **belangrijke rol** bij maatschappelijke **onrust**

(Terpstra et al., 2021). Daarnaast zijn er binnen de specialistische opsporing *virtual agents*, die online onder dekmantel werken en ook worden ingezet ten behoeve van de intelligencepositie op het gebied van maatschappelijke onrust. Online gegevensvergaring vindt zowel handmatig als geautomatiseerd plaats. Voor de geautomatiseerde vergaring wordt uiteenlopende software gebruikt. De verzamelde gegevens worden in de regel gecombineerd met andere (politie)gegevens en geanalyseerd om te komen tot intelligenceproducten. Een voorbeeld van een intelligenceproduct is een rapport waarin boerenactiegroepen zijn beschreven die zich bezighouden met buitenwettelijke methoden van actievoeren.

Spanning I: offline en online

In de samenleving zijn offline en online werelden die voortdurend in elkaar overlopen (Lane, (2019). Dit geldt ook voor de gegevensverzameling voor de politie: de politie verzamelt zowel offline als online gegevens en combineert deze met elkaar. In berichtgeving over de online gegevensverzameling heeft de politie de neiging online gegevensverzameling op gelijke voet te stellen met offline gegevensverzameling. De politie-eenheid Den Haag gaf naar aanleiding van de berichtgeving over de virtual agent die – 'vermomd' als activiste – meekeek en meedeed in chatgroepen van Extinction Rebellion bijvoorbeeld aan dat dit te vergelijken is met het surveilleren door agenten in burgerkleding op straat.[2] Daarmee oogt de gegevensverzameling door de virtual agent licht en past het binnen de algemene taakstelling.

2 www.trouw.nl/binnenland/hoe-ver-mag-de-politie-gaan-bij-het-heimelijk-meekijken-in-chatgroepen

Digitale surveillance is snel **diepgaander** dan **traditionele surveillance**

Het is echter de vraag of deze redenering voldoende hout snijdt. Digitale surveillance is namelijk (snel) diepgaander dan traditionele surveillance. Een politieagent die in burger in de wijk loopt en door de gordijnen kijkt of een 'interessante' burger thuis is, krijgt op dat moment een weinig diepgaand inzicht in het leven van die burger. Een politieagent die met een niet tot de politie herleidbaar account (functioneel account) een profiel van een burger op Facebook bekijkt, krijgt in veel gevallen een diepgaander inzicht, zoals inzicht in relaties en activiteiten.

Online gegevensverzameling is dus een ander type activiteit met andere effecten dan offline gegevensverzameling (Ferguson, 2022). Dit heeft onder andere als gevolg dat het juridisch kader voor regulering van offline gegevensverzameling niet of nauwelijks geschikt is voor regulering van online gegevensverzameling (Commissie Koops, 2018). In de praktijk moet niettemin van dit juridisch kader gebruik worden gemaakt, omdat er vooralsnog geen – op online gegevensverzameling toegesneden – juridisch kader is.

Spanning II: een niet meer dan geringe en meer dan geringe inbreuk

OSINT moet worden gebaseerd op de algemene taakstellende bevoegdheid van de politie, die wordt ontleend aan artikel 3 Politiewet. Deze bevoegdheid kan breed worden ingezet ten behoeve van het politiewerk (Zuurveen & Stol, 2020). De inzet wordt begrensd door het effect ervan op de grondrechten van burgers. Op basis van artikel 3 mogen opsporingsambtenaren van de politie uitsluitend een niet meer dan geringe inbreuk op deze grondrechten maken. Dit betreft onder andere het recht op eerbiediging van de persoonlijke levenssfeer. Dit recht wil eenvoudig geformuleerd zeggen dat iedere burger het recht heeft om (door de overheid) met rust te worden gelaten.

Online gegevensverzameling door de politie is – zoals gezegd – sneller diepgaander dan offline gegevensverzameling: er wordt relatief snel een min of meer volledig beeld van aspecten van iemands leven verkregen. Dit geldt in het bijzonder wanneer online verzamelde gegevens worden gecombineerd met andere gegevens. Ieder gegeven op zichzelf geeft dan wellicht nog niet zoveel inzicht, maar het resultaat van het combineren en analyseren doet dit wel (Fedorova et al., 2022). Als je sleutelpersonen binnen een protestgroep in kaart brengt, hun identiteit weet vast te stellen, online gegevens verzamelt, gegevens uit politiesystemen en de Basisregistratie Personen gebruikt, kun je een min of meer volledig beeld van aspecten van iemands leven krijgen.[3] Op dat moment kan er al sprake zijn van een meer dan geringe inbreuk in de persoonlijke levenssfeer.

Dit betekent dat de politie met OSINT moet stoppen zodra de drempel van de 'meer dan geringe inbreuk' in zicht komt (Commissie Koops, 2018). Dit roept een spanning op. Van de politie wordt verwacht dat zij zicht heeft op maatschappelijke ontwikkelingen, weet wat er bij bijvoorbeeld demonstraties kan worden verwacht en daarop anticipeert. Het voldoen aan deze verwachting wordt bemoeilijkt doordat de politie op het gebied van OSINT snel tegen grenzen aanloopt.

Spanning III: een publiek toegankelijke en afgeschermde bron

OSINT staat voor 'open source intelligence'. Open source wil zeggen dat het om publiek toegankelijke bronnen gaat. De grens tussen een publiek toegankelijke en afgeschermde online bron is echter niet duidelijk. In de Memorie van Toelichting op het gemoderniseerde Wetboek van Strafvordering is enige helderheid gegeven. Tot een publiek toegankelijke bron

3 Hierbij moet de politie overigens alert zijn op het gebruik van commerciële datasets die worden aangeboden door leveranciers van software, zoals (extra opties binnen) Maltego. Ik heb geen kennis over dit gebruik, maar wil er slechts op wijzen dat dit een risico is in het kader van inbreuk op de persoonlijke levenssfeer. Zie het rapport van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (2022) over automated OSINT in de context van de inlichtingen- en veiligheidsdiensten.

Literatuur

- Bantema, W., Twickler, S.M.A., Munneke, S.A.J., Duchateau, M. & Stol, W.Ph. (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld.* Den Haag: Sdu.
- Bekkers, F., De Jong, E., Jasper, L., & MacLaughlin, E. (2023). *Maatschappelijke ontgoocheling van de middenklasse. Optreden, oorzaken en gevolgen.* The Hague Centre for Strategic Studies.
- Beugelsdijk, S. (2021). *De verdeelde Nederlanden. Hoe een perfecte storm een klein land dreigt te splijten (en wat we daaraan kunnen doen).* Amsterdam: Balans.
- Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops) (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving.* Den Haag.

kan toegang worden verkregen zonder een beveiliging te doorbreken of omzeilen, zonder het aanwenden van technische ingrepen, valse signalen of valse sleutels of het aannemen van een valse hoedanigheid.[4] Het gaat dus niet om de aard van de bron, maar om de wijze van toegang. Ik neem Facebook als voorbeeld. Er is sprake van een publiektoegankelijke bron als een politiefunctionaris met een functioneel account gegevens van een Facebookprofiel van een burger overneemt. Er is sprake van een afgeschermde bron als de politiefunctionaris vrienden wordt met de betreffende burger en vervolgens gegevens overneemt. Deze gegevens zijn namelijk niet voor iedereen toegankelijk, maar alleen voor vrienden en de betreffende burger geeft actief toegang door een vriendschapsverzoek te accepteren.

Het onderscheid tussen een publiek toegankelijke en afgeschermde bron is van belang, omdat – op basis van het gemoderniseerde Wetboek van Strafvordering – mag worden aangenomen dat het verzamelen van gegevens in afgeschermde bron om een 'zwaardere' bevoegdheid vraagt. Dit impliceert naar mijn idee dat het overnemen van gegevens uit afgeschermde bronnen op basis van artikel 3 niet mogelijk is of in ieder geval ter discussie staat. Dit zorgt voor een spanning, want de communicatie tussen burgers die voor de intelligencepositie van belang is, vindt tegenwoordig vooral plaats in allerlei online groepen. Het is in de praktijk niet altijd duidelijk in welke mate dergelijke groepen als afgeschermde bronnen moeten worden opgevat. In de praktijk blijken eenheden hier verschillend mee om te gaan: sommige eenheden zijn op grond van artikel 3 niet of nauwelijks aanwezig in online groepen, anderen zijn dat wel (Landman & Groothuis, 2022).

Spanning IV: (informatie)officier en burgemeester

In de Politiewet is het eenduidig geformuleerd: de politie treedt op onder het gezag van de burgemeester als het de openbare orde betreft en onder het gezag van de officier van justitie als het gaat om strafrechtelijke handhaving. Maar hoe zit dit bij online gegevensverzameling

> De politie is **op zoek** naar haar **gezag** in het kader van **online gegevensvergaring** op het gebied van **maatschappelijke onrust**

gericht in het kader van maatschappelijke onrust? De officier van justitie is het gezag bij strafrechtelijke handhaving, maar in veel gevallen gaat het om situaties waarin er (nog) geen specifieke verdenking is van enig strafbaar feit. De informatieofficier geeft richting aan en oefent gezag uit over de onderdelen van de politie die belast zijn met het informatieproces ter ondersteuning van de strafrechtelijke handhaving, maar het gaat hier om het informatieproces ter ondersteuning van (ook) de openbare orde. De burgemeester is het gezag bij het optreden in het kader van de openbare orde, maar het gaat hier om online gegevensverzameling in het kader van mogelijke openbare orde verstoringen. Dit is een andere vorm van 'optreden' dan waar het gezag van de burgemeester van oorsprong betrekking op heeft.

Het voorgaande heeft tot gevolg dat de politie op zoek is naar haar gezag in het kader van online gegevensvergaring op het gebied van maatschappelijke onrust. In de praktijk leidt dit tot verschillen (Landman & Groothuis, 2022). In een deel van de eenheden wordt er vanuit de intelligenceorganisatie – of vanuit de specialistische opsporing waar virtual agents werkzaam zijn – afgestemd met de informatieofficier. In sommige eenheden wordt er (af en toe) afgestemd met de burgemeester, omdat het om openbare orde aspecten gaat. In algemene zin geldt echter dat de burgemeester niet gewend is aan deze rol en het grenzeloze karakter van bijvoorbeeld online groepen zich moeizaam verhoudt tot het lokale karakter van het gezag (Bantema et al., 2018). In de praktijk zijn er met betrekking tot de beslissingsbevoegdheid dus

4 Zie p. 499 van de MvT, ambtelijke versie juli 2020.

Literatuur (vervolg)

- Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (2021). *Automated OSINT: tools en bronnen voor openbronnenonderzoek*. CTIVD
- Duijn, P. (2011). Intelligence en recherchestrategieën. In N. Kop, R. van der Wal & G. Snel (red.), *Opsporing belicht: over strategieën in de opsporingspraktijk* (pp. 63-94). Apeldoorn: Politieacademie.
- Eysink Smeets, M. (2022). *Onrust begrijpen begint bij anders kijken. Een veiligheidspsychologisch perspectief op maatschappelijke onrust*. Utrecht: Centrum voor Criminaliteitspreventie en Veiligheid.
- Fedorova, M.I., Te Molder, R.M., Dubelaar, M.J., Lestrade, S.M.A., & Walree, T.F. (2022). *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*. Nijmegen: Radboud University Press.
- Ferguson, A.G. (2022). Why digital policing is different. *Ohio State Law Journal*, 1-32.

> Het **risico** is dat er in toenemende mate een **politie ontstaat** die opereert op de **grens** van uitingen én gedragingen van **burgers**

onduidelijkheden, die binnen de politie zorgen voor een spanningsveld: het gezag is nodig als houvast in soms onduidelijke situaties, maar het gezag is zoekende naar diens eigen rol.

Spanning V: uiting en gedraging

De vijfde en laatste spanning heeft een iets ander karakter dan de vier voorgaande spanningen, maar verdient naar mijn idee wel aandacht. De online gegevensverzameling in het kader van maatschappelijk ongenoegen heeft onder andere het karakter van het (al dan niet geautomatiseerd) monitoren van allerlei uitingen die burgers doen. Burgers die uitingen doen die wijzen op mogelijke strafbare feiten, openbare orde verstoringen of anderszins zorgelijk zijn, worden in meer of mindere mate aan nadere gegevensverzameling en analyse onderworpen. Dit kan vervolgens leiden tot vormen van proactieve optreden. Gegeven de maatschappelijke ontwikkelingen is dit tot op zekere hoogte nodig en begrijpelijk. Het wordt ook van de politie verwacht, want voorkomen is beter dan genezen.

Deze praktijk gaat echter gepaard met de kans dat er in toenemende mate een politie ontstaat die opereert op de grens van uitingen én gedragingen van burgers (Schuilenburg, 2016).

In februari 2023 was er een jongeman die naar aanleiding van de megawinst van Ahold Delhaize had getweet dat het moreel acceptabel was om te stelen bij Albert Heijn, omdat er over de rug van de basisbehoeften van burgers megawinsten werden gemaakt. Dit resulteerde in een wijkagent aan de deur die aangaf dat ze een signaal had gekregen van de 'digi-afdeling'. Ze waarschuwde de jongeman en gaf aan dat als het 'verder zou gaan met hem', de politie zou gaan kijken wat er kan worden gedaan met het account. Ook werd aangegeven dat hij online gevolgd zou worden. Dit voorbeeld illustreert mijns inziens hoe de politie op basis van (online) intelligence aan het schuiven is op de grens tussen uiting en gedraging. Het gevaar ontstaat dat het hebben en uiten van bepaalde gedachten steeds meer voorwerp van politiecontrole gaat worden (Schuilenburg, 2016). Dit roept een fundamentele spanning op tussen het belang van proactief politieoptreden enerzijds en het belang van de vrijheidssfeer van burgers anderzijds. Deze spanning leidt naar de vraag wat voor een politie wij in onze samenleving willen hebben.

Tot slot: legitiem politiewerk mogelijk maken

De politie staat voor de opgave om de beschreven spanningen te hanteren en waar mogelijk op te lossen. Om dit te goed te kunnen doen, is een passend juridisch kader nodig. De modernisering van het Wetboek van Strafvordering is een verbetering voor internetrechercheren – want er komt een (specifieke) wettelijke grondslag voor het stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen – maar hier heeft OSINT weinig tot niets aan. Niet-strafvorderlijke normering is van belang. Niet om het politiewerk te begrenzen, maar om legitiem politiewerk mogelijk te maken.

Literatuur (vervolg)

- Fukuyama, F. (2019). *Identiteit. Waardigheid, ressentiment en identiteitspolitiek*. Amsterdam: Atlas Contact.
- Kop, N., & Klerks, P. (2009). *Doctrine intelligencegestuurd politiewerk*. Apeldoorn: Politieacademie.
- Landman, W. & Groothuis, S. (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie*. Den Haag: Sdu.
- Lane, J. (2019). *The digital street*. Oxford University Press.
- Ministerie van Justitie & Veiligheid (2022). *Veiligheidsagenda 2023-2026*. Ministerie van Justitie & Veiligheid.
- Schuilenburg, M.B. (2016). Predictive policing. De opkomst van een gedachtenpolitie? *Ars aequi, 65*(12), 931-936.
- Terpstra, J., Salet, R., Duijneveldt, I. van & Havinga, T. (2021). *Gebiedsgebonden politiewerk in ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving*. Den Haag: Sdu.
- Zuurveen, R. & Stol, W. (2020). *Benutten van digitale sporen*. Den Haag: Sdu.