

Een praktijk in ontwikkeling

Online gegevensvergaring door de politie

Wouter Landman

Als gevolg van het internetgebruik en smartphonegebruik door burgers is er online steeds meer informatie beschikbaar is. Om zicht te houden op ontwikkelingen in de samenleving en strafbare feiten op te sporen, vergaart de politie online gegevens. In dit artikel is in kaart gebracht hoe de politie in Nederland gebruik maakt van online gegevensvergaring en welke actuele vraagstukken zich hierbij voordoen. Online gegevensvergaring is binnen de politie in ontwikkeling en hierbij doen zich uiteenlopende vraagstukken voor, waaronder het beoordelen van de betrouwbaarheid van online gegevens, nieuwe bevoegdheden en toenemende omvang van online vergaarde gegevens die moeten worden geanalyseerd.

1 De noodzaak van online gegevensvergaring voor het politiewerk

1.1 Hybridisering van criminaliteit en openbare-ordeverstoringen

De politie heeft tot taak om te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die dat behoeven. De uitvoering van deze taak vindt in toenemende mate plaats in een hybride wereld waarin offline en online interacties en ervaringen sterk met elkaar verweven zijn (zie Barrico, 2019; Floridi, 2014). Dit maakt dat ook criminaliteit en openbare-ordeverstoringen in toenemende mate bestaan uit een track van samenhangende incidenten, die afwisselend een online en offline karakter hebben (zie o.a. De Boer et al., 2024; Mehlbaum et al., 2025; Roks et al., 2021; Van Steden et al., 2025).

Op 7 november 2024, de dag van de wedstrijd tussen Ajax en Maccabi Tel Aviv, wordt Rachid O. lid van de appgroep Buurthuis 2.¹ Hij heeft op sociale media een linkje gevonden waarmee hij in de appgroep kan komen. In deze appgroep zijn de avond ervoor en afgelopen nacht allerlei berichten gedeeld over wat de supporters van Maccabi Tel Aviv hebben gedaan, waaronder het verwijderen van een Palestijnse vlag van een gevel, mishandeling van taxichauffeurs (die langs de supporters kwamen rijden en 'free Palestine' riepen) en het zingen van kwetsende liederen over de Palestijnen. Op het moment dat Rachid O. in de appgroep komt, gaan er allerlei opruiende en antisemitische berichten rond. Ook Rachid O. plaatst dergelijke berichten. 'Er lopen duizenden Israëliërs door de stad. Deze kans krijg ik miss nooit meer', appt Rachid O. in Buurthuis 2, 'om

1 Deze passage is gebaseerd op reconstructies van het NRC: www.nrc.nl/nieuws/2024/12/28/hoer-amsterdam-even-strijdtoneel-werd-van-de-gaza-oorlog en www.nrc.nl/nieuws/2024/12/09/nog-voordat-de-maccabi-rellen-uitbraken-keek-de-politie-al-mee-in-pro-palestijnse-appgroepen.

kk joden te slaan'. Later die dag rijdt hij met drie vrienden van Utrecht naar Amsterdam. Aan het einde van de avond trekken de jongemannen richting Amsterdam Centraal, waar de metro's met Maccabi-fans aankomen. 's Middags is er in Buurthuis 2 al gedeeld wat de bedoeling is: na de wedstrijd groeperen in de stad en losse groepen Israëliërs aanvallen. Tussen tien voor twaalf en half twee die nacht is iedereen die met een geel shirt of gele sjaal door Amsterdam loopt dan wel wordt verondersteld Joods te zijn een potentieel doelwit van jongemannen zoals Rachid O. Er vinden talloze 'flitsaanvallen' plaats waarbij gewonden vallen. Deze 'flitsaanvallen' worden door de daders vaak gefilmd en daarna trots in appgroepen gedeeld en verheerlijkt.

De uitvoering van de politietaak vindt van oudsher plaats in de fysieke wereld. De ontwikkelingen in de samenleving maken dat het politiewerk in toenemende mate ook online moet plaatsvinden (Europol, 2025). Als gevolg van het internetgebruik (waaronder sociale media) en smartphonegebruik (met camera's) door burgers is er online steeds meer informatie beschikbaar is, die voor het politiewerk relevant kan zijn (Feenstra, 2018; Stol & Strikwerda, 2018; Van Puyvelde & Rienzi, 2025). Om zicht te houden op ontwikkelingen in de samenleving en strafbare feiten op te sporen, moet de politie gebruik maken van online gegevens (Landman & Groothuis, 2022). Om die reden zijn politieorganisaties wereldwijd gaan investeren in het online vergaren van gegevens (Fortin et al., 2021; Pastor-Galindo et al., 2020; Sampson, 2017). Dit geldt ook voor de politie in Nederland.

1.2 Doel en opbouw van dit artikel

Het doel van dit artikel is het geven van inzicht in de wijze waarop de politie in Nederland op hoofdlijnen invulling geeft aan online gegevensvergarig en welke vraagstukken zich hierbij op dit moment voordoen. De volgende probleemstelling staat centraal: op welke wijze maakt de politie in Nederland op hoofdlijnen gebruik van online gegevensvergarig en welke vraagstukken doen zich hierbij op dit moment voor? De inhoud van dit artikel is deels gebaseerd op empirisch onderzoek dat door de auteur naar online gegevensvergarig door de politie is verricht (Landman & Groothuis, 2022).² De inzichten uit dit empirisch onderzoek zijn geactualiseerd op basis van interviews met vier sleutelpersonen binnen de politie, actuele literatuur en kennis van actuele ontwikkelingen, waaronder op het gebied van wetgeving.

Het artikel is als volgt opgebouwd. Paragraaf 2 behandelt de hoofdlijnen van de wijze waarop de politie gebruikmaakt van online gegevensvergarig. Eerst wordt ingegaan op online gegevensvergarig als vakgebied en vervolgens vindt een toelichting plaats op de twee domeinen waarin online gegevensvergarig wordt ingezet: intelligence en opsporing. Tot slot wordt aandacht besteed aan online gegevensvergarig in de basisteams waar online gegevensvergarig voor zowel

2 Par. 2 is gebaseerd op het onderzoek van Landman & Groothuis (2022) en geactualiseerd op basis van de interviews die voor dit artikel zijn afgenomen. Par. 3 is volledig nieuw ten opzichte van het onderzoek uit 2022.

intelligence als opsporing invulling krijgt. Paragraaf 3 gaat over actuele vraagstukken en ontwikkelingen, waaronder synthetische media, de toenemende omvang van online gegevens, de inbreuk op grondrechten en toenemende beslotenheid van online bronnen. Paragraaf 4 rondt af met een conclusie.

2 Online gegevensvergaring door de politie: opsporing en intelligence

2.1 Online gegevensvergaring gedefinieerd

Binnen de politie worden er voor en rondom ‘online gegevensvergaring’ verschillende termen gebruikt (Landman & Groothuis, 2022). Dit komt vooral doordat er binnen de politie voor verschillende doelen online gegevens worden vergaard en op deze vergaring verschillende juridische regimes van toepassing zijn. Er worden in de eerste plaats online gegevens vergaard voor opsporing. Onder opsporing wordt verstaan: het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen. Binnen de politie worden daarnaast online gegevens vergaard voor intelligence. Onder intelligence wordt verstaan: informatie die wordt gebruikt voor het nemen van beslissingen over de uitvoering van het politiewerk (zie Kop & Klerks, 2009).³ Anders gezegd: bij opsporing gaat de gegevensvergaring om bewijs en bij intelligence om sturingsinformatie (zie Duijn, 2011; Sampson, 2017). Opsporingshandelingen vinden plaats op basis van een strafrechtelijk regime, terwijl vergaringsactiviteiten op het gebied van intelligence (vooralsnog) plaatsvinden op basis van de algemene taakstellende bevoegdheid van de politie, die wordt ontleend aan artikel 3 Politiewet 2012. Kortom: er zijn binnen de politie twee varianten van online gegevensvergaring, die van elkaar moeten worden onderscheiden. Het (belang van het) onderscheid tussen beide neemt niet weg dat in de praktijk online gegevensvergaring voor intelligence in sommige gevallen overgaat in online gegevensvergaring voor opsporing (zie ook Sampson, 2017).

Op de dag van de wedstrijd tussen Ajax en Maccabi Tel Aviv (7 november 2024) monitort de politie in Amsterdam WhatsApp-groepen waarin Pro-Palestijnse demonstranten (aanvankelijk) informatie uitwisselen over een geplande betoging bij de Johan Cruijff Arena.⁴ Een van de appgroepen die de politie monitort, heeft de naam Free Palestine. Rond 10:00 uur 's ochtends wordt in deze appgroep een linkje gedeeld voor een nieuwe groep: Buurthuis 2. Deze appgroep wordt vervolgens ook door de politie gemonitord. Rond het middaguur wordt daar een bericht geplaatst ‘ik zie 3 stuks lopen met die sjaals om’. Daarop volgt het bericht van een ander: ‘knal ze neer’. De politie krijgt van het Openbaar

3 Intelligence moet worden onderscheiden van inlichtingen. Bij inlichtingen betreft het heimelijk inwinnen van informatie bij personen (informanten). Binnen de politie worden inlichtingen vergaard door de teams criminele inlichtingen (TCI) en openbare orde inlichtingen (TOOI). Zie Van der Plas & Brown (2017). Inlichtingen zijn een bron van intelligence.

4 Deze passage is gebaseerd op reconstructies van het NRC: www.nrc.nl/nieuws/2024/12/28/hoer-amsterdam-even-strijdtonel-werd-van-de-gaza-oorlog en www.nrc.nl/nieuws/2024/12/09/nog-voordat-de-maccabi-rellen-uitbraken-keek-de-politie-al-mee-in-pro-palestijnse-appgroepen.

Ministerie (vanwege het strafbare feit opruiing) toestemming om het berichtenverkeer in deze nieuwe appgroep ‘veilig te stellen’. Zo gaat intelligence over in opsporen.

Online gegevensvergaring (OGG) gebruik ik als overkoepelende aanduiding voor de activiteit en het vakgebied. Online gegevensvergaring definieer ik als het verzamelen, valideren en analyseren van gegevens uit online bronnen ten behoeve van het politiewerk. Online gegevensvergaring voor opsporing noem ik in dit artikel *internetrecherchen*. Online gegevensvergaring voor intelligence noem ik in dit artikel *open source intelligence* (OSINT). Bij deze definitie moet worden opgemerkt dat in internationaal verband en buiten de politie OSINT als term wordt gebruikt voor de (overkoepelende) activiteit en het vakgebied (zie bijv. Higgins, 2021). Ook binnen de politie in Nederland wordt OSINT geregeld in de context van opsporing gebruikt, in het bijzonder in het domein van cybercrime. Er zijn twee redenen om dit in dit artikel niet te doen. De eerste reden is dat het zinvol is om onderscheid te maken tussen opsporing en intelligence. De tweede reden is dat het woord ‘open’ een begrenzing geeft die de term OSINT minder geschikt maakt voor het geheel en ook voor het intelligenciewerk al te smal kan zijn (zie ook par. 3.4). Om die reden gebruik ik de formulering ‘online bronnen’, waaronder zowel open of publiek toegankelijke bronnen (surface web en deep web, waaronder het dark web) als besloten bronnen vallen.

2.2 *Online gegevensvergaring voor opsporing: internetrecherchen*

Internetrecherchen vindt plaats binnen een opsporingsonderzoek. Een opsporingsonderzoek is gericht op reconstrueren van wat er is gebeurd of gaande is; er wordt gepoogd de ware toedracht van een misdrijf te achterhalen (Kop et al., 2025). De reconstructie bestaat idealiter uit het beantwoorden van de ‘zeven gouden W-vragen’ (De Poot et al., 2004); wie, wat, waar, waarmee, op welke wijze, wanneer en waarom. In een opsporingsonderzoek worden in de regel meerdere opsporingsmethoden ingezet (Kop et al., 2025), zoals een buurtonderzoek, een verhoor, DNA-onderzoek, een telefoontap en dergelijke. De verschillende opsporingsmethoden leveren stukjes informatie op (‘puzzelstukjes’) die in het onderzoek in samenhang bij elkaar worden gebracht om te komen tot de reconstructie van het strafbaar feit (Landman et al., 2020). Uit onderzoek komt naar voren dat internetrecherchen binnen de politie weliswaar een groeiende praktijk is,⁵ maar tegelijkertijd nog niet structureel of standaard wordt overwogen bij de start van een opsporingsonderzoek of gedurende een opsporingsonderzoek (Landman & Groothuis, 2022). Het is in dat opzicht een relatief nieuwe opsporingsmethode, die nog niet voor alle opsporingsambtenaren van de politie gebruikelijk is. De opsporing in Nederland is op dit punt nog niet overal ‘bij de tijd’.

In het gebruik van internetrecherchen doen zich verschillen voor tussen typen misdrijven en tussen opsporingsteams. Met typen misdrijven wordt verwezen naar het onderscheid tussen veelvoorkomende criminaliteit (bijv. fietsendiefstal, winkeldiefstal, eenvoudige mishandeling) high impact criminaliteit (bijv. straat-

5 Zie ook de memorie van toelichting bij het nieuwe Wetboek van Strafvordering, p. 572.

roof, woninginbraken, zedendelicten, levensdelicten) en ondermijnende criminaliteit (bijv. in/uitvoer en productie van drugs, mensenhandel, milieucriminaliteit, witwassen).⁶ Bij levensdelicten wordt in de regel een Team Grootchalige Opsporing (TGO) ingezet. In geval van een TGO zijn vrijwel alle specialismen voor het onderzoek beschikbaar, waaronder internetrecherchers. Als er kansen liggen op het gebied van internetrecherchers – en dit is vaak het geval – is het waarschijnlijk dat internetrecherchers wordt ingezet (zie Landman & Groothuis, 2022). In andere typen opsporingsonderzoeken is deze vanzelfsprekendheid minder groot. De inzet van internetrecherchers is in die gevallen vooral afhankelijk van de inhoudelijke aard van het delict en de mindset en expertise van de betrokken rechercheurs en de onderzoeksleider. Bij bepaalde typen delicten is internetrecherchers gebruikelijker dan bij andere typen delicten. Zo is internetrecherchers bij cybercriminaliteit een veelgebruikte methode (zie ook Baraz & Montasari, 2023; Davies, 2020). Dit hangt niet alleen samen met de kans dat internetrecherchers bijdraagt aan het vinden van relevante informatie voor het opsporingsonderzoek, maar ook met de aanwezige affiniteit en expertise op het gebied van internetrecherchers. Hierbij geldt dat de mate waarin rechercheonderdelen investeren in expertise op het gebied van internetrecherchers uiteenloopt. In het ene rechercheonderdeel – bijvoorbeeld het cybercrimeteam – heeft men bijvoorbeeld een fulltime specialist die uitsluitend bezig is met internetrecherchers en in het andere rechercheonderdeel beschikt men over een rechercheur met een taakaccent internetrecherchers, die er nauwelijks aan toekomt. Dit heeft logischerwijs veel invloed op de mate waarin er in opsporingsonderzoek online gegevens (kunnen) worden vergaard. Binnen het opsporingsdomein van de politie is er op het gebied van online gegevensvergaring ook een (sub)discipline die heimelijk of ‘undercover’ werkt. Dit zijn de ‘virtual agents’, die werken binnen de specialistische opsporing. Het onderscheidende kenmerk van ‘virtual agents’ ten opzichte van de reguliere internetrecherchers is dat zij met zorgvuldig opgebouwde profielen/aliassen – ‘onder dekmantel’ – communiceren met mensen in het kader van een opsporingsonderzoek (zie ook Oerlemans, 2017). Zij interfereren in het leven van de betrokken burgers door met hen de interactie aan te gaan. Dit doen zij vooral in afgeschermd online omgevingen, waaronder besloten groepen op onder andere Telegram. Hierdoor kunnen zij gegevens vergaren die door andere opsporingsambtenaren niet zomaar te vergaren zijn (zie Landman & Groothuis, 2022).

2.3 Online gegevensvergaring voor intelligence: open source intelligence

OSINT is gericht op het verzamelen van online gegevens die kunnen worden gebruikt voor het nemen van beslissingen over de uitvoering van het politiewerk. De online verzamelde informatie draagt bij aan het creëren van een intelligencepositie, die inzicht geeft in wat er gebeurt en eventueel kan gaan gebeuren. Er is dan nog geen sprake van specifieke strafbare feiten die worden onderzocht en ook niet van de intentie om strafvorderlijke beslissingen te nemen. Een intelligencepositie bestaat in de regel uit meerdere informatiebronnen (Landman & Groothuis, 2022; Miller, 2018). Dit betreft onder andere gegevens die zijn verzameld in het straat-

6 Zie de Aanwijzing voor de opsporing: <https://wetten.overheid.nl/BWBR0034586/2014-01-01>.

werk, opsporingsonderzoeken en door middel van inlichtingen via informanten. Een intelligencepositie wordt gebruikt voor het ontwikkelen van ‘intelligenceproducten’, waaronder fenomeenbeelden en informatiebeelden tijdens crises.

OSINT wordt binnen de politie uitgevoerd vanuit de intelligenceorganisatie. In iedere operationele eenheid van de politie is een intelligenceorganisatie ingericht. Een intelligenceorganisatie heeft van oudsher primair tot taak om bestaande gegevens bij elkaar te brengen, te veredelen (waaronder corrigeren, ordenen, labelen) en te analyseren/duiden. OSINT is in dat opzicht een afwijkende activiteit binnen de intelligenceorganisatie, omdat het hierbij gaat om gegevensvergarig. Anders gezegd: OSINT is een vorm van onderzoek dat tot nieuwe gegevensverzameling leidt en dit verschilt van het raadplegen en verwerken van bestaande gegevens. De opkomst van OSINT is de voornaamste reden dat de medewerkers van de intelligenceorganisatie in het verleden een zogeheten executieve status hebben gekregen (Landman & Groothuis, 2022).

OSINT wordt binnen de politie ingezet in verschillende contexten of omstandigheden. In deze subparagraaf wordt hier op hoofdlijnen op ingegaan. De eerste context is het opbouwen van gestructureerde intelligenceposities over verschillende fenomenen of thema’s. Binnen de politie wordt gewerkt met een Nationale Intelligence Agenda (NIA). De NIA bevat diverse thema’s waarop de politie een gestructureerde intelligencepositie wil opbouwen, waaronder georganiseerde criminaliteit, openbare orde en veiligheid en (contra)terrorisme, extremisme en radicalisering. Binnen thema’s wordt onderscheid gemaakt tussen verschillende subthema’s of focuslijnen. De mate waarin OSINT een rol speelt in het opbouwen van een intelligencepositie verschilt tussen de thema’s en focuslijnen (Landman & Groothuis, 2022). In geval van openbare orde en veiligheid wordt bijvoorbeeld veel gebruikgemaakt van OSINT, terwijl de intelligencepositie op het gebied van georganiseerde criminaliteit sterker leunt op gegevens uit opsporingsonderzoeken en criminele inlichtingen. Een gestructureerde intelligencepositie wordt vooral gebruikt voor het opleveren van uiteenlopende intelligenceproducten, die worden gebruikt als sturingsinformatie in onder andere stuurploegen binnen de opsporing. Deze intelligenceproducten worden onder meer gebruikt voor het kiezen van opsporingsonderzoeken.

De tweede context bestaat uit acute situaties waarvoor *realtime intelligence* nodig is. Dit zijn min of meer actuele gegevens, die direct worden verwerkt en geanalyseerd en als sturingsinformatie beschikbaar worden gesteld (De Boer & Van den Berg, 2017). OSINT is een waardevolle bron van realtime intelligence (Staniforth, 2016). Acute situaties bestaan in de eerste plaats uit incidenten, die op straat plaatsvinden. De regionale eenheden van de politie beschikken over een Realtime Intelligence Center (RTIC). Het RTIC werkt in het Operationeel Centrum (OC) van de politie en voorziet de operatie – in het bijzonder de incidentafhandeling – van real-time intelligence (zie ook Scholtens et al., 2016). Als er een melding in het OC binnenkomt, dan raadpleegt een medewerker van het RTIC – op basis van de informatie uit de melding (zoals namen en adresgegevens) – zowel politiestructuren als publiek toegankelijke bronnen. Informatie die relevant is voor de afhandeling van de melding wordt doorgegeven aan collega’s op straat.

Naast ‘reguliere’ incidenten op straat zijn er ook (acute) situaties waarin grootschalig moet worden opgetreden en realtime intelligence nodig is. In dat geval is er veelal een Staf Grootschalig en Bijzonder Optreden (SGBO) actief waarvan een Hoofd Informatie (HIN) een onderdeel is. De HIN is verantwoordelijk voor het deelp proces informatie en voor het opleveren van een actueel informatiebeeld van het (grootschalige) incident dan wel de crisis. In veel gevallen worden er online gegevens vergaard ten behoeve van het informatiebeeld. Hiervoor is er (veelal) een OSINT-piket of iets vergelijkbaars ingericht, dat kan worden geactiveerd als het SGBO in werking komt. Een of meer OSINT-specialisten voorzien het HIN en daarmee het SGBO dan 24/7 van actuele online vergaarde gegevens.

In de nacht van de wedstrijd tussen Ajax en Maccabi Tel Aviv monitort de politie appgroepen en sociale media vanuit het Command en Control Center van de Staf SGBO in bureau IJ-tunnel. Op basis van deze informatie en informatie vanuit andere bronnen (waaronder meldingen meldkamer, politiemensen op straat) wordt er een zo actueel mogelijk beeld van de situatie in de stad gegeven. Dit beeld gebruikt de politie onder andere om te bepalen waar inzet moet plaatsvinden. Het duiden van de online gegevens is complex, onder andere voor wat betreft het onderscheiden van opruiing en daadwerkelijke dreiging (Inspectie JenV, 2025).

Een derde context waarin OSINT een rol speelt, is bewaken, beveiligen en beschermen. Bewaken, beveiligen en beschermen is sinds 2022 een hoofdtaak van de politie, omdat de dreiging tegen personen, organisaties en locaties in de afgelopen tien jaar is toegenomen en dit niet meer als een neventaak kon worden georganiseerd (zie o.a. Bakker, 2023). De mate waarin en wijze waarop personen, organisaties en locaties worden bewaakt, beveiligd en beschermt, hangen af van de dreigingsinschattingen die worden gemaakt. OSINT wordt gebruikt bij het maken van deze dreigingsinschattingen.

2.4 Online gegevensvergarig in de basisteams: digitaal wijkagenten

Online gegevensvergarig vindt – tot slot – ook plaats binnen de basisteams van de politie. De basisteams van de politie geven uitvoering aan de zogeheten basispolitiezorg. Hieronder valt onder andere de incidentafhandeling, toezicht en handhaving in de wijk, de intake en opsporing van veelvoorkomende criminaliteit en toezicht op evenementen en horeca. Gezien de breedte van de taken voor het basisteam kan zowel internetrecherchen als OSINT meerwaarde hebben. Binnen basisteams wordt in toenemende mate invulling gegeven aan online gegevensvergarig (Landman & Groothuis, 2022; zie ook Van Steden et al., 2025). Online gegevensvergarig vindt vooral plaats door zogeheten ‘digitaal wijkagenten’ (zie ook Terpstra et al., 2021). Deze rol is in 2017 ontstaan en heeft zich sinds als een olievlek verspreid over basisteams in Nederland (zie Boelens & Landman, 2021). Op dit moment heeft meer dan de helft van de 167 basisteams één of meer digitaal wijkagenten aangesteld. Hierbij moet worden opgemerkt dat online gegevensvergarig – en dan vooral OSINT – een van de taken in het takenpakket van de digitaal wijkagent is.

3 Online gegevensvergaring door de politie: actuele vraagstukken en ontwikkelingen

3.1 Synthetische media en beoordelen van betrouwbaarheid

Online (vergaarde) gegevens moeten worden gevalideerd om deze bruikbaar te maken voor opsporings- en intelligencedoeleinden (Gibson et al., 2016; Van Puyvelde & Rienzi, 2025). De noodzaak van validatie is niet nieuw, maar is in de afgelopen jaren wel verder toegenomen. Dit komt doordat wat wij (online) waarnemen in toenemende mate een synthetisch karakter heeft (Van der Sloot, 2024). We worden steeds meer geconfronteerd met zogeheten synthetische media: tekst, audio, foto en video die met (generatieve) artificiële intelligentie (AI) zijn gemaakt of bewerkt. Dit heeft voor online gegevensvergaring door de politie veel consequenties, omdat er een toenemende kans is dat gegevens die worden verzameld zijn gemanipuleerd. Dit zet de bewijs- en sturingswaarde van deze gegevens op losse schroeven (zie ook Den Dunnen, nog te publiceren). Het is eveneens mogelijk dat deze manipulatie gericht wordt ingezet om online gegevensvergaring door de politie te verstoren (zie ook Gibson, 2016). In dat geval hebben de synthetische gegevens het karakter van desinformatie: het doelbewust verspreiden van misleidende informatie met als doel schade aan te brengen.

Het voorgaande impliceert dat kritisch denken en reflecteren van OGG-professionals binnen de politie steeds belangrijker wordt. Er moet een voortdurend besef zijn dat de gegevens die (online) worden vergaard, kunnen zijn gemanipuleerd. Dit besef moet leiden tot het nemen van (extra) stappen om de betrouwbaarheid van gegevens vast te stellen (Den Dunnen, nog te publiceren). Dit houdt onder andere in dat onderzoek wordt gedaan naar de autoriteit en het doel van de bron en de context en accuraatheid van de informatie (Gibson et al., 2016; Van Puyvelde & Rienzi, 2025). Om de betrouwbaarheid van gegevens te kunnen beoordelen, is het combineren van online bronnen en andere bronnen (triangulatie, crossreferentie) cruciaal (Van Puyvelde & Rienzi, 2025). Daarnaast kan technologie helpen bij het beoordelen van de betrouwbaarheid van (online) gegevens. Het Nederlands Forensisch Instituut (NFI) doet bijvoorbeeld samen met de Universiteit van Amsterdam al geruime tijd onderzoek naar methoden van en tools voor (in het bijzonder) deep-fakedetectie (zie o.a. NFI, 2025). De verwachting is dat opsporingsambtenaren van de politie in de toekomst steeds meer digitale hulpmiddelen kunnen benutten in het beoordelen van de betrouwbaarheid van gegevens.

3.2 Inbreuk op grondrechten en nieuwe wetgeving

Gegevens op het internet zijn in meer of mindere mate open te benaderen en door iedereen in te zien en over te nemen. Het staat politiemensen echter niet vrij om 'in het wilde weg' te grasduinen op het internet (zie Koops, 2012; Wermeskerken, 2016). Online gegevensvergaring door de politie kan namelijk inbreuk maken op grondrechten van burgers, in het bijzonder op het recht op eerbiediging van de persoonlijke levenssfeer (privacy). Mede om die reden moet online gegevensvergaring door de politie worden gereguleerd door wet- en regelgeving. Voor een geringe inbreuk op de persoonlijke levenssfeer van burgers is geen specifieke wettelijke basis nodig. Een specifieke wettelijke basis is pas nodig als de online gegevensverga-

ring een stelselmatig karakter krijgt en een meer dan geringe inbreuk op de persoonlijke levenssfeer van burgers maakt. Hiervan is sprake als de politie systematisch en gericht (aspecten van) de persoonlijke levenssfeer van een burger in beeld brengt en op deze wijze een min of meer volledig beeld van aspecten van iemands privéleven krijgt (zie Stol & Strikwerda, 2018), zoals zijn dagelijkse gewoonten, zijn verblijfplaats, zijn verplaatsingen, de activiteiten die hij uitvoert en zijn sociale relaties.⁷

Hoewel online gegevensvergaring door de politie al ruim twintig jaar plaatsvindt, zijn er vooralsnog geen specifieke – op de online context toegesneden – juridische grondslagen voor. In het kader van intelligence wordt er gebruikgemaakt van artikel 3 Politiewet 2012 en in het kader van opsporing wordt er waar nodig gebruikgemaakt van bijzondere opsporingsbevoegdheden, die oorspronkelijk niet zijn bedoeld voor online gegevensvergaring. Dit worden ook wel ‘vangnetbepalingen’ genoemd (zie Stevens, 2021). Voor beide taken is er sprake van een mismatch tussen de huidige praktijk en het juridisch kader. Bij intelligence is de mismatch dat er geen wettelijke bevoegdheid is waarop online gegevensvergaring met een meer dan geringe inbreuk op de persoonlijke levenssfeer kan worden gemaakt, terwijl het in de praktijk geregeld wel noodzakelijk is om een meer dan geringe inbreuk te maken (zie ook Landman & Groothuis, 2022).⁸ Bij opsporing is de mismatch dat er vangnetbepalingen worden gebruikt. Dit is een tijdelijke noodoplossing (Klaar, 2022), die al geruime tijd duurt.

Voor opsporing geldt dat er – met de inwerkingtreding van het nieuwe Wetboek voor Strafvordering (WvSv) per 1 april 2029 – een nieuwe bevoegdheid wordt geïntroduceerd: het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen (art. 2.8.8 en art. 2.9.1 WvSv voor het verkennend onderzoek). Deze bevoegdheid kan de politie – op bevel van de officier van justitie – inzetten om in geval van verdenking van een misdrijf stelselmatig persoonsgegevens over te nemen uit publiek toegankelijke bronnen. Voor online gegevensvergaring in het kader van intelligence kan deze bevoegdheid niet worden gebruikt. Dit is vooral een probleem voor het domein waarin online gegevensvergaring voor de politie essentieel is: openbare-ordehandhaving. Om die reden heeft de commissie-Koops in 2018 al geadviseerd om ook voor handhaving van de openbare orde een wettelijke grondslag te creëren (Commissie modernisering opsporingsonderzoek in het digitale tijdperk, 2018). Aan dit advies is uiteindelijk invulling gegeven. Begin juli 2025 is het wetsvoorstel ‘Wet gegevensvergaring openbare orde’ in consultatie gegaan. Dit (bestuursrechtelijke) wetsvoorstel bevat twee bevoegdheden op basis waarvan aan de politie of de Koninklijke Marechaussee het bevel kan worden gegeven (relevante) online gegevens te vergaren over een (dreigende) ernstige verstoring van de openbare orde. De eerste bevoegdheid betreft het zoeken naar en het

7 Deze voorbeelden zijn gebaseerd op de memorie van toelichting bij de consultatieversie van de Wet gegevensvergaring openbare orde.

8 Overigens is er in landen om ons heen ook geen specifieke wettelijke basis voor online gegevensvergaring door de politie waarbij een meer dan geringe inbreuk op de persoonlijke levenssfeer wordt gemaakt (zie Winter et al., 2025). In sommige gevallen – zoals in Frankrijk – valt de online gegevensvergaring door de politie onder (aparte) wetgeving voor inlichtingenactiviteiten, die van toepassing is op meerdere diensten. Deze wetgeving bevat dan de noodzakelijke waarborgen.

overnemen van persoonsgegevens uit publiek toegankelijke bronnen. De tweede bevoegdheid gaat over het in publiek toegankelijke bronnen volgen van personen (en overnemen van persoonsgegevens) van wie aannemelijk is dat zij een substantiële rol hebben in een (dreigende) ernstige verstoring van de openbare orde. De voorgestelde bevoegdheden worden zonder medeweten van de betrokken burgers uitgeoefend.⁹ Het voornaamste verschil tussen de twee voorgestelde bevoegdheden is de wijze waarop gegevens over de (dreigende) ernstige verstoring van de openbare orde worden vergaard en de inbreuk die daarmee wordt gemaakt op de persoonlijke levenssfeer.

Met het nieuwe WvSv en het wetsvoorstel voor openbare orde wordt het vacuüm waarvan bij online gegevensvergaring sprake is ten dele opgelost en wordt de positie van het gezag – in het bijzonder van de burgemeester¹⁰ – versterkt. Tegelijkertijd is het de vraag of de bestaande problemen (vanuit het perspectief van de politie) hiermee in voldoende mate worden opgelost. Dit geldt vooral voor online gegevensvergaring voor intelligence. Het wetsvoorstel voor gegevensvergaring openbare orde beperkt zich tot situaties waarin er sprake is van een specifieke, in meer of mindere mate concrete, ernstige verstoring van de openbare orde die plaatsvindt of naar verwachting zal plaatsvinden. De politie kan deze bevoegdheid dus niet inzetten om een meer algemeen beeld te verkrijgen of structureel intelligence te vergaren in het kader van openbare-ordedreigingen. De belangrijkste ‘beperking’ is echter dat het wetsvoorstel uitsluitend betrekking heeft op publiek toegankelijke bronnen.

3.3 Toenemende beslotenheid en nieuwe wensen

De ‘O’ in OSINT staat voor ‘open’. Hiermee wordt verwezen naar open bronnen. In juridische zin wordt de eerder aangehaalde term ‘publiek toegankelijke’ bronnen gebruikt. In zowel het nieuwe WvSv als het wetsvoorstel voor openbare orde is aangesloten bij de definitie van publiek toegankelijke bronnen van de commissie-Koops (2018). Het belangrijkste criterium voor publieke toegankelijkheid is de afwezigheid van een minimaal niveau van beveiliging. Dit wil zeggen dat er een effectieve toegangscontrole moet plaatsvinden. Inloggen met een wachtwoord is bijvoorbeeld een effectieve toegangscontrole en dit geldt ook voor het goedkeuren van een verzoek tot deelname aan een chatgroep door de beheerder van de groep.

9 Met het oog op de bescherming van grondrechten – in het bijzonder het recht op eerbiediging van de persoonlijke levenssfeer – zijn er in het wetsvoorstel waarborgen opgenomen. Een van de belangrijkste waarborgen is een voorafgaande, onafhankelijke toets door de rechter-commissaris op de inzet van de bevoegdheden. Daarnaast is er een aangepast regime voor de verwerking van de persoonsgegevens die met de uitoefening van de bevoegdheden zijn vergaard.

10 Hierbij moet worden benadrukt dat deze rol voor veel burgemeesters relatief nieuw is (zie ook Landman & Groothuis, 2022). Burgemeesters hebben van oudsher het gezag over de politie voor wat betreft de handhaving van de openbare orde. De aandacht voor het gezag over de gegevensvergaring in het kader van de openbare orde is van veel recentere datum. Dit speelt niet alleen bij online gegevensvergaring, maar ook bij gegevensvergaring door middel van informanten door het Team Openbare Orde Inlichtingen (TOOI) van de politie. Zie ook www.regioburgemeesters.nl/documentatie/tooi/. Vanwege het nieuwe karakter van de rol van de burgemeester moeten er ‘gezagsmatige zaken’ worden geregeld, waaronder permanente bestuurlijke bereikbaarheid en beschikbaarheid (zie ook Engberts & Brouwer, 2025).

Als er geen feitelijke toegangscontrole is – bijvoorbeeld in geval van een openbare link naar een appgroep waarbij iedereen wordt binnengelaten (zie het voorbeeld van ‘Buurthuis2’) – dan is het vanuit deze redenering een publiek toegankelijke bron. Of er sprake is van een publiek toegankelijke bron of een besloten bron moet (dus) per geval worden bepaald, waarbij er grijze gebieden zijn waarin moet worden besloten.

Binnen de politie heeft men de ervaring dat de communicatie tussen burgers die relevant is voor onder andere de openbare orde en bewaken, beveiligen & beschermen zich in toenemende verplaatst naar besloten online omgevingen (zie Landman & Groothuis, 2022). Dit betreft in het bijzonder uiteenlopende besloten appgroepen (waaronder Telegram en Whatsapp), waarbij de beheerder van de appgroep toegang moet geven of een nieuw lid moet toevoegen. De politie ervaart als gevolg hiervan in toenemende mate een spanning tussen de verwachting van politiek en maatschappij dat zij een goede informatiepositie heeft en de mogelijkheden die er zijn om deze informatiepositie te realiseren. De toenemende – door de politie gesignaleerde – ‘beslotenheid’ maakt het lastiger om tijdig een goede informatiepositie op te bouwen waarmee proactief kan worden opgetreden (zie o.a. Postma et al., 2025).

Tegen deze achtergrond is er tijdens het Tweede Kamerdebat over de incidenten rondom Ajax – Maccabi Tel Aviv een motie ingediend door Tweede Kamerlid Yeşilgöz-Zegerius waarin de minister is verzocht om de politie meer mogelijkheden te bieden om mee te kijken in (besloten) Telegramgroepen.¹¹ Deze mogelijkheden gaan over meekijken in besloten (Telegram)groepen zonder dat er sprake is van een verdenking. De minister heeft toegezegd hiermee aan de slag te gaan.¹² Indien hier wetgeving voor wordt ontwikkeld, is dit een aanzienlijke uitbreiding van de bevoegdheden die de politie op het gebied van online gegevensvergaring heeft. De impact op grondrechten van burgers hangt af van de omstandigheden waarin de politie de eventuele nieuwe bevoegdheden mag inzetten en de waarborgen die er rondom de inzet zijn. Op voorhand kan niettemin worden gesteld dat een dergelijke bevoegdheid onder burgers kan leiden tot een gevoel van permanente dreiging van surveillance.¹³ Dit kan er onder andere aan bijdragen dat burgers zich minder vrij voelen om met elkaar te communiceren, ongeacht of de politie op dat moment ook daadwerkelijk meeleeft met hun communicatie. Dit wordt ook wel het *chilling effect* genoemd (zie Lodder & Schuilenburg, 2016).

11 Zie hiervoor het Tweede halfjaarbericht politie van de minister van Justitie en Veiligheid van 13 december 2024.

12 In het Tweede Kamerdebat naar aanleiding van de rellen in Den Haag op 20 september 2025 is wederom een motie aangenomen waarin de regering wordt gevraagd om de politie meer mogelijkheden te geven om mee te kunnen kijken in besloten socialemediagroepen waar berichten over aangekondigde rellen circuleren.

13 In meer algemene zin geldt dat onbekend is wat burgers ervan vinden dat de politie meer mogelijkheden krijgt om online gegevens (over hen) te vergaren. Zie voor de uitkomsten van actueel onderzoek het artikel van Bantema et al. in dit themanummer.

3.4 Omvang van gegevens en de selectie- en analyseopgave

Onze hybride manier van leven maakt dat er online enorme hoeveelheden data beschikbaar zijn die relevant kunnen zijn voor online gegevensvergarings door de politie. Er is sprake van een overload aan data (Gibson et al., 2016; Pastor-Galindo et al., 2020; Van Puyvelde & Rienzi, 2025). In de praktijk is dit voor de politie in het bijzonder merkbaar tijdens grootschalige incidenten waarbij er in korte tijd heel veel *nieuwe* berichten online worden geplaatst. Dit heeft zich onder andere voorgedaan tijdens de avondklokrellen in januari 2021 en bij de ongeregelde heden rondom Ajax – Maccabi Tel Aviv in november 2024. In dergelijke situaties worden er op diverse platformen en in online groepen met talloze leden soms wel honderden berichten per minuut geplaatst (zie Moors et al., 2022).

Het handmatig monitoren en analyseren van gegevens die met deze omvang en snelheid worden geproduceerd, is vrijwel onmogelijk. Om die reden zoeken politieorganisaties wereldwijd oplossingen in het gebruik van technologie voor het vergaren, verwerken en analyseren van online gegevens (Van Puyvelde & Rienzi, 2025). De politie in Nederland gebruikt uiteenlopende softwareprogramma's waarmee online gegevens geautomatiseerd kunnen worden verzameld en geanalyseerd (zie Landman & Groothuis, 2022). Deze programma's maken gebruik van (zelflerende) algoritmen die het mogelijk maken om heel veel bronnen tegelijkertijd te bevragen, ordenen en visualiseren (Klaar, 2022). De politie maakt gebruik van software die is ontwikkeld door commerciële partijen – zoals Public Sonar en Maltego – en ontwikkelt eigen software. Op beide terreinen is veel ontwikkeling (zie ook CTIVD, 2021). De voortdurende doorontwikkeling van AI biedt mogelijkheden om de efficiëntie en effectiviteit van online gegevensvergarings verder te verbeteren (zie o.a. Merkley, 2025; Puyvelde & Rienzi, 2025). Professionals binnen de politie hebben (veelal) de wens om deze mogelijkheden te benutten en verlangen dat de politieorganisatie investeert in software (Landman & Groothuis, 2022).

Naast de mogelijkheden die geavanceerde software de politie biedt, is het gebruik ook omgeven met tal van ethische en juridische kwesties (zie ook Landman, 2023; Schuilenburg, 2024). Het gebruik kan leiden tot inbreuken op grondrechten van burgers, waaronder het recht op privacy en het recht op gelijke behandeling. De risico's voor grondrechten van burgers in het algemeen en de privacy van burgers in het bijzonder hangen af van de precieze wijze waarop software wordt ingesteld en gebruikt (Klaar, 2022). Duidelijk is in ieder geval wel dat het huidige juridische kader niet voorziet in een specifieke wettelijke grondslag voor geautomatiseerde online gegevensvergarings. Dit is volgens diverse auteurs wel nodig (Lodder & Schuilenburg, 2016; Oerlemans, 2017; Stol & Strikwerda, 2018). Dit wordt met de aanstaande wetgeving niet of nauwelijks opgelost. De vertaling van wetgeving naar het gebruik van software stelt opsporingsambtenaren en gezagsdragers dus voor uitdagingen (Klaar, 2022).

3.5 Wens van brede inbedding en noodzaak van specialisatie

Online gegevensvergarings is een vakgebied dat primair bestaat uit een verzameling van methoden, en onderliggende 'body of knowledge', die worden ingezet om online gegevens te verzamelen, valideren en analyseren (zie ook Van Puyvelde & Rienzi, 2025). Binnen inlichtingen- en opsporingsdiensten wereldwijd is er een voort-

durende discussie over of dit vakgebied generalistisch of specialistisch moet worden georganiseerd (Van Puyvelde & Rienzi, 2025). Ook de politie in Nederland heeft te maken met dit vraagstuk. Aan de ene kant is er een wens om online gegevensvergaring breed in te bedden. Als in het dagelijks leven van burgers offline en online sterk met elkaar zijn verweven, dan ligt het immers voor de hand om offline en online in het politiewerk ook meer te integreren. Dit veronderstelt een generalistische benadering waarbij online gegevensvergaring onderdeel is van (vrijwel) ieders werk. Aan de andere kant is een deel van de in te zetten methoden complex om uit te voeren (zie Van Puyvelde & Rienzi, 2025). Hierbij komt dat de methoden – onder andere vanwege ontwikkelingen op het internet (zoals nieuwe standaarden en protocollen) en innovaties (waaronder tools) – voortdurend in ontwikkeling zijn. Het is dus cruciaal om kennis en vaardigheden te onderhouden. De internationale OSINT-gemeenschap gebruikt in dit verband ook wel het begrip NERD: *never ending research & development* (zie Landman & Groothuis, 2022). Een derde element is wet- en regelgeving. Een rechtmatige uitvoering van online gegevensvergaring vereist het vermogen om wet- en regelgeving toe te passen op de uitvoering van de werkzaamheden. Er is – al met al – dus ook veel voor te zeggen dat de complexiteit van en dynamiek in het vakgebied vragen om een meer specialistische benadering waarbij online gegevensvergaring wordt belegd bij aparte teams en medewerkers.

Binnen de politie in Nederland wordt geprobeerd om de spanning tussen (de wens van) generalisme en (noodzaak van) specialisme hanteerbaar te maken door onderscheid te maken tussen verschillende niveaus van online gegevensvergaring. Dit onderscheid is oorspronkelijk gemaakt in het OGG5-model (zie Landman & Groothuis, 2022). In dit model zijn vijf niveaus opgenomen die verschillen in onder andere de mate van tijdsbesteding (aan OGG), de internetdiepte (surface web, deep web, dark web), de wijze van bronbevraging (wel of geen alias en aard van de alias), wel/geen interactie en gebruik van tools. Dit model heeft zich recent doorontwikkeld tot het zogeheten OPW5-model. OPW staat voor online politiewerk en dit is een verbreding ten opzichte van online gegevensvergaring. Het onderscheid tussen verschillende niveaus is behulpzaam om aan te geven wat wordt verwacht van het generalisme (eenvoudige methoden en tools, surface web, enz.) en van het specialisme. De praktijk leert echter dat het voor generalisten binnen de politie moeilijk is om aan de verwachtingen te voldoen (zie Landman & Groothuis, 2022). Dit geldt in het bijzonder binnen de opsporing, omdat de activiteiten die moeten worden verricht afhankelijk zijn van de ‘probleemstelling’ in het opsporingsonderzoek. Rechercheurs die ‘af en toe’ online gegevens vergaren en dit ‘erbij doen’, zijn niet in staat om hun kennis en vaardigheden op een niveau te houden dat aansluit bij wat veelal nodig is in een opsporingsonderzoek. Dit is een van de redenen dat de mogelijkheden van internetrecherchen door de politie in Nederland beperkt worden benut. Meer specialisatie lijkt wenselijk (Landman & Groothuis, 2022).

4 Conclusie en discussie

In dit artikel is op hoofdlijnen in kaart gebracht op welke wijze de politie in Nederland gebruik maakt van online gegevensvergarings en welke vraagstukken zich hierbij op dit moment voordoen. De conclusie is dat online gegevensvergarings binnen de politie een praktijk in ontwikkeling is. In steeds meer organisatieonderdelen van de politie zijn er politiemensen die uitvoering geven aan online gegevensvergarings. De wetgever beweegt mee met de ontwikkelingen in de samenleving en de politiepraktijk: specifieke bevoegdheden voor online gegevensvergarings voor de strafrechtelijke orde en openbare orde zijn aanstaande.

Er is veel voor te zeggen dat de samenleving recht heeft op een politie die in staat is om (op een rechtmatige manier) online gegevens te verzamelen en te verwerken. De vraag is echter hoever de politie daarin zou moeten kunnen gaan. Nu online gegevensvergarings door de politie toeneemt, is dit een vraag die maatschappelijk relevanter wordt. De (politiek-maatschappelijke) verwachting dat de politie ‘op de hoogte moet zijn’ kan gemakkelijk leiden tot steeds vergaande, niet-strafvorderlijke, bevoegdheden van de politie op het gebied van online gegevensvergarings. De motie om de politie meer mogelijkheden te geven om ‘mee te kijken’ in besloten groepen is hier een voorbode van. Het is tegen deze achtergrond belangrijk om stil te blijven staan bij de vraag wat voor een politie we in de samenleving willen hebben (Landman, 2023). Dit betekent dat de verschillende belangen goed moeten worden afgewogen alvorens de bevoegdheden van de politie verder uit te breiden. Er wordt altijd een prijs betaald. ‘We can’t have it all.’ (Marx, 2016)

Literatuur

- Bakker, E. (2023). Bewaken en beveiligen en de politie. Verleden, heden, toekomst. In J. van Hoorn & M. van Bavel, *Onze politie in een kwetsbare rechtsstaat* (pp. 111–126). Antwerpen/’s-Hertogenbosch: Gompel&Svacina.
- Baraz, A., & Montasari, R. (2023). Law enforcement and the policing of cyberspace. In R. Montasari, V. Carpenter & A.J. Masys (Eds.), *Digital transformation in policing: The promise, perils and solutions* (pp. 59–83). Cham: Springer International Publishing.
- Baricco, A. (2018). *The game*. Amsterdam: De Bezige Bij.
- Bazzell, M., & Edison, J. (2024). *OSINT techniques: resources for uncovering online information*. Inteltechniques.com
- Boelens, M. & Landman, W. (2021). *Pionieren in gebiedsgebonden politiewerk. Een onderzoek naar de digitale wijkagent in het basisteam*. Horn: Moduliprint.
- Commissie modernisering opsporingsonderzoek in het digitale tijdperk (commissie-Koops). (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving*. Den Haag.
- CTIVD. (2021). *Automated OSINT: tools en bronnen voor openbronnenonderzoek*. Den Haag: Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.
- Davies, G. (2020). Shining a light on policing of the dark web: an analysis of UK investigatory powers. *The Journal of Criminal Law*, 84(5), 407–426.
- De Boer, W., & Van den Berg, C. (2017). Real-time intelligence (RTI). In M. den Hengst, T. ten Brink & J. ter Mors (red.), *Informatiegestuurd politiewerk in de praktijk* (pp. 241–248). Deventer: Vakmedianet.

- De Boer, D., Postma, L., & Bantema, W. (2024). *Gehackt of toch online aangejaagd? Een evaluatie van de (online) aanpak van de gemeente Alkmaar na de Legia Warszawa-incidenten*. Leeuwarden: NHL Stenden.
- De Poot, C. J., Bokhorst, R. J., Koppen, P. J., & Muller, E. R. (2004). *Rechercheportret. Over dilemma's in de opsporing*. Alphen aan den Rijn: Kluwer.
- 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.
- Dunnen, M. den (n.n.g.). *Het failliet van de eigen waarneming. De fundamentele impact van generatieve AI*. In W. Landman, S. de Kimpe, E. de Pauw, W. Broer & W. Hardyns (Red.), *Digitalisatie van politiewerk*. Antwerpen/s-Hertogenbosch: Gompel&Scavina.
- Engberts, A.B. & Brouwer, C.J. (2025). Wet 'Gegevensvergaring openbare orde'. Meer mogelijkheden om informatie uit open bronnen te halen. *Het Tijdschrift voor de Politie*, 87(4), 26–29.
- Europol. (2025). *Policing in an online world. Relevance in the 21st century*. Luxembourg: Publications Office of the European Union.
- Feenstra, M. (2018). Opsporingsmiddelen in ontwikkeling. Open-bronnenonderzoek als nieuwe "tap". *Proces*, 97(6), 367–375.
- Floridi, L. (2014). Introduction. In L. Floridi (Ed.), *The online manifesto. Being human in a hyperconnected era* (pp. 7–15). Cham/Heidelberg/New York/Dordrecht/London: Springer.
- Fortin, F., Delle Donne, J., & Knop, J. (2021). The use of social media in intelligence and its impact of police work. In J.J. Nolan, F. Crispino & T. Parsons (Eds.), *Policing in an age of reform. An agenda for research and practice* (pp. 213–231). London/New York: Palgrave Macmillan.
- Halvar Larsen, O., Ngo, H. G., & Le-Khac, N. (2023). A quantitative study of the law enforcement in using open source intelligence techniques trough undergraduate practical training. *Forensic Science International: Digitale Investigation*, 47, 301622.
- Higgins, E. (2021). *Wij zijn bellingcat. Hoe gewone mensen de onderzoeksjournalisten van de toekomst werden*. Amsterdam: Spectrum.
- Inspectie Justitie en Veiligheid. (2025). *Tussen voorzien en onvoorzien – politie in een complexe werkelijkheid. De aanpak van de ongeregelde heden in Amsterdam op 7 en 8 november 2024: voorbereiding en optreden in beeld*. Den Haag: Inspectie JenV.
- Klaar, R. J. A. (2022). De strafvorderlijke normering van het geautomatiseerd overnemen van persoonsgegevens uit publiek toegankelijke bronnen met behulp van webcrawlers'. *Platform Modernisering Strafvordering*, maart 2022.
- Koops, B. J. (2012). Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten. *Tijdschrift voor Veiligheid*, 11(2), 30–46.
- Kop, N., Van Boxem, G. & Hulshof, R. (2025). *De kunst van het opsporen*. Den Haag: Boom.
- Kop, N., & Klerks, P. (2009). *Doctrine intelligencegestuurd politiewerk*. Apeldoorn: Politieacademie.
- Landman, W. (2023). *Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk*. Den Haag: Sdu Uitgevers.
- Landman, W., & Groothuis, S. (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie*. Den Haag: Sdu Uitgevers.
- Landman, W., Kouwenhoven, R. M. & Brussen, M. (2020). *Kijk naar het systeem. Begrijpen en beïnvloeden van opsporingspraktijken*. Den Haag: Sdu Uitgevers.
- Lodder, A. R. & Schuilenburg, M. B. (2016). Politie web-crawlers en predictive policing. *Computerrecht*, 81(3), 150–154.

- Marx, G. T. (2016). *Windows into the soul. Surveillance and society in an age of high technology*. Chicago: The University of Chicago Press.
- Mehlbaum, S., van den Akker, K., Broekhuizen, J., & Verweij, A. (2025). *Geklapt, gefilmd en gedeeld. Onderzoek naar hybride straatgeweld onder jongeren*. Den Haag: Sdu Uitgevers.
- Merkley, J. J. (2025). *AI-powered OSINT. The future of digital investigations*.
- Miller, B. H. (2018). Open Source Intelligence (OSINT): an oxymoron? *International Journal of Intelligence and CounterIntelligence*, 31(4), 702–719.
- Moors, H., Klarenbeek, L., Berger, E., Dückers, M., Van Duin, M., Kist, G., Luesink, M., Schrijvenaars, T., & Van der Wijngaart, M. (2022). *Avondklokrellen: lokale dynamiek in een mondiale crisis. Analyse van de voedingsbodem van de ordeverstoringen in vier Noord-Brabantse steden*. Bureau EMMA.
- Nederlands Forensisch Instituut. (2025). Hoe onze hartslag kan verraden dat een video deepfake is. www.forensischinstituut.nl/actueel/achtergrondverhalen-nfi/hoe-onze-hartslag-kan-verraden-dat-een-video-deepfake-is---eafs-2025-deel-2
- Oerlemans, J. J. (2017). *Normering van digitale opsporingsmethoden*. Breda: Nederlandse Defensie Academie.
- Oerlemans, J. J. (2020). Cybercriminaliteit en opsporing. In W. van der Wagen, J. J. Oerlemans & M. Weulen Kranenbarg (Red.), *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (pp. 195–258). Den Haag: Boom Criminologie.
- Pastor-Galindo, J., Nespoli, P., Mármol, F.G., & Pérez, G.M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE access*, 8, 10282–10304.
- Politie (2012). *Inrichtingsplan Nationale Politie*. Den Haag: Politie.
- Postma, L., de Boer, M., & Bantema, W. (2025). *Schuldig tot het tegendeel bewezen is? Een evaluatie van de (online) aanpak van een gemeente en politie naar aanleiding van online onrust*. Leeuwarden: NHL Stenden.
- Ratcliffe, J. (2016). *Intelligence-led policing* (2nd edition). New York: Routledge.
- Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2021). The hybridization of street offending in the Netherlands. *The British Journal of Criminology*, 61(4), 926–945.
- Sampson, F. (2017). Intelligent evidence: using open source intelligence (OSINT) in criminal proceedings. *The Police Journal: Theory, Practice and Principles*, 90(1), 55–69.
- Scholtens, A., den Hengst, M., & Waterreus, R. (2016). *Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie*. Amsterdam: Reed Business.
- Schuilenburg, M. (2024). *Making surveillance public: why you should be more woke about AI and algorithms*. The Hague: Eleven International Publishing.
- Staniforth, A. (2016). Police use of open source intelligence: the longer arm of law. In B. Akhgar, P. S. Bayerl & F. Sampson (Eds.), *Open source intelligence investigation: from strategy to implementation* (pp. 21–32). Cham: Springer International Publishing.
- Steden, R. van, ter Woerds, S., Merk, A., Schuppers, D., Willekers, M., Jansen, R., & Ruiter, S. (2025). *Online blauw. Een onderzoek naar de rol van basisteams in de aanpak van digitale criminaliteit en ervaringen van slachtoffers met de politie*. Den Haag: Lefebvre Sdu.
- Stevens, L. (2021). Over vangnetbepalingen voor de opsporing. *Delikt en Delinkwent*, 51(10), 871–882.
- Stol, W., & Strikwerda, L. (2018). Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving, *Tijdschrift voor Veiligheid*, 17(1-2), 8–22.

- Terpstra, J., Salet, R., Van Duijneveldt, I., & Havinga, T. (2021). *Gebiedsgebonden politiewerk in ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving*. Den Haag: Sdu Uitgevers.
- Van de Sloot, B. (2024). *Regulating the synthetic society. Generative AI, legal questions and societal challenges*. Oxford/New York/Dublin: Hart Publishing.
- Van der Plas, A. & Brown, C. (2017). Inwinning. In M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk* (pp. 179–192). Deventer: Vakmedianet.
- Van Puyvelde, D., & Rienzi, F. T. (2025). The rise of open-source intelligence. *European Journal of International Security*, 1–15.
- Van Wermeskerken, H. (2016). Privacy op Facebook. *Blauw*, 12(5), 16–19.
- Winter, H., Boxum, C., Cazemier, J., Drouen, T. & Roest, S. (2025). *Internationale verkenning bevoegdheden online gegevensvergaring politie bij (dreigende) openbare ordeverstoringen*. Groningen: Pro Facto.