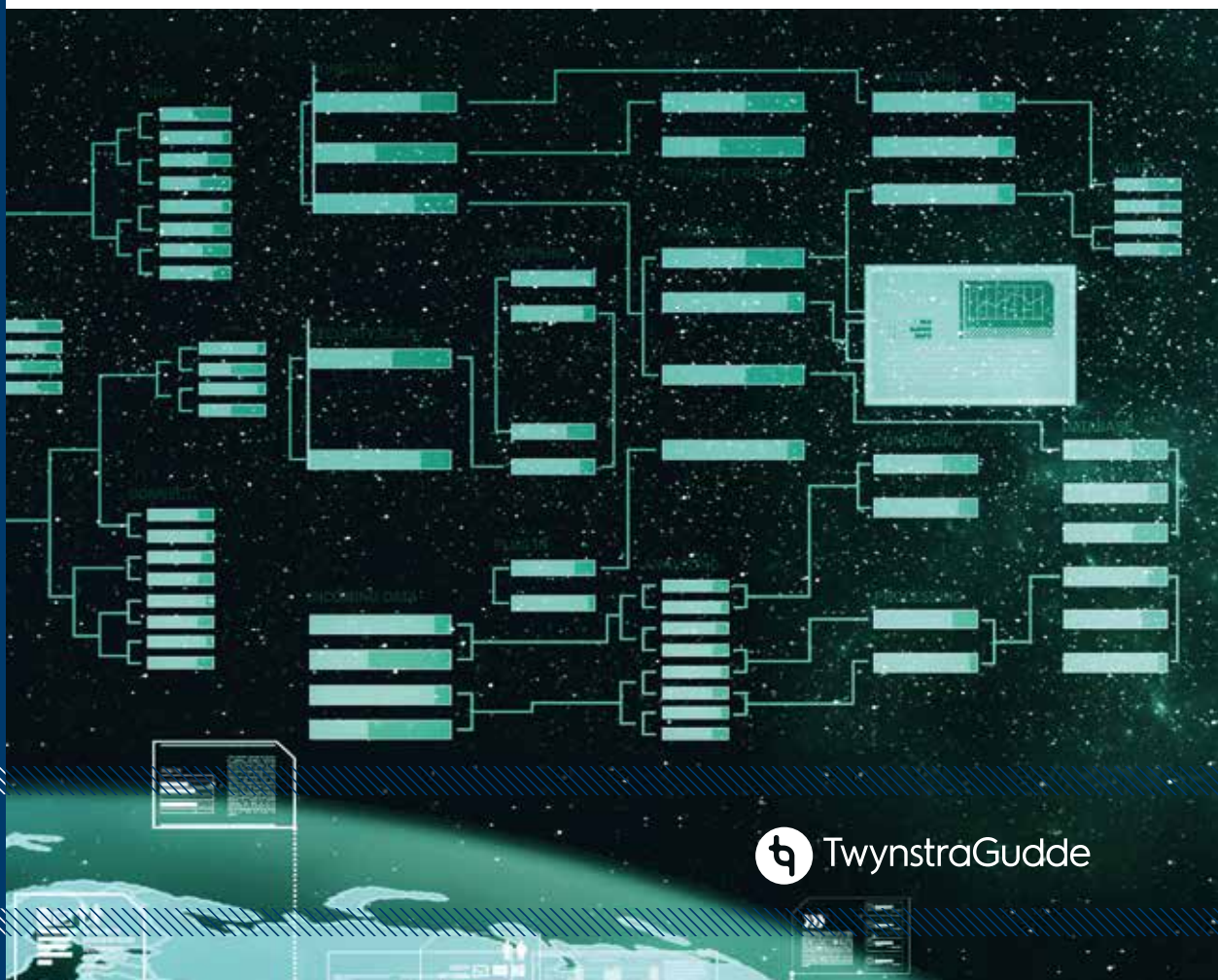
Politie & Wetenschap

Politiewerk op het web

Een verkennend onderzoek naar online gegevensvergaring door de politie

Wouter Landman, Sanne Groothuis



TwynstraGudde

Politiewerk op het web

Politiewerk op het web

Een verkennend onderzoek naar online gegevensvergaring door de politie

Wouter Landman

Sanne Groothuis

POLITIE & Wetenschap

TwynstraGudde

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

Omslagontwerp: Imago Mediabuilders, Amersfoort
Afbeelding omslag: Shutterstock
ISBN: 9789012408394
NUR: 600

Inhoudsopgave

Voorwoord

Onderzoek doen is het leukst als je het kunt doen naar een onderwerp waarnaar je nieuwsgierig bent en waar je in wilt duiken. Wij waren nieuwsgierig naar online gegevensvergaring door de politie en hebben dan ook met veel plezier dit verkennende onderzoek naar dit onderwerp uitgevoerd. Met dank aan Politie & Wetenschap.

Het plezier in de uitvoering van dit onderzoek kwam niet alleen door het onderwerp, maar zeker ook door de mensen. We hebben ruim veertig politiemensen gesproken die met veel passie en energie over hun werk hebben verteld. Dit waren hele waardevolle en leuke gesprekken. We willen hen bedanken voor de bijdrage die zij aan dit onderzoek hebben geleverd.

We richten een derde woord van dank aan de leescommissie:
- Willem Bantema (lector bestuur en digitalisering NHL Stenden Hogeschool)
- Maaike Borst (voorzitter landelijke vakgroep internetonderzoek)
- Reinder Doeleman (programmadirecteur intelligence)
- Hugo Passchier (hoofd cluster beleidsontwikkeling portefeuille GGP)[1]
- Adriaan Rottenberg (Politie & Wetenschap)
- Daniel Trottier (associate professor media en communicatie Erasmus Universiteit)

De bespreking in de leescommissie en nagezonden opmerkingen van de leden van de leescommissie waren zeer bruikbaar op weg naar afronding van dit rapport.

Amersfoort, september 2022

Wouter Landman en Sanne Groothuis

1 Mark Zoetekouw heeft met Hugo Passchier meegelezen. Hij is werkzaam bij de Landelijke Eenheid als jurist op het gebied van cybercrime & digitale technologie en tevens promovendus bij het departement Rechtsgeleerdheid van de Universiteit Utrecht.

Lijst van afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AVIM	Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel
BOB	Bijzondere Opsporingsbevoegdheden
BT	Basisteam
COP of OCP	Operationeel Coördinatiepunt
COT	Crisisonderzoeksteam
CTER	Contraterrorisme en Radicalisering
CTIVD	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
DLIO	Dienst Landelijke Informatieorganisatie
DRIO	Dienst Regionale Informatieorganisatie
DLR	Dienst Landelijke Recherche
DR	Districtsrecherche
DRR	Dienst Regionale Recherche
EVRM	Europees Verdrag voor de Rechten van de Mens
GGP	Gebiedsgebonden Politie
GO	Generieke Opsporing
HIN	Hoofd Informatie
IK	Informatieknooppunt
iRN	internet Research Network
KMar	Koninklijke Marechaussee
LE	Landelijke Eenheid
MMA	Meld Misdaad Anoniem
MvT	Memorie van Toelichting
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OC	Operationeel Centrum
OE	Operationeel Expert
OGG	Online gegevens(ver)garing
OM	Openbaar Ministerie
OMG	Outlaw Motorcycle Gang
OPSEC	Operational Security
OSINT	Open Source Intelligence
O&T	Observatie & Techniek

PC	Personal Computer
Pw	Politiewet
RI	Regionale Informatie
RIK	Regionaal Informatieknooppunt
RTIC	Real-Time Intelligence Center
SGBO	Staf Grootschalig en Bijzonder Optreden
SO	Specialistische Opsporing
Sv	Strafvordering
TCI	Team Criminele inlichtingen
TDO	Team Digitale Opsporing
TGO	Team Grootschalige Opsporing
THTC	Team High Tech Crime
TMM	Team Migratiecriminaliteit en Mensenhandel
TO	Thematische Opsporing
TOOI	Team Openbare Orde Inlichtingen
VA	Virtual Agent
VVC	Veelvoorkomende Criminaliteit
VPN	Virtual Private Network
Wpg	Wet politiegegevens

1 Op verkenning naar online gegevensvergaring

Voorliggend rapport doet verslag van een verkennend onderzoek naar het online vergaren van gegevens door de politie. In dit hoofdstuk wordt het onderzoek ingeleid. In paragraaf 1 gaan we in op (de opkomst van) internet als onderzoeksomgeving. Daarna worden de probleemstelling en onderzoeksvragen behandeld. Paragraaf 3 gaat over de relevantie van het onderzoek en paragraaf 4 over de aanpak en het verloop van het onderzoek. We ronden af met de opbouw van dit rapport.

1.1 Internet als onderzoeksomgeving

In *The Game* reconstrueert Baricco (2018) de digitale revolutie. Deze revolutie begint met de eerste mainframe computers uit de jaren vijftig van de vorige eeuw. In 1971 vond er een doorbraak plaats: de introductie van de microprocessor van Intel. Deze was slechts enkele millimeters groot, maar even krachtig als de reusachtige mainframes uit de jaren vijftig. Deze ontwikkeling legde de basis voor de komst van de Personal Computer (PC) in de jaren tachtig van de vorige eeuw. In een tijdsbestek van vier jaar verschenen er drie PC's: Commodore 64, IBM en Mac. En toen veranderde de wereld pas echt, aldus Baricco. Het ging volgens hem niet zomaar om de uitvinding van de computer, maar om het idee dat dit een persoonlijk, individueel instrument werd. Met de komst van de PC deed een revolutionaire verandering in de fysieke en mentale houding van de mens zijn intrede: mens, knoppen en scherm. Een houding waarin velen van ons inmiddels uren per dag doorbrengen.

In de jaren negentig volgde de opkomst van het internet. Er waren eerst losstaande netwerken van computers en toen werd er een protocol ontwikkeld (TCP/IP) waarmee de netwerken onderling werden verbonden. En zo ontstond een wereldwijd netwerk: het internet. Volgens Baricco was aan het einde van de jaren negentig de basisinfrastructuur af. In dit klassieke tijdperk van de digitale revolutie 1) zijn de gegevens die de wereld bevatte tot een vloeibare toestand gereduceerd, 2) is een eindeloos buizenstelsel aangelegd waar die vloeistof met duizelingwekkende snelheid doorheen kan stromen en waaruit het in alle huizen van de mensen kon opborrelen, en 3) zijn zeer geraffineerde kranen en wasbakken uitgevonden die kunnen dienen als terminals voor dat gigantische waterleidingnet. En daarmee werd de basis gelegd voor een samenleving van mens-toetsenbord-scherm.

Na de eeuwwisseling ontwikkelde het internet zich van een passief, informatie gevend medium (Web 1.0) naar een interactief medium (Web 2.0) waaraan gebruikers op allerlei manieren kunnen bijdragen: via het geven van reacties, plaatsen van eigen content, beoordelen van de content van anderen, et cetera. Sociale netwerksites – zoals MySpace, Hyves en Facebook – komen op en ook andere sociale media, zoals YouTube, doen hun intrede. Volgens Baricco (2018) is er met sociale media een nevenwereld gecreëerd, die is gekoppeld aan de gewone wereld. De introductie van de smartphone heeft er vervolgens aan bijgedragen dat wij (burgers) deze nevenwereld – in de woorden van Baricco – hebben 'gekoloniseerd'; dit betekent vooral dat we er veel tijd in doorbrengen.

> *'Dat er in 2008 al 100 miljoen mensen op Facebook zaten, vonden we toen al ongelooflijk. Hyves en Second Life waren destijds booming. Nu zijn er alleen al in het online spel Fortnite 350 miljoen mensen te vinden. In 2020 telt Facebook 2,4 miljard gebruikers, YouTube 2 miljard, WhatsApp 1,6 miljard, TikTok 800 miljoen, Instagram 1 miljard en Reddit 382 miljoen gebruikers. Wereldwijd is men gemiddeld bijna 7 uur per dag op internet actief, waarvan 2,5 uur op sociale media. Er wordt iedere minuut 500 uur aan videocontent geüpload op YouTube. Deze informatierevolutie drukt niet alleen stempel op onze levens, maar ook op de financiële markten.'* (Van Doorn et al., 2021: 17)

De (door)ontwikkeling van het internet heeft voor de politie en het politiewerk uiteenlopende consequenties gehad. We noemen er een aantal zonder de intentie uitputtend te zijn. Het gaat in de eerste plaats om de digitalisering van criminaliteit: de veelvoorkomende (vermogens)criminaliteit heeft zich in belangrijke mate verplaatst naar het digitale domein en er zijn allerlei nieuwe cyberdelicten ontstaan (zie ook Landman, 2022). Daarnaast zijn er allerhande andere vormen van online immoreel gedrag ontstaan, zoals het verspreiden van desinformatie, doxing, haatzaaien en cyberpesten (zie o.a. Rathenau Instituut, 2021). Sociale media kunnen ook bijdragen aan verdeeldheid en fungeren als katalysator van ressentiment onder burgers (zie o.a. Beugelsdijk 2021). Een ander effect van sociale media op de verhouding tussen burgers is de vergroting van het organisatievermogen; het kan een mobiliserende werking hebben (zie Stol, 2021), zoals onder andere bleek tijdens 'Project X' in Haren (zie o.a. Adang, 2013).

Het voorgaande legt het accent op de veranderingen in de omgeving van de politie en in zekere zin ook op de bedreigingen. Er is echter ook een andere kant. Het internet biedt de politie allerlei mogelijkheden. Hierbij kan onder andere worden gedacht aan de communicatie en samenwerking met burgers, onder andere via de sociale mediapagina's van politieteams (zie bijvoorbeeld Meijer et al. 2013; Smulders, 2017). Het internet is daarnaast een (open) bron van gegevens voor de politie. Web 1.0 bood de politie nieuwe mogelijkheden, bijvoorbeeld gegevensvergaring via websites en open databanken (zie ook Van Treeck & Stol, 2000). Met de ontwikkeling naar Web 2.0 namen deze mogelijkheden in een rap tempo toe. Door de opkomst van sociale media is er steeds

meer informatie over personen online beschikbaar gekomen die voor de politie interessant kan zijn (zie Feenstra, 2018; Koops, 2013; Stol & Strikwerda, 2018; Trottier, 2015a). Binnen politieorganisaties wereldwijd is langzamerhand het besef gegroeid dat deze potentie kan en misschien wel moet worden benut.

> *'The dramatic increase in the use and proliferation of the internet over the last 15–20 years has seen increasingly large amounts of personal information made, not necessarily intentionally, available online. Consequently, law enforcement agencies have recognised they must open their eyes to this information and begin to use it to their advantage, especially since one of the key benefits of utilising open source information is that it is significantly less expensive to collect than other intelligence.'* (Ramwell et al., 2016: 197)

In de afgelopen (ongeveer) tien jaar is het internet in toenemende mate een onderzoeksomgeving voor de politie geworden, die een aanvulling is op de bestaande mogelijkheden om gegevens te verzamelen (Koops, 2012; Oosterhoff, 2016). Dit vakgebied – dat internationaal ook wel wordt aangeduid met *open source intelligence* (OSINT) – heeft zich in de afgelopen jaren binnen politieorganisaties sterk ontwikkeld. Politieorganisaties wereldwijd zijn steeds meer de potentie gaan inzien van het internet – en in het bijzonder sociale media – als bron van intelligence en bewijs (Sampson, 2017). Sociale media zijn volgens sommigen zelfs een *game changer* in intelligence en (tactische) opsporing (Smilda & De Vries, 2017). Empirisch onderzoek naar dit opkomende vakgebied is in ons land schaars. Met voorliggend onderzoek willen we hiermee een begin maken.

1.2 Een verkennend onderzoek

De doelstelling van dit onderzoek is het verkrijgen van inzicht in het online vergaren van gegevens door de politie ten behoeve van intelligence en opsporing. Het is een beschrijvend onderzoek met een verkennend karakter. We behandelen verschillende onderwerpen met betrekking tot online gegevens vergaring op hoofdlijnen. Het is daarmee ook eerder een breed dan een diep onderzoek.

De volgende probleemstelling staat centraal:
Op welke wijze maakt de politie gebruik van het online vergaren van gegevens (OGG) ten behoeve van intelligence en opsporing?

De probleemstelling is geconcretiseerd in de volgende deelvragen:
- Op welke wijze is OGG binnen de politie ingebed c.q. georganiseerd?
- Hoe verloopt de samenwerking op het gebied van OGG binnen de politie?
- Hoe wordt OGG ingezet in het kader van intelligence en opsporing en met welke opbrengsten?
- Hoe wordt omgegaan met juridische kaders en bevoegdheden?

- Hoe worden kennis en vaardigheden aangeleerd en onderhouden?
- Van welke tools wordt (waarvoor) gebruikgemaakt?

Met betrekking tot de probleemstelling en onderzoeksvragen is een aantal opmerkingen van belang.

De begrippen die in dit rapport worden gebruikt, kunnen gemakkelijk zorgen voor verwarring. Dit komt doordat er in de politiepraktijk verschillende termen in gebruik zijn. Dit hangt vooral samen met het gegeven dat binnen de politie online gegevens worden vergaard ten behoeve van intelligence én opsporing[1]. Het onderscheid tussen intelligence en opsporing is een onderscheid in doeleinde en bevoegdheden (zie ook hoofdstuk 2 en paragraaf 3.2). Wij hebben ervoor gekozen om het onderscheid tussen intelligence en opsporing tot uitdrukking te brengen in de terminologie die in dit rapport wordt gebruikt. Dit heeft ertoe geleid dat we drie begrippen hanteren:
- online vergaren van gegevens (OGG) voor de overkoepelende activiteit[2] en het vakgebied;
- OSINT voor het online vergaren van gegevens ten behoeve van intelligence;
- internetrechercheren voor het online vergaren van gegevens ten behoeve van opsporing.

In de volgende twee hoofdstukken wordt het bovenstaande nader verduidelijkt, onder andere door in te gaan op het juridische kader en op enkele hoofdlijnen met betrekking tot OGG binnen de politie.

De tweede opmerking is dat de zinsnede 'op welke wijze' uit de probleemstelling breed moet worden opgevat. Het gaat, zoals de onderzoeksvragen laten zien, om verschillende thema's in relatie tot OGG, zoals organisatie, niveaus van expertise, de professionals zelf, professionalisering, technologie, opbrengsten en dergelijke. We hebben *niet* in detail onderzocht hoe gegevens online worden vergaard door middel van uiteenlopende methoden, zoals *reverse image search* en *API fuzzing* (zie bijvoorbeeld de handboeken van Bazzell, 2022; Bielska et al. 2020). Dit heeft twee redenen. De eerste reden is dat dit niet mogelijk is in een verkennend onderzoek. Wij hebben data over verschillende onderwerpen verzameld. Het gedetailleerd inzoomen op operationele werkzaamheden vraagt (naar ons idee) een ander type onderzoek, bijvoorbeeld observatieonderzoek of het bestuderen van enkele specifieke intelligenceprocessen en opsporingsonderzoeken. Een tweede reden is dat het veelal technische methoden betreft, die ook nog eens voortdurend in ontwikkeling zijn (zie ook paragraaf 6.1). Inzicht hierin is voor een beperkte doelgroep relevant en interessant en vraagt daarnaast om onderzoekers met een andere bagage dan waarover wij beschikken.

1 Dienstverlening (webcare) laten we hier buiten beschouwing, omdat dit buiten de afbakening van dit onderzoek valt.
2 Het betreft het verzamelen en overnemen van online gegevens.

1.3 Relevantie van het onderzoek

De politie heeft een strategische agenda 2021-2025 die is bedoeld als leidraad voor de ontwikkeling van politiewerk en de politieorganisatie.[3] In deze agenda is het politiewerk op het web als een strategisch thema gedefinieerd. Het belang van dit thema voor de politiepraktijk komt ook tot uitdrukking in de Strategische onderzoeksagenda voor de Politie 2019-2022, waarin de politie in verbinding met wijk-web-wereld als een strategisch onderzoeksthema is opgenomen. Er is binnen de politieorganisatie behoefte aan onderzoek naar politiewerk op het web. Dit is de primaire reden dat wij in het kader van de Call van Politie & Wetenschap een voorstel tot onderzoek naar politiewerk op het web hebben ingediend, dat vervolgens is gehonoreerd.

Het politiewerk op het web ten behoeve van intelligence en opsporing is ook vanuit een maatschappelijk perspectief relevant. Het gaat hierbij in de eerste plaats om de bijdrage die dit werk of vakgebied (OGG) kan leveren aan de operationele prestaties van de politie. Welke meerwaarde heeft het voor het politiewerk? Maar ook de maatschappelijke risico's zijn relevant. Het online vergaren van gegevens kan inbreuk maken op de persoonlijke levenssfeer van burgers en die inbreuk moet rechtmatig zijn (zie hoofdstuk 2). In 2021 heeft mediaberichtgeving over het online monitoren van burgers – door middel van onder andere nepaccounts[4] – door gemeenten[5] en de Nationaal Coördinator Terrorismebestrijding (NCTV)[6] veel stof doen opwaaien. Naar aanleiding hiervan werken de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie & Veiligheid aan juridische kaders voor gemeenten. Het wetsvoorstel voor de (ruimere) bevoegdheden van de NCTV is al klaar en leidt tot kritiek van onder andere de Raad van State[7] en de Autoriteit Persoonsgegevens[8]. Deze ontwikkelingen zorgen ervoor dat er meer aandacht is gekomen voor de online gegevensvergaring door overheden. De politie bevindt zich in een andere situatie dan gemeenten en de NCTV, aangezien de bevoegdheid van opsporingsambtenaren om online gegevens te vergaren als zodanig niet ter discussie staat. Dit neemt niet weg dat de juridische grondslag – in het bijzonder voor het gebruik van onderzoeksprofielen – en het toezicht op de gegevensvergaring thema's zijn die in de maatschappelijke schijnwerpers staan, zo bleek ook uit berichtgeving van de *NRC* in mei 2021.[9] Kortom: het politiewerk op het web is een maatschappelijk relevant en gevoelig thema.

3 Deze agenda heet 'Veiligheid, vertrouwen en verbinding' en is opgesteld door de Directie Strategie & Innovatie (versie 1.0, april 2021).
4 In dit rapport wordt – in het kader van politiewerk – de term 'onderzoeksprofielen' gebruikt. In de citaten van respondenten komen de termen 'nepaccounts' en 'fake accounts' wel geregeld terug. In sommige eenheden wordt ook wel de meer neutrale term 'functionele accounts' gebruikt.
5 Het betreft mediaberichtgeving naar aanleiding van het onderzoek van Bantema et al (2021).
6 https://www.nrc.nl/nieuws/2021/04/09/nctv-volgt-heimelijk-burgers-op-sociale-media-a4039223
7 https://www.raadvanstate.nl/actueel/nieuws/@126194/w16-21-0218-ii/
8 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/nctv-wetsvoorstel-lijkt-vrijbrief-en-maakt-controle-moeilijk
9 https://www.nrc.nl/nieuws/2021/05/27/infiltreren-in-een-online-buurtfeest-a4045202 en https://www.nrc.nl/nieuws/2021/05/27/kritiek-op-inzet-nepaccounts-door-politie-a4045203

Tot slot de wetenschappelijke relevantie. Hoewel er wel is gepubliceerd over online gegevensvergaring door de politie in Nederland,[10] is er vooralsnog niet of nauwelijks empirisch onderzoek verricht.[11] Er is in dat opzicht sprake van een opmerkelijke discrepantie tussen het belang dat inmiddels aan dit vakgebied wordt toegekend en de omvang van het empirisch onderzoek dat ernaar is verricht. Voorliggend onderzoek is een eerste stap om dit gat enigszins te dichten.

1.4 Aanpak en verloop van het onderzoek

In het ontwerp van het onderzoek hebben we gekozen voor een kwalitatief onderzoek. De voornaamste reden hiervoor was dat het 'op welke wijze' uit de probleemstelling naar ons idee vraagt om diepgaande informatie die door kwalitatief onderzoek kan worden verkregen. We waren geïnteresseerd in de ervaringen en interpretaties – onder andere ten aanzien van bevoegdheden – van degenen die zich binnen de politie bezighouden met OGG. We hebben kwantitatief onderzoek ten behoeve van de generaliseerbaarheid – een min of meer *overall* beeld – overwogen, maar waren ervan overtuigd dat een goede vragenlijst eigenlijk pas na dit onderzoek kan worden gemaakt.

Het kwalitatieve onderzoek is in drie fasen uitgevoerd:
- verkennen in praktijk en wetenschap;
- uitvoeren van empirisch onderzoek;
- analyseren van data.

De verkenning in praktijk en wetenschap is gestart in de eerste helft van 2019. Door middel van literatuuronderzoek en oriënterende interviews is meer inzicht verkregen in het wettelijk kader waarbinnen online gegevensvergaring door de politie plaatsvindt en in de wijze waarop dit vakgebied binnen de politie op hoofdlijnen is georganiseerd. Het betrof vier oriënterende (groeps)interviews met respondenten die werkzaam zijn bij een basisteam, een regionale informatieorganisatie, de landelijke eenheid (oriëntatie op opsporing) en de Politieacademie. Voor het literatuuronderzoek geldt dat dit gedurende de gehele onderzoeksperiode heeft doorgelopen. Naast literatuur over het juridisch kader en OGG als vakgebied (met focus op toepassing in de politiecontext) hebben we berichtgeving gevolgd die gedurende de onderzoeksperiode over OGG is verschenen. Het gaat dan in het bijzonder om nieuwsberichten over het online monitoren van burgers, berichten van politiemensen op LinkedIn over hun werkzaamheden op het gebied van OGG en vacatures binnen de politie die hierop betrekking hebben.

10 Dit betreft vooral publicaties over het juridische kader waarbinnen het online vergaren van gegevens plaatsvindt of zou moeten plaatsvinden (zie het volgende hoofdstuk).

11 Uitzonderingen zijn Trottier (2015b) in Europees verband, Oosterhoff (2016) in Nederland voor wat betreft het gebruik van sociale media in de opsporing (scriptie) en Ferwerda (2022) over het gebruik van open bronnen in de opsporing van internationale misdrijven (scriptie).

Dit 'mediaonderzoek' had geen systematisch karakter en is vooral gebruikt om de dataverzameling aan te vullen en te verifiëren.[12]

Op basis van de verkenning is ervoor gekozen om in het vervolg van het (empirisch) onderzoek een onderscheid te maken tussen vier (organisatorische) domeinen, te weten:
- basisteam;
- districtsrecherche;
- regionale recherche;
- informatieorganisatie.

We hebben ervoor gekozen ons te richten op respondenten die OGG in hun politiewerk gebruiken dan wel verantwoordelijk zijn voor de ontwikkeling van het vakgebied. Voor ieder domein is – op basis van de verkenning – een aparte vragenlijst gemaakt. Bij de start van het onderzoek streefden we naar het interviewen van (ongeveer) tien respondenten in ieder domein én naar het (*overall*) betrekken van alle eenheden. Dit met als doel een brede verkenning te realiseren zonder te streven naar volledige representativiteit.[13] We hadden vooraf geen beeld van wie zich binnen de politie bezighouden met OGG. Het betreft namelijk geen functie, maar een vakgebied dat vanuit diverse functies wordt uitgeoefend. We hebben bij de selectie van respondenten vooral gebruikgemaakt van de sneeuwbalmethode: iedere respondent bracht ons bij een volgende.

Het onderzoek is gestart met interviews in de basisteams (najaar 2019–voorjaar 2020). Hierbij lag de focus op de digitaal wijkagent, omdat we ervan uit zijn gegaan dat binnen het basisteam vooral de digitaal wijkagent invulling geeft aan OGG. Gedurende de uitvoering van dit deelonderzoek kwam er van de landelijk portefeuillehouder Gebiedsgebonden Politie (GGP) de vraag of er een aparte rapportage kon worden gemaakt over de digitaal wijkagent. Aanleiding hiervoor was de behoefte aan meer inzicht in het werk en de dilemma's van de digitaal wijkagent. In samenspraak met de landelijke portefeuillehouder en Politie & Wetenschap is ervoor gekozen om het oorspronkelijke onderzoek uit te breiden. Er zijn acht digitaal wijkagenten van acht verschillende basisteams geïnterviewd, waarvan drie digitaal wijkagenten twee keer. De reden voor het vervolginterview was dat de tijd gedurende het eerste interview te beperkt bleek. Er heeft daarnaast een groepsinterview plaatsgevonden met drie (andere) digitaal wijkagenten. Het betreft dus elf respondenten in totaal. Ook hebben in de periferie van de gesprekken met de digitaal wijkagenten interviews plaatsgevonden met

12 Bijvoorbeeld: komen we in vacatureteksten hele andere activiteiten tegen dan die we via de interviews in beeld hebben gekregen?

13 Hiermee wordt bedoeld: een volledig beeld van de ervaringen en opvattingen van de doelgroep (politiemensen die zich bezighouden met OGG).

vier teamchefs,[14] een hoofdagent met OGG (OSINT) als taakaccent en een senior tactische opsporing van een basisteam die affiniteit had met het online vergaren van gegevens. De focus in deze gesprekken lag op het thema 'digitaal wijkagent'. De uitkomsten van dit deelonderzoek zijn gepubliceerd in 'Pionieren in gebiedsgebonden politiewerk' (Boelens & Landman, 2021). De uitkomsten zijn tevens toegelicht in het landelijke overleg van de digitaal wijkagenten. Tijdens deze (digitale) bijeenkomst waren 25 digitaal wijkagenten aanwezig en is er via de Mentimeter een aantal gesloten vragen aan hen voorgelegd. De antwoorden op deze vragen zijn ook als data ('bijvangst') meegenomen in het onderzoek.

Er hebben vervolgens negen interviews plaatsgevonden met internetrechercheurs in vier districtsrecherches van vier verschillende regionale eenheden (tweede helft 2020). Dit betreft vooral rechercheurs die internetrechercheren als een taakaccent binnen de districtsrecherche (DR) hebben. Eén respondent is een fulltime internetrechercheur binnen een DR. Het derde deel van het empirisch onderzoek bestond uit zeventien interviews met achttien respondenten die als fulltime specialist op het gebied van OGG werkzaam zijn of leidinggeven aan specialisten op het gebied van OGG. Dit betreft negen specialisten uit de regionale en landelijke informatieorganisatie (DRIO/DLIO) en negen specialisten uit de regionale rechercheorganisatie (DRR). Alle eenheden hebben in dit deel van het onderzoek geparticipeerd. De meeste eenheden hebben geparticipeerd vanuit zowel de informatieorganisatie als de rechercheorganisatie. Op advies van enkele respondenten hebben we daarnaast twee respondenten geïnterviewd die werkzaam zijn voor een landelijk project op het gebied van OSINT en onderdeel zijn van het Politiedienstencentrum van de politie. Dit derde deel van het onderzoek heeft plaatsgevonden in de eerste helft van 2021.

We hebben in totaal 41 respondenten geïnterviewd.[15] De data uit de interviews zijn door middel van een thematische analyse gecodeerd (zie Verhoeven, 2020). De beide onderzoekers hebben eerst ieder zes interviewtranscripten doorgenomen en open gecodeerd om op basis van deze codes ieder tot overkoepelende thema's te komen. Deze thema's zijn met elkaar vergeleken en hebben geleid tot een lijst met thema's. Vervolgens zijn alle interviewtranscripten tussen de beide onderzoekers verdeeld. De data uit de transcripten zijn vergeleken met de reeds gedefinieerde thema's, waarbij de onderzoekers meermaals tussentijds aandacht hebben besteed aan onderlinge consistentie in de analyse. Dit heeft geleid tot een verdere uitwerking van de thema's en tot enkele thema's die in de oorspronkelijke lijst ontbraken. Relevante tekstdelen uit de transcripten zijn in een analysedocument gezet. Dit analysedocument is gebruikt als basis voor dit rapport.

14 De data uit de interviews met de teamchefs zijn niet relevant voor voorliggend onderzoek. Om die reden zijn de teamchefs niet meegenomen in het respondentenoverzicht (zie bijlage 1).

15 De vier teamchefs zijn hierin niet meegenomen (zie vorige noot).

1.5 Leeswijzer

Dit rapport is als volgt opgebouwd.

Hoofdstuk 2 gaat in op het juridische kader voor het online vergaren van gegevens door de politie. Dit juridische kader is van belang, omdat het inzicht geeft in de huidige juridische grondslagen op basis waarvan de politie bepaalde werkzaamheden mag uitvoeren. Het geeft daarmee ook een indruk van de grenzen tussen verschillende disciplines die zich binnen de politie bezighouden met het online vergaren van gegevens.

Hoofdstuk 3 is bedoeld als 'setting the scene': het geeft op hoofdlijnen inzicht in OGG binnen de politie. Op basis van de data uit de interviews gaan we in op de opkomst van OGG binnen de politie, het perspectief van respondenten op definities, de verschillende niveaus van OGG, de organisatie van OGG binnen de politie en de samenwerking binnen de politie op het gebied van OGG.

Hoofdstuk 4 en 5 behandelen OSINT en internetrechercheren als twee deelgebieden of doeleinden van OGG. Deze hoofdstukken kennen een vergelijkbare opbouw, die bestaat uit de inzet van online gegevensvergaring, de inbedding en werkwijze van de (betreffende) professionals, het gebruik van bevoegdheden en de opbrengsten van OGG. Ieder hoofdstuk wordt afgesloten met een praktijkcase die het gebruik van online gegevens illustreert.

Hoofdstuk 6 gaat over mensen en middelen op het gebied van OGG. Dit hoofdstuk geeft inzicht in de professionals, hun opleidingen, de wijze waarop zij hun vak onderhouden, de hardware die zij gebruiken en de tools (software) die zij benutten. Hierbij is er op onderdelen enige overlap met de twee voorgaande hoofdstukken.

Hoofdstuk 7 bevat de conclusies van dit verkennende onderzoek. We gaan daarnaast in op de beperkingen van het onderzoek en geven aandachtspunten mee voor de toekomst. Het hoofdstuk is zelfstandig leesbaar en dient tevens als samenvatting.

2 Online gegevensvergaring: juridisch kader

Gegevens op het internet zijn in meer of mindere mate open te benaderen en door iedereen in te zien. Het staat politiemensen echter niet vrij om 'in het wilde weg' te grasduinen op het internet (zie Koops, 2013; Wermeskerken, 2016). Politiemensen zijn bij online gegevensvergaring aan meer regels gebonden dan bijvoorbeeld Bellingcat, een onderzoekscollectief dat (uitsluitend) gebruikmaakt van OSINT. Inzicht in het juridisch kader is van belang voor een goed begrip van het online vergaren van gegevens door de politie. Dit hoofdstuk behandelt juridische aspecten van online gegevensvergaring. We gaan eerst in op de vergelijking tussen de fysieke en digitale wereld, aangezien deze vergelijking relevant is voor het juridisch kader. Vervolgens behandelen we in paragraaf 2 de wetten die relevant zijn voor het juridisch kader. In de paragrafen die volgen, gaan we in op enkele centrale vraagstukken met betrekking tot het juridisch kader. We sluiten af met een samenvatting.

2.1 Tussen de fysieke en digitale wereld

Online gegevensvergaring door de politie is al twintig jaar in ontwikkeling is (zie paragraaf 3.1), maar er zijn vooralsnog geen specifieke juridische grondslagen voor (zie ook Koops, 2013; Feenstra, 2018). Dit gaat – voor wat betreft de opsporing – veranderen op het moment dat het nieuwe wetboek van Strafvordering (Sv) in werking treedt, omdat hierin een specifieke grondslag voor (stelselmatige) online gegevensvergaring is opgenomen.[16] Het nieuwe of gemoderniseerde wetboek van Sv treedt naar verwachting in 2026 in werking. Tot die tijd vindt online gegevensvergaring plaats op basis van een juridisch kader dat hier niet specifiek voor is bedoeld. Het is een tijdelijke noodoplossing (zie Klaar, 2022), die inmiddels al geruime tijd duurt.

De huidige juridische situatie heeft als consequentie dat wetgeving die oorspronkelijk is bedoeld voor de fysieke, offline wereld wordt toegepast op de digitale, online wereld. Deze toepassing is niet zonder problemen, omdat er een 'vertaling' of 'interpretatieslag' moet worden gemaakt van de fysieke wereld naar de digitale wereld. Deze vertaling is veelal uitdagend, omdat de kenmerken van de fysieke wereld en digitale wereld op

16 We gebruiken deze formulering, omdat die aansluit bij de terminologie die in dit rapport wordt gebruikt. De formele aanduiding van de bevoegdheid is: 'het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen'. Zie de laatste versie van het wetsvoorstel van juli 2020.

een aantal punten fundamenteel verschillen (zie ook Koops, 2013). De fysieke en digitale wereld zijn weliswaar met elkaar verbonden – ze vormen in de belevingswereld één realiteit (Barrico, 2018)[17] – maar tijd en ruimte hebben in beide werelden een andere betekenis. De Commissie Koops (2018: 36)[18] merkt hierover het volgende op:

> *'(…) het overnemen van informatie uit publiek toegankelijke bronnen kan zich beperken tot een lichte privacyinbreuk, maar ook dusdanige vormen aannemen dat iemands halve privéleven naar voren kan komen. Daarbij vervagen klassieke scheidslijnen die in de 20ste eeuw hanteerbare aanknopingspunten boden om het privéleven af te bakenen: het huis is niet langer de plaats bij uitstek waarbinnen het privéleven zich afspeelt, het lichaam raakt verbonden met de omgeving door technologie, en wat over een communicatie-infrastructuur gaat is niet beperkt tot gesprekken of berichten die mensen uitwisselen, maar omvat allerlei vormen van gegevensverkeer.'*

Kortom: het bestaande juridisch kader dat is bedoeld om opsporingsmethoden – of breder: gebruik van bevoegdheden in het kader van politiewerk – te reguleren, is niet zomaar geschikt voor politiewerk op het web.[19] Er zal niettemin mee moeten worden gewerkt. De volgende paragraaf behandelt dit juridisch kader kort. In de daarna volgende paragrafen worden enkele vraagstukken verdiept die relevant zijn voor dit onderzoek. In deze verdieping wordt het juridisch kader verder uitgewerkt.

2.2 Online gegevensvergaring en wetgeving

Het juridisch kader voor online gegevensvergaring door de politie wordt bepaald door wetgeving die betrekking heeft op de bescherming van burgers én op bevoegdheden van de politie. Met betrekking tot de bescherming van burgers is het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) het meest van belang. In dit verdrag is onder andere opgenomen dat iedere burger recht heeft op eerbiediging van diens persoonlijke levenssfeer (art. 8). Dit wordt ook wel het recht op privacy genoemd. De doelstelling van dit artikel is het individu te beschermen tegen willekeurige inmenging door de overheid in zijn privéleven. Online gegevensvergaring is een vorm van dergelijke inmenging. Het recht op privacy is echter geen absoluut recht. Onder voorwaarden is een inbreuk toegestaan. Iedere inbreuk

17 Dit wordt ook wel 'interrealiteit' genoemd (zie ook Van Egmond, 2017).

18 De Commissie Koops heeft de wetgever met haar rapport 'Regulering van opsporingsbevoegdheden in een digitale omgeving' geadviseerd over een eerdere versie van het wetsvoorstel Modernisering Sv.

19 Hier heeft niet alleen de politie mee te maken; het geldt voor de politiefunctie als geheel (zie ook Van Dijk et al., 2022). Toen de burgemeester van Utrecht in 2021 een online gebiedsverbod oplegde aan een jongen, woonachtig in Zeist, kwam ook direct de vraag naar boven of een bestuurlijke maatregel uit de fysieke wereld wel kon worden toegepast in de digitale wereld. Zie hiervoor de brief die de minister van Justitie & Veiligheid op 28 januari 2022 naar de Tweede Kamer stuurde n.a.v. vragen vanuit de Tweede Kamer over het opgelegde online gebiedsverbod. Zie ook Bantema et al. (2018) en https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/online-gebiedsverbod-juridisch-onhoudbaar

op dit recht moet, uitgaande van de Grondwet (art. 10), plaatsvinden op basis van een wet in formele zin.

De politie kan op basis van twee wetten met online gegevensvergaring een inbreuk maken op het recht op privacy, te weten:
- Politiewet (Pw);
- Wetboek van Strafvordering (Sv).

In art. 3 Pw zijn de taken van de politie opgenomen. Aan dit artikel ontlenen opsporingsambtenaren van de politie hun algemene taakstellende bevoegdheid. Deze bevoegdheid kan breed worden ingezet ten behoeve van de uitvoering van politiewerk (Zuurveen & Stol, 2020). Een voordeel van een dergelijke brede bepaling is dat de politie kan vernieuwen in de manier van werken zonder dat er iedere keer nieuwe wetgeving nodig is (zie Borgers, 2015). De inzet van deze brede bevoegdheid wordt begrensd door het effect ervan op de grondrechten van burgers.[20] Op basis van art. 3 Pw mogen opsporingsambtenaren van de politie inbreuk maken op de grondrechten van burgers, voor zover dit een *niet meer dan geringe inbreuk* betreft[21] (zie paragraaf 2.3). Anders gezegd: voor een geringe inbreuk is geen specifieke wettelijke basis nodig. De vraag is echter hoe dit uitgangspunt op het internet moet worden opgevat. In de memorie van toelichting (MvT) bij de Wet computercriminaliteit II uit 1999 werd hierover het volgende opgemerkt:[22]

> *'Zoals de politie, al dan niet in burger, op straat mag surveilleren en rondkijken, zo mag een rechercheur vanachter zijn computer hetzelfde doen op Internet. Een uitdrukkelijke wettelijke grondslag is daarvoor niet nodig, mits dat optreden gerekend kan worden tot de uitvoering van de politietaak (…) Verder geldt dat wanneer het onderzoek een stelselmatig karakter krijgt, het een aparte juridische legitimatie behoeft.'*

Dit wil dus zeggen dat de politie op basis van de algemene taakstellende bevoegdheden online gegevens mag vergaren, mits deze gegevensvergaring geen stelselmatig karakter heeft. Stelselmatig wil zeggen dat het een meer dan geringe inbreuk op grondrechten – het gaat hierbij in het bijzonder om het recht op privacy – maakt (zie paragraaf 2.3). De mogelijkheid om op basis van de algemene taakstellende bevoegdheid online gege-

20 Het gaat daarnaast – voor wat betreft de opsporing – om de integriteit en beheersbaarheid van de opsporing. Dit wil zeggen dat brede bepalingen kunnen worden gebruikt, voor zover deze niet (zeer) risicovol zijn voor de integriteit en beheersbaarheid van de opsporing (zie Borgers, 2015). In dit juridisch kader – dat betrekking heeft op online gegevensvergaring – is dit criterium naar ons idee minder relevant en richten we ons uitsluitend op het effect van handelingen op de grondrechten van burgers.

21 In dit verband wordt vaak verwezen naar het *Zwolsman*-arrest uit 1995. In dit arrest heeft de Hoge Raad geoordeeld dat de algemene taakstelling van de politie (toen nog opgenomen in art. 2 Pw) voldoende grondslag biedt voor beperkte inbreuken op de persoonlijke levenssfeer. Zie http://arresten.eu/strafrecht/hr-19-12-1995-nj-1996-249-zwolsman/

22 Zie *Kamerstukken II* 1998/99, 26671, nr. 3, p. 35.

vens te vergaren werd jaren na de MvT op de Wet computercriminaliteit II bevestigd in jurisprudentie. In 2011 werd door de rechtbank Den Haag bevestigd dat opsporingsambtenaren op basis van art. 3 Pw gebruik mogen maken van Google Earth, mits er niet stelselmatig gegevens van internet worden overgenomen (zie Oerlemans, 2017). In 2015 werd in de *Context*-zaak eveneens aangegeven dat art. 3 Pw kan worden gebruikt voor online gegevensvergaring, in dit geval via Facebook (zie Lassche, 2021). Kortom: opsporingsambtenaren van de politie kunnen op basis van art. 3 Pw zelfstandig, dus zonder bevel van een bevoegde autoriteit, online gegevens vergaren. De vraag is echter wanneer bij online gegevensvergaring een geringe inbreuk overgaat in een meer dan geringe inbreuk op de privacy van de betrokkenen. Hierop wordt in de volgende paragraaf ingegaan.

Online gegevensvergaring kan daarnaast worden gebaseerd op het Wetboek van Sv. Het Wetboek van Sv kent in de eerste plaats (ook) algemene taakstellende bevoegdheden, die zijn opgenomen in art. 141 en 142. Opsporingsambtenaren mogen op basis van deze artikelen hetzelfde als op basis van art. 3 Pw.[23] Dit wil zeggen: handelingen verrichten die een niet meer dan geringe inbreuk op grondrechten maken. Indien online gegevensvergaring door de politie een meer dan geringe inbreuk maakt op de privacy van een verdachte – er moet dan dus sprake zijn van een verdenking in de zin van art. 27 Sv – is een bijzondere opsporingsbevoegdheid nodig. In het Wetboek van Sv zijn sinds 2000 in boek I bijzondere opsporingsbevoegdheden (BOB) opgenomen.[24] Ook hiervoor geldt: deze bevoegdheden zijn niet of nauwelijks bedoeld voor opsporing in de context van het internet. Ten tijde van de totstandkoming van de Wet BOB speelde het internet een marginale rol in de opsporing (Feenstra, 2018). De wetgever heeft destijds wel aangegeven dat bijzondere opsporingsbevoegdheden ook in de digitale wereld kunnen worden toegepast (Oerlemans, 2017). Deze vertaling is echter niet concreet gemaakt. Ook hierop wordt in de volgende paragraaf nader ingegaan.

De Politiewet en het Wetboek van Sv geven juridische kaders voor uitvoering van de politietaak. Er is daarnaast wetgeving die betrekking heeft op de omgang met gegevens: de Wet politiegegevens (Wpg). De Wpg is van toepassing op het geautomatiseerd verwerken of het verwerken in een bestand van *persoonsgegevens* ten behoeve van uitvoering van de politietaak. Verwerken wordt in de Wpg breed opgevat (zie ook Oerlemans, 2017), waaronder: verzamelen, vastleggen, bewaren, gebruiken, combineren, verspreiden. In dat opzicht zijn de Pw, het Wetboek van Sv en de Wpg deels overlappende wetten voor wat betreft online gegevensvergaring. Hierbij moet wel worden opgemerkt dat de Wpg zeer beperkt ingaat op de feitelijke gegevensvergaring. Lid 1 en 2 van art. 3 van de Wpg kunnen worden beschouwd als scharnier tussen de vergaring enerzijds en verdere verwerking anderzijds (Gritter, 2018). Hierin is opgenomen dat 1) politiegege-

23 Hierbij moet worden opgemerkt dat art. 3 Pw ook kan worden gebruikt voor niet-strafvorderlijk optreden (zie par. 2.8). Art. 3 Pw heeft dus wel een grotere reikwijdte.

24 Deze verandering is het gevolg van de Wet BOB.

vens slechts worden verwerkt voor zover dit noodzakelijk is voor de bij of krachtens deze wet (Wpg) geformuleerde doeleinden, en dat 2) politiegegevens slechts worden verwerkt voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens – gelet op de doeleinden waarvoor zij worden verwerkt – toereikend, terzakedienend en niet bovenmatig zijn. De overige bepalingen van de Wpg gaan vooral in op de verdere verwerking (zie ook Galič, 2022). Omdat dit onderzoek zich niet richt op de verdere verwerking van online vergaarde gegevens – de grens ligt bij het overnemen van gegevens – laten we de Wpg buiten beschouwing. We beperken ons tot de algemeen taakstellende bepalingen en bijzondere opsporingsbevoegdheden op basis waarvan online gegevensvergaring plaatsvindt.

2.3 Het vraagstuk van stelselmatigheid

In het juridisch kader voor online gegevensvergaring is de inbreuk die dit maakt op de privacy van burgers het voornaamste vraagstuk. Het onderscheid tussen een geringe en meer dan geringe inbreuk op de privacy staat hierbij centraal. De kernvraag is wanneer bij online gegevensvergaring sprake is van een meer dan geringe inbreuk op de privacy.

Er is sprake van een meer dan geringe inbreuk wanneer 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). Hierbij moet worden benadrukt dat het gaat om aspecten van iemands privéleven (zie Commissie Koops, 2018). Het hoeft geen groot deel van iemands privéleven te zijn. Het gaat erom dat een bepaald deel min of meer volledig naar voren komt, bijvoorbeeld door een beeld te vormen van alle contacten van de persoon vanuit een bepaalde rol (zoals als eigenaar van een horecagelegenheid). Het systematische en gerichte karakter waarmee de persoonlijke levenssfeer van een burger in beeld wordt gebracht, wordt in het domein van strafvordering tot uitdrukking gebracht met de term '*stelselmatigheid*'. Anders gezegd: stelselmatigheid wordt gebruikt om een 'geringe inbreuk' te onderscheiden van een 'meer dan geringe inbreuk' (zie ook Commissie Koops, 2018). Je zou ook kunnen zeggen: de (meer dan) geringe inbreuk is het effect c.q. de opbrengst en de stelselmatigheid is de manier van werken.

De vervolgvraag is wanneer het online vergaren van gegevens een stelselmatig karakter heeft. Deze vraag is lastig te beantwoorden. In de MvT bij de Wet BOB zijn vijf factoren benoemd die bepalen of er sprake is van stelselmatigheid[25] (Feenstra, 2018; Oerlemans, 2017): 1) duur, 2) plaats, 3) intensiteit, 4) frequentie, en 5) het gebruik van een technisch hulpmiddel. Door de Commissie Koops (2018) is benadrukt dat deze beoordelingsfactoren niet relevant zijn voor – of niet rechtstreeks zijn te 'vertalen' naar – het

25 Dit betreft stelselmatige observatie.

digitale domein.[26] Ook bij een beperkte duur, intensiteit en frequentie kan er een meer dan geringe inbreuk worden gemaakt op de privacy van een verdachte. Dit heeft te maken met het verschil tussen offline en online. De politie kan offline iemands gedrag observeren, maar niet terugkijken. Dit kan online wel. Wanneer de politie op het internet gegevens over een persoon opzoekt, kan er worden teruggekeken (zie Koops, 2013). Dit kan een grote bron van gegevens zijn die een vrij compleet beeld kan geven van (aspecten van) iemands leven. Bijvoorbeeld: door het veiligstellen van een Facebookprofiel dat al jaren actief is, kan een min of meer volledig beeld worden verkregen van aspecten van iemands privéleven. Kortom: frequentie is niet of in ieder geval beperkt relevant.

Het voorgaande maakt duidelijk dat 1) het effect van online gegevensvergaring op de privacy van burgers zich lastig laat concretiseren ('een min of meer volledig beeld van aspecten van iemands privéleven'), en 2) de bestaande factoren die kunnen worden gebruikt bij het bepalen van stelselmatigheid in de werkwijze of het proces beperkt houvast geven voor online gegevensvergaring. Waaraan kan dan wel houvast worden ontleend? In de eerste plaats aan het beleid van het OM en de politie. Door het OM en de politie is in 2016 een *Leidraad bevoegdheden informatievergaring op internet* (opsporing) opgesteld[27] (zie ook Stol & Strikwerda, 2018). Deze Leidraad is echter niet (volledig) openbaar.[28] De teksten die wel openbaar zijn (gemaakt), geven aanvullend inzicht in stelselmatigheid. Stelselmatigheid moet volgens de Leidraad worden beoordeeld op basis van de combinatie van handelingen. Op zichzelf staande handelingen, zoals zoekslagen, kunnen een beperkte inbreuk maken, maar de combinatie ervan kan in een meer dan geringe inbreuk resulteren. Om die reden heeft de Commissie Koops (2018) ook benadrukt dat opsporingsambtenaren idealiter stapsgewijs te werk gaan, zodat tussentijds kan worden geconstateerd of het punt van stelselmatigheid is bereikt of bereikt zal gaan worden. De Commissie erkent echter ook dat bij online gegevensvergaring vaak minder tussenstappen in het onderzoeksproces mogelijk zijn. Er kunnen met één handeling veel gegevens worden vergaard.

De Leidraad maakt tevens duidelijk dat de stelselmatigheid zoveel als mogelijk van tevoren moet worden ingeschat.[29] Dit is een belangrijk punt: een bijzondere opsporingsbevoegdheid moet voorafgaand aan de uitvoering van de betreffende opsporingsmethode worden aangevraagd. Het gaat om de vraag of het op voorhand redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van bepaalde aspecten van iemands

26 Daarnaast geldt ook voor toepassing in de fysieke wereld dat stelselmatigheid een weinig eenduidige definitie of interpretatie heeft (Feenstra, 2018; Lassche, 2021; Oerlemans, 2017).

27 Aanleiding hiervoor waren onder andere de grote verschillen in de wijze waarop de bevoegdheden, die oorspronkelijk waren bedoeld voor offline politiewerk, werden vertaald naar het online politiewerk.

28 Zie wel https://www.politie.nl/binaries/content/assets/politie/wob/00-landelijk/integrale-aanpak-jihadisme/20160519---2237---bijlagen-bij-besluit.pdf

29 De matrix die in de Leidraad is opgenomen, is hierbij een hulpmiddel.

privéleven kan worden verkregen[30] (zie Commissie Koops, 2018). Van tevoren moet door opsporingsambtenaren worden bedacht welke gegevens worden verzameld, over welke personen, in welke bronnen en met welke middelen en hoeveel gegevens dit naar verwachting zal opleveren (Lassche, 2021). Op basis hiervan kan een inschatting worden gemaakt van de inbreuk die op iemands persoonlijke levenssfeer zal worden gemaakt. Van de opsporingsambtenaar wordt verwacht dat die diens eerdere ervaringen met online gegevensvergaring – en daarop gebaseerde ervaringsregels – betrekt (zie Commissie Koops, 2018).

Het bovenstaande geeft naar ons idee iets meer inkleuring aan het begrip 'stelselmatigheid' in het huidige juridische kader.[31] Er is tegelijkertijd nog veel ruimte voor interpretatie (zie ook Feenstra, 2018; Oerlemans, 2017). De empirische hoofdstukken bieden enig inzicht in hoe in de politiepraktijk met het criterium van stelselmatigheid wordt omgegaan.

2.4 Het vraagstuk van de passende bijzondere opsporingsbevoegdheid

Het strafvorderlijk legaliteitsbeginsel vereist een specifieke bevoegdheid wanneer bij de opsporing van strafbare feiten een meer dan geringe inbreuk wordt gemaakt op grondrechten van burgers (Feenstra, 2018; Stol & Strikwerda, 2018). Dit geldt ook voor online gegevensvergaring. In het Wetboek van Sv zijn er dan twee opties: stelselmatige observatie (art. 126g Sv) of stelselmatige informatie-inwinning (art. 126j Sv). Onder juristen is er discussie over welke bevoegdheid het meest passend is.

Stelselmatige observatie wordt door de meeste juristen als de minst passende bevoegdheid gezien. Online observatie wordt door hen beschouwd als een problematisch concept, aangezien er van observatie in letterlijke zin geen sprake is (Feenstra, 2018; Lassche, 2021; Stol & Strikwerda, 2018). Bij online gegevensvergaring staat het resultaat van het gedrag centraal (iets dat online is geplaatst, gedrag heeft al plaatsgevonden) en er kan niet (direct) worden vastgesteld om wie het gaat. Er worden in de regel gegevens uit het verleden overgenomen. Dit verhoudt zich moeizaam tot het concept van observatie. Oerlemans (2017) betoogt echter dat stelselmatige observatie het meest passend is, omdat het gaat om het waarnemen van het gedrag van persoon op het internet via

30 Indien de uitoefening van de algemene bevoegdheid (art. 3 Pw) leidt tot een min of meer volledig beeld van bepaalde aspecten van iemands privéleven, terwijl dat niet op voorhand redelijkerwijs voorzienbaar was, dan maakt dit die uitoefening niet met terugwerkende kracht stelselmatig. Anders gezegd: het is dan nog steeds rechtmatig. De onvoorzienbaar aangetroffen gegevens gelden dan als bijvangst en kunnen als zodanig worden gebruikt voor het bewijs (Commissie Koops, 2018).

31 Na inwerkingtreding van het gemoderniseerde Wetboek van Sv komt er meer duidelijkheid over de operationalisering van dit begrip. De Commissie Koops (2018) heeft in haar advies maar liefst zeventien factoren benoemd die kunnen worden gebruikt voor het vaststellen van stelselmatigheid in het kader van de nieuwe bevoegdheid op het gebied van stelselmatige online gegevensvergaring (uit open bronnen). Deze factoren zijn ook grotendeels gebruikt in de MvT bij de nieuwe bevoegdheid. Voor deze factoren geldt echter dat ze nog niet van toepassing zijn, omdat het gemoderniseerde Wetboek Sv nog niet van kracht is.

onder andere sociale media, discussiefora en chatkanalen. Het online gedrag van een persoon uit zich in die gevallen in het plaatsen van statusupdates of het delen van berichten op sociale media, het deelnemen aan of starten van discussies op forums of het communiceren met anderen in chatkanalen. Anders gezegd: online gegevensvergaring kan volgens hem worden uitgelegd als observatie in een online context.

Stelselmatige informatie-inwinning wordt in de regel beschouwd als de meest passende bevoegdheid (Feenstra, 2018; Lassche, 2021; Stol & Strikwerda, 2018). 'De minst slechte optie' is wellicht een betere formulering, omdat de keuze voor stelselmatige informatie-inwinning in belangrijke mate voortvloeit uit de kritiek op het gebruik van stelselmatige observatie voor stelselmatige online gegevensvergaring. Hierbij kan worden opgemerkt dat de wetgever bij de introductie van de Wet BOB expliciet heeft aangegeven dat stelselmatige informatie-inwinning ook op internet kan worden toegepast (Oerlemans, 2018a). Het belangrijkste bezwaar tegen het gebruik van deze bevoegdheid voor online gegevensvergaring is dat stelselmatige informatie-inwinning veronderstelt dat de opsporingsambtenaar actief interfereert in het leven van de verdachte. Hiervan is bij online gegevensvergaring in veel gevallen geen sprake, behalve wanneer de opsporingsambtenaar onder dekmantel werkt. Juist om die reden pleit Oerlemans (2017) ervoor om stelselmatige informatie-inwinning in een online context te reserveren voor online undercoverwerkzaamheden waarbij actieve interactie met de verdachte(n) plaatsvindt (zie paragraaf 2.6). Hierbij kan worden opgemerkt dat de wetgever in de MvT bij de Wet BOB heeft benadrukt dat stelselmatige inwinning een zwaarder middel is dan stelselmatige observatie, omdat de opsporingsambtenaar niet alleen observeert, maar actief interfereert in het leven van de verdachte (Stol & Strikwerda, 2018). Het gaat verder dan alleen waarnemen of luisteren. In die zin 'past' deze bevoegdheid niet bij online gegevensvergaring waarbij er geen interferentie is in het leven van de verdachte(n).

De conclusie op basis van het voorgaande is dat iedere bestaande, bijzondere opsporingsbevoegdheid diens eigen problemen of tekortkomingen heeft in het kader van gebruik voor stelselmatige online gegevensvergaring. Gegeven deze tekortkomingen lijkt stelselmatige informatie-inwinning onder juristen de voorkeur te hebben.

2.5 Het vraagstuk van de open bron

Een volgend vraagstuk in het juridisch kader voor online gegevensvergaring heeft betrekking op het onderscheid tussen open of publiek toegankelijke bronnen enerzijds en gesloten of afgeschermde bronnen anderzijds. Dit onderscheid wordt hieronder toegelicht.

In de juridische literatuur wordt een open bron beschouwd als een bron waartoe *in beginsel* eenieder toegang kan verkrijgen (zie Feenstra, 2018; Koops, 2013). Ook bronnen waarvoor toegangsregistratie nodig is, kunnen worden beschouwd als een open

bron (zie Feenstra, 2018). Het gaat er vooral om dat het verkrijgen van toegang *zonder selectie* plaatsvindt. Dit wil zeggen dat niemand kan worden uitgesloten. Anders gezegd: 'open' verwijst dus niet naar 'open toegang', wat wil zeggen dat het altijd om een bron moet gaan die direct, zonder in te loggen, toegankelijk is. De Commissie Koops (2018) sluit zich, in haar advies over het reguleren van opsporingsbevoegdheden in een digitale omgeving, aan bij deze invalshoek en formuleert het als volgt (p. 152):

> *'Open bronnen kenmerken zich dus doordat in beginsel eenieder er toegang toe kan verkrijgen en dat voor zover toegang gebonden is aan een account, het verkrijgen van een account een (semi)geautomatiseerd proces is waarbij niet bepaalde groepen worden uitgesloten van registratie. Open bronnen staan dus tegenover afgeschermde bronnen, die zich kenmerken doordat er een controle plaatsvindt op wie degene is die toegang wil hebben tot de bron.'*

De Commissie Koops (2018) verheldert de definitie van open bron nader door erop te wijzen dat het niet gaat om de intrinsieke kenmerken van de bron,[32] maar om *de wijze van toegang*. Het voornaamste criterium is (dus) of er sprake is van een daadwerkelijke toegangscontrole of anders gezegd: een vorm van beveiliging. Gegevens die niet zijn onderworpen aan een (daadwerkelijke) toegangscontrole en waartoe toegang kan worden verkregen zonder de (web)server binnen te dringen, zijn open (zie Klaar, 2022). In deze definitie van open bron behoren betaaldiensten zonder daadwerkelijke toegangscontrole (zoals de Kamer van Koophandel) en het bezoeken van openbare profielen op sociale media tot open bronnen.[33] Ook voor het darkweb – het gedeelte van het internet dat alleen toegankelijk is via speciale software – geldt dat het een open bron is. Iedereen die deze software downloadt, kan surfen op het darkweb. Het gebruik van deze definitie van open bron houdt in dat een groot deel van de informatie op het internet, namelijk alles waar je zonder enige vorm van restrictie bij kunt komen, als open bron kan worden beschouwd[34] (Feenstra, 2018).

Uiteenlopende juristen wijzen erop dat de term 'open bron' verwarring kan oproepen (zie bijvoorbeeld Feenstra, 2018; Oerlemans, 2017). Deze term zou de indruk (kunnen) geven dat het gaat om bronnen die volledig open te benaderen zijn (dus zonder in te loggen). Daarnaast wijst de Commissie Koops (2018) erop dat 'open bron' de suggestie kan wekken dat de bron ongelimiteerd of vrij kan worden gebruikt, wat dus niet terecht is (zie paragraaf 2.3). In plaats van 'open bron' wordt daarom de voorkeur gegeven aan de term 'publiek toegankelijke bron', waarmee ook aansluiting wordt gevonden bij het Cybercrimeverdrag (zie Feenstra, 2018). Het advies van de Commissie Koops met betrekking tot deze terminologie is overgenomen in het gemoderniseerde Wetboek van Sv. In dit onderzoek gebruiken wij echter de term 'open bron', omdat dit in de

32 Bijvoorbeeld de online vindbaarheid van de gegevens.
33 Feenstra (2018) gebruikt in dit geval (na toegangsregistratie) de term 'semi-open bron', maar dit is geen aparte (juridische) categorie.
34 Volgens respondenten in dit onderzoek wordt dit deel wel steeds kleiner. Zie hiervoor par. 4.3.

politiepraktijk vooralsnog gebruikelijk(er) is. De verwachting is dat na de inwerkingtreding van het gemoderniseerde Wetboek van Sv de terminologie in de politiepraktijk geleidelijk gaat veranderen.[35]

Open bronnen staan tegenover afgeschermde bronnen. Bij deze bronnen is sprake van controle op degene die toegang wil tot de bron. Om het onderscheid tussen open en afgeschermde bronnen te verduidelijken, kan een profiel op Facebook als voorbeeld dienen. Een openbaar profiel is een open bron. Een profiel dat alleen kan worden ingezien na acceptatie van een vriendverzoek is een afgeschermde bron. Het gegeven dat een opsporingsambtenaar moet inloggen, maakt het dus geen afgeschermde bron, want iedereen kan een Facebook account krijgen. Er is geen sprake van selectie. In geval van een vriendschapsverzoek is er wel sprake van selectie en dus is het een afgeschermde bron. De opsporingsambtenaar beoogt dan toegang te krijgen tot gegevens die niet voor een ieder toegankelijk zijn, maar enkel voor vrienden (zie Commissie Koops, 2018). Daarnaast wordt er op individueel niveau toegang verleend, waarbij de uitkomst onzeker is. Of anders gezegd: er is selectie en dus (meer of minder strak) 'deurbeleid'. Om toegang te krijgen tot een afgeschermde bron, moet een opsporingsambtenaar zich – in de regel met behulp van een onderzoeksprofiel – kenbaar maken en al dan niet interacteren met anderen. In de volgende paragraaf gaan we hier nader op in.

Het is tot slot van belang te benadrukken dat in het huidige juridische kader het onderscheid tussen open en afgeschermde bronnen alleen relevant is in relatie tot stelselmatigheid.[36] Als een opsporingsambtenaar (persoons)gegevens vergaart in een besloten of afgeschermde omgeving, is er eerder sprake van een meer dan geringe inbreuk op de persoonlijke levenssfeer. Burgers kunnen namelijk niet of in mindere mate voorzien dat opsporingsambtenaren deze gegevens overnemen. Dit is een verschil met publiek toegankelijke gegevens. Burgers die gegevens publiek toegankelijk op het internet plaatsen kunnen dit voorzien en dus uitgaan van minder privacy (zie ook Feenstra, 2018).

35 Een ander argument van de Commissie Koops (2018) om de term 'publiek toegankelijke bron' (in het wetvoorstel) te hanteren, is dat het de uitvoering bewust maakt van de introductie van een nieuwe bevoegdheid, te weten: het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Een nieuwe term heeft volgens de Commissie een signaalfunctie dat in het juridisch kader iets is veranderd.

36 Bij inwerkingtreding van het nieuwe Wetboek van Sv wordt het onderscheid tussen open (dan geformuleerd als 'publieke toegankelijke') bronnen en afgeschermde bronnen relevanter, omdat er een nieuwe bevoegdheid wordt geïntroduceerd: het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Deze bevoegdheid houdt qua zwaarte het midden tussen art. 3 Pw en art. 126j Sv. Art. 3 Pw is bedoeld voor niet-stelselmatige online gegevensvergaring en art. 126 Sv is bedoeld voor het actief aangaan van interactie door bijvoorbeeld vrienden te worden en te chatten met een verdachte of meerdere verdachten (zie ook par. 2.6).

2.6 Het vraagstuk van het onderzoeksprofiel

In de MvT bij de eerder aangehaalde Wet computercriminaliteit II (1999) is door de minister aangegeven dat opsporingsambtenaren onder een pseudoniem mogen opereren, mits er geen sprake is van misleiding. De minister redeneert als volgt:[37]

> *'Het is immers op veel delen van Internet niet ongebruikelijk om je daar anoniem of onder een pseudoniem te bewegen. De overige deelnemers kunnen er in die gevallen op bedacht zijn dat ze in werkelijkheid met iemand anders van doen hebben.'*

Er is destijds niet door de minister aangegeven op basis van welke bevoegdheid opsporingsambtenaren onder een pseudoniem – wij noemen dit een onderzoeksprofiel – mogen opereren. De jurisprudentie in het kader van de eerdergenoemde *Context*-zaak geeft aan dat er voor het aanmaken en gebruiken van een onderzoeksprofiel in beginsel geen bijzondere opsporingsbevoegdheid nodig is (zie Feenstra, 2018). Opnieuw geldt: het gaat niet zozeer om het gebruik van het onderzoeksprofiel, maar om de vraag of er sprake is van stelselmatigheid in de online gegevensvergaring. En dan geldt wat eerder is aangegeven (zie paragraaf 2.5): als een opsporingsambtenaar een onderzoeksprofiel gebruikt om in een afgeschermde omgeving (persoons)gegevens te vergaren, dan is er eerder dan in een open omgeving sprake van een meer dan geringe inbreuk op de privacy en dus van stelselmatigheid. De redenering is dan dat (een) verdachte(n) niet of in mindere mate kan/kunnen voorzien dat opsporingsambtenaren gegevens vergaren.

Dan de stap naar de door de minister genoemde 'misleiding'. Van misleiding is sprake als een verdachte wordt geactiveerd om gegevens prijs te geven zonder dat deze weet dat deze gegevens worden gebruikt voor opsporingsdoeleinden. In dat geval is er – net als in de fysieke wereld – sprake van online undercoverwerkzaamheden waarbij wordt geïnterfereerd in het leven van de verdachte.

> *'Daarbij kan worden gedacht aan interacties op chatkanalen, via private messaging diensten, via sociale mediadiensten, online discussieforums en online zwarte markten. Slechts met de juiste kennis van internetsubculturen, kunnen opsporingsambtenaren op een geloofwaardige manier op internet communiceren en relaties aangaan met mensen in het kader van een opsporingsonderzoek.'* (Oerlemans, 2017: 27)

In geval van online undercoverwerk – werken onder dekmantel – is er altijd een bijzondere opsporingsbevoegdheid nodig. Met de Wet BOB zijn er in het Wetboek van Sv drie bijzondere opsporingsbevoegdheden geïntroduceerd voor undercoverwerkzaamheden (Oerlemans, 2018a):

- stelselmatige informatie-inwinning;
- pseudokoop en pseudodienstverlening;
- infiltratie.

37 Zie *Kamerstukken II* 1998/99, 26671, nr. 3, p. 35.

In het kader van dit onderzoek is alleen stelselmatige informatie-inwinning relevant.[38] Stelselmatige informatie-inwinning is in paragraaf 2.4 gedefinieerd als de meest passende bijzondere opsporingsbevoegdheid wanneer door middel van online gegevensvergaring een meer dan geringe inbreuk plaatsvindt op de privacy van een persoon. Er hoeft dan geen sprake te zijn van online undercoverwerkzaamheden, maar dezelfde bevoegdheid is wel bruikbaar voor deze werkzaamheden. In geval van online undercoverwerkzaamheden komt er iets bij: de opsporingsambtenaar interacteert met een verdachte. Naarmate er meer interactie plaatsvindt, is er in de regel sprake van meer inbreuk op iemands privacy. De interactie kan ingrijpend zijn voor de betrokken verdachte, omdat de undercoveragent in meer of mindere mate een relatie opbouwt (Oerlemans, 2018a).

Kortom: het gebruik van een onderzoeksprofiel wil niet direct zeggen dat een bijzondere opsporingsbevoegdheid nodig is. Het hangt ervan af wat de opsporingsambtenaar met het onderzoeksprofiel doet. Wie een onderzoeksprofiel gebruikt om via de openbare delen van Facebook gegevens te verzamelen zonder een meer dan geringe inbreuk te maken, heeft geen bijzondere opsporingsbevoegdheid nodig. Wie een onderzoeksprofiel gebruikt om in een besloten groep met strakke toegangscontrole 'mee te kijken', heeft een bijzondere opsporingsbevoegdheid nodig. Wie een onderzoeksprofiel gebruikt om vrienden te worden met een verdachte en met de verdachte te chatten, werkt onder dekmantel en heeft een bijzondere opsporingsbevoegdheid nodig.[39] Opvallend is dat optie twee en drie op basis van dezelfde opsporingsbevoegdheid kunnen plaatsvinden.

Het is tot slot van belang op te merken dat voorliggend onderzoek niet gaat over online undercover werkzaamheden. In die zin is de grens tussen toegang verkrijgen tot een afgeschermde bron en 'kijken' én toegang verkrijgen en 'meepraten' ook de grens van dit onderzoek.[40] In het volgende hoofdstuk wordt ook duidelijk dat undercoverbevoegdheden in een online context worden toegepast door specifieke opsporingsambtenaren binnen de politie, te weten: *virtual agents* (VA's) (zie paragraaf 3.4). Met deze virtual agents hebben we niet gesproken.

38 De pseudokoop wil zeggen dat een undercoveragent een aankoop doet op internet van een goed (zoals drugs of wapens) of gegevens (zoals gestolen persoonsgegevens). Hierbij mag geen sprake zijn van uitlokking, wat wil zeggen dat een persoon er niet toe mag worden bewogen een delict te plegen dat die niet voornemens was. Bij infiltratie wordt er geparticipeerd in een criminele organisatie teneinde bewijsmateriaal over strafbare feiten te verzamelen. Het is hierbij mogelijk dat (geautoriseerde) strafbare feiten worden gepleegd. Infiltratieoperaties kunnen ook in een online context worden ingezet, zoals op online fora of handelswebsites waarbij het vermoeden bestaat dat strafbare feiten in georganiseerd verband worden gepleegd. Zo kan een online infiltratieoperatie worden gebruikt om in de hiërarchie van een online drugsmarktplaats op te klimmen.

39 Zie in dit verband ook de jurisprudentie in het kader van de eerdergenoemde *Context*-zaak (zie ook Feenstra, 2018; Oerlemans, 2018a; Stol & Strikwerda, 2018).

40 Hierbij moet wel worden opgemerkt dat dit in de praktijk in potentie een dunne grens is, zoals ook uit hoofdstuk 4 en 5 zal blijken. Hierbij speelt mee dat beide op basis van dezelfde bevoegdheid kunnen plaatsvinden.

2.7 Het vraagstuk van niet-strafvorderlijke online gegevensvergaring

In de voorgaande paragrafen is het vrijwel uitsluitend over het juridisch kader voor online gegevensvergaring ten behoeve van de opsporing gegaan. Voorliggend onderzoek verkent echter ook online gegevensvergaring ten behoeve van intelligence. Dit betreft dus online gegevensvergaring buiten het kader van het Wetboek van Sv. Dit roept een vraag op: wat mag de politie in haar intelligencewerk? De Commissie Koops (2018: 151) heeft hierover het volgende opgemerkt:

> *'De grondslag die hiervoor (online gegevensvergaring met een niet-strafvorderlijk karakter, red.) wordt gehanteerd, zijn de algemene taakstellende artikelen. Bij gebreke van een specifieke wettelijke grondslag betekent dit dat het onderzoek moet worden beëindigd zodra de drempel van de "meer dan geringe inbreuk" in beeld komt. In de huidige praktijk worden allerlei maatschappelijke vraagstukken bij de politie neergelegd, zonder dat in de wet voorzien is in een passend bijbehorend juridisch kader. In dit rapport wordt alleen geadviseerd over een regeling in het Wetboek van Strafvordering, maar de commissie wijst erop dat de wetgever ook voor het overnemen van persoonsgegevens uit publiek toegankelijke bronnen in het kader van andere politietaken een normerend kader zou moeten stellen, dat bij voorkeur zo veel mogelijk zou moeten aansluiten bij de terminologie en voorwaarden die binnen strafvordering worden gehanteerd.'*

De Commissie geeft dus aan dat er vrijwel geen rechtsregels zijn voor online gegevensvergaring met een niet-strafvorderlijk doel. De wetgever zou volgens de Commissie daarom snel een regeling tot stand moeten brengen en hiermee niet moeten wachten tot de inwerkingtreding van het gemoderniseerde Wetboek van Sv (naar verwachting in 2026). Een dergelijke regeling is er echter nog niet. Opnieuw geldt: er is wel politiebeleid. Respondenten uit het onderzoek geven aan dat er sinds 2017 een Leidraad – en daarin opgenomen matrix – is voor informatievergaring op het internet voor niet-strafvorderlijk handelen. Deze leidraad is echter niet openbaar.

Het centrale uitgangspunt is desondanks eenvoudig: de politie moet de online gegevensvergaring ten behoeve van intelligence baseren op art. 3 Pw. In algemene zin geldt namelijk dat de politie voor het uitsluitend verbeteren van de intelligencepositie geen bijzondere opsporingsbevoegdheden mag inzetten (zie Van den Eeden et al., 2021). Dit wil zeggen dat er activiteiten mogen worden verricht die redelijkerwijs voorzien in het maken van een niet meer dan geringe inbreuk op de persoonlijke levenssfeer van een burger.[41] Hierbij moet worden opgemerkt dat stelselmatigheid een strafvorderlijk be-

41 Het is van belang op te merken dat een meer dan geringe inbreuk vooral ontstaat bij het vergaren van persoonsgegevens. Of anders gezegd: de beperkingen van online gegevensvergaring door de politie hebben in het bijzonder betrekking op persoonsgegevens (zie Koops, 2013). Bij het vergaren van andersoortige gegevens – zoals gegevens over rechtspersonen – zal geen of veel minder snel sprake zijn van een inbreuk op de privacy of op andere grondrechten van burgers.

grip is. Voor online gegevensvergaring ten behoeve van andere doeleinden (waaronder intelligence) is dit begrip minder passend. Er kan in die gevallen beter aansluiting worden gevonden bij de vereisten van proportionaliteit en subsidiariteit (zie ook Lassche, 2021). Het vereiste van proportionaliteit wil zeggen dat de inbreuk op de persoonlijke levenssfeer van de betrokken personen in redelijke verhouding moet staan tot het algemeen belang/het doel. Het vereiste van subsidiariteit wil zeggen dat de voorgenomen handeling de minst ingrijpende wijze moet zijn om het gewenste doel te bereiken.

Uit met name het vereiste van proportionaliteit volgt dat er bij online gegevensvergaring over een persoon die geen verdachte is eerder sprake is van een meer dan geringe inbreuk op de privacy (zie Wermeskerken, 2016). De betreffende persoon wordt immers nog nergens van verdacht, wat maakt dat een inbreuk eerder disproportioneel is in relatie tot het doel dat ermee wordt beoogd. Of anders gezegd: het algemeen belang weegt minder zwaar dan in geval van een verdachte.

Het voorgaande heeft als consequentie dat in het kader van online gegevensvergaring ten behoeve van intelligence veel 'grijs gebied' is. Meer dan in geval van opsporing. Afstemming met het gezag is in voorkomende gevallen van belang om politiemensen houvast te geven. Dit brengt ons op een volgend punt: wie is het gezag? Het antwoord op die vraag lijkt te zijn: dit hangt ervan af. De politie heeft twee gezagsdragers: de officier van justitie voor de handhaving van de strafrechtelijke rechtsorde en de burgemeester voor de handhaving van de openbare orde. Dit onderscheid is ook van belang voor online gegevensvergaring in het kader van intelligence. Waar het gaat om de voorfase van de opsporing is de (informatie)officier van justitie het gezag en de gesprekspartner van de politie (zie Inspectie JenV, 2018). Dit impliceert dat in het kader van intelligencevergaring op tal van thema's – zoals mensenhandel, drugs en CTER – afstemming met de informatieofficier kan worden gezocht.

Dit geldt echter niet voor de openbare orde. De burgemeester is het gezag bij het handhaven van de openbare orde (art. 11 Pw). De burgemeester kan de betrokken ambtenaren van de politie aanwijzingen geven voor de vervulling van taken op het gebied van de openbare orde. De vraag is of deze aanwijzingen ook betrekking kunnen hebben op online gegevensvergaring in het kader van (mogelijke) openbare ordeverstoringen. In de (juridische) literatuur hebben we hier geen uitsluitsel over kunnen vinden. Dit hangt mogelijk samen met de meer algemene zoektocht naar de rol van de burgemeester in het digitale domein (zie de onderzoeken van Bantema et al., 2018, 2020, 2021).

2.8 Het vraagstuk van geautomatiseerde online gegevensvergaring

Het online vergaren van gegevens wil in het kader van dit onderzoek zeggen dat opsporingsambtenaren van de politie gegevens opzoeken en overnemen van het internet. Dit kan op twee manieren plaatsvinden: handmatig en geautomatiseerd (Feenstra, 2018; Oerlemans, 2017).

Het handmatig online vergaren van gegevens wil zeggen dat een opsporingsambtenaar zelf naar websites of platformen gaat of gebruikmaakt van zoekmachines en gevonden gegevens overneemt in bijvoorbeeld een informatierapport of een proces-verbaal. In geval van geautomatiseerd online vergaren van gegevens wordt gebruikgemaakt van software die automatisch naar relevante gegevens zoekt, bijvoorbeeld op basis van bepaalde zoektermen (Oerlemans, 2017). Deze software wordt in de wereld van intelligence aangeduid met *automated OSINT* (zie bijvoorbeeld CTIVD, 2021), terwijl in de opsporingswereld de verzamelterm 'webcrawlers' gebruikelijk is (zie ook Commissie Koops, 2018; Lodder & Schuilenburg, 2016). Dergelijke software, of het nu voor OSINT of internetrechercheren is, kan door commerciële aanbieders worden geleverd of binnen de politieorganisatie zelf zijn ontwikkeld. Zo heeft de politie in eigen beheer een webcrawler mensenhandel ontwikkeld.[42] Naast 'webcrawlers' wordt er ook gebruikgemaakt van 'webscrapers' die vergaarde – en al dan niet nader geselecteerde – gegevens downloaden op computerservers[43] (Oerlemans, 2017).

Het gebruik van software voor geautomatiseerde online gegevensvergaring draagt (in potentie) bij aan het meer efficiënt en effectief online verzamelen van gegevens (Koops, 2013; Oerlemans, 2017). De werking van deze software berust op algoritmen die bepalen op welke wijze zoekresultaten voor de gebruiker worden gegenereerd, geordend en gerangschikt (Klaar, 2022). Dit wordt ook wel datamining genoemd (zie ook Brinkhoff, 2017; Gritter, 2018). Door gebruik te maken van software kunnen (in de regel) heel veel bronnen tegelijkertijd worden bevraagd, geordend en gevisualiseerd. Dit is technisch gezien een zich (in potentie oneindig) herhalend zoek- en verwerkingsproces[44] (Klaar, 2022).

Een relevante vraag is wat het gebruik van software voor online gegevensvergaring voor gevolgen heeft voor de mate waarin sprake is van een meer dan geringe inbreuk op de privacy van burgers. Hierover wordt in de literatuur verschillend geoordeeld. Diverse auteurs betogen dat het gebruik van software voor geautomatiseerd vergaren al snel leidt tot een grote(re) inbreuk op iemands persoonlijke levenssfeer (zie Brinkhoff, 2017; Koops, 2013; Stol & Strikwerda, 2018). Feenstra (2018) hanteert een ander perspectief en wijst erop dat het gebruik van software niet per definitie een grotere inbreuk op iemands persoonlijke levenssfeer oplevert, omdat 1) er naast ruimer ook specifieker onderzoek kan worden gedaan,[45] en 2) er met dergelijke software (over het algemeen) geen contact met personen wordt aangegaan om bijvoorbeeld toegelaten te worden.

42 Zie de brief van de minister van Justitie & Veiligheid aan de Tweede Kamer van 18 november 2020 over opsporing en vervolging mensenhandel.

43 Volgens Klaar (2022) zijn er vooralsnog geen aanwijzingen dat er webscrapers in het kader van de opsporing worden ingezet.

44 Zie voor verdere technische aspecten het artikel van Klaar (2022).

45 Klaar (2022) geeft aan dat de configuratie van webcrawlers (op termijn) een steeds specifieker 'sleepnet' toelaten, wat maakt dat de inbreuk op de persoonlijke levenssfeer geringer wordt.

Met andere woorden: het gebruik van dergelijke software kan volgens Feenstra (2018) in de regel plaatsvinden op algemeen taakstellende artikelen.

Voor deze discussie is het van belang om ook het onderscheid tussen intelligence en opsporing erbij te betrekken. Indien door middel van software gegevens worden vergaard over burgers die niet worden verdacht van een misdrijf – bijvoorbeeld door sociale media te scannen met het oog op mogelijk opruiende berichten – dan is het de vraag of de grens van een meer dan geringe inbreuk eerder wordt bereikt. Ook op deze vraag wordt in de literatuur geen eenduidig antwoord gegeven. Oerlemans (2017) redeneert in de richting van een meer dan geringe inbreuk, terwijl Gritter (2018) stelt dat dergelijke vormen van monitoring zijn te beschouwen als een repressieve controle – vergelijkbaar met een alcoholcontrole in de fysieke wereld – die geen specifieke wettelijke grondslag nodig heeft.[46]

> *'Het door de politie ongericht binnenhalen van grote hoeveelheden data in het kader van repressieve controle raakt ontegenzeggelijk indringende aspecten van de privacy, maar dat betekent niet per se dat buiten de begrenzing van artikel 3 Politiewet 2012 wordt gehandeld.'* (Gritter, 2018: 114)

Kortom: er worden verschillende redeneerlijnen gevolgd. Deze redeneerlijnen kunnen naar ons idee naast elkaar bestaan, omdat de inbreuk van het gebruik van software op de persoonlijke levenssfeer van personen afhankelijk is van de precieze wijze waarop de software wordt gebruikt. Hoe wordt de software ingesteld en hoe worden de automatisch vergaarde gegevens vervolgens onderzocht (zie Klaar, 2022)? Naarmate er minder specifiek wordt gezocht, er meer privacygevoelige gegevens worden vergaard en de betreffende gegevens minder publiek toegankelijk zijn, is er eerder sprake van een meer dan geringe inbreuk op de persoonlijke levenssfeer. Dit moet per geval worden beoordeeld.

Duidelijk is in ieder geval wel dat het huidige juridische kader niet voorziet in een specifieke wettelijke grondslag voor geautomatiseerde online gegevensvergaring. Dit is volgens diverse auteurs wel nodig (Brinkhoff, 2017; Lodder & Schuilenburg, 2016; Oerlemans, 2017; Stol & Strikwerda, 2018). In het gemoderniseerde Wetboek van Sv wordt dit niet opgelost (zie ook paragraaf 7.3). Met de (uitwerking van de) nieuwe bevoegdheid voor online gegevensvergaring ontstaat er vermoedelijk meer houvast, maar de vertaling naar het gebruik van software stelt opsporingsambtenaren en gezagsdragers nog steeds voor uitdagingen (Klaar, 2022).

---

46 Behalve wanneer sprake is van omvangrijke gegevensvergaring over personen waarmee een meer dan geringe inbreuk wordt gemaakt op de persoonlijke levenssfeer. Overigens benadrukt Gritter (2018) dat het privacyvraagstuk bij automatische online gegevensvergaring meer betrekking heeft op het verder verwerken en bewaren van de vergaarde gegevens dan op de vergaring zelf. En dan is de Wpg van toepassing.

2.9 Samenvattend: een 'tijdelijke' noodoplossing

Online gegevensvergaring heeft betrekking op het zoeken, vinden en overnemen van gegevens uit internetbronnen. Dit hoofdstuk heeft duidelijk gemaakt dat het juridisch kader voor online gegevensvergaring moet worden gebaseerd op wetgeving die oorspronkelijk niet is bedoeld voor politiewerk op het web. Dit heeft als consequentie dat wetgeving die is gemaakt voor politiewerk in de fysieke wereld moet worden 'vertaald' naar politiewerk op het web. Deze vertaling gaat gepaard met obstakels, tekortkomingen en discussies en moet worden beschouwd als een tijdelijke noodoplossing, in afwachting van een specifieke juridische grondslag voor wat betreft de opsporing in het gemoderniseerde Wetboek van Sv.[47] Deze tijdelijke noodoplossing is echter niet zo tijdelijk, want deze wordt al twee decennia gebruikt en er moet nog tot minimaal 2026 een beroep op worden gedaan.

In dit hoofdstuk is op basis van (juridische) literatuur de vertaalslag gemaakt van wetgeving voor de fysieke wereld naar de digitale wereld. Het juridisch kader dat op basis hiervan is ontstaan, wordt in tabel 2.1 samengevat.

Tabel 2.1. Samenvatting juridisch kader

Activiteit	Wettelijke basis
Online gegevensvergaring met een niet-strafvorderlijk doel met een geringe inbreuk op grondrechten van betrokkenen	Art. 3 Pw
Niet stelselmatige online gegevensvergaring ten behoeve van opsporing	Art. 3 Pw of art. 141/142 Sv
Stelselmatige online gegevensvergaring ten behoeve van opsporing zonder interactie met de verdachte(n)	Art. 126g Sv of art. 126j Sv
Stelselmatige online gegevensvergaring ten behoeve van opsporing met interactie met de verdachte(n)	Art. 126j Sv

Aanvullend op deze tabel zijn twee opmerkingen van belang:

1. Het gebruik van een onderzoeksprofiel kan plaatsvinden op basis van zowel algemeen taakstellende bepalingen als bijzondere opsporingsbevoegdheden (in dat geval art. 126j Sv). Het gaat om de vraag hoe het onderzoeksprofiel wordt gebruikt en waarin dit gebruik resulteert. Indien het onderzoeksprofiel wordt gebruikt om toegang te verkrijgen tot afgeschermde internetbronnen komt stelselmatigheid snel in beeld, omdat er veelal een meer dan geringe inbreuk op de privacy van betrokkenen wordt gemaakt. Dit komt niet alleen of zozeer door het beeld dat wordt verkregen van bepaalde aspecten van iemands leven, maar ook en vooral doordat burgers niet of in mindere mate kunnen voorzien dat opsporingsambtenaren in dergelijke

47 Voor online gegevensvergaring met een niet-strafvorderlijk doel verandert de situatie niet, al hebben we van respondenten begrepen dat hierop ook actie wordt ondernomen. Een bijkomende vraag is in welke mate de nieuwe bevoegdheid in de opsporing de bestaande onduidelijkheden 'oplost'. Zie hiervoor ook par. 7.3.

bronnen gegevens over hen verzamelen. Dit is in open bronnen in meerdere mate het geval.

2. Het gebruik van software voor het geautomatiseerd online vergaren van gegevens kan plaatsvinden op basis van zowel algemeen taakstellende bepalingen als bijzondere opsporingsbevoegdheden. Wederom geldt: het gaat om de vraag hoe de software wordt gebruikt en waarin dit gebruik resulteert. Het hangt af van hoe de software wordt ingesteld en hoe de gecrawlde gegevens vervolgens worden onderzocht. Naarmate er minder specifiek wordt gezocht (groter 'sleepnet'), er meer privacygevoelige gegevens worden vergaard en de betreffende gegevens minder publiek toegankelijk zijn, is er eerder sprake van een meer dan geringe inbreuk op de privacy van betrokken personen.

Tot zover het juridische kader, dat ook al enig inzicht geeft in de wijze waarop online gegevens kunnen worden vergaard. Het volgende hoofdstuk heeft een empirisch karakter en geeft op hoofdlijnen weer hoe het online vergaren van gegevens binnen de politieorganisatie is ingebed. Dit is de opstap naar de hoofdstukken over OSINT en internetrechercheren.

3 Online gegevensvergaring: hoofdlijnen

Dit hoofdstuk is bedoeld als een – op het empirisch onderzoek gebaseerde – inleiding op het online vergaren van gegevens door de politie. We gaan achtereenvolgens in op de opkomst van online gegevensvergaring binnen de politieorganisatie, het onderscheid tussen intelligence en opsporing, de niveaus van expertise, de organisatie en de samenwerking binnen de politieorganisatie.

3.1 Opkomst van online gegevensvergaring

Gedurende dit onderzoek hebben wij met ruim veertig politiemensen gesproken over OGG binnen de politie. In deze gesprekken is ook aan de orde gekomen hoe respondenten met OGG in aanraking zijn gekomen. Op basis hiervan kunnen we, aangevuld met literatuur, op hoofdlijnen reconstrueren hoe dit vakgebied zich in de afgelopen twintig jaar heeft ontwikkeld. Deze reconstructie is niet compleet, maar geeft wel een indruk.

Beginnen & verkennen: eind jaren negentig – 2010
Het begin van OGG gaat terug tot het einde van de jaren negentig. Het internet (Web 1.0) staat nog niet zo lang in de steigers en binnen de politie begint de interesse in het gebruik van internet voor met name opsporingsdoeleinden op gang te komen. Hiervoor wordt het begrip 'Internet Rechercheren' geïntroduceerd. Er is een landelijk project en de eerste twaalf rechercheurs volgen een opleiding Internet aan de toenmalige rechercheschool in Zutphen.[48]

> *'Ik ben met OGG in aanraking gekomen in 1998 toen ik hoofd van de Infodesk werd. Toen was er een landelijk project, dat heette Internet Rechercheren. We kregen computers die op het netwerk waren aangesloten. Daarmee gingen politiemensen een beetje hobbymatig het internet verkennen.'* (33)

De internetrechercheurs van destijds zijn 'hobbyisten' die vanuit de politieorganisatie de eerste stappen zetten in het beroepsmatig gebruik van het internet. Het internet geeft hen toegang tot tal van (nieuwe) open bronnen, zoals databanken en gegevens

48 Zie ook https://www.digitaleopsporing.nl/internet-rechercheren-heet-nu-osint/

over bedrijven (Van Treeck & Stol, 2000). Om veilig onderzoek op het internet te kunnen doen, wordt in 2004 in het regiokorps Gelderland-Zuid het internet Research Network (iRN) ontwikkeld.[49] Dit is een gesloten infrastructuur waarmee politiemensen veilig en anoniem gebruik kunnen maken van het internet. Deze betekenisvolle stap neemt niet weg dat aan het begin van het nieuwe millennium het aantal politiemensen dat online gegevens vergaart ten behoeve van opsporing nog zeer klein is.

Pionieren & toenemende bewustwording: 2010-2017
Op basis van de interviews hebben we de indruk dat de interesse voor OGG binnen de politie omstreeks 2010 begint toe te nemen: het wordt breder opgepakt. Verschillende respondenten zijn in deze periode binnen de politie met OGG begonnen.

> *'Ik ben er zo'n tien jaar geleden mee in aanraking gekomen, via een internettraining van Fox-IT. We werden wel braaf met zijn allen naar een dure opleiding gestuurd, maar er werd niet gestuurd op de opvolging ervan. Toen ik na de opleiding vroeg of ik aan de slag mocht op een iRN computer was de reactie "nee, we hebben genoeg andere dingen te doen".'* (21)

> *'In die periode bestond het begrip OSINT volgens mij nog niet. En internetrechercheren werd ook nog niet veel gebruikt. Ja, dat waren mensen die iets met onderzoek en internet hadden. Bepaalde eenheden (toentertijd regio's, red.) waren wat verder, maar het waren toch vooral een paar pioniers die ermee bezig waren.'* (29)

> *'Een jaar of zeven geleden is mijn OSINT werk begonnen. Toen was het allemaal nog redelijk klein. Er was veel te halen uit open bronnen, maar we waren er nog nauwelijks mee bezig. Alleen de "gekkies".'* (37)

De groeiende aandacht voor OGG in deze periode moet naar ons idee worden begrepen in het licht van de opkomst van sociale media die in deze periode plaatsvindt. Web 1.0 verandert in Web 2.0 (zie paragraaf 1.1). Op het internet is meer voor de politie te halen en de noodzaak om online gegevens te vergaren groeit ook. Tegelijkertijd geven respondenten aan dat OGG in deze periode (nog) wordt gekenmerkt door 'pionieren'. Er wordt wel geïnvesteerd in opleidingen en trainingen, onder andere in het kader van het project 'Gebruik Open Bronnen Internet', maar in de praktijk zakt de inzet van OGG ook snel weer weg. In een artikel in het politieblad *Blauw* uit 2012 wordt geconstateerd dat het gebruik van open bronnen op het internet nog geen gemeengoed is binnen de politie, maar hierin wel langzaam verandering komt (Streefkerk, 2012).

In 2012 vindt de overgang naar de nationale politieorganisatie plaats. OGG is als vakgebied niet of nauwelijks zichtbaar in het Inrichtingsplan (Politie, 2012). De term 'in-

49 https://www.commit-nl.nl/universities/politie-gelderland-zuid

ternet' komt af en toe voor, maar vooral in relatie tot communicatie en dienstverlening. Het begrip 'open bronnen' wordt een enkele keer gebruikt. In de eerste plaats in het kader van het Real Time Intelligence Center (RTIC): zij dienen open bronnen te gebruiken bij hun taak om de politie-eenheden in het veld 24/7 van relevante operationele informatie te voorzien (zie ook paragrafen 3.4 en 4.1). Daarnaast wordt er bij de afdeling Landelijke Informatie van de Dienst Landelijke Informatieorganisatie (DLIO) van de Landelijke Eenheid (LE) een team Open Bronnen ingericht.[50]

> *'In 2012 waren het zeven mensen inclusief mijzelf en de teamleider. We hadden alle zeven een iRN computer. En in die tijd pakten we alle OSINT zaken op. Zo is het begonnen. Dat waren zware jaren, we dachten toen "hier moeten we echt iets mee als politie".'* (38)

De zinsnede 'hier moeten we echt iets mee als politie' geeft een beeld van de mate waarin OGG in 2012 binnen de politie is ingebed: het staat (nog steeds) in de kinderschoenen. Ondertussen neemt de externe noodzaak toe. In 2012 loopt een via Facebook gepubliceerde uitnodiging voor een verjaardagsfeest in Haren uit de hand: via een sneeuwbaleffect melden duizenden mensen zich aan. Het verwijderen van het 'event' op Facebook haalt niets meer uit. Het feest is onder de noemer van Project X inmiddels gekaapt en wordt een hype op sociale media. Er komen duizenden mensen naar Haren en er ontstaan rellen. Naar aanleiding van de evaluatie zegt de minister van Veiligheid & Justitie aan de Tweede Kamer toe dat sociale media een vast onderdeel van het politiewerk worden.[51]

In de jaren na de vorming van de nationale politieorganisatie is OGG in eerste instantie vooral een (landelijk) thema binnen het domein van intelligence. Mede tegen die achtergrond wordt de term OSINT ook meer gebruikt, zo geven respondenten aan. In 2015 verschijnt er vanuit de portefeuille Intelligence een position paper over OSINT in de informatieorganisatie (Politie, 2015). In dit document wordt geconstateerd dat de regionale informatieorganisaties en landelijke informatieorganisatie nog niet voldoende zijn toegerust om OSINT onderdeel te laten zijn van de dagelijkse werkzaamheden. In het position paper wordt uitgewerkt welke taken op het gebied van OSINT waar binnen de informatieorganisatie moeten worden uitgevoerd. Het uitgangspunt hierbij is dat gegevens uit open bronnen precies dezelfde functie hebben als gegevens uit traditionele bronnen: bijdragen aan intelligence ten behoeve van de sturing op en uitvoering van politiewerk. OSINT moet daarom worden geïntegreerd in de informatiepro-

50 In het Inrichtingsplan zijn drie taken voor dit team benoemd: 1) monitoren van (criminele) dreigingen gericht tegen personen, objecten en evenementen (de openbare orde) via open bronnen, 2) leveren van een bijdrage aan het actuele operationele beeld ten behoeve van de informatiepositie van het RTIC en zorgen voor het uitleren van methoden en technieken aan het RTIC, en 3) verrichten van werkzaamheden in het voorbereidende proces van bewaken en beveiligen, opsporing en handhaving.

51 Zie hiervoor de brief van de minister van Veiligheid en Justitie aan de Tweede Kamer naar aanleiding van het rapport van de commissie-Haren van 28 maart 2013.

cessen. Dit veronderstelt dat iedere medewerker binnen de informatieorganisatie moet beschikken over de vaardigheden om OSINT toe te passen binnen het werkproces, zo wordt aangegeven. Daarnaast moet in de regionale informatieorganisaties (specialistische) expertise, coördinatie en een voorziening voor opschaling worden ingericht. Dit wordt in het document de 'OSINT taak' genoemd. De landelijke informatieorganisatie voorziet, aanvullend op de eenheden, in diepte-expertise ontwikkeling en landelijke operationele coördinatie. De hoofdlijnen van het position paper komen ook terecht in het landelijke werkingsdocument van de informatieorganisatie, dat kan worden beschouwd als een nadere uitwerking van het Inrichtingsplan. Er komt een landelijk OSINT project om de gewenste ontwikkeling 'een duwtje in de rug te geven' (respondent 42). Binnen de (nieuw ingerichte) informatieorganisaties wordt geïnvesteerd in het professionaliseren van mensen en middelen. Dit betreft onder andere het aanschaffen van technologie voor online monitoring voor zowel het RTIC als de bredere informatieorganisatie.

Eind 2015 wordt er tevens een landelijk programma sociale media gestart met sociale media in de opsporing als een van de deelprojecten. Het betreft dan het vergaren van gegevens via sociale media en sociale media als middel in het kader van opsporingscommunicatie. In 2016 wordt een position paper over sociale media in de opsporing gepubliceerd waarin, op basis van eigen onderzoek, wordt ingegaan op de stand van zaken (Politie, 2016). Er wordt geconstateerd dat binnen de politieorganisatie het besef groeit dat sociale media een grote rol gaan spelen in de toekomst van de opsporing (zie ook Smilda & De Vries, 2017). Tegelijkertijd geven de auteurs aan dat het gebruik van sociale media in de opsporing niet is georganiseerd in de werkprocessen. De eenheden zijn vooral afhankelijk van 'zelfgemaakte' specialisten en pioniers op het gebied van sociale media die zich inzetten om collega's enthousiast te maken en het gebruik binnen de politieorganisatie te borgen. Met betrekking tot cultuur wordt opgemerkt dat vooral leidinggevenden vasthouden aan de traditionele aanpak van opsporingsonderzoeken en hierdoor het gebruik van sociale media in de opsporing remmen.

Professionaliseren & verbreden: vanaf 2018
In 2017 nemen enkele internetpioniers van verschillende eenheden het initiatief om de werkzaamheden op het gebied van OGG te ordenen. Deze behoefte vloeit voort uit de toenemende differentiatie in werkzaamheden: van eenvoudige werkzaamheden tot zeer complexe (diep-specialistische) werkzaamheden. Ze gaan een paar dagen met elkaar 'op de hei' en ontwikkelen een model waarin onderscheid wordt gemaakt tussen vijf niveaus waarop werkzaamheden op het gebied van OGG worden verricht: het OGG5 model (zie paragraaf 3.3). Met dit model wordt ook de term Online Gegevens Garing (OGG) geïntroduceerd om zodoende de domeinen van intelligence (OSINT) en opsporing (internetrechercheren) te overstijgen.

> *'De top had geen idee van OSINT. Dat er veel verschil is, van basiswerkzaamheden tot diepgaande en complexe onderzoeken met aliassen. Er was behoefte om het meer op*

te splitsen. Daar is toen OGG5 uitgekomen. Dat model is erg behulpzaam voor de politieorganisatie, maar ook daarbuiten. Onder andere de KMar (Koninklijke Marechaussee, red.) en Defensie hebben het model ook geadopteerd.' (38)

Respondenten signaleren dat OGG vanaf 2017-2018 meer vaste voet aan de grond krijgt. Binnen de informatieorganisatie zijn de eenvoudige werkzaamheden op het gebied van OSINT breder ingebed geraakt en binnen de opsporing begint dit voor wat betreft internetrechercheren ook op gang te komen, al is het zeker nog geen standaardhandeling voor de gemiddelde rechercheur (zie Feenstra, 2018). Daarnaast begint er op het gebied van OGG beweging te komen in de basisteams, in het bijzonder door het ontstaan van een nieuwe rol: de digitaal wijkagent (zie Boelens & Landman, 2021; zie ook paragraaf 3.4). Deze ontwikkelingen nemen niet weg dat respondenten spreken van 'golfbewegingen': naar aanleiding van incidenten of successen neemt de aandacht toe, maar daarna verslapt deze in de regel ook weer. Daarnaast is er – in het bijzonder in de informatieorganisatie – behoefte aan meer eenduidigheid op het gebied van middelen. Om die reden ontstaat er in 2020 een nieuw landelijk OSINT-project om het vakgebied in de informatieorganisatie te professionaliseren.[52]

'Wij zijn de tweede stuurgroep OSINT. De eerste stuurgroep was een paar jaar geleden. Toen lag de nadruk op het opzetten van een community op het gebied van OSINT, verkrijgen van hard- en software, introduceren van de OGG niveaus en opleidingen. Dat hebben we twee jaar gedaan. Toen hebben we gezegd: het moet van de lijn zijn. We hebben als uitgangspunt genomen: het is geen apart vakgebied, maar een vaardigheid die iedere intelligence medewerker moet hebben. Er is na het eerste project een tijdje geen project geweest. Na verloop van tijd kwamen er toch nieuwe vragen op landelijk niveau. Vooral de behoefte om door te ontwikkelen op technologie. Maar ook voor OGG niveau 3 en 4. Die hebben hard- en software nodig, maar het liefst wel een standaard. Dat de ICT organisatie ook weet: dit is nodig. Daarom zijn we daarmee aan de slag gegaan.' (36)

Vrijwel alle respondenten wijzen erop dat de meer recente gebeurtenissen op het gebied van openbare orde – demonstraties, maar vooral de avondklokrellen – ervoor hebben gezorgd dat op strategisch niveau meer belang wordt gehecht aan OGG. Hierdoor gaan er deuren open in termen van onder andere het werven van meer specialisten op het gebied van OGG.[53]

'Maatschappelijk ongenoegen zorgt wel voor een versnelling. Wij hebben van de eenheidsleiding nu goedkeuring om 9 mensen aan te nemen op niveau 4 (zie paragraaf 3.3, red.).' (37)

52 In de tweede helft van 2021 zijn de portefeuilles opsporing en GGP ook aan het landelijke project verbonden.
53 Zie ook https://nos.nl/artikel/2414236-avondklokrellen-hebben-politiewerk-blijvend-veranderd

Kortom: het vakgebied OGG heeft in de afgelopen twintig jaar binnen de politieorganisatie aan belang gewonnen. Steeds meer politiemensen – vooral in de informatieorganisatie – 'doen er iets mee', maar tegelijkertijd is het zeker nog geen gemeengoed.

3.2 OGG = OSINT + internetrechercheren

Tijdens de oriëntatiefase van het onderzoek viel het ons op dat er verschillende begrippen in omloop zijn voor OGG ten behoeve van politiewerk. In de interviews hebben we respondenten gevraagd naar hun perspectief op de terminologie.

Op basis van de interviews constateren wij dat de diversiteit in terminologie die binnen de politie wordt gebruikt, samenhangt met het onderscheid tussen intelligence en opsporing. Respondenten benadrukken dat dit onderscheid meer verwijst naar het doel dat met het online vergaren van gegevens wordt beoogd dan naar de methoden waarmee de gegevens worden vergaard.[54]

> *'De manier waarop je werkt, is grotendeels hetzelfde. De wijze waarop je zoekt, de methoden die je inzet en deels ook de tools die je gebruikt. Het grootste verschil zit in de bril die je opzet. Waarnaar ben je op zoek? Intel zit meer aan de voorkant. Opsporing gaat uit van een strafbaar feit. We proberen met internetrechercheren een plusje te vinden. We doen vanuit de opsporing geen onderzoek naar een thema of monitoren niet aan de voorkant of er onrusten zijn. Maar op het moment dat er iets is gebeurd, dan gaan we onderzoeken. We onderzoeken vaak een persoon, een verdachte of meerdere verdachten.'* (21)

Het online vergaren van gegevens ten behoeve van intelligence is volgens respondenten gericht op het monitoren van trends en ontwikkelingen met betrekking tot een bepaald veiligheidsthema (zie ook hoofdstuk 4). Er is dan (nog) geen sprake van specifieke strafbare feiten die worden onderzocht; het gaat om de bijdrage aan het creëren van een informatiepositie die inzicht geeft in wat er gebeurt en eventueel kan gaan gebeuren. Dit is sturingsinformatie, die wordt opgenomen in 'informatieproducten' (zoals een veiligheidsbeeld of een informatierapport).

> *'Vanuit intelligence is het altijd de bedoeling dat je gaat voor sturings- of ondersteuningsinformatie. Het doel van opsporing is waarheidsvinding. Dat zijn twee verschillende dingen.'* (30)

Opsporing vindt plaats in het kader van een verdenking van een *gepleegd* strafbaar feit en is – zoals bovenstaande respondent benadrukt – gericht op het verzamelen van (steun)bewijs ten behoeve van waarheidsvinding. De gegevens die in het kader van opsporing worden verzameld, worden geregistreerd in SUMM-IT en eventueel vastge-

54 Zie ook Dubberley, Koenig & Murray (2020).

legd in een proces-verbaal (zie ook paragraaf 5.2). In het kader van opsporing kan – na toestemming van de officier van justitie – gebruik worden gemaakt van bijzondere opsporingsbevoegdheden, terwijl het online vergaren van gegevens in het kader van intelligence dient plaats te vinden op basis van art. 3 Pw (zie paragraaf 2.7).

In verschillende interviews hebben respondenten benadrukt dat in de praktijk intelligence en opsporing in elkaar kunnen overvloeien (zie ook Duijn, 2011; Sampson, 2017). Bijvoorbeeld: op het ene moment monitor je op sociale media het sentiment en de tendens rondom de avondklok in een bepaalde stad en op het andere moment lees je een bericht van een persoon dat neigt naar opruiing (zie ook paragraaf 4.5). Op het moment dat een persoon nader wordt onderzocht, gaat intelligence over in opsporing. Omdat er bij nader onderzoek veelal ook meer inbreuk op iemands persoonlijke levenssfeer wordt gemaakt, kunnen bijzondere opsporingsbevoegdheden nodig zijn.

Dan naar de terminologie. Voor online gegevensvergaring in het kader van opsporing is vanaf het begin de term 'internetrechercheren' gebruikt (zie paragraaf 3.1). In het kader van intelligence is binnen de politie – na verloop van tijd – de term OSINT gebruikelijk geworden. OSINT is een meer algemene (maatschappelijke) term die wordt gebruikt om de discipline van 'online openbronnenonderzoek' te duiden (zie ook Higgins, 2021). Om die reden zijn sommige respondenten van mening dat OSINT de overkoepelende term zou moeten zijn.

> *'OSINT is buiten de politie gewoon OSINT. Alleen binnen de politie zeggen we: OSINT is intelligence. Maar dat is niet het werk wat ik doe, want wat ik doe, is internetrechercheren. De 'i' is binnen de DRIO intelligence en binnen de recherche-omgeving is de 'i' internetrechercheren.'* (24)

> *'Ze zijn het OGG gaan noemen, omdat OSINT verwijst naar het intelligence gedeelte. Ze (beleidsbepalers, red.) vinden het ook een akelig woord, een beetje heimelijk. OGG klinkt wat vriendelijker. Maar het is eigenlijk OSINT, dus ik blijf dat zo noemen.'* (34)

Andere respondenten zijn van mening dat OSINT geen passende aanduiding is voor het online verzamelen van gegevens voor opsporingsonderzoek, omdat de 'I' verwijst naar intelligence.

> *'Die term (OSINT, red.) vind ik grotendeels misplaatst. Intelligence vind ik echt het genereren van sturingsinformatie en daar duiding op geven (…) Vandaar dat ze het geen OSINT willen noemen, maar online gegevens vergaring, ook in het nieuwe Wetboek van Strafvordering.[55] Je moet het een naampje geven, maar je doet veel meer dan vergaren, je moet het ook analyseren.'* (18)

55 Dit klopt overigens niet. In het (voorstel voor het) gemoderniseerde Wetboek van Sv wordt de volgende formulering gebruikt: het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen.

Kortom: in de praktijk is het gebruik van begrippen niet eenduidig. Zoals eerder aangegeven (zie paragraaf 1.2): wij gebruiken online gegevensvergaring (OGG) als overkoepelend begrip en hieronder vallen OSINT (intelligence) en internetrechercheren (opsporing). Wij zijn van mening dat dit het duidelijkst is. In de volgende paragraaf gaan we door op OGG.

3.3 Vijf niveaus van OGG

In paragraaf 1 van dit hoofdstuk is beschreven dat er binnen de politie in 2017 een indeling is gemaakt in vijf niveaus waarop het online vergaren van gegevens plaatsvindt. Hoewel dit initiatief destijds vanuit een landelijk project op het gebied van intelligence is ondernomen, is de betreffende indeling van toepassing op zowel de intelligence als de opsporing.[56] Zie tabel 3.1 voor het model.

Tabel 3.1. OGG5 model

	N1	N2	N3	N4	N5
Tijdsbesteding	Incidenteel	Structureel	Dagelijks	Fulltime	Onderzoeks-afhankelijk
Internetdiepte	Clearweb	Deepweb	Deepweb	Darkweb	Onderzoeks-afhankelijk
Uitvoering	Raadplegen, zoeken	Monitoren, onderzoeken	Onderzoeken, identificeren, coördineren, ondersteunen proces	Diepgaand onderzoeken	Wetenschappelijk onderzoeken
Onderzoeksvraag	Zoektermen	Eenvoudige zoekvragen	Meervoudige zoekvragen	Complexe informatievragen	Wetenschappelijke onderzoeksvragen
Bronbevraging	Geen alias	Algemeen alias	Thematisch alias	Complex alias	Onderzoeks-afhankelijk
Interactie	Geen	Geen	Passief	Actief	Onderzoeks-afhankelijk
Hardware	iRN-computer	iRN-computer	iRN-computer	Eigen programmatuur	Onderzoeks-afhankelijk
Tools	Vrij beschikbaar	Landelijk aangekocht	Landelijk aangekocht	Specialistisch	Onderzoeks-afhankelijk
Kennisoverdracht	Team	Afdeling (mentor)	Eenheid (meester)	(inter)nationaal	(inter)nationaal

Hoe hoger het niveau (dit geldt vooral voor 1 t/m 4), hoe complexer de werkzaamheden. Het onderscheid in niveaus valt niet samen met een onderscheid in functies, al is er wel een relatie. Degenen die werken op lagere niveaus zijn eerder generalisten, terwijl degenen die werken op hogere niveaus veelal operationeel specialisten zijn. Maar

56 Sommige respondenten zijn van mening dat het model minder bruikbaar is voor de opsporing. Binnen de digitale opsporing heeft men ook een eigen model dat een bredere invalshoek heeft dan online gegevensvergaring. Dit betreft een beroepsprofiel digitale opsporing (DO-5 model). In dit model wordt gebruikgemaakt van c.q. verwezen naar het OGG5 model voor wat betreft onderzoek op internet.

nogmaals: het valt er niet mee samen (zie ook paragraaf 3.5). Een generalist kan ook beschikken over de kennis & kunde om op OGG-niveau 4 te werken. Om het model te verhelderen, is er in de uitwerking van het model bij ieder niveau een praktijkvoorbeeld opgenomen. Deze praktijkvoorbeelden nemen wij hier over, zodat de inhoud van de tabel meer tot leven komt. Deze voorbeelden geven tevens een indruk van OGG-werkzaamheden.[57]

OGG-niveau 1
Een vrouw komt aan de balie aangifte doen van een gestolen laptop, die intussen op marktplaats te koop is gezet. De baliemedewerker verifieert het verhaal door de website marktplaats te openen met behulp van een iRN-pc. De medewerker vindt de aangeboden laptop en maakt van de advertentie een screenshot. Het screenshot en andere relevante online gegevens, zoals URL, naam/alias, emailadres en telefoonnummer neemt de medewerker op in het dossier.

OGG-niveau 2
Een slachtoffer doet melding van onvrijwillige seks na een afspraak via Facebook. De medewerker onderzoekt met behulp van een iRN-pc de online gegevens van de verdachte, op basis van de informatie die bij het slachtoffer bekend is, zoals roepnaam, Facebook-alias en profielfoto's. De medewerker onderzoekt en vergelijkt meerdere online en offline bronnen, om de online identiteit van de verdachte te koppelen aan een officiële (fysieke) identiteit. De medewerker legt zijn bevindingen vast voor het onderzoek en draagt deze over aan het onderzoeksteam.

OGG-niveau 3
Een medewerker houdt zich bezig met het thema voetbalvandalisme. Zijn alias als hardcore Feyenoordaanhanger is goed opgebouwd, met juiste foto's, vrienden en likes. Via een besloten Facebookgroep ontdekt hij dat er een knokpartij op het strand van Monster aanstaande is. De medewerker legt deze informatie inclusief beeldmateriaal vast en deelt de bevindingen onder andere met het Centraal Informatiepunt Voetbalvandalisme. Daarnaast bouwt de medewerker op basis van meervoudige query's een dashboard, zodat hijzelf en collega's op niveau 2 aanstaande ontwikkelingen en mogelijke incidenten rond de aangekondigde actie kunnen monitoren.

> *'Ik vind het onderscheid tussen niveau 2 en 3 het meest duidelijk. Niveau 4 wordt diffuser. Sommigen zeggen dat een virtual agent (VA) niveau 4 is.[58] Ik heb zelf het idee dat dit een andersoortig werkproces is. Dat gaat niet over hoe goed je bent met OSINT, maar dat is heimelijk werken.'* (36)

57 Opvallend is dat er in zowel de tabel als de voorbeelden niet wordt ingegaan op de bevoegdheden die worden gebruikt voor de uitvoering van activiteiten.
58 Op basis van de actieve interactie (zie tabel) is het aannemelijk dat een VA OGG niveau 4 is.

OGG-niveau 4
Een specialist op het gebied van bitcoins ontdekt, via haar complexe alias, dat er binnen de kring van CTER-verdachten op het deepweb wordt gesproken over een virus dat ransomware gaat verspreiden op overheidscomputers. Na diepgaand onderzoek ontdekt zij de vermeende locatie van een aantal betrokken IP-adressen, deze blijken grotendeels van één geolocatie te komen. De specialist legt de bevindingen vast en draagt deze over aan het landelijke CTER team, de Financial Intelligence Unit (FIU) en andere relevante partners. Ook deelt de specialist diens bevindingen en werkwijze op nationaal niveau, met andere collega's op niveau 4.

> *'N4 OGG zijn super specialisten. Die zijn ook in staat om op het deep web te werken en meer specialistische vragen te beantwoorden. Zij werken ook met query's om zo informatie van het internet af te halen. N5 is wetenschappelijk niveau. Ik weet niet of en waar die zijn binnen de politie. Ik denk dat die op projectbasis worden ingehuurd.'* (33)

OGG-niveau 5
OGG-niveau 5 is een 'afwijkend' niveau, omdat het gaat om medewerkers die geen operationele taken uitvoeren, maar die wetenschappelijk onderzoek verrichten naar internetfenomenen, zoals *deepfakes*. De medewerker vertaalt onderzoeksresultaten en implicaties hiervan naar de andere OGG-niveaus, draagt bij aan beleidsontwikkelingen en onderhoudt contact met onderzoeksinstituten en universiteiten. Een van de respondenten, die aan de wieg heeft gestaan van het OGG5 model, formuleert dit als volgt:

> *'Niveau 5 is gericht op expertise. De scheidslijn tussen executief en niet executief moet je heel helder houden. Je wilt geen oneigenlijke acties van een wetenschapper. Wij doen nu zaken met een promovendus. Die is in dienst van de politie, maar die heeft niets te maken met onze operationele opdrachten. Het wetenschappelijk onderzoek sluit wel aan bij onze werkelijkheid. Het gaat bijvoorbeeld om het categoriseren van reacties en accounts op Twitter, zodat wij kunnen inschatten wie een risico vormen voor verstoring van de openbare orde. Zo werkt het samen.'* (38)

We hebben geprobeerd te achterhalen hoeveel politiemensen op welk niveau werkzaam zijn. Dat is niet goed gelukt, omdat de niveaus niet op deze wijze worden gebruikt en er (dus) ook geen registraties van zijn. Voor zover er onderbouwde schattingen zijn, hebben die vooral betrekking op de informatieorganisatie. Deze schatting houdt in dat er landelijk gezien ongeveer 1500-2000 informatiemedewerkers op niveau 2 werken, enkele honderden op niveau 3 en tientallen op niveau 4. Voor de recherche geldt dat er niet of in mindere mate wordt uitgegaan van een algemeen basisniveau (zoals in de informatieorganisatie). De aanname van enkele respondenten is dat er vooral (mogelijk 100-150) medewerkers op niveau 3 en 4 werken. Bij al dit soort schattingen moet worden beseft dat het uitgangspunt dat eenieder neemt kan verschillen: de gevolgde

opleiding, het niveau dat iemand in het werk denkt te hebben of het niveau dat men in het werk aantoonbaar heeft op basis van activiteiten en kennis & kunde. Sommige respondenten benadrukken bijvoorbeeld dat iemand die op niveau 4 werkt scripts moet kunnen schrijven en dat zijn er zeker geen honderden binnen de politie.

3.4 Organisatie van OGG

Intelligence en opsporing zijn disciplines of domeinen, die ook neerslaan in werkprocessen. In de volgende twee hoofdstukken gaan we op ieder domein apart in. Alvorens dit te doen, is het van meerwaarde om op hoofdlijnen te beschrijven hoe OGG binnen de politieorganisatie is ingebed: waar kom je het in de organisatiestructuur tegen? Op basis van de interviews hebben we hier een indruk van gekregen, al is die vermoedelijk niet compleet. We gaan eerst in op de informatieorganisatie, dan op de rechercheorganisatie en ronden af met de basisteams. De nadruk ligt vooral op de regionale eenheden en in mindere mate op de LE.

Informatieorganisatie
Internetbronnen zijn voor de informatieorganisatie van groot en toenemend belang, zo geven diverse respondenten aan. In het verleden zijn (vrijwel) alle medewerkers van de informatieorganisatie opgeleid ten behoeve van eenvoudige OSINT-werkzaamheden. Dit was onderdeel van de landelijke standaardisering en professionalisering die vanaf 2016 is ingezet (zie paragraaf 3.1). Mede vanwege de brede inbedding van OSINT-werkzaamheden hebben alle medewerkers van de informatieorganisatie een executieve status gekregen. Het online verzamelen van gegevens is een vorm van onderzoek en verschilt van het raadplegen van politiesystemen (met bestaande gegevens).

> *'OSINT is ook de reden dat de intelligence medewerker executief is geworden. Je bent toch informatie aan het verzamelen. Je gaat zelf inwinnen. Dat is anders dan het werken met al bestaande politiegegevens.'* (36)

De brede inbedding impliceert dat het online vergaren van gegevens in (vrijwel) de gehele informatieorganisatie plaatsvindt.[59] Dit betreft in het bijzonder de afdeling Regionale Informatie (RI) waarvan het RTIC en het Regionaal Informatieknooppunt (RIK) een onderdeel zijn. 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). Het RIK verzorgt informatiecoördinatie op thema's die landelijk zijn geprioriteerd, zoals cybercriminaliteit, ondermijning en mensenhandel. Ten behoeve van de intelligencepositie op deze thema's wordt in meer of mindere mate een beroep gedaan op OSINT (zie ook hoofdstuk 4). Daarnaast is OSINT

59 Zoals eerder aangegeven (zie par. 3.1): de Landelijke Eenheid heeft als enige eenheid in de inrichting een apart team 'open bronnen'. Er zijn in sommige eenheden wel informele teams, wat wil zeggen dat specialisten uit verschillende organisatieonderdelen in de praktijk een team vormen.

ingebed in de afdeling informatieknooppunten. Deze afdeling bestaat uit verschillende (lokaal verankerde) informatieknooppunten (IK's) die zijn gekoppeld aan de districten en diensten.[60] Ten behoeve van de informatieproducten die aan districten en diensten worden geleverd, wordt in meer of mindere mate gebruikgemaakt van OSINT (zie ook hoofdstuk 4). Zo levert het IK van de Dienst Regionale Recherche (DRR) onder andere informatieproducten voor de weging, voorbereiding en sturing van opsporingsonderzoeken (zie ook Inspectie Justitie & Veiligheid, 2018). Ten behoeve van deze informatieproducten worden (geregeld) ook online gegevens vergaard. Tot slot kan worden opgemerkt dat ook de organisatieonderdelen die inlichtingen verzamelen, gebruikmaken van open bronnen. Dit betreft de Regionale Inlichtingendienst (ID Wiv[61]) die inlichtingen verzamelt in opdracht van de Algemene Inlichtingen en Veiligheidsdienst (AIVD) en de 'eigen' inlichtingenteams van de politie: Team Criminele inlichtingen (TCI) en Team Openbare Orde Inlichtingen (TOOI).[62]

Bij het bovenstaande moet worden opgemerkt dat de inrichting van de informatieorganisaties binnen de politie sterk in ontwikkeling is, zo komt uit de interviews naar voren. Ten tijde van de vorming van de nationale politieorganisatie zijn de regionale informatieorganisaties sterk geografisch (in)gericht. In verschillende eenheden is in de afgelopen jaren een meer thematische (in)richting dominant geworden. Dit wil zeggen dat er thematische teams, clusters of *squads*[63] zijn ingericht – zoals ondermijning (of specifieker: drugs), cybercriminaliteit, contraterrorisme en radicalisering (CTER) en openbare orde en veiligheid – die verantwoordelijk zijn voor het opbouwen van informatieposities, het maken van daarop gebaseerde informatieproducten en het beantwoorden van allerlei (specialistische) informatievragen van andere organisatieonderdelen. OSINT is, net als in de oude structuur, verankerd in verschillende organisatieonderdelen. Ten behoeve van de ontwikkeling van vakgebieden – zoals OSINT – zijn er daarnaast groepen die dwars door de thema's heen werken. Kortom: een soort matrixstructuur. Een van onze respondenten is 'chapter lead' op het gebied van OSINT.

> *'Ik zie mezelf als een vakgroepleider die ervoor zorgt dat de kennis en kunde op het gebied van OSINT breder wordt ingebed. Het doel is de kennis en kunde op het gebied van OSINT van iedere medewerker te verhogen.'* (31)

Naast de oriëntatie op intelligence zijn er eenheden waarin de informatieorganisatie de recherche ondersteunt met het online vergaren van gegevens in opsporingsonderzoeken. Zoals eerder aangegeven: de methoden en technieken zijn op hoofdlijnen hetzelf-

60 Deze knooppunten worden ook wel gezien als de frontoffice van de informatieorganisatie.
61 Wiv verwijst naar de Wet op de inlichtingen- en veiligheidsdiensten. Dit organisatieonderdeel van de politie werkt, net als de AIVD en de Militaire Inlichtingen- en Veiligheidsdienst, op basis van deze wet.
62 Zie ook Terpstra et al. 2021 vanuit het perspectief van het basisteam.
63 Een squad is onderdeel van een organisatiemodel dat ooit door Spotify is geïntroduceerd. Een enkele DRIO gebruikt dit model voor de inrichting van de eigen organisatie.

de, het gaat om een verschil in doeleinden en (mogelijk) bevoegdheden. Er zijn echter ook eenheden die in de afgelopen jaren hebben gekozen voor een strikte(re) scheiding tussen intelligence en opsporing.

> *'In deze eenheid is ervoor gekozen om er wat meer rigide in te zitten. Wie iets in een PV zet, doet opsporing. Dat doen de mensen van de informatieorganisatie in principe niet. Maar dat verschilt per eenheid.'* (21)

> *'Er zit een heel groot grijs gebied tussen intelligence en opsporing. Voor sommige eenheden stroomt het in elkaar over en andere eenheden maken er echt een organisatorisch onderscheid in.'* (27)

> *'Tussen eenheden zijn er veel verschillen met betrekking tot de capaciteit voor de opsporing (voor online gegevens verzamelen, red.). Sommige DRIO's ondersteunen in onderzoeken. Andere DRIO's doen dit niet of veel minder. Daar is het steviger binnen de recherche georganiseerd.'* (36)

De consequentie van een strikt onderscheid tussen intelligence en opsporing is vooral dat medewerkers van de informatieorganisatie niet worden ingezet voor opsporingswerkzaamheden. Deze striktheid doet zich vooral voor in de eenheden die internetrechercheren in de afgelopen jaren stevig(er) hebben verankerd binnen de recherche. Dit wil zeggen dat er op diverse plekken binnen de recherche specialisten zijn op het gebied van internetrechercheren. In dat geval is men minder afhankelijk van de informatieorganisatie voor inzet ten behoeve van opsporing. Er zijn echter ook eenheden waar nauwelijks specialisten op het gebied van internetrechercheren aanwezig zijn, dan wel dit vakgebied nog volop in opbouw is. In deze eenheden worden medewerkers van de informatieorganisatie geregeld ingezet in of ten behoeve van opsporingsonderzoeken.

Rechercheorganisatie

De inbedding van internetrechercheren binnen de recherche verschilt tussen eenheden meer dan de inbedding van OSINT binnen de informatieorganisatie, zo geven diverse respondenten aan. Dit blijkt ook uit de afsluiting van het deel over de informatieorganisatie: er zijn eenheden die voor de inzet van OGG binnen de opsporing (deels) afhankelijk zijn van de informatieorganisatie en er zijn eenheden die het volledig binnen de recherche hebben georganiseerd. We hebben geen gedetailleerd beeld van hoe die organisatie eruitziet, maar kunnen wel de volgende hoofdlijnen schetsen.[64]

In ieder politiedistrict is er een districtsrecherche. Binnen de districtsrecherche zijn het veelal rechercheurs die internetrechercheren als taakaccent hebben, al zijn er ook dis-

64 Dit betreft de regionale eenheden. Bij de landelijke eenheid is de hoofdlijn vermoedelijk hetzelfde, maar zijn er specifieke teams die over meer capaciteit op het gebied van internetrechercheren beschikken, in het bijzonder het Team High Tech Crime (THTC) en het dark web team, beide onderdeel van de Dienst Landelijke Recherche (DLR).

trictsrecherches die over een fulltime internetrechercheur beschikken. In sommige eenheden zijn deze rechercheurs onderdeel van een digitaal platform waar verschillende digitale expertises zijn verankerd, terwijl er ook eenheden zijn waar de digitale platformen zich niet bezighouden met internetrechercheren.

Dan de DRR. Het uitvoerende recherchewerk wordt vooral uitgevoerd door de afdelingen Generieke Opsporing (GO) en Thematische Opsporing (TO). Binnen de GO is er in veel eenheden wel eens geïnvesteerd in opleidingen op het gebied van internetrechercheren, maar er zijn volgens respondenten uit de eenheden weinig rechercheurs die er actief mee bezig zijn en het actief onderhouden. De GO heeft ook een digitaal platform. In sommige eenheden beschikt dit platform over expertise op het gebied van OGG, maar het algemene beeld is dat het platform zich vooral bezighoudt met het onderzoeken van gegevensdragers, waaronder smartphones.

De afdeling TO bestaat uit diverse thematische teams: milieu, financieel-economische criminaliteit, zeden, kinderporno, cybercrime en sommige eenheden hebben ook een team op het gebied van CTER. Voor de cybercrime teams geldt dat een of meer fulltime internetrechercheurs onderdeel zijn van de (standaard) inrichting van het team. Voor wat betreft de andere thematische teams zijn er verschillen tussen teams en eenheden ten aanzien van de aanwezigheid van rechercheurs die (ook) internetrechercheren. In algemene zin is die aanwezigheid in de thematische teams overigens niet vanzelfsprekend, zo merken respondenten (vaak met enige verbazing) op. Ook de afdeling TO heeft een digitaal platform – of meerdere digitale platformen –, maar daarvoor geldt hetzelfde als voor de afdeling GO: men ondersteunt veelal niet of nauwelijks op het gebied van internetrechercheren.

De DRR beschikt daarnaast over een Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel (AVIM), waarvan het team migratiecriminaliteit en mensenhandel (TMM) een onderdeel is. Op basis van de interviews en andere bronnen kunnen we constateren dat er wederom veel verschillen tussen eenheden zijn. Er zijn eenheden die een eigen (fulltime) internetrechercheur hebben, terwijl er ook eenheden zijn die vooral een beroep doen op ondersteunende afdelingen.

Met ondersteunende afdelingen wordt naast de digitale platformen vooral verwezen naar het Team Digitale Opsporing (TDO) van de afdeling Specialistische Opsporing (SO). Dit team voert geen opsporingsonderzoeken uit, maar ondersteunt de generieke en thematische opsporing.[65] TDO is binnen de (regionale) recherche de plek waar de meeste (gespecialiseerde) internetrechercheurs werkzaam zijn. De mate waarin dit het geval is, verschilt tussen eenheden. Het gaat van één-twee internetrechercheurs tot vijfzes. Dit lijkt niet alleen samen te hangen met de omvang van de eenheid, maar ook met historie en het belang dat aan internetrechercheren wordt toegekend. We hebben res-

65 Dit wordt ook wel tweedelijns ondersteuning genoemd. De digitale platformen zijn de eerste lijn.

pondenten gesproken die al jaren werken bij een TDO waar internetrechercheren stevig is ingebed en we hebben respondenten gesproken die twee jaar geleden als enige internetrechercheur zijn gestart om het vakgebied (opnieuw) op te bouwen. Binnen de afdeling SO kunnen daarnaast internetrechercheurs werkzaam zijn bij het Team Financiële Opsporing, die internet gebruiken voor financieel onderzoek. Hierbij ligt de focus op het achterhalen van vermogen en onderzoek naar geldstromen op basis van online gegevens, waaronder gegevens over cryptovaluta.

De afdeling SO heeft ook een team Observatie & Techniek (O&T) waar 'virtual agents' (VA) werkzaam zijn. Dit zijn politiemensen die online onder dekmantel werken (zie ook Oerlemans, 2018a). Zij winnen heimelijk online gegevens in en werken (vooral) in besloten groepen en platformen.[66] De VA is ondersteunend naar zowel recherche- als informatieorganisatie. Er is sprake van landelijke, operationele coördinatie en samenwerking. Zo werken virtual agents uit verschillende eenheden samen op een thema, bijvoorbeeld ondermijning of CTER. De werkzaamheden van de VA vallen wel onder het online vergaren van gegevens, maar het betreft een aparte (sub)discipline binnen de politie. De VA werkt niet uitsluitend binnen het team O&T. Er zijn ook binnen TMM virtual agents werkzaam, die onder andere met lokprofielen klanten van kinderprostituees proberen op te sporen.[67] De werkzaamheden van virtual agents hebben wij – zoals eerder aangegeven – niet specifiek onderzocht, maar het bestaan van deze rol is voor het gehele beeld wel van belang.

Uit de interviews komt tevens naar voren dat er omstandigheden kunnen zijn waarin specialisten vanuit de rechercheorganisatie bijdragen aan het intelligencewerk. Dit komt minder vaak voor dan vice versa, maar het gebeurt wel. De coronarellen zijn hiervan een recent voorbeeld. De behoefte om maatschappelijke onrust en ongenoegen online te monitoren en hierbij direct over te gaan tot het identificeren van verdachten (vaak van opruiing) was volgens respondenten zo groot dat specialisten op het gebied van internetrechercheren in diverse eenheden ook zijn ingezet op het grensvlak tussen intelligence en opsporing.

> *'Bij de coronarellen is het eigenlijk een intelligence feestje waarbij wij vanuit de opsporing helpen, omdat er paniek is. Maar we hebben wel gezegd: "zet ons dan wel in op ons specialisme. Laat het monitoren door de DRIO doen, want wij hebben daar de tools ook niet voor". Als iemand binnen de groep echt een opruier is, dan gaan wij proberen uit te zoeken wie die persoon is.'* (21)

66 Ze worden hierin begeleid door een landelijk team werken onder dekmantel van de LE.

67 https://www.ad.nl/binnenland/deze-agenten-doen-zich-online-voor-als-17-jarige-prostituees-hij-vraagt-hoe-groot-mijn-pik-is~a089458a/

Basisteam

Binnen basisteams worden ook in toenemende mate werkzaamheden op het gebied van OGG uitgevoerd, al zijn de verschillen tussen basisteams op dit punt groot. Deze werkzaamheden worden vooral uitgevoerd door digitaal wijkagenten (zie ook Terpstra et al., 2021). Deze rol is in 2017 in het basisteam van Roosendaal ontstaan en heeft zich in de afgelopen jaren als een olievlek verspreid over basisteams in Nederland (zie ook Boelens & Landman, 2021).[68] In september 2021 had ongeveer een derde van de basisteams een digitaal wijkagent en was het aantal nog steeds groeiende. Digitaal wijkagenten verrichten verschillende digitale taken waarvan OGG – en dan in het bijzonder OSINT – er één is. Naast OSINT betreft het de aanpak/preventie van digitale criminaliteit, webcare en het opleiden en coachen van collega's op het gebied van digitaal politiewerk (Boelens & Landman, 2021; De Vries & Bantema, 2022). Met betrekking tot de precieze rolinvulling doen zich verschillen voor tussen basisteams.

In de basisteams zijn OSINT en internetrechercheren niet voorbehouden aan de digitaal wijkagent. In sommige basisteams worden er politieagenten aangesteld met een taakaccent OSINT. Dit komt naar onze indruk nog beperkt voor. Wat vaker voorkomt, is dat digitaal wijkagenten hun collega's opleiden, zodat zij veilig kunnen zoeken en surveilleren op het internet. Er is door pionierende digitaal wijkagenten een opleidingsprogramma samengesteld dat door collega digitaal wijkagenten op steeds meer basisteams wordt 'uitgerold'. Een hiermee samenhangende ontwikkeling is dat er in steeds meer eenheden 'digi-kamers' zijn waar hard- en software aanwezig is waarmee daarvoor opgeleide politieagenten uit de basisteams onder andere OSINT-werkzaamheden kunnen uitvoeren.[69]

> *'Voor de drie districten komen er vier digikamers. Een digikamer is een plek waar digitaal politiewerk plaatsvindt en waar collega's bij elkaar komen en bijvoorbeeld training kunnen krijgen. Een aantal weken geleden hebben een paar mensen een basisopleiding gekregen. Dit zijn mensen die hun hand hebben opgestoken toen we vroegen wie het leuk vindt om met internet aan de slag te gaan. Begin maart (2021, red.) gaan de kamers draaien en dan hebben de mensen uit de basisteams ook hard- en software om intelligencewerk te doen.'* (30)

68 Enkele jaren eerder was er ook een digitale wijkagent in het Habbo Hotel. Dit was een avatar in een virtuele omgeving (van het Habbo Hotel) waarmee jongeren konden chatten (zowel openbaar als privé). Deze digitale wijkagent had (dus) een ander karakter dan de digitaal wijkagent die in 2017 is ontstaan. Zie hiervoor Van Egmond (2017) en Boelens & Landman (2021).

69 Het concept van een 'digikamer' is ontstaan in Zeeland-West-Brabant. In Amsterdam en Rotterdam zijn inmiddels ook digikamers en ook andere eenheden (waaronder Noord-Nederland) experimenteren hiermee. In een van de interviews werd benoemd dat er plannen zijn om dit concept landelijk op te schalen. Hierbij moet worden benadrukt dat een digikamer een voorziening is voor digitaal politiewerk in brede zin. Het beperkt zich niet tot OSINT of internetrechercheren, maar heeft onder andere ook betrekking op het uitlezen van smartphones en andere (kleine) gegevensdragers.

Voor internetrechercheren geldt dat het ook plaatsvindt in het cluster dat zich binnen het basisteam bezighoudt met de aanpak van veelvoorkomende criminaliteit (VVC) (zie ook Terpstra et al., 2021). In sommige basisteams is er in dergelijke clusters in behoorlijke mate expertise op het gebied van internetrechercheren aanwezig. Verschillende respondenten hebben erop gewezen dat deze expertise steeds meer van belang is vanwege de toenemende digitale criminaliteit.

3.5 Samenwerking op het gebied van OGG

De vorige paragraaf heeft laten zien dat het online vergaren van gegevens ten behoeve van intelligence en opsporing op verschillende plekken in de politieorganisatie plaatsvindt. Het aantal plekken is in de afgelopen jaren ook toegenomen, onder andere door de ontwikkeling van de digitaal wijkagent in de basisteams. Uit de interviews komt naar voren dat dit heeft geleid tot vraagstukken en initiatieven op het gebied van samenwerking. Dit thema staat in deze paragraaf centraal.

Ten tijde van de interviews was het vraagstuk van samenwerking voor de participerende respondenten zeer actueel. In diverse eenheden werden en worden initiatieven ondernomen om de samenwerking tussen verschillende organisatieonderdelen op het gebied van OGG op gang te brengen of te intensiveren. Deze samenwerking heeft een uiteenlopend karakter. De samenwerking heeft in de eerste plaats betrekking op het afstemmen van werkzaamheden. Wie doet wat? Binnen de eigen discipline (intelligence of recherche) is deze afstemming in de regel georganiseerd. De fulltime specialisten binnen zowel de informatieorganisatie als de recherche weten elkaar over het algemeen goed te vinden, zo blijkt uit de interviews. Zij zijn in de praktijk geregeld een informeel team of zijn op zijn minst een netwerk binnen de eigen dienst. Binnen de informatieorganisatie vindt daarnaast afstemming plaats tussen de 'reguliere' OSINT-specialisten en degenen die zich in het kader van inlichtingen en werken onder dekmantel met online gegevensvergaring bezighouden.

> *'Wij (informeel team, red.) stemmen nu af met TOOI, TCI, ID Wiv en de virtual agents.*[70] *Het zou ideaal zijn als de recherche ook een groepje heeft waarmee we kunnen afstemmen.'* (23)

Bovenstaand citaat laat zien dat in deze eenheid de afstemming tussen de disciplines (intelligence en recherche) niet of in mindere mate aanwezig is. En dat geldt niet alleen voor deze eenheid. Een van de respondenten sprak zelfs over een 'Berlijnse muur' die tussen beide diensten zou staan (26b). Dit wil zeggen: men heeft niet of nauwelijks contact met elkaar. Afgaande op onze data, is dit *overall* gezien een wat stevige uit-

70 Virtual agents zijn – zoals eerder aangegeven – onderdeel van het team O&T van de afdeling SO (zie par. 3.4). Deze politiemensen zijn dus geen onderdeel van de informatieorganisatie.

spraak, maar in de interviews zijn verschillende voorbeelden gegeven van moeizame afstemming of samenwerking op het gebied van OGG.

> *'Er zijn ook wel problemen geweest met de informatieorganisatie, omdat er natuurlijk grijs gebied is. Wanneer is het voor opsporing en wanneer is het voor intelligence? We willen elkaar niet voor de voeten lopen, maar dat gebeurt automatisch. Er ontstond wrijving toen de indruk ontstond dat ik verder zou gaan waar de DRIO niet verder kon. Toen heb ik mijn handen ervan afgetrokken en mijn teamchef op de hoogte gesteld en is zij het gaan oplossen.' (35)*

> *'Vorig jaar liepen we er wel tegenaan: wat hoort bij de DRIO en wat hoort bij ons (TDO, red.)? Er ontstond wrijving toen er een nieuw OSINT piket bij de DRIO kwam voor TGO's (teams grootschalige opsporing, red.). Normaal werd ik daarvoor gebeld. Nu zei een leidinggevende "Nee, ik bel jou niet meer, want dat gaat nu via het OSINT piket van de DRIO." Toen kreeg ik het gevoel van "Ho wacht, dat klinkt als concurrentie". Op een gegeven moment zaten er bij een onderzoek drie internetrechercheurs die niets mochten doen, want de DRIO-rechercheur zou komen. De informatiecoördinator[71] werd ook met iets opgezadeld waarvan die niet wist wat hij ermee aan moest. We hebben een gesprek met elkaar gehad over de samenwerking. Hoe kunnen we beter worden van elkaar en elkaar ondersteunen, zodat we geen concurrenten worden van elkaar?'* (25)

Het probleem van 'elkaar voor de voeten lopen' speelt vooral in de eenheden waarin zowel de DRIO als het TDO (omvangrijke) opsporingsonderzoeken met OGG-expertise ondersteunt én er tussen hen weinig afstemming is. Er kan dan sprake zijn van overlap en concurrentiegevoelens. Uit de interviews komt naar voren dat er oplossingen worden gezocht voor de (ongewenste) overlap. De eerste oplossing is in de vorige paragraaf al behandeld: het beter of strakker scheiden van intelligence en opsporing. Dit betekent in de praktijk dat de informatieorganisatie geen opsporingsonderzoeken meer ondersteunt en dit (volledig) bij de rechercheorganisatie komt te liggen.

> *'Op een gegeven moment hebben we gezegd: we moeten het veranderen. De recherche en informatieorganisatie kregen last van elkaar. We moesten het beter scheiden. Inmiddels is er een goed contact met TDO, die doen de opsporingskant van OSINT.'* (37)

De tweede oplossing is frequente afstemming. Zo is er in een van de eenheden een afstemmingsoverleg ontstaan tussen de OSINT-specialisten van de informatieorganisatie en de internetrechercheurs van TDO. Men komt twee keer per week bij elkaar om alle verzoeken tot ondersteuning van opsporingsonderzoeken naast elkaar te leggen en te bespreken wie wat gaat doen. Het uitgangspunt in de taakverdeling is dat de

71 In een opsporingsonderzoek coördineert een informatiecoördinator de inbreng vanuit de informatieorganisatie.

OSINT-specialisten van de DRIO (eenvoudige) verzoeken oppakken die op afstand van het onderzoeksteam kunnen worden uitgevoerd, terwijl de internetrechercheurs ingaan op de (complexere) verzoeken waarbij nabijheid tot dan wel inbedding in het onderzoeksteam wenselijk is (zie ook paragraaf 5.2).[72] Er zijn ook eenheden waarin de specialisten van de DRIO en DRR zo nauw samenwerken dat zij een informeel team vormen.

> *'Ik ben nu bezig om in <naam eenheid> een OSINT-team op te richten. We hebben nu zes mensen die er fulltime mee bezig zijn binnen DRIO en DRR en daaromheen een flexibele schil.'* (34)

Niet in alle eenheden lijkt de afstemming tussen de informatieorganisatie en recherche voor wat betreft internetrechercheren op gang te komen. Dit heeft verschillende oorzaken. We hebben de indruk dat het in grote eenheden uitdagender is om het voor elkaar te krijgen; daar heeft men eerder het gevoel van een 'Berlijnse muur'. Daarnaast lijkt er in de 'onderstroom' soms wat gedoe te zijn. Respondenten uit verschillende eenheden benoemen dat de recenter aangestelde internetrechercheurs[73] een hogere salarisschaal hebben dan hun collega OSINT-specialisten van de informatieorganisatie. Dit zou zorgen voor scheve gezichten in de informatieorganisatie.[74] In een van de eenheden werd expliciet benoemd dat dit een negatieve invloed heeft op de werkrelatie. De internetrechercheurs doen naar eigen zeggen geregeld een uitnodiging tot samenwerking aan hun collega's van de informatieorganisatie, maar deze zou niet worden beantwoord.

Een tweede afstemmingsvraagstuk is verbonden aan de opkomst van OGG in de basisteams, in het bijzonder door digitaal wijkagenten. Dit is een relatief recente ontwikkeling, die door de specialisten die al langer werken op het gebied van OSINT of internetrechercheren veelal positief wordt gewaardeerd. Zo raakt politiewerk op het web breder ingebed.

> *'De ontwikkeling van de digitaal wijkagent vind ik goed. Die hebben hun meerwaarde echt wel bewezen. We hebben er ook een goede verstandhouding mee. Ze komen bij ons (specialisten internetrecherche, red.) om te vragen wat mag. Je ziet ook dat ze in sommige teams wel een beetje de cowboy uithangen.'* (21)

> *'Ik zie dat als iets positiefs, want het scheelt mij werk. Ik hoef dingen op lokaal niveau niet meer uit te lopen, want daar zit de digitaal wijkagent in. Zo hebben we een colle-*

72 Wat hierbij opvalt, is dat er door respondenten niet wordt gerefereerd aan het onderscheid in bevoegdheden, bijvoorbeeld: de OSINT-specialisten van de DRIO werken niet-stelselmatig.

73 Dit zijn veelal specialisten die van buiten de politieorganisatie komen en executief worden met specifieke inzetbaarheid, wat onder andere impliceert dat een beperkte politieopleiding (14 weken) nodig is.

74 Zie ook Landman et al. (2020) over onrechtvaardigheidsgevoelens als gevolg van de onderlinge werkschaalvergelijking.

ga die zit ontzettend goed in de motorgangs, die kent iedereen en is ook goed op de hoogte van eventueel afbreukrisico.' (24)

De positieve waardering voor de ontwikkeling in (een deel van) de basisteams neemt niet weg dat er ook enige argwaan is. Deze argwaan vloeit voort uit de thematiek die in bovenstaand citaat is opgenomen. Een deel van de specialisten op regionaal niveau vermoedt dat digitaal wijkagenten niet altijd voldoende bekwaam zijn in het veilig en rechtmatig online vergaren van gegevens dan wel bewust de grens van 'wat mag' opzoeken of overgaan (zie ook paragraaf 4.3).

'Vanuit de opsporing hebben we ook gekeken naar de digitaal wijkagent. Wat gaat die doen? In hoeverre houdt die het veilig? Kijkt die met een blauw account naar wat leeft in de wijk en doet die met zijn blauwe account ook opsporing? Wij zoeken als rechercheur altijd met een alter ego. Dus daar waren we heel benieuwd naar. Is de digitaal wijkagent er voldoende bedreven in? Ik probeer de verbinding te maken tussen DRIO en digitaal wijkagent en tussen ons. We zitten op hetzelfde medium en zoeken actief. Hoe kunnen we elkaar helpen?' (22)

'Ik heb gevraagd of we eens een gesprek kunnen hebben over wat zij doen, of er overlap is. Ik ben ook wel benieuwd of ze het goed doen. Ik krijg wel eens het idee dat ze gewoon aan de slag gaan en dat de afbreukrisico's groot zijn.' (32)

Naast enige argwaan klinkt in bovenstaande citaten ook de behoefte aan afstemming en samenwerking door. Men houdt zich bezig met hetzelfde vakgebied en er is mogelijk overlap in werkzaamheden, vooral op het gebied van intelligence. Op basis van de interviews constateren we dat in een groot deel van de eenheden pogingen worden ondernomen om de onderlinge afstemming op gang te brengen, al bevindt deze ontwikkeling zich nog in een pril stadium.[75]

'Een paar weken geleden werden we benaderd door de portefeuillehouder GGP: "Ik wil iets doen met digitaal wijkagenten, kunnen jullie daarin helpen". Er zijn digitaal wijkagenten begonnen, maar is veel overlap in werkzaamheden. We weten niet van elkaar in welke groepen we zitten. Er zit geen visie achter, dat merk je. Dus nu zijn we bezig om het meer bij elkaar te brengen. Dat bevindt zich in een beginstadium. Ik kreeg toevallig een stuk onder ogen over de digitaal wijkagent. Daarin werd een voorbeeld gegeven van wat een digitaal wijkagent zou kunnen doen. Dat was bij uitstek een voorbeeld waarbij je als DRIO-medewerker denkt "Dat is mijn werk". En daarin zie je dus de behoefte aan afstemming die er nu nog te weinig is.' (37)

Samenwerking tussen de verschillende organisatieonderdelen heeft, naast afstemming van operationele werkzaamheden, betrekking op vak-ontwikkeling (zie ook para-

75 Dit geldt in veel basisteams ook voor de rol van digitaal wijkagent.

graaf 6.1). In verschillende eenheden probeert men door de eenheid heen een netwerk te vormen waarin professionals op het gebied van OGG kennis kunnen uitwisselen en elkaar kunnen helpen c.q. ondersteunen.

> *'Wij zijn begonnen met het verbinden van de eilandjes. Mensen hebben de neiging om te blijven zitten in het eigen team, maar willen tegelijkertijd wel verbinding met elkaar, zodat je elkaar snel kunt vinden en helpen. Je wilt samen optrekken in ontwikkeling van het vakgebied.' (28)*

In het kader van samenwerking is tot slot de landelijke samenwerking van belang. Diverse respondenten hebben aangegeven dat er een noodzaak is tot landelijke afstemming op het gebied van monitoring (dit betreft dus OSINT en niet internetrechercheren). Deze noodzaak vloeit onder andere voort uit hun ervaring met recente demonstraties en rellen en het bredere fenomeen van 'maatschappelijk ongenoegen' (zie paragraaf 4.1). Er is volgens respondenten op dit moment weinig afstemming over de verdeling van de taken op het gebied van monitoring, terwijl er wel in alle eenheden min of meer gelijktijdig monitoring plaatsvond met onvermijdelijke overlap in werkzaamheden, bijvoorbeeld in de vorm van aanwezigheid in dezelfde (besloten) groepen.[76]

> *'Wij kunnen in de eenheid wel alles goed met elkaar afstemmen, maar open bronnen hebben geen grenzen. Dus er moet landelijk veel meer afstemming zijn over wie gaat waarnaar kijken. Want als ze in Groningen iemand zitten te monitoren die in Den Haag gaat demonstreren, dan zitten dus meerdere mensen die persoon te monitoren. Dat heeft met afstemming te maken.'* (37)

> *'Neem bijvoorbeeld de boerenprotesten. Alle eenheden monitoren dit, maar landelijke afstemming is lastig. Door onze eenheid rijden ze alleen maar heen, terwijl in Den Haag staan ze op het Malieveld te protesteren. Je zou ook kunnen afspreken dat de boerenprotesten worden gemonitord door Den Haag en Den Haag geeft aan eenheden door wat het beeld is.'* (39)

> *'Er zijn wel besloten groepen waar denk ik meer politiemensen in zitten dan raddraaiers.[77]'* (23)

Kortom: er lijkt met betrekking tot bepaalde veiligheidsthema's (zoals maatschappelijk ongenoegen) en bij (dreigende) openbare-ordeverstoringen met een nationaal karakter behoefte te zijn aan landelijke informatiecoördinatie: welke OSINT-taken worden waar uitgevoerd?

---

76 Dit geldt volgens respondenten breder dan de politie. Ook de AIVD kan in dezelfde groepen aanwezig zijn als de politie.

77 Zie ook https://www.nrc.nl/nieuws/2021/05/27/infiltreren-in-een-online-buurtfeest-a4045202

In de twee volgende hoofdstukken wordt nader ingegaan op het online vergaren van gegevens ten behoeve van intelligence (OSINT) en opsporing (internetrechercheren).

4 Open source intelligence

Dit hoofdstuk gaat in op het online vergaren van gegevens ten behoeve van intelligence: OSINT. In paragaaf 1 behandelen we de inzet van OSINT in het intelligenceproces. In paragraaf 2 staan de inbedding en werkwijze van OSINT-medewerkers centraal. Paragraaf 3 gaat over het gebruik van bevoegdheden en paragraaf 4 over de opbrengsten van OSINT. We ronden het hoofdstuk af met een praktijkcasus in paragraaf 5, te weten de zogenaamde avondklokrellen.

4.1 Inzet van open source intelligence

Intelligence(proces) en informatieproducten
De opkomst van het begrip intelligence binnen de politie houdt verband met het concept of de politiestrategie van *intelligence-led policing* (zie Ratcliffe, 2008). In Nederland is deze – uit het Verenigd Koninkrijk overgenomen – strategie vertaald als intelligencegestuurd politiewerk (Kop & Klerks, 2009). Intelligence is hierbij gedefinieerd als geanalyseerde informatie en kennis op grond waarvan beslissingen over de uitvoering van de politietaak worden genomen. Intelligence is dus sturingsinformatie: *information designed for action* (Duijn, 2011). Het is in de context van politiewerk van belang om dit type informatie te onderscheiden van bewijs, zoals dit in opsporingsonderzoek wordt vergaard en in een procesdossier wordt opgenomen (Duijn, 2011; Sampson, 2017). Intelligence kan – in tegenstelling tot bewijs – ook uit aannames en interpretaties bestaan.

In het intelligenceproces worden intelligence- of informatieposities opgebouwd over fenomenen door middel van een cyclisch proces (Duijn, 2011). Dit wil zeggen dat er bij voortduring gegevens worden verzameld, bewerkt en geïnterpreteerd en in de vorm van informatieproducten worden gedeeld. Er zijn vele typen informatieproducten, zoals een ondermijningsbeeld, een analyse van een crimineel samenwerkingsverband of een informatierapport over een concreet subject. Een belangrijk deel van de gegevensverzameling vindt plaats in het operationele politiewerk in de basispolitiezorg (art. 8-gegevens[78]) en recherche (art. 9-gegevens) en wordt geregistreerd in de daarvoor bestemde politiesystemen (vooral BVH en SUMM-IT). Daarnaast worden inlichtingen verzameld door onder andere gebruik te maken van informanten (art. 10-gegevens). Het gaat in veel gevallen om gegevens die via waarnemingen van mensen worden

78 Dit verwijst in deze alinea naar de Wpg.

verzameld: human intelligence.[79] Daarnaast worden door politiemensen gegevens vergaard die er online al zijn: OSINT. OSINT is dus een van de bronnen die wordt gebruikt in het intelligenceproces (zie ook Miller, 2018).

Met betrekking tot het intelligenceproces is het tot slot van belang om een onderscheid te maken tussen het gebruik van gegevens uit het verleden en het gebruik van (min of meer) actuele gegevens. Een analyse van een crimineel samenwerkingsverband of een anti-overheidsgroep is bijvoorbeeld gebaseerd op gegevens die in het verleden zijn verzameld. Die gegevens zijn verwerkt (waaronder gecombineerd) en geïnterpreteerd en dit leidt tot een beeld van het betreffende criminele samenwerkingsverband of de betreffende groep. Real-time intelligence is daarentegen gebaseerd op min of meer actuele gegevens, die direct worden verwerkt en geanalyseerd en als sturingsinformatie beschikbaar worden gesteld (zie De Boer & Van den Berg, 2017). Hierbij kan worden gedacht aan het monitoren van grootschalige incidenten ten behoeve van een Staf Grootschalig en Bijzonder Optreden (SGBO), maar ook aan het geven van extra informatie aan politiemensen op straat bij de incidentafhandeling door het RTIC.

Inzet van OSINT voor thematische informatieposities
Zoals gezegd: in het intelligenceproces worden informatieposities opgebouwd en hierbij wordt, naast allerlei gegevens uit politiesystemen, gebruikgemaakt van online vergaarde gegevens. De informatieposities hebben betrekking op een thema of fenomeen en daarbinnen zijn er vaak weer sub-thema's (zie ook paragraaf 3.4). Binnen ondermijning gaat het *bijvoorbeeld* om drugs en excessief geweld en binnen CTER om rechts-extremisme en (terugkerende) uitreizigers. Maar het kan ook gaan om thema's die gedurende het jaar een tijdelijk karakter hebben, zoals de handel in illegaal vuurwerk. De mate waarin online vergaarde gegevens een rol spelen in het opbouwen van een informatiepositie verschilt tussen de thema's. Dit hangt onder andere af van de aard van het thema.

> *'We maken binnen de DRIO's de shift naar thematische informatiecoördinatie en komen meer los van de geografie (zie paragraaf 3.4, red.). Er is informatiecoördinatie op bijvoorbeeld openbare orde, CTER, cybercriminaliteit, OMG (outlaw motorcycle gang, red.), drillraps. Bij al die onderwerpen is OSINT een van de bronnen. Bij de een meer dan de ander. Bij drillraps haal je bijna de hele informatiepositie van het internet. En die combineer je met eigen gegevens. Bij openbare orde is het ook veel OSINT. CTER is weer minder openbaar.'* (36)

In uiteenlopende interviews is door respondenten een onderscheid gemaakt tussen twee manieren waarop OSINT wordt gebruikt bij het opbouwen van informatieposi-

79 Deze begrippen/afkortingen zijn afkomstig uit de inlichtingenwereld waarin bijvoorbeeld ook SIGINT (signals intelligence) relevant is. Zie Staniforth (2016) voor een overzicht.

ties: monitoren en identificeren.[80] Monitoren heeft betrekking op trends & ontwikkelingen (nadruk op vooruitkijken). Hierbij kan worden gedacht aan ontwikkelingen in het buitenland, verdieping van bepaalde sub-thema's, in kaart brengen van nieuwe fenomenen (zoals deepfakes), crime scripts en dergelijke. Neem een fenomeen als illegaal vuurwerk. OSINT wordt ingezet om het logistieke proces achter de handel in illegaal vuurwerk in kaart te brengen, waaronder sociale mediakanalen waarop illegaal vuurwerk wordt aangeboden, communicatiekanalen die klanten en leveranciers gebruiken, locaties van leveranciers, locaties/gebieden van klanten, verzendmethoden en betalingswijzen (zie ook Lam & Kop, 2020c).

Identificeren is specifieker en gaat onder andere over bepaalde groeperingen of criminele samenwerkingsverbanden, personen die daarin actief zijn en hun onderlinge relaties (hoe ziet het netwerk eruit?). Respondenten geven aan dat bij ieder thema monitoren en identificeren nodig zijn, maar de balans tussen beide per thema verschilt. Bij OMG ligt er bijvoorbeeld meer nadruk op identificeren dan op monitoren, terwijl bij openbare orde monitoren een grotere rol speelt. Het ene thema is op het gebied van OSINT ook specialistischer dan het andere. CTER wordt diverse keren genoemd als een specialistisch thema. Dit wil zeggen dat een OSINT-specialist zich dit niet zomaar eigen maakt. Dit komt onder andere door wat in bovenstaand citaat is aangegeven: het is minder openbaar. Men komt sneller in online undercoverwerkzaamheden terecht en moet zich kunnen voordoen als een groepslid[81](zie ook paragraaf 2.6).

In de interviews wordt openbare orde veelvuldig genoemd als een thema waarvoor OSINT heel belangrijk is en waarop veel capaciteit wordt ingezet.

> *'Op dit moment zitten we (OSINT-specialisten DRIO, red.) volledig op monitoring. Dus op Koningsdag, corona, maatschappelijke onrust en ook lopende processen zoals CTER.'* (34)

Er zijn bij voortduring gebeurtenissen en ontwikkelingen die van invloed kunnen zijn op de openbare orde en die kunnen verstoren. Hierbij kan worden gedacht aan voetbalwedstrijden, sinterklaas, demonstraties en dergelijke. Hoeveel mensen verwachten we? Welke groepen? In welke mate zijn openbare-ordeverstoringen te verwachten? Dit soort vragen wordt onder andere met behulp van OSINT beantwoord. OSINT is logischerwijs vooral van meerwaarde voor openbare-ordeverstoringen die online worden aangejaagd.

---

80 Niet iedereen maakt expliciet het onderscheid tussen monitoren en identificeren, maar dit onderscheid zit vaak wel verweven in wat zij zeggen.

81 Dit is een belangrijke constatering: ook in het kader van intelligence wordt onder dekmantel gewerkt (zie ook de passage over de VA in par. 3.4), in het bijzonder op het thema CTER. Dit heeft ook te maken met het gegeven dat op basis van terrorismewetgeving in een eerder stadium bijzondere opsporingsbevoegdheden kunnen worden ingezet. Een 'aanwijzing' is voldoende, in plaats van een 'verdenking'. Dit heeft als consequentie dat de grens tussen intelligence en opsporing diffuser wordt of anders gezegd: het komt dichter bij elkaar.

> *'Stel er is een demonstratie aangevraagd in <plaatsnaam> en er wordt gevraagd hoeveel mensen komen hierop af, hoeveel daarvan willen echt demonstreren en hoeveel willen rellen. Monitoring kan gaan over wat gaat er gebeuren.'* (26)

De nadruk die online aangejaagde ordeverstoringen in de interviews hebben gekregen, hangt vermoedelijk samen met het moment waarop de interviews hebben plaatsgevonden: enkele weken of maanden na de avondklokrellen in januari 2021. In deze periode lag er veel nadruk op het monitoren van een breed fenomeen, dat binnen de politie 'maatschappelijk ongenoegen' wordt genoemd.[82] Deze monitoring vindt niet alleen plaats via gebeurtenissen, maar ook door groepen – zoals Viruswaarheid, Farmer Defence Force en QAnon – in de gaten te houden. Hoe ontwikkelt het aantal aanhangers zich? Hoe activistisch zijn ze? Welke dreiging gaat er van de groep uit? Hoe meer dit gaat over specifieke personen en hun relaties, hoe meer monitoren overgaat in identificeren. En hoe meer (alertheid op) bevoegdheden een rol gaan spelen, omdat er persoonsgegevens worden vergaard.

Inzet van OSINT voor gebiedsgebonden informatieposities
Zoals eerder aangegeven: ook in (een deel van de) basisteams worden werkzaamheden op het gebied van OSINT uitgevoerd. Dit wil zeggen dat er wordt gemonitord wat zich online afspeelt en gegevens worden verzameld over mogelijke problemen, zodat hier eventueel op kan worden geanticipeerd (zie ook Terpstra et al., 2021). Er lijkt in basisteams een groeiende behoefte aanwezig te zijn om, aanvullend op de informatieorganisatie, met OSINT aan de slag te gaan. De respondenten uit de informatieorganisatie die wij hebben gesproken, begrijpen deze behoefte.[83]

> *'OSINT is niet het monopolie van de informatieorganisatie. Ik vind het niet vreemd dat mensen in de basisteams ook OSINT willen toepassen.'* (36)

De digitaal wijkagent speelt bij OSINT in het basisteam een belangrijke rol (zie ook Terpstra et al., 2021). Uit de interviews met digitaal wijkagenten komt naar voren dat de mate waarin zij actief zijn op het gebied van OSINT verschilt. Voor de meeste digitaal wijkagenten geldt dat OSINT een van de dominante taken is,[84] maar er zijn ook digitaal wijkagenten die op dat gebied weinig activiteiten uitvoeren. Dit heeft vaak ook te maken met de mate waarin zij zich bekwaam voelen om OSINT-werkzaamheden uit te voeren.

82 Dit is, voor zover wij weten, op het moment van schrijven (begin 2022) nog steeds het geval.
83 Men heeft soms wel twijfel bij de wijze waarop dit in de basisteams gebeurt, in het bijzonder waar het gaat om het gebruik van bevoegdheden (zie par. 4.3).
84 OSINT is voor veel digitaal wijkagenten ook het taakgebied dat hen de meeste voldoening geeft. Dit baseren we op een peiling onder 25 digitaal wijkagenten (zie par. 1.4).

> *'Ik verricht verschillende taken: voorlichting over internetgedrag en criminaliteit, webcare, collega's coachen, maar het grootste gedeelte is toch wel OSINT: monitoren van open bronnen. Wat voor tendensen zie ik. Die is gewoon heel breed.'* (4)

> *'Ik heb daar (OSINT, red.) nog niet voldoende zelfvertrouwen voor. Ik ben wel bezig met dat uit te bouwen en geef me op voor cursussen. Je zou wel een bepaald opleidingsniveau moeten hebben. Er zijn nu veel verschillen tussen eenheden. Bepaalde eenheden hebben strikte regels, maar er zijn ook eenheden die maar wat doen.'* (9)

Digitaal wijkagenten dragen bij aan de informatiepositie van het basisteam en richten hun OSINT-activiteiten zoveel mogelijk op het eigen werkgebied. Een gebiedsoriëntatie is dominant. In deze gebiedsoriëntatie schuilt de meerwaarde ten opzichte van wat de informatieorganisatie doet.

> *'De informatieorganisatie monitort meer op eenheidsniveau in plaats van specifiek voor het werkgebied van het basisteam.'* (4)

Wat monitoren digitaal wijkagenten? Wij hebben hier geen volledig beeld van, maar kunnen op basis van de interviews wel een indruk geven.

De meeste voorbeelden in de interviews hebben betrekking op (eventuele) openbare-ordeproblemen in het werkgebied. Terpstra et al. (2021) wijzen erop dat deze problemen niet nieuw zijn, maar de dynamiek van mogelijke problemen wel. Door digitalisering is het bereik groter en is het voor de politie lastiger te voorspellen of er problemen zullen ontstaan en wat de ernst van die problemen zal zijn. Door online te monitoren, proberen digitaal wijkagenten een inschatting te maken van het sentiment onder en de actiebereidheid van burgers binnen en buiten het werkgebied. Het kan hierbij gaan om uiteenlopende onderwerpen of incidenten, zoals de opvang van asielzoekers in de gemeente, de terugkeer van iemand die is veroordeeld voor kinderporno in de wijk, het gebruik van geweld door de politie (video van het optreden die viraal was gegaan), de zwartepietendiscussie, openbare bijeenkomsten of feestjes, een aangekondigde demonstratie, evenementen en voetbalwedstrijden (zie ook Terpstra et al., 2021). Al dan niet samen met de informatieorganisatie wordt in de gaten gehouden wat er verschijnt op vooral sociale mediaplatformen. Wat leeft er? Worden er bedreigingen geuit? Is er iets dat nu of later actie van het basisteam kan vragen (zoals fysieke surveillance)?

> *'Bij de demonstraties van de gele hesjes in <plaatsnaam> kon ik voor de collega's goed in de gaten houden wat zich online afspeelde. Wat verwacht je dat er komen gaat? Zo kun je rust brengen in het team. In plaats van 200 mensen komen er 50. Dat heeft impact op de operationele inzet, maar dan moet je er wel op tijd mee komen.'* (7)

Daarnaast worden er verschillende voorbeelden gegeven van het online monitoren van lokale netwerken, zoals jeugdgroepen en leden van motorgangs. Dit vindt vaak op verzoek van wijkagenten plaats, maar soms ook naar aanleiding van een vraag van een teamchef of burgemeester.

> *'De burgemeester en teamleiding wilden meer over drillraps weten. Toen heb ik een heel onderzoek in open bronnen gedaan. Videoclips bekijken, artiestennamen noteren, verder zoeken op die namen, fora bekijken, combineren met informatie uit BVH. Zo kom je stapje voor stapje verder. Je maakt dan een rapport op en legt het vast in het systeem.*[85]' (7)

Tot slot zijn ook met betrekking tot de basisteams voorbeelden genoemd die gaan over tijdelijke fenomenen, zoals de handel in illegaal vuurwerk (in Telegram-groepen, zie ook de volgende paragrafen) en het online monitoren van mogelijke overtredingen van de coronaregels door horecaondernemingen tijdens de (intelligente) lockdown.

Terpstra et al. (2021) concluderen dat het online monitoren van (semi)open bronnen in de (door hun onderzochte) basisteams mondjesmaat en nog weinig gestructureerd plaatsvindt. Op basis van de interviews met digitaal wijkagenten hebben wij een vergelijkbare indruk. Tegelijkertijd merken we op dat met de toename van het aantal digitaal wijkagenten in de basisteams ook de activiteiten op het gebied van OSINT toenemen. In de basisteams gaat het – anders dan in de informatieorganisatie – om een combinatie van wijk en web, zo merken verschillende respondenten op. Bijvoorbeeld bij jeugdgroepen: er wordt zowel op straat als online geobserveerd. De digitaal wijkagent werkt hierin samen met (onder andere) wijkagenten en informatie gaat heen en weer tussen wijk en web.

Inzet van OSINT voor individuele dreigingsinschattingen
Een derde type gebruik van OSINT is niet scherp te onderscheiden van thematische informatieposities, maar verdient hier wel kort aandacht: dreigingsinschattingen. Het gaat dan in het bijzonder om dreigingsinschattingen die worden opgesteld in het kader van bewaken & beveiligen. Dit zijn (dus) inschattingen of risicoanalyses op individueel niveau, die kunnen worden onderscheiden van analyses op fenomeenniveau (dreigingsbeeld, veiligheidsbeeld). Het gaat hierbij om zeer uiteenlopende situaties, zoals stalking, eergerelateerd geweld en georganiseerde criminaliteit (liquidaties).

Als een potentiële dreiging door het OM als ernstig genoeg wordt aangemerkt, wordt er binnen enkele uren of dagen een informatieproduct opgeleverd. Ten behoeve hiervan worden politiesystemen geraadpleegd en OSINT-onderzoek gedaan. Het informatieproduct geeft een inschatting van de ernst van de dreiging en de waarschijnlijkheid dat die wordt uitgevoerd. Diverse respondenten geven aan dat de behoefte aan dreigings-

85 Dit voorbeeld beweegt richting opsporen.

inschattingen in het kader van bewaken & beveiligen in de afgelopen jaren is toegenomen. *Mede* om die reden heeft het landelijke platform van informatieorganisaties in de strategische personeelsplanning een uitbreiding van de OSINT-capaciteit opgenomen.[86]

Inzet van OSINT voor real-time intelligence
Een vierde type gebruik van OSINT heeft betrekking op real-time intelligence. Hiermee bedoelen we vooral dat het gaat om online vergaarde gegevens waarmee direct iets in de operatie wordt gedaan: men wordt real-time geïnformeerd. Het gaat dus niet zozeer om data die min of meer real-time zijn, al kan hier ook sprake van zijn, bijvoorbeeld over een actueel incident. Het gebruik van OSINT voor real-time intelligence vindt vooral plaats in het eerdergenoemde RTIC.

> *'Een van de toepassingen van OSINT vindt plaats in het RTIC. Er komt een melding binnen met adresgegevens en namen. Op basis daarvan kan er worden gekeken naar accounts die beschikbaar zijn. Op basis daarvan kunnen we informatie vergaren die kan helpen bij het afhandelen van de melding, bijvoorbeeld het aantal mensen dat er woont, foto's of andere aanvullende informatie. Het is niet standaard, maar als het een melding is van enige importantie, dan gaan we gelijk starten met OSINT op een adres of een persoon. Het is een combinatie van open bronnen en politiesystemen.'* (33)

De RTIC-medewerkers vergaren, op basis van de initiële gegevens van de melding, in deze gevallen online gegevens en raadplegen tevens (gesloten) politiebronnen. Vervolgens kiezen zij welke gegevens zij toevoegen aan de melding voor hun collega's op straat. Uit eerder onderzoek blijkt dat zij hierbij (naar eigen zeggen) vooral letten op de relevantie van de gegevens voor de veiligheid van hun collega's (zie Scholtens et al., 2016).

Een tweede toepassing van OSINT in het kader van real-time intelligence vindt plaats in geval van opschaling bij grootschalige incidenten. Dan is er een SGBO waarvan ook een Hoofd Informatie (HIN) onderdeel is. De HIN is verantwoordelijk voor het deelproces informatie. Afhankelijk van de aard van het incident kan er behoefte zijn aan het voortdurend online vergaren van gegevens ten behoeve van het informatiebeeld dat wordt gebruikt bij het nemen van beslissingen over de operationele inzet, ook wel een situatierapportage genoemd. Hiervoor is in de regel een OSINT-piket of iets vergelijkbaars[87] 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. Dit heeft onder andere tijdens de avondklokrellen plaatsgevonden (SGBO Corona).

86 Er zijn meer redenen of aanleidingen, waaronder de inzet op het gebied van maatschappelijk ongenoegen en daarmee samenhangend openbare orde.

87 In een van de eenheden is er bijvoorbeeld een Internet Ondersteuningsgroep ingericht met OGG-professionals vanuit verschillende organisatieonderdelen. Deze groep is begonnen als een piketgroep, maar er is inmiddels een permanente Internet Ondersteuningsgroep die bestaat uit vijf specialisten die zeven dagen per week tijdens kantooruren beschikbaar zijn voor inzet.

4.2 Inbedding en werkwijze van OSINT-medewerkers

Inbedding van OSINT-medewerkers
In paragraaf 3.4 is op hoofdlijnen beschreven hoe OGG is ingebed in de organisatiestructuur van de politieorganisatie. Het online vergaren van gegevens in het kader van intelligence (OSINT) vindt plaats in de informatieorganisatie en in toenemende mate in de basisteams. In de informatieorganisatie is het breed ingebed – een groot deel van de medewerkers heeft een basis in OSINT – maar het OGG-niveau verschilt. Het overgrote deel van de medewerkers in een eenheid beschikt over OGG niveau 2, een klein deel over niveau 3 en er zijn veelal enkele medewerkers die bekwaam zijn op niveau 4.[88]

> *'Bij de Regionale Informatie hebben we niveaus 2 en een aantal niveaus 3. Bij de Informatieknooppunten ook. Maar we kunnen niet ieder IK (informatieknooppunt, red.) een niveau 3 geven.[89] Daar hebben we teveel IK's voor. Bij de afdeling Regionale Informatie konden we mensen aannemen en hebben we geworven op OSINT.'* (36)

Het bovenstaande is de rode draad: bij de afdeling Regionale Informatie zijn enkele OSINT-specialisten op niveau 4 ondergebracht, al dan niet gekoppeld aan specifieke thema's. Voor de eenheden die een andere organisatiestructuur hebben (zie paragraaf 3.4), geldt dat de niveaus 3 veelal werken in de thematische organisatieonderdelen en bepaalde onderdelen (zoals openbare orde) ook over specialisten op niveau 4 beschikken. De specialisten op niveau 4 en soms ook 3 zijn fulltime bezig met OSINT. Dit betreft zowel het uitvoeren van OSINT-onderzoek als vakontwikkeling, waaronder het ontwikkelen en testen van tools, volgen van opleidingen en uitleren van OSINT-vaardigheden aan collega's binnen de DRIO (zie ook paragraaf 6.1). Deze fulltime specialisten vormen in verschillende eenheden in de regel met elkaar een informeel OSINT-team.[90]

> *'We hebben een eigen OSINT-club. Het mag officieel geen team worden genoemd, maar het zijn allemaal OSINT-specialisten die niets anders doen.'* (23)

> *'Ik hoor officieel bij het RIK (regionaal informatieknooppunt, red.), maar OSINT is eigenlijk een beetje een afdeling op zichzelf aan het worden.'* (32)

De digitaal wijkagenten zijn werkzaam in een basisteam. Binnen het basisteam zijn zij vaak ingebed in een van de geografische of thematische clusters. Dit hangt af van de

88 Er zijn overigens ook eenheden die OSINT-specialisten (niveau 3-4) extern inhuren.
89 Die wens is er in veel eenheden wel. Zie de eerdere opmerking over de gevraagde uitbreiding van OSINT-capaciteit.
90 Dit is vooral aan de orde bij de DRIO's die ingericht zijn conform het inrichtingsplan uit 2012. De DRIO's die toegroeien naar een nieuwe organisatiestructuur hebben naar onze indruk een matrixstructuur waarin OSINT een soort vakgroep is. Een specialist is in de praktijk dan onderdeel van twee teams: een thematisch team en een vakgroep.

inrichting van het basisteam. In het basisteam is de digitaal wijkagent in veel gevallen de enige medewerker met expertise op het gebied van OSINT[91] (zie ook Boelens & Landman, 2021). In sommige basisteams is er – zoals eerder aangegeven (zie paragraaf 3.4) – een toenemend aantal medewerkers dat over basis OSINT-vaardigheden beschikt. Daarnaast is er in sommige basisteams een 'cluster digitaal' waarin de digitaal wijkagent samenwerkt met andere collega's die digitaal zijn georiënteerd, zoals medewerkers van een cluster VVC en medewerkers die werken bij het socialemediateam van het basisteam.

Werkwijze van OSINT-specialisten
Zoals eerder aangegeven: dit verkennende onderzoek is niet gericht op het gedetailleerd in kaart brengen van hoe OGG binnen de politie wordt uitgevoerd. We beperken ons hier tot een aantal globale constateringen. Eerst over de OSINT-specialisten en dan over digitaal wijkagenten.

Een eerste constatering is dat OSINT-specialisten weliswaar zijn gespecialiseerd in het online vergaren van gegevens, maar dat zij daarnaast andere bronnen gebruiken. Dit betreft in het bijzonder gegevens uit de politiesystemen.

> *'Op OSINT zoeken kan iedereen. Wij hebben voordeel van gegevens uit politiesystemen die je kunt koppelen. Dat is ook wel nodig ter verificatie.'* (32)

Bij het online vergaren van gegevens gaan OSINT-medewerkers handmatig te werk én maken zij gebruik van het geautomatiseerd vergaren van gegevens. Voor de automatische vergaring maken zij onder andere gebruik van het softwareprogramma PublicSonar (zie ook paragraaf 6.2). PublicSonar is de standaard voor het basis OSINT-werk en wordt in alle informatieorganisaties gebruikt.[92] PublicSonar maakt gebruik van (meta)data van websites en (een deel van de) sociale mediaplatformen, indexeert deze en maakt deze doorzoekbaar. De gebruiker kan bouwstenen inrichten waarmee gegevens automatisch worden doorzocht en apart kunnen worden gezet voor nader (handmatig) onderzoek.

> *'Alle berichtgeving die op basis van onze kernwoorden een hit oplevert, wordt in een bak opzij gezet. Dit wordt door ons gescand en dan halen we daar dingen uit die we nader gaan bekijken.'* (33)

PublicSonar maakt volgens respondenten gebruik van gegevens die volledig open zijn, wat wil zeggen dat gegevens uit bijvoorbeeld besloten Facebookgroepen niet via de software kunnen worden vergaard. Om deze gegevens te vergaren, wordt er door

91 Naar eigen zeggen is men werkzaam op niveau 2 tot 3. We hebben in een groepssessie 24 digitaal wijkagenten ernaar gevraagd: dertien gaven aan op niveau 2 te werken en elf op niveau 3.

92 Dit was de uitkomst van een landelijke aanbesteding van jaren geleden. Er vond tijdens het veldwerk een nieuwe aanbesteding plaats voor OSINT-software.

OSINT-specialisten gebruikgemaakt van onderzoeksprofielen op socialemediaplatformen en Telegram. Op dit punt doen zich verschillen voor tussen informatieorganisaties. Binnen sommige informatieorganisaties worden geen onderzoeksprofielen gebruikt om in besloten groepen – waar dus sprake is van 'deurbeleid' – te participeren, terwijl dit in de meeste informatieorganisaties wel plaatsvindt.

> *'Binnen onze DRIO hebben we gezegd, wij gaan niet in besloten groepen, dat vinden we niet tot onze taak behoren. We doen het niet als je moet "aankloppen" om in een besloten groep te kunnen. Er zijn binnen de DRIO wel uitzonderingen, in de heimelijke inwinning en bijvoorbeeld CTER, maar hoe dat precies zit, weet ik niet.'* (31)

> *'Ik zit in zoveel groepjes. Je praat niet mee. Je gaat mensen niet een bepaalde richting opsturen. We kijken alleen mee.'* (32)

Bovenstaande citaten maken dit verschil duidelijk. Er zijn enerzijds informatieorganisaties die de grens leggen bij de aanwezigheid van (selectief) 'deurbeleid', wat wil zeggen dat iemand de opsporingsambtenaar toegang moet geven tot de groep en deze toegang niet vanzelfsprekend is (zie ook hoofdstuk 2). Er zijn anderzijds informatieorganisaties die de grens vooral leggen bij de interactie met subjecten (bij interactie komen we in het domein van de virtual agent terecht). Deze verschillen zijn gerelateerd aan de wijze waarop de reikwijdte van art. 3 Pw wordt uitgelegd. In de volgende paragraaf gaan we hier nader op in.

Met betrekking tot de werkwijze van OSINT-specialisten van de informatieorganisatie kan verder worden opgemerkt dat zij niet alleen online gegevens verzamelen, maar deze ook beoordelen c.q. duiden, opslaan en analyseren. Men maakt deelproducten die – vaak in combinatie met andere informatie – leiden tot informatieproducten die bedoeld zijn voor sturing van politiewerk.

> *'We zitten ook in boerengroepen. Als wij zien dat zij iets plannen/bekokstoven, moeten we dat ook laten weten – signaleren, duiden, rapportje opstellen en doorgeven.'* (32)

> *'De meerwaarde van wat wij met OSINT doen bij de DRIO is het analyseren en duiden. Het is niet een kwestie van gegevens verzamelen, nietje erdoorheen en opleveren, maar we vertellen iets over de kwaliteit, de bronnen en hoe je deze informatie moet zien.' (33)*

Bij het duiden en analyseren van online vergaarde gegevens werken OSINT-specialisten geregeld samen met vakinhoudelijke specialisten. Dit zijn collega's die specialist zijn op een bepaald thema, bijvoorbeeld OMG of synthetische drugs. In een toenemend aantal eenheden vindt deze samenwerking plaats in thematische teams, clusters of *squads* (zie paragraaf 3.4).

Tot slot een opmerking over het bewaren van online vergaarde gegevens. Er is een verschil met gegevens die via het politiewerk op straat, recherchewerk of inlichtingenwerk worden verzameld. Deze gegevens komen terecht in de registratie- of bronsystemen van de politie. Dit geldt niet voor gegevens die online zijn verzameld en zijn gevalideerd. Daar worden documenten van gemaakt, maar die komen niet in een database terecht. Dit heeft als gevolg dat deze gegevens ook niet kunnen worden gebruikt in datawarehouses waarin gegevens worden gecombineerd en geclassificeerd ten behoeve van (geavanceerde) analyses (zie hiervoor Landman, 2022).

> *'Gegevens uit open bronnen komen niet in onze databases terecht. Er worden nu documenten van gemaakt. In databases zit alleen data uit de bronsystemen. De OSINT-data kan dus niet op een vergelijkbare wijze worden gebruikt voor bijvoorbeeld analyses als de data uit bronsystemen. Bijvoorbeeld: in sociale netwerkanalyses van criminele netwerken zou je ook wel Facebook data willen gebruiken en die willen combineren met andere data. Dat kan nu niet. Voor de opsporing is dat anders. Dan ben je gericht op bepaalde subjecten en dat is best goed vast te leggen, in SUMM-IT. Maar voor het monitoren hebben we geen systemen voor het opslaan en analyseren van de OSINT-data. We zijn nu bezig om art. 8, 9 en 10 data te combineren om criminele netwerken goed in kaart te krijgen. Dat is supermooi, maar hoe mooi zou het zijn als daar ook socialemediadata bij kan worden gebruikt.*[93] *Dan krijg je weer hele andere inzichten in de connecties die er zijn.'* (37)

Werkwijze van digitaal wijkagenten

Wat is voor digitaal wijkagenten, die meerdere taken hebben, de aanleiding om met OSINT aan de slag te gaan? Uit de interviews komt naar voren dat de een meer op eigen initiatief online monitort, terwijl de ander vooral uitgaat van vragen van collega's, in het bijzonder 'reguliere' wijkagenten (zie ook Boelens & Landman, 2021).

> *'Ik doe qua werk hetzelfde als de wijkagent. De wijkagent gaat naar buiten en doet een ronde en ik doe dat online. Ik ga websites en platformen af en kijk wat bewoners zeggen en plaatsen. Ik leg dat ook geregeld vast in BVH. Zo versterken we onze informatiepositie.'* (5)

> *'Ik zit niet constant online te surveilleren. Je moet wel input krijgen. Die kan vanuit de leiding, wijkagenten of vanuit blauw komen. Dan ga je gewoon zoeken.'* (7)

De digitaal wijkagenten die op eigen initiatief monitoren, doen dit op basis van een bepaalde focus of afbakening. Dit kan in de eerste plaats een vast lijstje van pagina's en platformen zijn dat wordt langsgegaan (zie ook Terpstra et al., 2021). Daarnaast wordt door een deel van de digitaal wijkagenten gebruikgemaakt van PublicSonar. Zij maken op gebiedsgerichte wijze gebruik van bouwstenen.

93 Dan dient wel nadrukkelijk rekening te worden gehouden met het juridisch kader dat volgt uit de Wpg.

> *'Ik heb in PublicSonar een eigen bouwsteen ingericht. Zoekopdrachten worden gefilterd op geolocaties (…) Ik krijg alleen gegevens te zien die binnen mijn basisteam vallen en dat is heel handig. Ik had PublicSonar dinsdag aanstaan en toen zag ik een tweet voorbij komen van een persoon die al eerder voor opruiing heeft gezorgd.'* (4)

Er doen zich ook tussen digitaal wijkagenten verschillen voor met betrekking tot het gebruik van onderzoeksprofielen voor het monitoren op sociale media en in besloten groepen (zie ook Terpstra et al., 2021).[94] Er zijn digitaal wijkagenten die dit vanwege beleid van de eenheid of het team niet mogen en er zijn digitaal wijkagenten die hier wel gebruik van maken (zie ook paragraaf 4.3).[95]

> *'Ik heb een fake account en ik zit in een aantal groepen.'* (4)

> *'Ik moet wel fake accounts hebben om die groepen te checken, maar dat mag ik niet. Wij doen bijna geen socialmediaonderzoek. Als we het doen, is het tegen de interne regels.'* (6)

Ook voor deze verschillen geldt: ze zijn gerelateerd aan het gebruik van bevoegdheden. Hierover gaat de volgende paragraaf.

4.3 Gebruik van bevoegdheden

Onduidelijkheden in de praktijk

In hoofdstuk 2 is ingegaan op het juridisch kader. Voor het reguliere intelligencewerk geldt dat het dient plaats te vinden op basis van art. 3 Pw. Op basis van de algemene taakstellende bevoegdheid mogen online gegevens worden vergaard, mits deze vergaring geen meer dan geringe inbreuk op de persoonlijke levenssfeer van de betrokken burgers maakt. Er is in die zin – zo wordt ook door respondenten opgemerkt – geen verschil met het verzamelen van gegevens in het fysieke domein.

> *'Op het moment dat je nog geen verdenking hebt tegen een persoon kan het allemaal nog onder artikel 3 Politiewet. Of waarschijnlijk nog niet eens, want je bent randinformatie aan het verzamelen, je bent een beeld aan het verkrijgen.*[96] *Hetzelfde als je*

94 Het is van belang om het monitoren in besloten groepen ten behoeve van intelligence te onderscheiden van het lidmaatschap van een digitaal wijkagent in buurtgroepen. Uit de interviews met digitaal wijkagenten komt namelijk naar voren dat sommigen van hen ook lid zijn van bijvoorbeeld WhatsApp buurtgroepen (zie ook Mehlbaum & Van Steden, 2018). Dit doen zij met een profiel als digitaal wijkagent en dus niet met een onderzoeksprofiel. Het voornaamste doel hiervan is de verbinding met burgers en niet zozeer online gegevensvergaring.

95 Zie ook De Vries & Bantema (2022).

96 Wellicht ten overvloede: de zinsnede 'waarschijnlijk nog niet eens' klopt niet, want je werkt altijd minimaal op basis van art. 3 Pw. Ook de conclusie dat het allemaal op basis van art. 3 Pw kan zonder verdenking klopt niet. Op het moment dat het een meer dan geringe inbreuk maakt op de persoonlijke levenssfeer van betrokken burgers, is art. 3 Pw niet meer toereikend. Zie hiervoor hoofdstuk 2.

als wijkagent door de wijk heen aan het rijden bent om te kijken: "Goh wat gebeurt er nu allemaal in de wijk?".' (30)

De reikwijdte van art. 3 Pw is in de praktijk echter niet altijd duidelijk. Op basis van de interviews kunnen we constateren dat het vraagstuk in het kader van intelligence vooral betrekking heeft op het gebruik van onderzoeksprofielen om gegevens uit afgeschermde bronnen te vergaren.[97] Dit houdt verband met een constatering die door vrijwel alle respondenten wordt gedaan: het vergaren van relevante gegevens via open bronnen wordt steeds lastiger, omdat communicatie in toenemende mate plaatsvindt in besloten groepen.

'Het is complexer geworden om gegevens van internet te halen. Een goed voorbeeld is Facebook. In het begin kon je er alles vanaf halen en nu gaat het steeds meer dicht.' (34)

'We noemen het OSINT, maar die O van OSINT is steeds minder een O. Dat was vier jaar geleden nog wel zo. Dat is niet meer. Die spannende groepjes snappen best dat we meekijken, dus die verbergen zich. Dan kom je in lastiger gebied. Welke bevoegdheden heb je dan?' (37)

De onduidelijkheid die respondenten ervaren, heeft betrekking op de vraag wat men in dat kader mag op basis van art. 3 Pw. Een kernvraag hierbij is welke inbreuk toegang tot en aanwezigheid van een opsporingsambtenaar in een besloten groep maakt op de persoonlijke levenssfeer en of die inbreuk proportioneel is in relatie tot het doel/algemeen belang. Deze vraag is volgens respondenten niet gemakkelijk te beantwoorden. Maakt het uit of een groep tien leden heeft of duizend leden, bijvoorbeeld voor de mate van privacy die groepsleden denken te hebben? Maakt het uit of het een buurtgroep is of een anti-overheidsgroep? Het zijn vragen die sommige respondenten bezighouden.

'Je moet een goede afweging maken als het gaat om besloten groepen. Wanneer is een groep nu besloten? Wij moeten als overheid respect hebben voor de privacy van burgers. Als wij aan de voorkant kunnen nagaan hoeveel mensen er in zo'n groep zitten en wat de aard van de groep is, dan kunnen we ook inschatten welke mate van privacy mensen denken te hebben. Als het deurbeleid is dat je een hekel moet hebben aan de coronamaatregelen en je komt binnen bij een groep van driehonderd man, dan is de mate van privacyschending gering, dus dan durven wij te verkopen dat je dat op basis van artikel 3 kunt doen.[98] Maar als het bijvoorbeeld gaat om een groep van zes personen of een groep Urkers, dan kun je het niet doen ten aanzien van privacy, los van het feit dat je er niet inkomt.' (39)

97 Zie hoofdstuk 2 voor een overzicht van de juridische vraagstukken.
98 Hierbij is de lijn van redeneren die de informatieofficier hanteert ook van belang (zie volgende subparagraaf).

De vorige paragraaf heeft duidelijk gemaakt dat er tussen eenheden verschillend wordt omgegaan met deze onduidelijkheden. Er zijn OSINT-medewerkers – we hebben het nu over zowel de informatieorganisatie als de basisteams – die terughoudend zijn om op basis van art. 3 Pw in besloten groepen (met deurbeleid) te gaan en er zijn OSINT-medewerkers die hierin minder terughoudend zijn en de reikwijdte van art. 3 Pw ruimer interpreteren.

Bij het voorgaande is het van belang een eerder gemaakt punt te herhalen (zie paragraaf 3.5): OSINT-specialisten van de informatieorganisaties kijken soms enigszins argwanend naar de manier van werken in de basisteams. Zij hebben de indruk dat de digitaal wijkagenten in sommige basisteams weinig rekening houden met dan wel op de hoogte zijn van het juridisch kader en vooral gericht zijn op de gegevens die zij willen vergaren. Hierdoor zouden zij met hun manier van werken in besloten groepen art. 3 Pw te buiten gaan. Het gaat dan over aanwezigheid in besloten groepen met 'deurbeleid' en lichte vormen van interactie (die hier soms voor nodig zijn).

> *'Mensen zijn soms moeilijk te stoppen. Digitaal wijkagenten moeten niet in een besloten Telegram-groep gaan meepraten. Dat moeten ze anderen laten doen (virtual agents, red.). Dat is wel een uitdaging: mensen afremmen als ze zelf denken dat ze lekker bezig zijn.'* (30)

> *'Digitaal wijkagenten doen dingen die gewoon echt niet kunnen en ook niet mogen. Ik had laatst een gesprek met een digitaal wijkagent en die had het over heimelijk dingen doen. Ze willen een telefoon hebben om op Telegram te gaan, zodat ze heimelijk kunnen meekijken. Dat hoort toch niet bij een wijkagent? Op straat heb je toch ook een uniform aan?'* (39)

> *'Nu zijn er ineens digitaal wijkagenten die anoniem groepjes stelselmatig bekijken. Dat kan niet. Daar hebben ze de achtergrond en bevoegdheden niet voor.'* (41)

De digitaal wijkagenten ervaren – meer dan de OSINT-specialisten – onduidelijkheden met betrekking tot 'hoever zij mogen gaan'. In de interviews en groepsgesprekken werd meermaals aangegeven dat er op dit punt behoefte is aan landelijk beleid.

Afstemming met het gezag

De ervaren onduidelijkheden over de reikwijdte van art. 3 Pw maken dat er geregeld behoefte is aan afstemming met het gezag: wat kan wel en wat niet? In de interviews met respondenten ging het in dit kader vooral over online gegevensvergaring in relatie tot het thema openbare orde.

In hoofdstuk 2 is aangegeven dat het juridisch kader geen eenduidig antwoord biedt op de vraag tot welk gezag opsporingsambtenaren zich moeten richten als zij willen afstemmen over online gegevensvergaring ten behoeve van intelligence over openbare

orde. Deze onduidelijkheid in het juridisch kader werkt door in de praktijk. Dit wil zeggen dat er tussen eenheden verschillen zijn in de afstemming met het gezag. Er zijn eenheden die zich richten tot de informatieofficier van het OM.

> *'We vragen de officier bijvoorbeeld of we in een gesloten/besloten groep mogen deelnemen vanuit de DRIO om te kijken wat er wordt gezegd over locaties waar mensen heen gaan tijdens demonstraties. Dat zijn geen aparte bevoegdheden, dat doen we op basis van art. 3 Pw. Je mag alleen monitoren wat er wordt gezegd, geen mensen benaderen. Zodra de reden dat je zo'n groep ingaat voorbij is (bijvoorbeeld een demonstratie), dan moet je er weer uit.'* (37)

Enkele respondenten merken op dat informatieofficieren verschillend oordelen over de reikwijdte van art. 3 Pw in het kader van toegang tot en aanwezigheid in besloten groepen. Staan zij het wel of niet toe? En onder welke omstandigheden wel of niet? De aard van de groep, de grootte van de groep, het doel (monitoren of meer nadruk op identificeren). Dit versterkt de onduidelijkheid die de respondenten (veelal) toch al ervaren.

Er zijn ook eenheden die in het kader van online gegevensvergaring op het gebied van openbare orde afstemmen met de burgemeester. Zij redeneren: het is de openbare orde en dus de burgemeester.

> *'Voor de [corona]rellen hebben we toestemming gevraagd van de burgemeester, omdat er dusdanig veel info gemonitord werd (…) De burgemeester geeft algemeen toestemming van jullie mogen monitoren in de groepen en op een gegeven moment vragen we toestemming aan de officier van justitie van "Hé dit zien we gebeuren en mogen we verder gaan?"'.* (34)

Daarnaast zijn er eenheden die vinden dat de burgemeester het gezag is, maar merken dat de burgemeester dit niet als zodanig (h)erkent en in ieder geval niet gewend is aan die rol met betrekking tot online gegevensvergaring. Om die reden richten zij zich tot de informatieofficier.

> *'Openbare orde, strikt gezien moet de burgemeester je daarvoor toestemming geven om in besloten groepjes te gaan. Als je hier de burgemeester daarom vraagt kijken ze je aan met hè? Die bevoegdheid, zij weten niet wat ze daarmee moeten doen.'* (32)

Er wordt ook gewezen op praktische bezwaren. Het gezag van de burgemeester is gebonden aan de grenzen van de gemeente. De fenomenen en groepen die worden gemonitord, houden zich in de regel niet aan de gemeentegrenzen. Welke burgemeester moet dan worden benaderd om af te stemmen over de activiteiten op het gebied van OSINT (zie ook Bantema et al., 2018)?

'Ik heb nog weinig ervaringen met gezag in openbare-ordemonitoring. Maar ik voorzie wel dingetjes die een probleem kunnen zijn. Je hebt veel burgemeesters in je eenheid, welke moet je dan hebben als een groepje hooligans van de het ene naar het andere gebied gaat? Dat is nog een te ontdekken terrein. Het juridische kader is ook een zaak waar de wetgever zich goed over moet buigen. Wanneer is het wel/niet strafvorderlijk?' (31)

'We hebben ik weet niet hoeveel gemeenten, dat is niet te doen. Maar de politieagent op straat doet ook heel veel op basis van artikel 3 en die heeft ook niet continu toestemming nodig van het bevoegd gezag. Wij moeten onze medewerkers opleiden, zodat ze weten wat ze op eigen gezag en hun moreel kompas kunnen doen en dan komen ze vanzelf op een punt dat ze denken "Oh, dit moet ik even checken". Dan is het geen toestemming, maar meer dat het OM even meedenkt.' (39)

De respondenten in de eenheden die voor de monitoring van de openbare orde in voorkomende gevallen toestemming vragen aan c.q. afstemmen met de burgemeester wijzen erop dat zij alert moeten zijn op de overgang van het gezag naar de officier van justitie. Intelligence- en opsporingsactiviteiten kunnen elkaar in sommige gevallen direct opvolgen doordat het monitoren zicht geeft op individuen die strafbare feiten plegen en die individuen (en hun strafbare feiten) vervolgens nader worden onderzocht (zie ook paragraaf 3.2 over de dunne grens tussen beide).

4.4 Opbrengsten van OSINT

Bijdrage aan de informatiepositie
De opbrengst van OSINT is volgens respondenten – algemeen geformuleerd – dat een bijdrage wordt geleverd aan de informatiepositie van de politie over fenomenen, gebeurtenissen, groepen en individuen. OSINT is hierbij zowel aanvullend op als overlappend met de gegevens die de politie op andere manieren verzamelt. De precieze bijdrage van OSINT aan deze informatiepositie is (door respondenten) niet goed te duiden. Zoals eerder aangegeven (zie paragraaf 4.1): deze bijdrage verschilt ook per thema, groep of gebeurtenis. Bij bepaalde onderwerpen is de informatiepositie in belangrijke mate gebaseerd op online vergaarde gegevens. Dit geldt – zoals eerder aangegeven – bijvoorbeeld voor openbare orde. Respondenten vermoeden dat 70% of 80% van de data die worden gebruikt online is vergaard (respondent 23, 37). Bij andere onderwerpen vormen online vergaarde gegevens een (veel) kleiner deel van het totaal.

Inschatten wat er gaat gebeuren
Een tweede type – of eigenlijk meer specifieke – opbrengst van OSINT is de voorspellende waarde: wat kan de politie verwachten? We geven twee voorbeelden.

'Bijvoorbeeld: er lopen hier nogal wat jongeren met een mes op zak. Stel er heeft een gast iemand anders "geprikt", dan gaat de politie naar het PD (plaats delict, red.).

Wat we zien bij jongeren is dat ze heel snel informatie het op internet plaatsen. Je kunt die informatie gebruiken om de politie die naar het PD gaat van informatie te voorzien, om hun beeld te kunnen versterken. Met hoeveel mensen zijn ze er, zijn er meerdere gewonden, etc.' (26)

'Bijvoorbeeld een paar jaar geleden [in 2014], de situatie met Dwight Lodeweges die overstapte van Cambuur naar Heerenveen. Via OSINT zag men dat er gedoe zou ontstaan met supporters van Cambuur bij het stadion. Wij zeiden: zet de ME klaar, maar daar is niet voor gekozen. Dat is uit de hand gelopen en vervolgens ben je zeven maanden bezig om de verdachten te vinden. Dat had voorkomen kunnen worden.' (23)

Op basis van OSINT kunnen inschattingen worden gemaakt. Hoeveel mensen worden bij een demonstratie verwacht? Waar is de kans het grootst dat er rellen ontstaan? Wat kan de politie aantreffen als zij ter plaatse komt? Dergelijke inschattingen kunnen (mede) worden gebruikt om incidenten of escalaties te voorkomen en keuzes te maken in de operationele inzet. Een actueel voorbeeld op dit gebied betreft de avondklokrellen. Daarover gaat de volgende paragraaf.

4.5 Praktijkcasus: avondklokrellen

Om het gebruik en de opbrengsten van OSINT nader te duiden, gaan we in deze laatste paragraaf in op een praktijkcasus. Dit is een praktijkcasus die in interviews het meest is benoemd, namelijk de avondklokrellen in januari 2021. Dit betreft in het bijzonder de periode tussen 23 en 25 januari waarin er in verschillende steden grote openbare-ordeverstoringen waren met veel geweld. Een deel van onze respondenten (DRIO, BT, maar ook DRR) heeft in deze periode online gegevens vergaard. We baseren ons daarnaast op evaluaties en een analyse van mediaberichten.

Sociale media – en dan in het bijzonder Snapchat, Telegram en (in mindere mate) Whatsapp – speelden in de avondklokrellen een aanjagende rol.[99] Via sociale media gingen oproepen rond om te gaan rellen en deze media werden tevens ingezet om live verslag te doen van de rellen. We citeren het sectorhoofd van de DRIO van de eenheid Zeeland-West-Brabant: 'We hebben nog nooit gezien dat via sociale media in zo'n korte tijd zo veel verschillende mensen en groepen met diverse achtergronden elkaar wisten te vinden én daadwerkelijk de straat op gingen om te rellen.[100]'

99 Zie bijvoorbeeld ook: https://www.nu.nl/tech/6112568/hoe-sociale-media-werden-gebruikt-om-rellen-in-nederland-aan-te-wakkeren.html en https://www.rijnmond.nl/nieuws/203532/kijktip-hoe-sociale-media-jongeren-opzweept-om-te-rellen-en-waarom-het-zo-moeilijk-is-dit-tegen-te-houden

100 https://www.bndestem.nl/breda/politie-over-aanpak-rellen-we-waren-steeds-op-de-juiste-plek-op-de-juiste-tijd~a0727268/

In de periode voorafgaand aan de avondklokrellen werd in alle eenheden het sentiment rondom corona en breder 'maatschappelijk ongenoegen' online gevolgd. Specialisten van verschillende organisatieonderdelen – informatieorganisatie, rechercheorganisatie en BT's – waren in de dagen rond de avondklokrellen 24/7 actief om open bronnen en besloten groepen te monitoren.[101] De omvang van de online berichtgeving/gegevens maakte het in veel eenheden noodzakelijk om samen te werken (zie ook paragraaf 3.5). De informatieorganisatie kon het niet alleen.

> *'Bij de avondklokrellen was de basis binnen de DRIO te dun om alles op te pakken. Vanuit de digikamers (van de basisteams, red.) is het ook opgepakt. Die gingen met een clubje tot 23 uur 's avonds OSINT doen. Toen is wel gezegd "We moeten met elkaar in verbinding zijn"; er zijn liaisons ingericht die informatie naar de DRIO doorsluizen en vice versa.'* (31)

In diverse interviews is aangegeven dat OSINT-specialisten merkten dat hun collega's uit onder andere de basisteams (niet zijnde digitaal wijkagenten) met hun privé- en politie-accounts op het internet naar informatie zochten. Deze collega's stuurden allerlei screenshots naar hen door. Dit was goed bedoeld, maar niet functioneel voor het verkrijgen van een goed informatiebeeld waarin eventueel ook kon worden doorgepakt in de vorm van opsporing.

> *'Op zo'n avond ben ik bezig met veiligstellen wat ik op internet voorbij zie komen. Veel collega's gingen uit goede bedoelingen ook het internet op, maakten screenshots en stuurden die door. Ze doen dat vaak op de verkeerde manier. Je moet vaststellen waar je het vandaan hebt, hoe laat, de context, et cetera. Ik doe het dan liever zelf. We zaten allemaal naar dezelfde dingen te kijken. Het kost veel tijd en energie en levert weinig aanvullende informatie op, ook omdat je de context van die screenshots niet kent waardoor het niet bruikbaar is.'* (30)

Niet alleen politieagenten kwamen in hun privécontext allerlei informatie tegen; ook burgers hebben in deze periode de politie geïnformeerd over voornemens die zij tegenkwamen in chatgroepen (en waarmee men het dus niet eens was).[102] Al met al was er in veel eenheden een grote hoeveelheid online gegevens beschikbaar. In de evaluatie van het Crisisonderzoeksteam (COT, 2021b: 8) over de rellen in Oost-Brabant wordt het volgende geconstateerd: 'De SGBO Oost-Brabant signaleert mogelijke ongeregeldheden in 12 gemeenten in de eenheid. Op het hoogtepunt signaleert de SGBO Oost-Brabant 50-100 sociale media berichten over (oproepen tot) rellen per minuut.' Uit zowel evaluaties als interviews met respondenten komt naar voren dat de overvloed aan informatie én het gebrek aan inzicht in de betrouwbaarheid ervan (moeten we een op-

101 Het ging hierbij enerzijds om bestaande groepen waar burgers hun maatschappelijke ongenoegen uitten en anderzijds om gelegenheidsgroepen die specifiek gericht waren op de rellen (soms met duizenden deelnemers).

102 https://www.bndestem.nl/breda/politie-over-aanpak-rellen-we-waren-steeds-op-de-juiste-plek-op-de-juiste-tijd~a0727268/

roep serieus nemen?), maar ook veel desinformatie het uitdagend maakten om tot een goed informatiebeeld te komen. Deze ervaring maakt ook duidelijk wat eerder is gesteld: het OSINT-vak gaat niet alleen om het online vergaren van gegevens, maar ook over het beoordelen en duiden ervan (zie paragraaf 4.2).

Het (sterk op online gegevens gebaseerde) informatiebeeld heeft gedurende de periode van de avondklokrellen verschillende functies gehad. Op basis van online vergaarde gegevens zijn er acties ondernomen om rellen te voorkomen. In verschillende eenheden zijn opruiers geïdentificeerd en hebben interventies plaatsgevonden. Dit betreft zowel het voeren van stopgesprekken[103] als aanhoudingen. Respondenten geven aan dat op deze momenten intelligence en opsporing (het meest) in elkaar overlopen: de monitoring leidt tot zicht op individuen die opruien en daar wordt vervolgens (in sommige gevallen) strafrechtelijk op doorgepakt. In sommige eenheden gebeurt dit door dezelfde personen, terwijl in andere eenheden het werk wordt overgedragen.

> *'Voor het SGBO Corona zijn we aan het monitoren en zien we ook strafbare feiten. En dan stappen we gewoon door. Je moet wel oppassen hoe je het doet. Als je in opsporing zit en je gaat iemand stelselmatig bekijken, moet je een BOB-bevel maken. Dat probeer ik ook wel aan mensen duidelijk te maken: let op wat je aan het doen bent en op basis waarvan.'* (32)

> *'Maar dan geldt wel: als je informatie tegenkomt die interessant is voor het opsporingsonderzoek, dan zet je die informatie over. Het is binnen de informatieorganisatie niet je primaire taak.'* (37)

Tijdens de rellen hielden 'demonstranten' – vooral rellende jongeren – elkaar op de hoogte van de situatie 'ter plaatse'. Jongeren plaatsten berichten als 'waar moet ik nu naartoe' en 'waar is het nu aan' en er werden allerlei video's getoond van de rellen.[104] Door mee te kijken in deze groepen vergaarde de politie gegevens over afspraken en locaties. Het kon in veel eenheden op veel verschillende plekken misgaan, dus waar zorg je voor welke politiecapaciteit (zoals basispolitiezorg, verkenners, mobiele eenheid)? Het informatiebeeld werd gebruikt voor het maken van keuzes met betrekking tot de inzet van capaciteit en voor de operationele aansturing. Ook dit had volgens respondenten soms preventieve effecten. In de besloten groepen zagen OSINT-specialisten berichten voorbijkomen waarin werd aangegeven dat men ophield met protesteren vanwege de aanwezige politie.

---

103 Het doel van een stopgesprek is om mensen uit de anonimiteit te halen en uit te leggen wat de gevolgen zijn als men strafbare feiten pleegt. Een stopgesprek is altijd een fysiek gesprek waarbij agenten langskomen op het woonadres. Zo worden bijvoorbeeld ook ouders geconfronteerd met het (online) gedrag van hun kinderen. Zie https://www.politie.nl/nieuws/2021/januari/29/08-politie-zit-bovenop-opruiiers-en-onruststokers.html; zie ook https://www.omroepflevoland.nl/nieuws/214837/politie-infiltreert-in-chatgroepen-en-spreekt-oproerkraaiers-aan

104 https://www.rijnmond.nl/nieuws/203532/kijktip-hoe-sociale-media-jongeren-opzweept-om-te-rellen-en-waarom-het-zo-moeilijk-is-dit-tegen-te-houden

> *'In Telegram monitorden wij allemaal berichten over waar ze heen wilden gaan en die speelden wij de hele tijd door. Op Telegram zeiden ze op een gegeven moment "We houden ermee op, want er is teveel politie".'* (21)

De avondklokrellen hebben – tot slot – duidelijk gemaakt dat het op dit moment (in dit soort situaties) ontbreekt aan landelijke informatiecoördinatie, waaronder een landelijk beeld. Verschillende respondenten hebben aangegeven dat zij dit hebben gemist en het noodzakelijk vinden dat hier in de komende jaren in wordt geïnvesteerd (zie ook paragraaf 3.5).

Met deze praktijkcasus is het hoofdstuk over OSINT afgerond. In het volgende hoofdstuk gaan we in op OGG in de context van de opsporing: internetrechercheren.

5 Internetrechercheren

Dit hoofdstuk gaat in op het online vergaren van gegevens ten behoeve van opsporing: internetrechercheren. In paragaaf 1 behandelen we de inzet van internetrechercheren in het opsporingsproces. In paragraaf 2 staan de inbedding en werkwijze van internetrechercheurs centraal. Paragraaf 3 gaat over het gebruik van bevoegdheden en paragraaf 4 over de opbrengsten van internetrechercheren. We ronden het hoofdstuk af met een praktijkcasus.

5.1 Inzet van internetrechercheren

Opsporingsonderzoek
Een opsporingsonderzoek vindt plaats naar aanleiding van een gepleegd (dan wel voortdurend) delict of naar aanleiding van een vermoeden van voorbereidingshandelingen. Een opsporingsonderzoek kan in de eerste plaats starten op basis van een geconstateerd misdrijf. Dit worden ook wel reactieve opsporingsonderzoeken genoemd (zie De Poot et al., 2004). De delicten die op deze wijze worden opgespoord, hebben het karakter van brengdelicten: de politie komt via aangiften en meldingen van burgers op de hoogte van deze delicten (bijvoorbeeld vermogensdelicten). Er zijn daarnaast proactieve opsporingsonderzoeken. Deze onderzoeken starten op basis van informatie dat bepaalde personen zich vermoedelijk met bepaalde misdrijven bezighouden. De delicten die op deze wijze worden opgespoord, hebben vaak het karakter van haaldelicten: de politie moet hier actief informatie over inwinnen, er komt in de regel niemand aangifte van doen (bijvoorbeeld drugshandel).

In een opsporingsonderzoek is waarheidsvinding het doel: het reconstrueren van wat er is gebeurd of gaande is. Bij deze reconstructie wordt getracht de zeven gouden W-vragen zo volledig mogelijk te beantwoorden (De Poot et al., 2004): wie, wat, waar, waarmee, op welke wijze, wanneer en waarom. Ten behoeve van het beantwoorden van deze vragen worden gegevens verzameld. Hiervoor worden opsporingsmethoden ingezet, zoals een verhoor, een buurtonderzoek, een telefoontap of DNA-onderzoek. Internetrechercheren is een relatief nieuwe opsporingsmethode waarbij online gegevens worden vergaard. Er zijn over het algemeen meerdere opsporingsmethoden nodig om te kunnen reconstrueren wat er is gebeurd. Opsporingsmethoden worden naast elkaar ingezet en de informatie die iedere methode oplevert, wordt in samenhang met elkaar gebracht (zie ook Van Berkel et al., 2021). Of anders gezegd: iedere methode levert een

puzzelstukje op en met die puzzelstukjes wordt getracht om de puzzel te leggen (zie Bacon, 2016; Landman et al., 2020; Princen, 2015; Salet, 2015).

Inzet van internetrechercheren in werkvoorbereiding
Met betrekking tot de inzet van internetrechercheren is het in de eerste plaats van belang een onderscheid te maken tussen het voorbereiden en het uitvoeren van een opsporingsonderzoek. Het voorbereiden van een opsporingsonderzoek wordt ook wel 'werkvoorbereiding' genoemd. Dit werkproces vindt plaats op verschillende niveaus in de politieorganisatie, waaronder op regionaal en districtelijk niveau. Werkvoorbereiding bestaat uit het verzamelen en ordenen van informatie ten behoeve van het keuzeproces: wordt een zaak opgepakt? Werkvoorbereiding bevindt zich hiermee op het snijvlak van het intelligenceproces en opsporingsproces. Indien een zaak wordt opgepakt, levert werkvoorbereiding startinformatie voor het onderzoeksteam.
In een districtsrecherche is de werkvoorbereiding belegd bij een operationeel coördinatiepunt (afgekort met COP of OCP). Uit de interviews komt naar voren dat er tussen districtsrecherches verschillen zijn in de mate waarin in deze fase online gegevens worden vergaard.

> *'Ik heb eerst in een team van onze DR gewerkt. Bij de start van het onderzoek had je dan wel internetrecherche. "Kun je even kijken op internet wat je kunt vinden over deze persoon?" En dan houdt het ook wel op. Dan gaat het onderzoek starten met BOB-aanvragen en dat soort dingen. Dan valt internetrechercheren er vanaf. Daarom ben ik naar het OCP gegaan. Daar komen alle zaken binnen. Ik kijk aan de voorkant of ik iets kan vinden over de verdachte, getuigen, noem maar op.'* (14)

> *'Als je iemand hebt in het COP die op social media kijkt, dan heb je het informatiepakket op voorhand klaar, maar dat gebeurt nu niet. Het COP is in ontwikkeling. Daar is vrij recent vorm aan gegeven.'* (15)

Ook op regionaal niveau is er sprake van werkvoorbereiding, in het bijzonder voor proactieve opsporingsonderzoeken. Werkvoorbereiding kan plaatsvinden binnen de informatieorganisatie, binnen de rechercheorganisatie of in een gezamenlijk team.[105] Op dit punt doen zich verschillen tussen eenheden voor. In alle gevallen geldt dat er wordt toegewerkt naar informatie op basis waarvan een eventueel opsporingsonderzoek kan starten. Deze informatie is in de regel onderdeel van een informatierapport of een preweegdocument (zie ook Inspectie Justitie & Veiligheid, 2018). Deze informatieproducten gaan veelal over subjecten waarvan wordt vermoed dat zij zich bezighouden met strafbare feiten. Dit vermoeden is gebaseerd op bijvoorbeeld informatie die is binnengekomen via Meld Misdaad Anoniem (MMA) of is ingewonnen door het TCI.

105 Op dit moment spelen de zogenoemde crypto-analyseteams (met in de regel medewerkers vanuit de DRIO en DRR) een belangrijke rol in de werkvoorbereiding. Zij bereiden op basis van analyse van data uit met name EncroChat en SkyECC opsporingsonderzoeken voor die in rechercheteams worden uitgevoerd. In deze teams worden ook geregeld online gegevens vergaard ten behoeve van identificatie van verdachten.

Deze informatie wordt verrijkt door online gegevens te vergaren over de betreffende subjecten en hun relaties, in het bijzonder via sociale media. Op basis van de interviews hebben we de indruk dat het internet vrij consequent, maar wel beperkt/kortdurend, wordt geraadpleegd.[106]

Inzet van internetrechercheren in opsporingsonderzoek
Dan de uitvoering van opsporingsonderzoeken. Op basis van de interviews hebben we getracht inzicht te krijgen in de mate waarin internetrechercheren als opsporingsmethode wordt overwogen in opsporingsonderzoek. Het is – op basis van deze studie – niet mogelijk om hier precieze, gekwantificeerde uitspraken over te doen. Op basis van de interviews constateren wij dat internetrechercheren niet structureel of standaard wordt overwogen bij de start of gedurende een opsporingsonderzoek. Hierbij doen zich verschillen voor tussen (type) opsporingsonderzoeken. Om dit nader toe te lichten, maken wij gebruik van het *Toewijzingskader* (zie Inspectie Justitie & Veiligheid, 2019). In dit Toewijzingskader wordt een onderscheid gemaakt tussen de VVC die wordt aangepakt door het BT, de high impact crimes die worden opgepakt door de DR en de TGO, en ondermijningsonderzoeken die worden uitgevoerd door de DRR.

Uit de interviews komt naar voren dat de inzet van internetrechercheren in sommige eenheden standaard wordt overwogen bij TGO-onderzoeken. In andere eenheden is dit ook voorgesteld, maar niet van de grond gekomen (respondent 23).

> *'In TGO-onderzoek is het wel standaard; daar loopt een piket voor internetrechercheurs. De inzet van internetrechercheren wordt altijd overwogen bij een onderzoek.'* (25)

> *'In <naam eenheid> zijn toen digitaal coördinatoren geïntroduceerd, die bij de start van een TGO-onderzoek aansluiten, vragen stellen en adviseren over onder andere het gebruik van internetrechercheren.'* (24)

Uiteenlopende respondenten constateren dat bij ondermijningsonderzoeken internetrechercheren ook steeds vaker wordt overwogen. Bij onderzoeken in het kader van high-impact crime en VVC lijkt het overwegen van internetrechercheren minder standaard te zijn.[107] Dit wil zeggen dat het veel wisselender is en er verschillen zijn tussen rechercheteams, maar ook tussen opsporingsonderzoeken (zie vervolg). De internetrechercheurs van de DR die wij hebben geïnterviewd zijn vrijwel allemaal van mening dat er nog te weinig oog is voor de mogelijkheden van internetrechercheren in hun afdeling. Er is volgens hen meer uit te halen.

106 Dit geldt in het bijzonder wanneer het wordt uitgevoerd door de informatieorganisatie, omdat alle medewerkers hier in principe voor zijn opgeleid (OGG niveau 2).
107 Voor high-impact crimes kunnen wij dit overigens beter staven dan voor de VVC, omdat we de VVC-teams van de basisteams nauwelijks hebben meegenomen in dit verkennende onderzoek.

'Ik denk wel dat er veel winst te behalen is, want er wordt in veel zaken niet gekeken naar de mogelijkheden van internetrechercheren. Je moet het ook per zaak bekijken, want je moet niet in alle zaken internetrechercheren.' (13)

'Het is incidenteel. Het is echt dat collega's aan mij vragen: wil je hier even naar kijken, want ik denk dat hier iets te halen valt. Ik denk wel dat het steeds meer wordt, maar het is zeker niet standaard. Het gaat vaak om bijnamen of telefoonnummers en dat je dan kijkt wie je daaraan kunt koppelen. Als je er meer tijd en moeite in steekt, kun je er meer uit halen. Collega's weten niet wat ze wel en niet kunnen met internetrechercheren. Er zijn meer mogelijkheden dan ze denken.' (14)

'Het (internetrechercheren, red.) gebeurt weleens, maar kan in mijn ogen wel meer. De waan van de dag maakt dat er geen tijd is voor internetrechercheren.' (16)

Diverse respondenten hebben factoren benoemd die volgens hen een rol spelen bij de onderbenutting van internetrechercheren. Hieronder gaan we nader op deze factoren in.

Factoren die een rol (lijken te) spelen
Wat maakt dat internetrechercheren wel of niet wordt overwogen bij een opsporingsonderzoek? Op basis van de interviews is een aantal factoren te benoemen.

De eerste factor is het gepleegde delict en de betrokkenen die eventueel in beeld zijn. Met betrekking tot het gepleegde delict is geen heldere categorisering te maken. Respondenten geven aan dat internetrechercheren bij digitale criminaliteit[108] vaak noodzakelijk is, omdat het delict (deels) online is uitgevoerd. 'Bij oplichting op marktplaats kun je er niet omheen', aldus een van de respondenten (22). Maar ook bij andere (typen) delicten kan er een logica zijn die maakt dat internetrechercheren wordt overwogen. Dit hangt vaak samen met de specifieke omstandigheden.

'Het gebruik van internetrechercheren heeft ook te maken met de aard van het incident en de omstandigheden. Met een onnatuurlijke dood kan nog iets op Facebook zijn gezet, wat helpt om te achterhalen of het bijvoorbeeld om zelfdoding kan gaan. Of bij een overval kan een verdachte een bijnaam noemen van iemand, die je dan op social media kunt opzoeken om zo de identiteit te achterhalen en dan kun je weer in onze eigen systemen kijken.' (14)

108 Digitale criminaliteit valt uiteen in cybercriminaliteit (ICT is middel en doel) en gedigitaliseerde criminaliteit (ICT is middel). In de interviews ging het vaker over gedigitaliseerde criminaliteit dan cybercriminaliteit. Dit heeft ermee te maken dat opsporingsonderzoeken naar cybercriminaliteit vooral worden uitgevoerd door de cybercrime teams. Wij hebben geen respondenten uit die teams geïnterviewd.

De kenmerken van de betrokkenen spelen ook een rol: slachtoffers en (mogelijke) verdachten. Uit welke generatie komen ze? Welke rol speelt internet in hun leven? Hoe maken ze gebruik van internet in het algemeen en sociale media in het bijzonder?

> *'Het nut van internetrechercheren is per onderzoek verschillend. Waar heeft het delict plaatsgevonden, uit wat voor doelgroepen komen verdachten, in welke wereld of omgeving speelt het zich af, et cetera. Er was bijvoorbeeld een minderjarig meisje dood aangetroffen. Het verhaal eromheen bevond zich allemaal op internet. Dan moet je daar de focus op leggen en op sturen.'* (29)

De tweede factor heeft te maken met de 'mindset' van recherchemensen: er kan in rechercheonderdelen of onderzoeksteams een oriëntatie aanwezig zijn op bekende opsporingsmethoden (zie ook Landman et al., 2020; Zuurveen & Stol, 2020). Naarmate men meer georiënteerd is op 'traditionele' opsporingsmethoden zouden nieuwere opsporingsmethoden, zoals internetrechercheren, minder worden overwogen. Internetrechercheren zou pas in beeld komen als deze 'traditionele' opsporingsmethoden tot onvoldoende resultaat hebben geleid.

> *'Er zijn nog steeds collega's die "old school" denken – zoals we al 100 jaar rechercheren – en dat ook blijven doen. Die staan niet open en hebben geen breed vizier (…) Je kunt nooit iedereen overtuigen. Daar moet je ook geen tijd aan verspillen. Die groep wordt namelijk steeds kleiner en kleiner en op een gegeven moment dooft die uit.'* (21)

> *'Internetrechercheren wordt vaak pas ingezet als andere opsporingsmethoden onvoldoende resultaat geven. Veel oudere rechercheurs zitten vast in de traditionele patronen van het opsporingswerk.'* (23)

Ten derde en in het verlengde van het vorige punt: diverse respondenten – vooral vanuit de districtsrecherches – wijzen erop dat degene die leiding of sturing geeft aan het onderzoek een doorslaggevende rol heeft.[109] Zij hebben veel invloed op welke opsporingsmethoden worden ingezet. Iemand die affiniteit heeft met internetrechercheren, de mogelijkheden kent en overtuigd is van de (potentiële) meerwaarde zal eerder aansturen op de inzet ervan dan degene die deze affiniteit, kennis en overtuiging niet heeft (zie ook Zuurveen & Stol, 2020[110]).

> *'De coördinator van het onderzoek bepaalt het. Om dat te kunnen bepalen, moet die wel inzicht hebben in de mogelijkheden van openbronnenonderzoek. Als je niet over de juiste kennis beschikt, dan kun je geen goede keuzes maken.'* (15)

109 Leidinggeven aan opsporingsonderzoek vindt vaak gelaagd plaats. In een DR is er in de regel een senior die zaakscoördinator is en een operationeel expert (OE) die op iets meer afstand leidinggeeft aan het onderzoek. In een DRR is er vanuit de tactiek in de regel een OE die tactisch coördinator is en een operationeel specialist C die de rol van teamleider (hele onderzoek) vervult.

110 Dit betreft een onderzoek naar digitale sporen in brede zin.

'Het is afhankelijk van mensen die onderkennen dat je in opsporingsonderzoek iets kunt met internet; dat er sporen zijn achtergelaten die kunnen bijdragen. Onderzoeksleiders zijn daarin belangrijk.' (21)

Een aantal respondenten haalt specifiek aan dat zij merken dat sommige coördinatoren de indruk hebben dat internetrechercheren veel tijd kost in relatie tot wat het oplevert en daarom liever 'iets anders pakken'. Internetrechercheurs hebben daarentegen de overtuiging en ervaring dat andere opsporingsmethoden veel tijd (kunnen) kosten, terwijl diezelfde tijd voor internetrechercheren al snel als 'veel' wordt gezien. 'We gaan wel vier uur lang met een koptelefoon op zitten voor tapgesprekken, maar we gaan niet vier uur lang op internet kijken.' (respondent 17).

Er is volgens (veel) respondenten wel langzaam een kentering gaande: degenen die leiding geven aan opsporingsonderzoeken denken steeds vaker aan de mogelijkheid van internetrechercheren. Dit zou onder andere te maken hebben met de komst van relatief jonge seniors, operationeel experts en operationeel specialisten (die onderzoeken coördineren of leiden). Deze zouden meer affiniteit hebben met internetrechercheren dan hun oudere collega's. Hierbij wordt overigens wel opgemerkt dat het geen garantie is. 'Het is aan sommigen van hen ook voorbijgegaan.' (respondent 16).

'De coördinator van een onderzoek heeft veel invloed. Bij sommigen merk je: die is niet geïnteresseerd in internetrechercheren. Als ik mijn klep houd, gebeurt er niets. Heb je een jonge gast, dan zal die sneller naar het internet kijken. De oude stempel denkt er minder snel aan.' (18)

De zinsnede 'als ik mijn klep houd', laat zien dat de inzet van internetrechercheren (logischerwijs) niet alleen afhankelijk is van degene die leiding geeft aan het onderzoek. Uiteenlopende respondenten wijzen hierop: al denkt de teamleider of coördinator er niet aan, anderen doen ook geregeld de suggestie om internetrechercheren in te zetten. Maar ook hierbij geldt: men moet wel inzicht hebben in de (on)mogelijkheden van internetrechercheren. Rechercheurs met een taakaccent op het gebied van internetrechercheren of fulltime internetrechercheurs kunnen op dit gebied vaak de beste inschatting maken. En dat brengt ons op de volgende paragraaf: hun inbedding en werkwijze.

5.2 Inbedding en werkwijze van internetrechercheurs

Inbedding van internetrechercheurs

Met betrekking tot de inbedding van de internetrechercheur is het in de eerste plaats van belang om in te gaan op de verschillende posities die wij in dit onderzoek zijn tegengekomen. Wij hebben vier verschillende 'typen' internetrechercheurs gesproken, te weten:

1. rechercheur met internetrechercheren als taakaccent;
2. internetrechercheur in een uitvoerende rechercheafdeling;

3. internetrechercheur in een specialistische afdeling binnen de DRR;
4. OSINT-specialist binnen de DRIO die (ook) wordt ingezet binnen de recherche.[111]

Deze positie is onder andere van invloed op de mate waarin een (internet)rechercheur bezig is met internetrechercheren en op de verhouding tot de collega (tactische) rechercheurs. De rechercheur met internetrechercheren als taakaccent voert verschillende opsporingsmethoden uit, waaronder internetrechercheren. Het is daarnaast de bedoeling dat deze rechercheur binnen de afdeling – in ons onderzoek gaat het dan om districtsrecherches – vraagbaak is op het gebied van internetrechercheren. In de praktijk komt men moeizaam toe aan zowel eigen internetrecherchewerkzaamheden als het zijn van vraagbaak voor anderen, waaronder het meekijken naar mogelijkheden in andere onderzoeken.

> *'De afgelopen maanden ben ik vooral bezig geweest met een onderzoek naar een geweldsincident waaraan het slachtoffer is overleden. In dit onderzoek was internetrechercheren niet van meerwaarde. Ik ben er drie maanden niet aan toegekomen om iets met internetrechercheren te doen.'* (15)

Een fulltime internetrechercheur binnen een uitvoerend rechercheteam – in ons onderzoek betreft het eveneens de districtsrecherche – heeft meer mogelijkheden om aan uiteenlopende opsporingsonderzoeken binnen de afdeling een bijdrage te leveren, want die wordt (in principe) alleen voor internetrechercheren ingezet. Kenmerkend is dus dat deze fulltime internetrechercheur onderdeel is van de afdeling die de opsporingsonderzoeken uitvoert. Dit is een verschil met degenen die bij specialistische afdelingen werken (type 3 en 4). Internetrechercheurs die onderdeel zijn van specialistische afdelingen werken in de regel op meer fysieke en sociale afstand van de collega's die opsporingsonderzoeken uitvoeren. Hierbij geldt dat de afstand – zowel fysiek als sociaal – voor degenen die werken vanuit de DRIO het grootst is. Daarnaast is voor deze specialisten (beide typen) kenmerkend dat zij aanvullend zijn op wat de (uitvoerende) rechercheteams zelf doen op het gebied van internetrechercheren. Zij worden vooral ingezet in rechercheteams die geen eigen internetrechercheurs hebben en in geval van complexe vragen die niet (zelfstandig) door de daar aanwezige internetrechercheurs kunnen worden opgepakt.[112]

> *'Ik hoef mijn vinger niet meer op te steken om werk te krijgen, omdat ze mij wel kennen. Meestal word ik ingezet voor andere teams van de DRR; teams die geen eigen internetrechercheur hebben.'* (28)

111 Omdat het gaat om inzet in de opsporing gebruiken we hiervoor wel de term 'internetrechercheur'.
112 De verwijzing naar 'complexe vragen' hangt samen met het onderscheid in niveaus van OGG-werkzaamheden (zie par. 3.3).

'De mensen die iRN zijn opgeleid, kunnen zelf een eenvoudige scan doen. Als ze rare dingen tegenkomen, dan krijgen wij deze in de postbus. Dan gaan we naar het team toe en coachen we ze.' (34)

'De teams die eigen specialisten hebben, kunnen het prima zonder ons af. Sommige teams lopen vast en komen bij ons op de lijn.' (38)

Deze verschillende posities nemen niet weg dat internetrechercheurs vergelijkbare ervaringen hebben met betrekking tot de samenwerking met collega's in opsporingsonderzoeken. Deze ervaringen hebben betrekking op een aantal aspecten in de samenwerking.
Een eerste aspect heeft betrekking op de wijze waarop een internetrechercheur betrokken raakt bij een opsporingsonderzoek. Deze betrokkenheid begint in de regel met een vraag vanuit een onderzoeksteam waarop een internetrechercheur reageert.[113] Bij specialistische afdelingen (type 3 en 4) komen vragen soms niet vanzelf binnen, bijvoorbeeld doordat collega's (nog) onbekend zijn met de aanwezigheid van internetrechercheurs in de organisatie die kunnen worden ingezet voor opsporingsonderzoeken. Verschillende respondenten hebben voorbeelden gegeven van situaties waarin zij hun expertise actief hebben aangeboden bij uitvoerende (tactische) teams.

'In de opstartperiode (van internetrechercheren bij TDO, red.) ging ik naar de digitale platformen en tactische teams toe om mijn hulp aan te bieden waar ik dacht dat het zinvol was. Soms haal je er niets uit, maar meestal wel. Volgens mij heb ik drie keer een opdracht moeten halen en vanaf dat moment kwamen ze vanzelf naar mij toe.' (35)

'Het is geen standaard onderdeel van de start van een onderzoek. We houden zelf het nieuws in de gaten. Bijvoorbeeld: de dodelijke aanrijding van het meisje in Marken, dan bieden wij zelf onze hulp aan. Op die manier worden we bekender en worden we ook vaker gebeld, omdat ze ervaring met ons hebben opgedaan.' (24)

Een tweede aspect heeft betrekking op de interactie over de (start)vraag. Vrijwel alle internetrechercheurs hebben ervaringen met (te) algemene vragen. Dit betreft vaak vragen die gaan over specifieke subjecten en het karakter hebben van 'ik wil alles weten over …'. Dergelijke vragen zijn voor de internetrechercheur in de regel te breed en geven weinig houvast voor internetonderzoek.

'Ik probeer binnen mijn eigen districtsrecherche ook altijd aan te geven dat ik wel een goede onderzoeksvraag nodig heb, een concrete vraag. De interactie met de collega is belangrijk om er goed en gericht mee aan de slag te gaan.' (21)

113 Het kan in geval van een specialistisch cluster met internetrechercheurs of OSINT-specialisten ook een coördinator of aanspreekpunt zijn die reageert op binnenkomende vragen.

'Meestal krijg ik de vraag "Wil je alles van dit subject opzoeken op het internet?", maar dan mis ik de context. Die contextinformatie heb ik nodig om lekker te kunnen zoeken op internet en niet alleen de naam en bijvoorbeeld een geboortedatum. Dus meestal vraag ik dan nog "Wil je echt alles weten of ben je op zoek naar iets specifieks?".' (28)

Respondenten geven aan dat de collega's binnen onderzoeksteams niet altijd in staat zijn om de juiste vragen te stellen, al wordt ook diverse keren opgemerkt dat dit steeds beter gaat en zij in toenemende mate specifieke(re) vragen krijgen. Hoe gaan internetrechercheurs om met algemene vragen die weinig houvast bieden? Er worden verschillende strategieën gehanteerd. Een eerste, voor de hand liggende, strategie is om in onderling gesprek de vraag te concretiseren. Het is voor internetrechercheurs dan van meerwaarde om breder te worden geïnformeerd over het opsporingsonderzoek: personen, hun onderlinge relaties, omstandigheden en dergelijke. In interviews werd dit geregeld 'de context van de zaak' genoemd (zie ook Lam & Kop, 2020a). In enkele gesprekken kwam naar voren dat collega's soms terughoudend zijn met het delen van informatie.[114]

'De context van een zaak is voor mij wel van belang. Als ik helemaal niets van een onderzoek weet, weet ik ook niet waar ik op moet letten. Ik heb een keer ruzie gehad met een teamleider die het niet wilde vertellen. Die heb ik toen alles gegeven wat ik kon vinden, tot aan kampioen schaken toen die 4 was en voetballen bij de F. Toen werd de teamleider boos: "Wat moet ik hiermee?". Toen zei ik: "Dat weet ik niet, maar jij wilde alles".' (21)

'Ik zat bij de DRIO in <plaatsnaam>. Ik werd er niet goed van. "Ik wil alles weten van die, maar je mag niets weten van het onderzoek, want dat is geheim". Terwijl: ik heb vanuit intelligence een hogere autorisatie dan zij.[115] Op een gegeven moment kreeg ik weer een vraag van "Ik wil alles weten over die". Toen heb ik alles opgezocht en door de printer gerost, twee dozen vol. "Hier, dit is alles wat ik over die persoon kan vinden" en het op het bureau gegooid.' (30)

Bovenstaande citaten laten zien dat internetrechercheurs soms provocatief omgaan met de combinatie van een algemene (veelomvattende) vraag en weinig contextinformatie. De vraagsteller wordt dan overladen met informatie om zo duidelijk te maken dat er meer context nodig is om gericht aan de slag te kunnen gaan. Een tweede strategie is om 'getrapt' te werken. Dit wil zeggen: men voert naar aanleiding van een algemene startvraag een kortdurend internetonderzoek uit en op basis van de opbrengsten gaat men in gesprek over een eventueel (gerichter) vervolg. De achterliggende gedachte is: de vraagsteller weet niet altijd waar die precies naar op zoek is en er is in potentie zoveel te vinden op het internet, dus het is beter om het in tijd te begrenzen en dan verder te kijken.

114 Ook binnen hetzelfde team, dus type 1 of 2.
115 Wellicht ten overvloede: dit is 'type 4'.

'Er is oneindig veel data op het internet, dus wij hebben daar een afspraak over gemaakt. Aan "wie is subject X" spendeer ik een half uur. Dan krijg je na een half uur wat ik gevonden heb. Wij noemen dat in onze eenheid HUIB: half uur internet bevraging. Afhankelijk van de vervolgvraag gaan we ermee verder.' (33)

Een derde aspect van samenwerking heeft betrekking op de intensiteit van de betrokkenheid van de internetrechercheur en diens nabijheid ten opzichte van het onderzoeksteam. Dit aspect hangt samen met wat hierboven 'de context van de zaak' is genoemd. Uit de interviews komt naar voren dat de internetrechercheur diens werk het best kan doen als die goed op de hoogte is van (ontwikkelingen in) het opsporingsonderzoek. Dan kan men zich een eigen beeld vormen van het opsporingsonderzoek en op basis daarvan het internetonderzoek vormgeven. Uiteenlopende respondenten geven aan dat zij het best op de hoogte zijn wanneer zij 'dicht' op het onderzoeksteam werken, wat onder andere wil zeggen dat zij in SUMM-IT toegang hebben tot het onderzoek en kunnen meelezen.

'Ik heb de voorkeur om bij te lezen in het onderzoek en alles op te pakken waarbij ik denk dat internetrechercheren van meerwaarde is. Zo leren mensen wat ik kan toevoegen aan een onderzoek en het zorgt er ook voor dat zij in de toekomst betere vragen kunnen stellen.' (24)

'Ik mis nu de linkjes, omdat ik er niet in zit. Als ik wel in het onderzoek zou zitten, zou ik op die linkjes aanslaan voor internetonderzoek. Daarom willen we graag in de toekomst wel in het onderzoek zitten.' (32)

'In het begin hadden ze (collega's van onderzoeksteams, red.) vaak een brede vraag. Ze weten zelf vaak niet goed wat de vraag eigenlijk is, dan moet je ze nog verder helpen: waar ben je precies naar op zoek? Tegenwoordig lopen we meer langdurige onderzoeken met de recherche samen. Nu ben ik bezig met drie zaken. Dan houd ik SUMM-IT in de gaten, bel ik geregeld met de tactisch rechercheur van "Hé, online is dit gebeurd". Ik zit nu veel dichter op het tactisch team, dus weet beter wat relevant is en kan informatie online beter duiden.' (35)

Werkwijze van internetrechercheurs

Het voorgaande heeft duidelijk gemaakt: ieder internetonderzoek begint met een onderzoeksvraag en het is voor internetrechercheurs van belang dat dit een specifieke vraag is.[116] Deze vraag kan worden gesteld door een collega, maar voor internetrechercheurs die zijn ingebed in een onderzoeksteam geldt dat zij ook hun eigen onderzoeksvragen kunnen formuleren.

116 Het belang van specifieke onderzoeksvragen komt ook naar voren uit de evaluaties van de landelijke OSINT hackathons (zie Lam & Kop, 2020a, 2020b, 2020c).

'Als ik in SUMM-IT zie dat het nog niet is gelukt om te achterhalen welk telefoonnummer is gebruikt, dan denk ik "Hé interessant, daar ga ik wat mee doen" en dan maak ik een nieuw bericht aan in SUMM-IT waarin ik zet wat ik wel of niet heb gevonden.' (24)

Welke acties een internetrechercheur neemt om een onderzoeksvraag te beantwoorden, is afhankelijk van de inhoud van de vraag. Het is iedere keer maatwerk.

'De start van ieder internetonderzoek is een heldere vraag: wat wil je weten? Daarna ga je stapsgewijs verder en check je tussendoor telkens of je op de juiste weg ben en alles kunt herleiden naar de bron. Verder is het afhankelijk van de vraag; er is niets algemeens over te zeggen.' (30)

'Iedere vraag begint anders, maar er zijn wel overeenkomsten. Wat je continue moet doen, is haakjes vinden. Namen, hobby's, telefoonnummers, emailadressen, wachtwoorden, et cetera. Of je krijgt een afbeelding en dan moet je zoeken waar die is genomen. Het is heel moeilijk om te zeggen "Je begint zo en dan moet je die stap nemen en dan die".' (34)

In bovenstaand citaat wordt benadrukt dat de werkwijze van de internetrechercheur wel een aantal terugkerende kenmerken heeft. Deze benoemen we hier op hoofdlijnen.

Een eerste kenmerk – dat overigens ook van belang is voor intelligence, maar daar minder expliciet werd genoemd – heeft betrekking op de veiligheid van het internetonderzoek zelf. Dit wordt in de internationale (OSINT) gemeenschap ook wel OPSEC genoemd: *operational security*.

'Er wordt soms door collega's wat te gemakkelijk gedaan over internetrechercheren. "Dat is een beetje zoeken op internet", maar je moet bijvoorbeeld ook echt wel denken aan OPSEC. Hoe start je een internetonderzoek, hoe doe je dat veilig, zodat je het niet stuk maakt door hoe je begint.' (21)

Een tweede kenmerk heeft betrekking op de 'haakjes' uit een van de bovenstaande citaten: de internetrechercheur werkt van datapunt naar datapunt (zie ook paragraaf 5.5 en 6.1). Bijvoorbeeld het vinden van een verdachte om die te kunnen aanhouden: kinderen van de verdachte achterhaald via sociale media, een van de kinderen gevonden op Snapchat, via Snapchat ontdekt waar het kind op school zat en via de website van de school het rooster voor de tienminutengesprekken gevonden. Dit voorbeeld illustreert de werkwijze van haakje naar haakje.[117]

117 Zie par. 2.3 over stelselmatigheid: deze haakjes zijn afzonderlijke stappen die ook in combinatie tot stelselmatigheid kunnen leiden. Het voorbeeld maakt ook duidelijk dat het van tevoren lastig is in te schatten, omdat men niet weet hoeveel stappen er kunnen worden gemaakt. Het kan immers ook na twee haakjes stoppen, omdat er geen relevante gegevens meer te vinden zijn. Zie ook par. 5.3.

Een derde kenmerk is het gebruik van verschillende bronnen. De internetrechercheur werkt op het internet, maar maakt ook gebruik van andere bronnen om zo weer nieuwe haakjes te vinden waarop men door kan gaan. Een voorbeeld zijn gegevens uit gegevensdragers, zoals laptops en telefoons. Bijvoorbeeld: als er bij kindermisbruik een laptop van een verdachte in beslag is genomen, dan worden er door de bank genomen veel foto's aangetroffen. Die foto's kunnen worden gebruikt om nog onbekende slachtoffers te traceren. Daarnaast maken internetrechercheurs veel gebruik van politiesystemen. Het gaat dan in het bijzonder om de Basisvoorziening Informatie – Integrale Bevraging: een applicatie die politiemedewerkers in staat stelt om met één bevraging informatie uit verschillende bronsystemen te genereren.

Een vierde kenmerk is dat internetrechercheurs naar eigen zeggen veelal handmatig online gegevens vergaren. Men gaat handmatig van datapunt naar datapunt en maakt tussendoor screenshots van de gegevens die worden vergaard. Er worden af en toe tools gebruikt om gegevens automatisch van het internet af te halen. Dit zijn vaak zogenaamde add-ons: software waar een of meer nieuwe functies aan (veelal) de browser worden toegevoegd (zie ook paragraaf 6.2).

> *'Ik gebruik wel regelmatig add-ons. Daar heb ik hele lijsten van. Het verschilt per onderzoek welke ik gebruik. Bijvoorbeeld een instant data scraper waarmee ik in één keer een heleboel gegevens kan vinden en deze kan overzetten naar Excel.'* (24)

Daarnaast worden er binnen de politie eigen scripts geschreven. Een groot deel van de internetrechercheurs doet hierbij een beroep op technisch onderlegde collega's, maar er zijn ook enkele (geïnterviewde) internetrechercheurs die dit zelf doen. Deze scripts bieden de mogelijkheid om op maat de gegevensvergaring te automatiseren.

> *'Af en toe programmeer ik iets om mijn werk gemakkelijker te maken, om het te automatiseren. Bijvoorbeeld als ik één keer in de tien minuten op Facebook wil zoeken of iets naar voren komt. Dan schrijf je daar een script voor, zodat ik een melding krijg.'* (41)

Er wordt ook (soms) 'off the shelf' software gebruikt om de vergaarde gegevens te analyseren. In dit kader wordt door uiteenlopende internetrechercheurs de software 'Maltego' benoemd (zie ook paragraaf 6.2). Deze wordt gebruikt om gegevens (personen, maar ook webpagina's, domeinen, accounts, etc.) met elkaar te verbinden en de uitkomsten hiervan grafisch weer te geven.

> *'Als je connecties uit de gegevens wil halen, dan gebruiken we daar Maltego voor. Als je dat allemaal handmatig moet doen, dan is dat heel moeizaam.'* (34)

Een vijfde en laatste element heeft betrekking op de verslaglegging. Voor internetrechercheurs is het van belang dat zij bijhouden hoe zij te werk zijn gegaan, waaronder de zoekslagen die zij hebben gemaakt en de bronnen zij hebben bezocht. De gegevens die zij verzamelen, kunnen immers worden gebruikt in het uiteindelijke proces tegen de verdachte (Oerlemans, 2017). Uit de interviews komt naar voren dat internetrechercheurs bijhouden welke stappen zij zetten. Dit doen zij door printscreens te maken en in bijvoorbeeld een word-document te zetten of door gebruik te maken van de add-on Hunchly, die bijhoudt wat je online doet (zie ook Ferwerda, 2022).

> *'Hunchly houdt bij wat ik allemaal doe online. Soms zit je in een onderzoek en dan klik je door en klik je door, dan ga je een proces-verbaal opmaken en moet je soms 10 stappen terugdenken. Dat is soms niet meer te doen. Daarvoor is Hunchly heel handig.'* (35)

In SUMM-IT worden de opbrengsten van internetonderzoek gemuteerd. Wanneer de gegevens die zijn vergaard van belang zijn voor het procesdossier wordt er een proces-verbaal opgemaakt. Of er een proces-verbaal wordt gemaakt, hangt dus vooral af van wat er met online vergaarde gegevens gebeurt in het vervolg van de opsporing en vervolging.

> *'Ik maak soms een proces-verbaal. Als ik niets heb gevonden, dan zet ik het in een mutatie in SUMM-IT. Maar als het nodig is, maak ik er een proces-verbaal van. Als er bijvoorbeeld een motor gebruikt is bij een liquidatie en we vinden op Facebook van de verdachte een foto met die motor en er zit een deuk in, dan maak ik daar een proces-verbaal van. Daar zet ik in welke stappen ik heb gezet.'* (24)

> *'Het ligt eraan. Als het proces-verbaal noodzakelijk is, omdat er iets (bewijs, red.) op gebouwd gaat worden, dan maak ik er een. Ik heb veel telefonisch contact met rechercheurs en dat stem ik dan af. Bijvoorbeeld: als we via het Facebook account tot een telefoonnummer van een verdachte zijn gekomen, die vervolgens wordt gebruikt voor een tap, dan maak ik een proces-verbaal op. Dat telefoonnummer komt namelijk ergens vandaan.'* (35)

Vooral respondenten van districtsrecherches merken op dat de wijze waarop een proces-verbaal wordt gemaakt tussen internetrechercheurs verschilt. Wat zet je er wel en niet in? Zij hebben behoefte aan meer eenduidigheid, bijvoorbeeld door middel van een format, en missen op dit punt sturing.

> *'Bijvoorbeeld: de een zet wel een tijd erbij en de ander niet. Daar moet echt uniformiteit in komen. Ik heb al tig keer gezegd dat we om tafel moeten (…) Het is wel zwemmen. Er is geen begeleiding en sturing. Die behoefte heb ik wel.'* (18)

5.3 Gebruik van bevoegdheden

Stelselmatigheid in de praktijk
De geïnterviewde internetrechercheurs geven aan dat zij een aanzienlijk deel van hun werkzaamheden uitvoeren op basis van algemeen taakstellende bepalingen. Dit wil zeggen dat zij – naar eigen zeggen – online gegevens vergaren op een wijze die niet meer dan een geringe inbreuk maakt op de privacy van de persoon over wie gegevens worden verzameld.

> *'Het grote gros van mijn werk valt onder artikel 3. Dat komt ook doordat het vaak gaat over kleine en snelle zaken. Als je op een langdurige zaak zit waarbij je personen langer gaat volgen, dan vraag ik wel vaak of er een 126j kan worden aangevraagd. Bij TGO's weet je dat eigenlijk al van tevoren.'* (21)

De bovenstaande respondent interpreteert stelselmatigheid vooral in termen van de duur: als een verdachte langer wordt gevolgd, is er sprake van stelselmatigheid. Deze respondent was niet de enige die duur of 'frequentie' als criterium voor stelselmatigheid beschouwde. Met name sommige respondenten van de districtsrecherches brachten het belang van frequentie naar voren. Zij gaven ook aan dat zij 'uit de stelselmatigheid' bleven door in één keer zoveel mogelijk online gegevens over een persoon te vergaren.

> *'Als je vaker op dezelfde persoon zoekt, dan krijg je inzicht in de levenssfeer. Dan moet je een 126j aanvragen. Het is niet heel werkbaar om dat iedere keer te doen. Dus je moet jezelf realiseren: als ik ga zoeken, doe ik het in één keer goed. Dat is mijn conclusie. Ik heb tegen mezelf gezegd: zoek in één keer goed, haal alles eraf en stel dat veilig.'* (15)

> *'Ik doe één keer onderzoek en dat doe ik goed en uitgebreid. Ik pluis dan alle bronnen uit. Ik ga echt niet dagenlang hetzelfde onderzoek uitvoeren. Het is leuk dat je een jongerengroep inzichtelijk wil maken, maar je moet niet iedere dag hun gaan volgen en iedere dag het internet doorzoeken. Dat gaat 'm niet worden. Dat krijg je ook niet goed op papier (met een glimlach, red.).'* (17)

Op basis van het juridisch kader uit hoofdstuk 2 kunnen we constateren dat dit geen juiste interpretaties van stelselmatigheid zijn. Stelselmatigheid gaat over de inbreuk die het online vergaren van persoonsgegevens maakt op de persoonlijke levenssfeer van de verdachte en niet over de duur of frequentie. Ook met één zoekactie kan er een meer dan geringe inbreuk op de privacy van de verdachte worden gemaakt en dus sprake zijn van stelselmatigheid.

Met betrekking tot stelselmatigheid leefde er bij respondenten – naast duur en frequentie – nog een derde thema: het gebruik van onderzoeksprofielen, in het bijzonder

voor toegang tot afgeschermde bronnen. Het gebruik van onderzoeksprofielen is onder onze respondenten vanzelfsprekend: zij zoeken online geen gegevens over verdachten met een naar hen herleidbaar account. Hierbij geven respondenten aan dat zij geen interactie aangaan met een verdachte.

> *'Ik heb veel fake profielen, maar ik zal nooit contact leggen met iemand die ik onderzoek om zo meer informatie in te winnen. Dat doen wij (districtsrecherche, red.) niet.' (17)*

De verschillen van inzicht hebben vooral betrekking op het verkrijgen van toegang tot afgeschermde bronnen met een onderzoeksprofiel. Volgens sommige respondenten is er dan per definitie sprake van stelselmatigheid en dus is een bijzondere opsporingsbevoegdheid vereist, terwijl anderen de nadruk leggen op de gegevens waartoe toegang wordt verkregen: als er geen min of meer volledig beeld van de aspecten van iemands leven wordt verkregen, dan is er nog geen sprake van stelselmatigheid. Daarnaast bestaat er onduidelijkheid over wat als een afgeschermde bron moet worden beschouwd.

> *'Is Facebook een gesloten netwerk? Ik kan ja en nee zeggen. Ja, want je moet inloggen en nee, want als ik een account heb en jij hebt jouw profiel niet afgeschermd, dan kan ik alles zien. Bij een gesloten chatgroep weet je het wel. En Instagram is bijvoorbeeld ook heel duidelijk: je hebt een privé account of niet en bij een privé account moet je bevriend zijn om informatie te zien.'* (24)

De conclusie op basis van het voorgaande is dat een deel van de respondenten onvoldoende begrip heeft van het juridisch kader ten behoeve van online gegevensvergaring in strafrechtelijk onderzoek (zie ook Jansen et al., 2020: 69). Deze respondenten zijn geneigd om in het kader van stelselmatigheid naar de kenmerken van activiteiten (duur, frequentie) of de aard van bron te kijken in plaats van naar de inbreuk die wordt gemaakt op de persoonlijke levenssfeer van een verdachte vanwege de gegevens die worden vergaard en/of de mate van privacy die deze mag verwachten in de betreffende omgeving. Degenen die denken dat 'in één keer op alles zoeken en veilig stellen' mag op basis van algemeen taakstellende bepalingen, zullen in de praktijk vermoedelijk op onrechtmatige wijze online gegevens vergaren.[118] Het gebrek aan begrip van het juridisch kader speelt meer op het niveau van de DR (taakaccenthouders) dan op regionaal niveau (fulltime specialist), al komt het bij respondenten die werkzaam zijn op regionaal niveau ook voor.

118 In die zin is de denklijn 'een afgeschermde bron = stelselmatig' een minder problematische denklijn, omdat men eerder een bijzondere opsporingsbevoegdheid aanvraagt dan wellicht nodig is. Hierbij moet wel worden benadrukt dat het gebruik van een onderzoeksprofiel om toegang te krijgen tot een afgeschermde bron ook snel zal leiden tot stelselmatigheid. Voor de volledigheid: het gaat dan niet alleen om de gegevens die worden vergaard, maar ook om het gegeven dat de verdachte in een afgeschermde omgeving mag uitgaan van meer privacy dan in een open omgeving. Daarmee wordt er eerder inbreuk gemaakt.

Er zijn uit de interviews punten naar voren gekomen die meer inzicht kunnen geven in wat maakt dat sommige respondenten beperkt begrip hebben van het juridisch kader. Zo valt in de eerste plaats op dat sommige respondenten de *Leidraad bevoegdheden informatievergaring op internet* ten behoeve van de opsporing niet kennen. Dit geldt vooral voor een enkele internetrechercheur van de DR en voor digitaal wijkagenten (zie ook Jansen et al., 2020). Een andere oorzaak die een rol kan spelen, heeft betrekking op opleidingen of breder: vakonderhoud. Sommige respondenten geven aan dat er in hun opleiding niet of nauwelijks is ingegaan op het gebruik van bevoegdheden in de context van politiewerk. Dit betreft opleidingen van private aanbieders (zie paragraaf 6.1). Anderen merken op dat zij jaren geleden een opleiding hebben gevolgd en er sinds die tijd geen actualisering van hun kennis over bevoegdheden heeft plaatsgevonden.

> *'Ik ben vijf jaar geleden op cursus geweest. Ik doe eigenlijk wat ik altijd gedaan heb. Ik ga ervan uit dat het nog steeds mag en kan. Niemand zegt dat het niet goed is. Ik mis sturing en duidelijkheid. Iedereen doet maar wat op dit moment. Iedereen vult het op zijn eigen manier in. Als je het niet terugkrijgt, zal het wel goed zijn toch? Een slimme advocaat zal denk ik altijd wel iets vinden.'* (18)

Een derde mogelijke oorzaak heeft betrekking op de afstemming met het OM (zie de volgende subparagraaf). Diverse respondenten merken op dat officieren van justitie verschillend omgaan met stelselmatigheid. Dit kan bij politiemensen voor verwarring zorgen.

Het voorgaande had betrekking op internetrechercheurs die stelselmatigheid interpreteren op een wijze die niet overeenkomt met het juridisch kader. Het is van belang op te merken dat er ook een enkele respondent is die de leidraad wel kent, maar er bewust van afwijkt. Zij beschouwen de leidraad als te rigide. Het toepassen van de leidraad zou ertoe leiden dat er bij voortduring moet worden gevraagd om een bijzondere opsporingsbevoegdheid. Zij kiezen ervoor om ruimer met de leidraad om te gaan. Dit wil in de praktijk zeggen dat internetrechercheurs meer doen op basis van algemeen taakstellende bepalingen dan volgens de leidraad is toegestaan.[119]

> *'Er is op een gegeven moment een matrix gemaakt waarin staat wat je onder welke bevoegdheden mag doen. Die is heel duidelijk, maar ook wel heel rigide. Bijvoorbeeld: als ik iemand op Facebook bekijk en ik klik drie keer op zijn profiel, dan zou ik al bij een officier van justitie moeten aankloppen. Daar maak ik geen vrienden mee, dus daar gaan we iets ruimer mee om.'* (21)

119 We vermoeden dat men hiermee ook meer doet op basis van algemeen taakstellende bepalingen dan volgens het juridisch kader is toegestaan. Dit weten we niet zeker, want we kennen de matrix uit de leidraad niet.

Tot slot: welke bevoegdheid wordt gebruikt indien er sprake is van stelselmatigheid? Respondenten verwijzen naar het gebruik van stelselmatige informatie-inwinning (art. 126j Sv). We hebben geen respondenten gehoord over het gebruik van stelselmatige observatie als juridische grondslag. Op basis van de interviews kunnen we constateren dat stelselmatige informatie-inwinning geregeld wordt ingezet, al zijn er veel verschillen tussen respondenten. Van een enkele keer in de loopbaan, via een enkele keer per jaar, tot meer dan tien keer per jaar.

> *'Artikel 3 biedt best wel veel. Als het stelselmatig wordt, dan is het vaak een 126j. Dat komt wel vaak voor.'* (25)

> *'Ik heb nu toevallig een zaak met een 126j. Ik ben iedere week twee dagen in de week aan het kijken naar die persoon en zijn activiteiten, dus dat is zeker stelselmatig.'* (35)

Afstemming met het gezag

Uit de interviews komt naar voren dat er over bevoegdheden geregeld afstemming wordt gezocht met de officier van justitie. Dit betreft de officier die het gezag over het betreffende opsporingsonderzoek heeft (zaaksofficier). Wie deze afstemming zoekt, kan verschillen: de teamleider of coördinator van het onderzoek, een tactisch rechercheur waarmee de internetrechercheur samenwerkt of (soms) de internetrechercheur zelf.[120] De afstemming is vooral gericht op de vraag of er sprake is van stelselmatigheid en er dus een bijzondere opsporingsbevoegdheid nodig is. Er zijn tussen opsporingsambtenaren verschillen ten aanzien van hoe 'snel' zij een officier van justitie raadplegen in geval van onzekerheid over bevoegdheden: de een gaat eerder uit van het eigen inschattingsvermogen en de ander neemt liever het zekere voor het onzekere. De omstandigheden – zoals de aard van het opsporingsonderzoek of de methode die wordt toegepast – spelen ook een rol.

> *'Stel je voor ik kan helemaal niets vinden over iemand, dan wil ik kijken of ik de personen rondom kan bevragen of ik informatie kan vinden. Afhankelijk van het onderzoek overleg ik dat met een officier van justitie. Dit heeft ook te maken met het strafbare feit dat gepleegd is. Bij de billentikker in het park (dit is een voorbeeld dat eerder in het gesprek is gegeven, red.) kunnen we het gemakkelijker zelf bepalen, maar bij mensen die in grootschalige drugshandel zitten en liquidaties dan vind ik het prettig het bij de officier te checken of ik dit onder normale bevoegdheid kan doen of dat ik ervoor een BOB-verzoek moet indienen.'* (24)

> *'Er kan een heleboel onder artikel 3, maar een heleboel ook niet. Als ik bijvoorbeeld een socialenetwerkanalyse wil uitvoeren, dan stem ik af met de officier van justitie. Ik*

120 Dit hangt ook af van hoe de internetrechercheur in het opsporingsonderzoek is ingebed: een internetrechercheur die geen onderdeel is van het onderzoeksteam neemt door de bank genomen niet zelf contact op met de officier van justitie (zie par. 5.2).

had een situatie in <plaatsnaam> met zes jongens die scooters stalen. Vier jongens waren geïdentificeerd. Die hadden een Facebook profiel en een vriendenlijst. Die data heb ik in Maltego (software, red.) gebruikt voor een socialenetwerkanalyse. Dan kun je bijvoorbeeld zien met wie die vier jongens allemaal ook bevriend zijn. Daar kunnen die twee anderen tussen zitten. Dat mag niet op basis van artikel 3. Daarvoor moet ik naar de officier van justitie en wie weet is er een BOB-verzoek nodig.' (24)

De ervaringen met afstemming met de officier van justitie zijn wisselend. Er zijn respondenten die aangeven dat officieren verschillend reageren op hun vragen en verzoeken: de ene officier vindt al snel dat er sprake is van stelselmatigheid, terwijl de andere officier hier 'rekkelijker' naar kijkt.

'Ik heb het liefst maar met één officier van justitie contact, omdat die maar één mening heeft. Als ik met drie officieren spreek, heb ik drie meningen. Ik merk langzamerhand wel verandering, maar ik merk nog veel verschil over stelselmatigheid.' (39)

'Er kan nog wel eens verschil van interpretatie bestaan bij officieren van Justitie, vooral over stelselmatigheid. De ene zegt "Ja, iedereen kan erbij" en de ander zegt "Ja, leuk, maar je ziet wel zijn hele privéleven".' (41)

Vooral enkele internetrechercheurs van districtsrecherches geven aan dat sommige officieren van justitie naar hun idee weinig expertise hebben op het gebied van internetrechercheren. Deze officieren zouden daardoor soms oordelen dat een bijzondere opsporingsbevoegdheid niet nodig is, terwijl de internetrechercheurs denken dat dit wel nodig is.[121]

'Op Facebook zou iemand in een gesloten groep van alles gezegd hebben over vernieling en brandstichting. Ik dacht aan een 126j. Je gaat toch ergens naar binnen met een fake account. Ik kreeg vandaag bericht terug. De officier van justitie vond het goed, maar wel op basis van artikel 3, want het is niet stelselmatig. De officier weet volgens mij zelf niet welke artikelen erbij horen. Ik denk niet dat het heel bekend is bij de officieren. Je gaat ergens naar binnen toe. Artikel 3 is gewoon rondkijken. Het is wel een moeilijk verhaal. Zo lang doen we het nog niet. Daar valt nog wel veel te halen.' (14)

De meeste respondenten ervaren echter dat de afstemming met de officier van justitie over internetrechercheren steeds soepeler verloopt. Dit komt volgens hen doordat de nieuwigheid er inmiddels wel vanaf is; ook officieren hebben meer ervaring opgedaan met de inzet van bevoegdheden in een online omgeving.

121 Dit citaat heeft betrekking op de inhoud van de vorige subparagraaf. De interpretatie is: besloten groep = stelselmatigheid.

'Officieren raken er meer mee bekend en merken dat sommige dingen minder spannend zijn dan ze lijken. We moesten in het begin uitleggen dat we voor Facebook een fake account nodig hadden om te kijken. Nu hoor je daar niemand over. Je overtreedt alleen de regels van Facebook. Dat hebben we inmiddels allang goed gevonden. Je komt wel snel terecht in stelmatigheid. Bij een aantal keer kijken, vraag ik een 126j. Die wordt wel snel gegeven bij feiten waar het van belang is. Dat valt binnen de kaders. Als je uitlegt dat je stelselmatigheid alleen gebruikt om verschillende keren te kijken, dan is het goed. Het is toch iets anders dan een observatieteam.' (21)

5.4 Opbrengsten van internetrechercheren

Internetrechercheren als één van de puzzelstukjes
Aan het begin van dit hoofdstuk is aangegeven dat er in een opsporingsonderzoek in de regel verschillende opsporingsmethoden worden ingezet. De informatie die iedere methode oplevert, wordt in samenhang met elkaar gebracht (zie ook Van Berkel et al., 2021). Het beste resultaat kan worden behaald als de juiste combinatie van opsporingsmethoden wordt ingezet, maar op voorhand is het niet aan te geven wat de juiste combinatie is (zie De Poot et al., 2004). Dit komt onder andere doordat het vooraf lastig is in te schatten wat een opsporingsmethode aan bewijsmiddelen (hoofdbewijs of steunbewijs) of sturingsinformatie gaat opleveren.[122]

Het bovenstaande geldt ook voor internetrechercheren. Respondenten geven bij voortduring twee boodschappen: 1) de opbrengsten van internetrechercheren zijn wisselend: de ene keer heeft het veel meerwaarde voor een opsporingsonderzoek en de andere keer weinig tot niets, en 2) de informatie die via internetrechercheren wordt verzameld is vaak één van de puzzelstukjes in een groter geheel.[123] Op basis van de data uit de interviews hebben we de opbrengsten van internetrechercheren onderverdeeld in een aantal categorieën.

Identificeren
Een eerste opbrengst van internetrechercheren is het identificeren van degenen die betrokken zijn bij een strafbaar feit. Het antwoord op de wie-vraag (zie ook Smilda & de Vries, 2017). Dit betreft in de eerste plaats de verdachte(n). Internetrechercheren heeft vooral meerwaarde wanneer er een 'haakje' is naar een mogelijke (mede)verdachte, maar diens identiteit nog onbekend is. Er is dan wel een telefoonnummer dat is gebruikt of een bijnaam die bijvoorbeeld in gesprekken op de telefoontap wordt ge-

122 Hoofdbewijs wil zeggen dat een bewijsmiddel (stuk informatie) de delictsomschrijving van het ten laste gelegde strafbare feit geheel dekt. Steunbewijs wil zeggen dat een bewijsmiddel slechts een deel dekt, maar wel een bevestiging bevat van een deel van het hoofdbewijs. Sturingsinformatie wil zeggen dat de verzamelde informatie wordt gebruikt om bepaalde wegen in het onderzoek (niet) in te slaan.

123 Zie ook de scriptie van Ferwerda (2022) waarin ze constateert dat er weinig onderzoek is gedaan naar het gebruik van online vergaarde gegevens als bewijs.

noemd of online wordt gebruikt.[124] Via internetrechercheren kan in sommige gevallen de identiteit van een (mede)verdachte worden achterhaald.

> *'Na de coronarellen hadden we iemand die een politieagent had bedreigd. Die heette online overal <online pseudoniem>. Wie is deze persoon? Gekeken naar zijn foto's, hij had foto's van zijn vriendin, toen gekeken naar hoe heet die, dat gevonden, toen woonadres gevonden en via daar achter zijn naam gekomen. Dat zijn van die perfecte momenten, dat je het helemaal rond hebt gebreid.'* (35)

Als de identiteit is achterhaald en er sprake is van een verdenking – in de zin van art. 27 Sv – dan opent dit de mogelijkheid tot het eventueel inzetten van bijzondere opsporingsbevoegdheden.

> *'We hadden camerabeelden van een mishandeling waarop twee verdachten in beeld te zien waren. Op basis van de aangifte en een getuigenverklaring kregen we meer aanknopingspunten om hun identiteit te achterhalen. Via internetonderzoek kwamen we op een foto waarop die twee personen samen stonden, in precies dezelfde kleding als op de camerabeelden. Hierdoor kregen we meer zekerheid over hun identiteit en zo kregen we toestemming om telefoontaps in te zetten en hoorden we ze over de mishandeling spreken (…) Internetonderzoek levert vaak een puzzelstukje op dat in combinatie met andere opsporingshandelingen tot bewijs kan leiden.'* (2)

In het bovenstaande gaat het om het identificeren van een of meer verdachten. De verdachte staat vaak centraal in de vraag naar 'wie'. Internetrechercheren kan daarnaast bijdragen aan het identificeren van slachtoffers en mogelijke getuigen.

> *'Bij misbruik wordt er vaak een laptop van een verdachte in beslag genomen. Daar komen vaak veel foto's uit waarmee nog onbekende slachtoffers kunnen worden geïdentificeerd en getraceerd. Die kunnen dan ook een stem krijgen en worden aangespoord om aangifte te doen.'* (21)

> *'Er was bijvoorbeeld een zaak van een kerel die hardloopsters op de billen tikte. Het onderzoeksteam vermoedde dat veel hardloopsters gebruikmaakten van Strava en data uploadden. We hebben internetrechercheren gebruikt voor het identificeren van nieuwe slachtoffers en getuigen om tot nieuwe leads te komen.'* (24)

Het is van belang op te merken dat identificatie geregeld niet alleen op basis van internetrechercheren kan plaatsvinden. In de interviews is aangegeven dat er regelmatig

124 Een specifieke context waarin identificering op basis van internetrechercheren regelmatig plaatsvindt, is de identificatie van accounts die zijn gebruikt in de chatberichten die criminelen naar elkaar verstuurden via versleutelde communicatie en die door de politie zijn veiliggesteld. Zie https://jjoerlemans.com/2021/12/30/overzicht-cryptophone-operaties/ voor een overzicht. Zie ook par. 5.1 over werkvoorbereiding en dan in het bijzonder de voetnoot over de crypto-analyseteams.

gegevens worden gevorderd bij sociale mediaplatformen (zie ook Oerlemans, 2020).[125] Dit wil zeggen dat bij bijvoorbeeld Facebook de IP adressen[126] worden opgevraagd waarmee is ingelogd op een bepaald account, inclusief de gegevens die aan het account zijn gekoppeld. Hiermee kunnen subjecten worden geïdentificeerd.

Verrijken
Een tweede opbrengst van internetrechercheren heeft betrekking op het verrijken van de al bekende gegevens over het leven van een betrokkene. Dit is vaak een verdachte, maar kan ook een slachtoffer zijn. Over veel personen is online informatie te vinden, zeker als iemand actief is op sociale media. Via internetonderzoek kan het 'digitaal aura' van iemand in kaart worden gebracht. Wat voor activiteiten voert iemand uit? Waar komt die vaak? Heeft die een partner? Wie? Welke bezittingen worden getoond? En zo zijn er meer vragen over het leven van een persoon die – mogelijk – door internetrechercheren kunnen worden beantwoord. Zo wordt een completer beeld verkregen van het leven van een persoon.

> *'Het heeft veel meerwaarde voor het compleet maken van het sociale plaatje van een persoon: dagelijkse activiteiten, hobby's, bezittingen, familie, et cetera.'* (19)

> *'Gegevens van sociale media hebben een grote bijdrage in het verhoor. Ik vind het prettig om een gevoel te hebben bij wie voor me zit. Wat vindt hij belangrijk? Een foto met een mooie Mercedes. Foto's van een wintersportvakantie. Foto's met vrienden in de kroeg.'* (18)

Bovenstaande citaten geven een indruk van hoe het verrijkte beeld over het leven van een persoon kan worden gebruikt in opsporingsonderzoek. Het geeft in de eerste plaats allerlei 'haakjes' voor andere activiteiten. Zo kan een internetrechercheur online een mobiel telefoonnummer van een verdachte vinden dat in het opsporingsonderzoek nog onbekend is. Dit biedt een mogelijkheid om een telefoontap in te zetten. Het verrijkte beeld kan ook aanknopingspunten geven om een verdachte te vinden (zie ook lokaliseren). Naast 'haakjes' voor andere activiteiten/methoden kan het verrijkte beeld van het leven worden gebruikt in het verhoor met een verdachte. De verhoorder kan het gebruiken om in te spelen op en te verbinden met de verdachte, maar ook om te confronteren. Een voorbeeld van een respondent: een delict is door een camera opgenomen en dit heeft geleid tot een mogelijke verdachte. Deze ontkent echter degene op beeld te zijn. Via internetrechercheren is een foto van de verdachte gevonden met dezelfde kleding aan als waarmee de dader op het beeld staat. Deze foto is in het verhoor gebruikt en heeft (vermoedelijk) bijgedragen aan een bekentenis.

125 Sociale mediaplatformen hebben hiervoor standaardprocedures c.q. -diensten.
126 Deze zijn ook bruikbaar in het kader van de volgende opbrengst: lokaliseren.

Relateren
Internetrechercheren kan daarnaast bijdragen aan het relateren van personen aan elkaar. Vooral gegevens op sociale media kunnen inzicht geven in relaties tussen personen. Wie heeft een connectie met wie? En wat is de aard van die connectie? Het gaat hierbij niet alleen om vriendenlijsten, maar ook om reacties die worden geplaatst en de inhoud van die reacties. Op basis hiervan kan een sociale netwerkanalyse worden gemaakt, al dan niet met behulp van software. Een dergelijke analyse kan op verschillende manieren meerwaarde hebben. Een voorbeeld hiervan is eerder gegeven in paragraaf 5.3: als er een delict in groepsverband is gepleegd en nog niet alle verdachten zijn geïdentificeerd, dan kan een netwerkanalyse bijdragen aan het verkrijgen van een zoekrichting. Als alle geïdentificeerde verdachten allemaal bevriend zijn met een tiental andere jongens, dan kunnen de nog niet geïdentificeerde verdachten zich hier tussen bevinden. Een ander voorbeeld is een verdachte die zegt een medeverdachte niet te kennen, maar internetonderzoek wijst uit dat ze digitaal bevriend zijn met elkaar, op elkaar reageren en op een foto schouder aan schouder staan. Deze bevindingen kunnen dan worden gebruikt in onder andere het verhoor van de betreffende verdachte.

Lokaliseren
In januari 2022 verscheen in de media het bericht dat een Italiaanse maffiabaas, die al twintig jaar lang werd gezocht door de politie, was aangehouden in Galapagar in Spanje[127] Hij was herkend via Google Street View. De Siciliaanse politie had al aanwijzingen dat hij in Spanje verbleef, maar wist niet waar. Via Google Street View zag de politie twee mannen die voor een winkel met de naam 'El Huerto de Manu' (de moestuin van Manu) stonden te praten. Een van deze mannen vertoonde sterke gelijkenissen met de gezochte maffiabaas, Gioacchino Gammino. In de buurt van deze winkel bleek ook nog een restaurant met de naam Manu te zijn ('Cocina de Manu'). Op de Facebookpagina van dit restaurant stond een foto van de kok, Manuel. Door een litteken op de kin van deze kok kon hij worden geïdentificeerd als Gioacchino Gammino. Toen hij werd aangehouden zou hij hebben gevraagd 'Hoe hebben jullie mij gevonden? Ik heb mijn familie al tien jaar niet meer gebeld!'

Dit is een voorbeeld van de vierde opbrengst van internetrechercheren: lokaliseren van personen. Dit is een van de meest voorkomende en ook meest onderscheidende bijdrage van internetrechercheren (ten opzichte van andere opsporingsmethoden). Onze respondenten hadden er in ieder geval vele voorbeelden van. Met betrekking tot lokaliseren kan een onderscheid worden gemaakt tussen verschillende typen personen. Het betreft in de eerste plaats het lokaliseren van personen die worden verdacht van het plegen van een of meer misdrijven, zoals in het voorbeeld van de Italiaanse maffiabaas. Hierbij wordt – overeenkomstig dit voorbeeld – geregeld gebruikgemaakt van foto's die op internet (in het bijzonder sociale media) staan.

127 https://nos.nl/artikel/2412126-maffiabaas-gepakt-dankzij-google-maps

> *'We zochten in Amsterdam een verdachte. We hebben zijn profiel bekeken en iedere foto bestudeerd totdat we de meest waarschijnlijke wijk konden achterhalen. We kwamen uit op Amsterdam West. Toen zagen we een foto met zijn vriendin. Toen zijn we gaan kijken: wat zien we op de foto en dat combineerden we met eerdere gemaakte foto's. Toen herkenden we een deel van een straat. Dan kom je in het klassieke deel van opsporen. Met je laptop onder je arm ga je dan naar buiten. Op de foto zagen we een witte terrasstoel met een bloemetje. Dan ga je fysiek kijken en dan zie je de woning met een balkon en de stoel met het bloemetje.'* (22)

In sommige gevallen leidt het lokaliseren van een verdachte door middel van internetonderzoek direct tot inzet van bijvoorbeeld een observatieteam of een arrestatieteam. Naast verdachten worden er ook soms onvindbare veroordeelden (voortvluchtigen) gelokaliseerd.[128] Verschillende respondenten hebben deelgenomen aan de landelijk georganiseerde FASTNL hackathon (zie Lam & Kop, 2020b). Tijdens deze dag hebben 86 OSINT experts van binnen en buiten de politie twaalf uur lang internetonderzoek verricht in 85 opsporingsonderzoeken die werden aangedragen door het team FASTNL van de landelijke eenheid. Dit heeft geleid tot zes traceringen van personen op landniveau, twaalf traceringen op plaatsniveau en vijftien traceringen op adresniveau. Tijdens de hackathon was de eerste aanhouding een feit en in de dagen erna volgden nog eens tien aanhoudingen als direct gevolg van de hackathon. Daarnaast werd – tijdens de hackathon – ontdekt dat één persoon in het buitenland was overleden en bleken twee personen in het buitenland te zijn gedetineerd.

Een andere categorie zijn vermissingen. Uiteenlopende respondenten hebben voorbeelden gegeven van situaties waarin vermiste personen door middel van internetrechercheren zijn gevonden.

> *'We hadden bijvoorbeeld een vermissing gehad. Is een team een heel weekend druk met uitzoeken waar dat meisje kan zitten. Ik kom maandagochtend binnen, vind haar op Snapchat, doe een spoedvordering bij Snapchat en heb binnen een paar uur een melding van een IP-adres in het noorden. Ze rijden ernaar toe en vinden het meisje.' (*21)

Verifiëren

Desinformatie op internet is een thema dat in de afgelopen jaren aan belang heeft gewonnen. Steeds meer Nederlanders maken zich zorgen over desinformatie of nepnieuws (zie Commissariaat voor de Media, 2021). Internetrechercheren kan bijdragen aan het verifiëren van informatie die verband houdt met mogelijke criminaliteit of die op een andere wijze de orde verstoort.

128 Zie ook https://www.standaard.be/cnt/dmf20220416_92657188 voor een hackathon in België waar drie voortvluchtigen werden opgespoord. Deze hackathon werd georganiseerd naar Nederlands voorbeeld en met hulp van Nederlandse collega's.

> *'We kregen een MMA-melding dat iemand op Facebook allemaal wapens had laten zien en dat die persoon in een paramilitaire Turkse groep zou zitten. Ik zag inderdaad een foto met wapens, maar op basis van image-reversed search kon ik laten zien dat de foto ergens anders vandaan kwam. De zogenaamde paramilitaire groep was een groep acteurs van een Turkse serie. Met tien minuten internetrechercheren had ik de MMA-melding platgegooid en voorkomen dat een heel team die persoon ging opzoeken. Dat scheelt dus een hoop inzet.'* (21)

Het bovenstaande voorbeeld geeft inzicht in een van de voordelen van verificatie: het kan politie-inzet voorkomen. Respondenten verwachten dat het belang van het verifieren van informatie door middel van internetrechercheren in de komende jaren toeneemt. Het internet is namelijk zowel een bron van desinformatie als van feiten. Higgins (2021) – de oprichter van Bellingcat – formuleert het treffend: 'paradoxaal genoeg zijn feiten in dit tijdperk van desinformatie bereikbaarder dan ooit'.

5.5 Praktijkcasus: lokaliseren van voortvluchtigen

Anton 'Tony' R. is een voormalig bewoner van een berucht woonwagenkamp in Oost-Brabant en is veroordeeld voor een zware mishandeling, enkele druggerelateerde feiten en witwassen. Hij is echter voortvluchtig. Een internetrechercheur probeert te achterhalen waar Anton zich bevindt.[129]

Hij begint met het googelen van de naam van het subject. Ze vinden een inschrijving van een bedrijf in de Kruispuntbank van Ondernemingen, een Belgische variant van de Kamer van Koophandel. Dit leidt tot een adres in Nederland. Dit is echter het al bekende adres op het woonwagenkamp waar hij in het verleden woonachtig was.

De rechercheur zoekt verder in de directe omgeving van het subject. Een gouden regel in het internetonderzoek is: oma's plaatsen altijd een foto van hun kleinzoon op hun Facebookpagina. Hij vindt inderdaad de moeder van het subject en een foto van haar kleinzoon, de zoon van het subject. De Facebookpagina van de oma leidt ook tot de dochter van het subject. Daarnaast valt de rechercheur een Facebookpagina op waarvan de naam een afkorting van één of meerdere andere namen lijkt te zijn. Op dit account is opnieuw de zoon van het subject zichtbaar, en de vrouw waarvan hij gescheiden zou zijn. Dan wordt hem duidelijk waaruit de afkorting bestaat: het zijn de eerste letters van de naam van ons subject, zijn vrouw en zijn zoon.

Dit brengt hem naar de volgende uitdaging: het account lokaliseren. Het gedetailleerd bekijken van de verschillende Facebookpagina's leidt tot (kleine) aanwijzingen naar een regio in Zuid-Frankrijk. Dan besluit de internetrechercheur om te kijken of de

129 Deze casebeschrijving hebben we overgenomen uit Lam & Kop (2020b). Vanwege de privacy van de betrokkenen en het opsporingsbelang zijn namen, feiten en locaties gefingeerd.

zoon van het subject Instagram heeft. Dat blijkt de zoon te hebben; hij is zelfs erg actief. Er staan meerdere foto's op met dezelfde zwarte Porsche Macan op de achtergrond. Met die Porsche in het achterhoofd klikt de rechercheur door de vele vakantiefoto's. Op een gegeven moment ziet hij een foto van een crossmotor bij een tankstation met op de achtergrond: een zwarte Porsche die wordt getankt, met daarnaast een man die volledig aan het signalement van het subject voldoet.

Maar waar is deze foto genomen? Google leert hem dat er in de betreffende regio in Zuid-Frankrijk acht tankstations van deze keten zijn. Op de foto is te zien dat dit tankstation in de buurt van water ligt. Op Google Maps klikt de internetrechercheur op goed geluk op een tankstation aan het water. Dit brengt hem naar de plek waar de zoon van ons subject de foto heeft genomen. Het is waarschijnlijk dat het subject in deze regio verblijft, maar waar woont hij?

De internetrechercheur bekijkt de zoon van het subject nog eens verder. Zo komt hij een foto tegen van het voltallige gezin tijdens een dorpsfeest in Frankrijk. Nog interessanter is echter een Instagrampost. Hij tagt daarin een locatie – een golf & country club – die ook in andere foto's naar voren kwam. Verder onderzoek naar deze golf & country club leert dat alle familieleden van ons subject de Facebookpagina van deze club liken. Tevens plaatst deze club Nederlandstalige advertenties op verschillende sociale media, wat volgens de internetrechercheur op zijn minst opvallend is voor een locatie aan de Franse Zuidkust. Wanneer de internetrechercheur verschillende satellietbeelden van deze locatie met elkaar vergelijkt, ziet hij tevens dat er telkens dezelfde zwarte auto op de parkeerplaats staat. En dat de contouren overeenkomen met de contouren van de eerder waargenomen zwarte Porsche waar ons subject in reed.

Met gebruik van Google Earth (3D) wordt de locatie nader bekeken. Langzaam begint de puzzel compleet te raken. De internetrechercheur kan de eerder gevonden foto's op de meter precies op de kaart plaatsen. Hij vindt zelfs het crossveldje waar de zoon mogelijk rijdt met de crossmotor. Het is zeer waarschijnlijk dat het subject eigenaar is of op een andere manier is gerelateerd aan de golf & country club en daar (in de omgeving) woont. Anton 'Tony' R. is vermoedelijk gelokaliseerd.

Met dit hoofdstuk hebben we de verkenning naar het gebruik van OGG in het kader van intelligence en opsporing afgerond. In het volgende hoofdstuk gaan we in op de mensen die zich bezighouden met OGG en hun professionalisering én op de middelen die zij gebruiken voor OGG.

6 Mensen en middelen

Dit hoofdstuk behandelt de mensen die werkzaam zijn in het vakgebied van online gegevensvergaring: wie zijn deze professionals en hoe zijn zij bezig met hun professionalisering? Daarnaast wordt (beknopt) ingegaan op de middelen die worden gebruikt bij online gegevensvergaring. Dit betreft hardware en met name software (tools).

6.1 Professionals & professionalisering

De achtergrond van OGG-professionals
Hoewel wij niet alle OGG-professionals binnen de politie hebben gesproken, geeft onze groep respondenten wel een indruk van de achtergrond van deze professionals. Het overgrote deel heeft een politieachtergrond, wat wil zeggen dat zij de initiële politieopleiding hebben gevolgd en uitvoerend politiewerk hebben uitgevoerd in de basispolitiezorg en veelal ook in opsporing. Vanwege hun affiniteit met internet zijn zij met OGG in aanraking gekomen.

> *'Ik ben op straat begonnen, daarna naar de recherche gegaan. Bij het overvallenteam dacht iemand "Dat internet is misschien wel wat". Een aantal mensen ging naar een internettraining van FOX IT, waaronder ik. Zo ben ik erin gerold.'* (21)

> *'Ik ben op straat begonnen, daarna doorgestroomd naar de recherche en vervolgens naar de informatieorganisatie gegaan om het CTER-taakveld op te zetten. Toen is ook OSINT-werk begonnen. Later kreeg ik als taak om OSINT binnen de DRIO vorm te geven.'* (37)

Specifiek voor de digitaal wijkagenten geldt dat zij allemaal al werkzaam waren in een basisteam. Toen de rol van digitaal wijkagent werd opengesteld, hebben zij hierop gesolliciteerd of zijn ze ervoor gevraagd. Ook voor hen geldt dat ze al affiniteit hadden met het internet. Ze voerden vaak al taken uit op het gebied van sociale media, zoals het onderhouden van de Facebookpagina van het basisteam of (andere) activiteiten op het gebied van webcare (zie ook Boelens & Landman, 2021). De rol van digitaal wijkagent bood hen de mogelijkheid om zich verder te specialiseren in het politiewerk op het web en hier meer tijd aan te besteden.

> *'Ik deed al veel werkzaamheden die een digitaal wijkagent verricht in mijn functie als generalist in de noodhulp met taakaccent social media. Daardoor was het een logische*

stap om voor digitaal wijkagent te gaan. Ik snap het nut, de noodzaak en de mogelijkheden van de digitaal wijkagent.' (4)

Een kleiner deel van onze respondenten is een zogenaamde 'zij-instromer'. Dit zijn uitsluitend specialisten op regionaal niveau (DRIO/DLIO en DRR). Zij hebben veelal een HBO- of WO-opleiding afgerond (o.a. criminologie, economie, biologie, ICT), in andere sectoren gewerkt en zijn op een gegeven moment met de politie in aanraking gekomen en overgestapt. De rode draad in hun achtergrond is dat ze al affiniteit met het internet hadden en veelal al ICT- en/of informatievaardig waren voordat zij bij de politie kwamen werken. De stap naar de politie werd in de regel gezet vanwege de behoefte om bij te dragen aan de maatschappelijke opdracht van de politie.

'Ik heb bij <naam bedrijf> gewerkt. Toen ik daar werkte, werd ik gevraagd om aan te sluiten bij het onderzoek van de politie naar Robert M. Een aantal van zijn slachtoffers had mogelijk een <naam bedrijf>-profiel. En daarna werd aan mij gevraagd of ik niet bij de politie wilde werken. Dat heb ik toen gedaan. <Naam bedrijf> was toch ten dode opgeschreven.' (24)

'Ik kom van buiten de politie. Ik heb economie gestudeerd en in de bancaire sector gewerkt. Ik ben als financieel analist bij de DRIO begonnen. Ik was wel handig digitaal, thuis een netwerkje aanleggen, onderzoekje op internet doen. Ik heb op een gegeven moment binnen de politie een training gehad over OSINT en viel toen op.' (31)

Gevolgde opleidingen op het gebied van OGG

We hebben de respondenten gevraagd naar de vakopleidingen (hieronder vallen ook trainingen en cursussen) die zij met betrekking tot OGG hebben gevolgd. In tabel 6.1 hebben we opleidingen opgenomen die in de interviews zijn genoemd.

Tabel 6.1. OGG-opleidingen genoemd door respondenten[130]

Organisatie	Opleiding	Korte beschrijving
Aware Online[131]	OSINT training I (beginner)	In deze opleiding leren deelnemers hoe zij veilig onderzoek op het internet kunnen verrichten en maken zij kennis met verschillende facetten van het doen van openbronnenonderzoek. Er wordt ingegaan op zoekmachines, websites, sociale mediaplatformen, het doen van onderzoek naar afbeeldingen en video's en het juridisch kader.
	OSINT training II (professional)	In deze (vervolg)opleiding leren deelnemers meer over onderzoek op (andere) sociale mediaplatformen, onderzoek van websites en over de eigen veiligheid. Ook wordt ingegaan op hoe virtuele machines en Android emulators werken, op onderzoek op deep en dark web en op een geavanceerde vorm van geolocating.

130 Dit is een overzicht op basis van de opleidingen die respondenten hebben gevolgd of volgen. Het is geen overzicht van aanbod waaruit politiemensen op dit moment kunnen kiezen.

131 https://www.aware-online.com/osint-training/

	OSINT training III (expert)	In deze opleiding leren deelnemers op een veilige wijze, binnen de kaders van de wet, gegevens uit open bronnen vergaren, monitoren, vastleggen en verwerken. Deze opleiding leidt (in combinatie met de twee voorgaande opleidingen) op tot expert op het gebied van OSINT.
Data-expert[132]	Basisopleiding internetrechercheren	In deze opleiding leren deelnemers hoe ze effectief gebruik kunnen maken van zoekmachines en -technieken en hoe ze veilig internetonderzoek kunnen verrichten.
	OSINT basis	In deze opleiding leren de deelnemers de basisvaardigheden die benodigd zijn om veilig/anoniem online gegevens te vergaren en deze gegevens te duiden en hierover te rapporteren/verbaliseren. De opleiding gaat in op het gebruik van zoekmachines, onderzoeken van afbeeldingen, e-mailheaders en de eerste stappen op het gebied van onderzoek op sociale media.
	OSINT Advanced	In deze (vervolg)opleiding leren deelnemers extra vaardigheden die benodigd zijn om een diepgaand onderzoek op het internet (inclusief dark web) uit te voeren. Er wordt aandacht besteed aan geavanceerde zoektechnieken, geolocatie-onderzoek en diepgaand onderzoek op sociale media. Ook wordt een eerste aanzet gemaakt tot onderzoek naar cryptovaluta.
	OSINT technical	In deze (vervolg)opleiding leren deelnemers de technische vaardigheden die benodigd zijn om een diepgaand onderzoek op het internet uit te voeren door gebruik te maken van Linux, scrapen en andere hulpmiddelen. Deelnemers leren een deels geautomatiseerd onderzoek uit te voeren met behulp van tools, virtual machines en Python.
Fox-IT Academy[133]	OSINT	In deze opleiding leren deelnemers wat de mogelijkheden en onderliggende technieken van internet zijn, hoe zij met de juiste tools kunnen zoeken en leren zij profielen op te maken van mensen en bedrijven op basis van sociale media informatie.
Intel Academie (onderdeel van de eenheden)	OSINT (basis) opleiding	In deze opleiding leren medewerkers van de DRIO basisvaardigheden voor OSINT-onderzoek (vergaren en duiden/verwerken in informatieproducten) ten behoeve van het intelligencewerk. Deze opleiding wordt op eenheidsniveau gegeven door specialisten van de DRIO.
International Anti Crime Academy (IACA)[134]	DIGOS135/OSINT Module 1	In deze opleiding leren deelnemers om digitale inlichtingen te verzamelen, verwerken en duiden over personen, bedrijven en netwerken. Men leert personen en organisaties online te volgen en te monitoren om zodoende hun plannen en activiteiten in kaart te brengen.
	DIGOS/OSINT module 2	In deze (vervolg)opleiding wordt ingegaan op het gebruik van Case Management Systems, operationele informatievaardigheden (level 2), digitale zaaksanalyse, het samenstellen van een lokale forensische database en het importeren van digitale informatie.
	DIGOS/OSINT module 3	In deze (vervolg)opleiding leren deelnemers digitale informatie te analyseren en visualiseren (o.a. met gebruik van Maltego), alternatieve onderzoeksmethoden en bronnen in te zetten en verdiepen zij hun operationele informatievaardigheden (level 3) en operatiemanagement. Succesvolle afronding van de drie modules leidt tot een post-hbo diploma.

132 https://www.dataexpert.nl/academy/categorieen/osint-trainingen/; Data-expert is in 2021 – middels een Europese Aanbesteding – geselecteerd om (naast de Politieacademie) OSINT-opleidingen te verzorgen.
133 Trainingen - Fox IT (fox-it.com)
134 OPLEIDINGEN – International Anti Crime Academy (anti-crime-academy.com)
135 DIGOS staat voor Digitaal Informatiegestuurd Operationeel Specialist. De IACA-opleidingen zijn breder dan OSINT; het gaat om meerdere digitale onderzoekstechnieken.

Politieacademie[136]	Opsporing en Internet en Social Media	In deze opleiding leren deelnemers zo veilig en effectief mogelijk te zoeken op internet, waaronder socialemediaplatformen. Er wordt onder andere ingegaan op de eigen veiligheid, het toetsen van de betrouwbaarheid van gevonden informatie en juridische (on)mogelijkheden.
	Internet en Opsporing[137]	In deze opleiding leren deelnemers zelfstandig een digitaal onderzoek uit te voeren bij internetgerelateerde delicten. Er komen diverse onderwerpen aan bod, waaronder netwerkprotocollen, sociale media en cryptovaluta.
SANS[138]	OSINT Gathering and Analysis	In deze opleiding leren deelnemers hoe zij gegevens op het internet (surface web, deep web en dark web) kunnen zoeken, verwerken en analyseren. Er wordt ingegaan op een breed aantal OSINT-onderwerpen, waaronder veiligheid, onderzoek naar personen, onderzoek van bedrijven, dark web.
	Advanced OSINT Gathering and Analysis	In deze opleiding leren deelnemers geavanceerde OSINT onderzoeken en analyses uit te voeren en veelgebruikte programmeertalen te gebruiken (zoals Python). Er wordt onder andere ingegaan op het beoordelen van de betrouwbaarheid van gegevens, onderzoek in besloten groepen, cryptovaluta en geautomatiseerde technieken voor OSINT.

Met betrekking tot de opleidingen die zijn en worden gevolgd, is een aantal aanvullende opmerkingen van belang. De eerste opmerking is dat er in de indeling van opleidingen een duidelijk onderscheid zichtbaar is tussen de basisvaardigheden op het gebied van OGG en de meer geavanceerde vaardigheden. In verschillende interviews brengen respondenten naar voren dat opleidingen in de regel te veel zijn gericht op bepaalde methoden en tools, terwijl het volgens hen van belang is dat opleidingen bijdragen aan meer begrip van hoe het internet werkt en aan het ontwikkelen van de juiste *mindset* voor online gegevensvergaring (zie vervolg).

> *'Wat nodig is voor een OSINT-specialist is kennis van het internet. Wat kun je bijvoorbeeld wel en niet met een IP-adres? Dat geeft een locatie en apparaat, maar brengt je niet naar een persoon.'* (33)

> *'Opleidingen gaan over de technieken. Die kan iedereen aanleren, maar het gaat om de denkwijze die je nodig hebt.'* (37)

> *'Ik heb leren autorijden, maar ik weet niet wat er onder de motorkap gebeurt. Zo werkt het met internetrechercheren ook. Als je de techniek niet kent, brengt dat een risico met zich mee.'* (41)

De tweede opmerking is dat verschillende respondenten erop wijzen dat er op dit moment nog geen opleidingseisen zijn verbonden aan de verschillende OGG-niveaus (zie paragraaf 3.3). Hier wordt binnen de politie aan gewerkt vanuit zowel de portefeuille

136 Politieacademie.nl - Onderwijsaanbod
137 Dit is een opleiding voor zowel digitaal rechercheurs als internetrechercheurs (OGG niveau 3 en 4).
138 Cyber Security Courses | SANS Institute

intelligence als de landelijke vakgroep internetonderzoek.[139] De derde opmerking is dat een deel van deze opleidingen na succesvolle afronding leidt tot een diploma of certificaat, punten op het gebied van permanente educatie en een registratie/titel, zoals 'Registered OSINT specialist' of 'Certified Open Source Expert'. Dit zijn algemene certificeringen, die worden gebruikt in allerlei sectoren, en dus geen politie-specifieke certificeringen (zoals bij een zedenrechercheur).[140] De vierde opmerking hangt hiermee samen: politiemensen volgen opleidingen op het gebied van OGG vooral bij (semi-)private organisaties en in mindere mate bij de Politieacademie (die politie-specifiek onderwijs verzorgt).[141]

> *'Er wordt veel privaat opgeleid en weinig via de Politieacademie. Er is jaren terug aan de Politieacademie gevraagd om een OSINT-opleiding te ontwikkelen. Na maanden kwam men met een paar A4 over de opzet van de opleiding. Dat was onvoldoende.'* (23)

Bij bovenstaand citaat moet worden opgemerkt dat het om 'jaren terug' gaat. Verschillende respondenten merken op dat in de afgelopen jaren het onderwijsaanbod van de Politieacademie op het gebied van OGG is verbeterd.[142]

> *'Ik heb als observator meegekeken met de basistraining van de Politieacademie en daar werd ik best wel blij van. Veel collega's willen vooral opleidingen volgen bij externe bureaus, terwijl de Politieacademie de eerste plek is om opleidingen te volgen. Die is wel echt bijgetrokken en dat was ook wel nodig, omdat mensen eerder niet terecht konden bij de Politieacademie voor hun opleidingswensen.'* (28)

Onderwijs door de Politieacademie wordt door respondenten belangrijk gevonden, omdat het politie-specifiek onderwijs is. Dit wil zeggen dat er (veel) aandacht wordt besteed aan het gebruik van bevoegdheden op het gebied van online gegevensvergaring. Dit is (volgens hen) 'buiten de poort' veel minder het geval. Daar leer je weliswaar methoden en technieken, maar krijg je niet of minder aangeleerd binnen welke – voor de politie – juridische kaders die methoden en technieken moeten worden ingezet (zie ook paragraaf 4.3 en 5.3). Om die reden is een deel van de respondenten van mening

139 De landelijke vakgroep werkt hierin samen met het Expertise Centrum Digitale Opsporing.

140 Hierbij moet worden opgemerkt dat VA's – die werkzaam zijn bij O&T (zie par. 3.4) – gecertificeerd moeten zijn, conform een brancherichtlijn die geldt voor stelselmatige informatie-inwinning.

141 Hierbij moet worden opgemerkt dat de Politieacademie ook intermediair is naar opleidingen van andere organisaties. Er is dus een onderscheid tussen opleidingen die door de Politieacademie zelf worden gegeven en opleidingen waarbij de Politieacademie intermediair is. Dit wordt ook wel 'makelen' genoemd. Zoals eerder aangegeven: Data-expert is op dit moment de partij waar de Politieacademie naar 'makelt', aangezien Data-expert is geselecteerd op basis van een Europese Aanbesteding.

142 Bij het onderwijs van de Politieacademie zijn tegenwoordig ook gastdocenten uit de praktijk betrokken, waaronder enkele respondenten.

dat de Politieacademie de basis op het gebied van OGG zou moeten verzorgen,[143] zodat de kennis over bevoegdheden 'erin zit'. Externe partijen kunnen hierop aanvullen.

> *'Tot niveau 3 zou je intern opgeleid moeten worden. De Politieacademie kan nu een mooie opleiding OSINT basis geven; dat is goed opgepakt. Daarin worden praktijk en regelgeving ook goed vervlochten. Op niveau 4 zijn het dusdanige specialisten, die weten waar hun bevoegdheden liggen en hoe politieprocessen werken als het gaat om OSINT. Zij kunnen naar een externe opleiding om daar weg te halen wat ze verder nodig hebben. Een externe opleiding kan dus heel goed zijn, maar alleen als je weet hoe je het in kunt zetten in relatie tot bevoegdheden.'* (38)

Bijhouden van het vak

Respondenten zijn behoorlijk eensgezind: opleidingen zijn (veelal) nuttig, maar je wordt goed in OGG door het te doen en door het vak bij te houden. Het bijhouden van het vak is volgens respondenten een voortdurende opgave, omdat OGG een dynamisch vak is (zie ook Lam & Kop, 2020b). Deze dynamiek wordt in de eerste plaats veroorzaakt door veranderingen met betrekking tot het internet. Zo doen nieuwe sociale mediaplatformen hun intrede en kan de techniek wijzigen.

> *'Dit kun je niet even doen, dat werkt niet. Als je het vier maanden niet doet, dan zijn dingen alweer veranderd en moet je ineens op TikTok zijn.'* (29)

> *'Technieken die wij vandaag gebruiken, kunnen morgen weer verouderd zijn. We zijn afhankelijk van de bronnen, dus als Facebook diens techniek erachter verandert, moeten wij daarin meeveranderen. Ook de protocollen op internet zijn regelmatig aan verandering onderhevig.'* (33)

Daarnaast is er – los van veranderingen op het internet – een continue ontwikkeling in de methoden en technieken die in het vakgebied worden gebruikt. Het handboek *Open Source Intelligence Techniques* van Michael Bazzell moet in principe ieder jaar worden geactualiseerd.[144] En ook op het gebied van tools is er veel ontwikkeling (zie ook paragraaf 6.2). Vanwege de continue ontwikkeling in methoden en technieken (inclusief tools) spreekt men in de internationale OSINT-gemeenschap ook wel over NERD: never ending research & development.

In welke mate houden de OGG-professionals hun vak bij en hoe doen ze dit? Het zijn vooral de fulltime specialisten die hun vak actief bijhouden. Dit doen zij op verschillende manieren. In de eerste plaats in (inter)nationale netwerken van OGG-specialis-

143 Hierbij kan worden opgemerkt dat de huidige opleidingen die de Politieacademie zelf verzorgt ook worden beschouwd als basisopleidingen. Diverse respondenten hebben aangegeven dat zij met bepaalde verwachtingen naar de opleiding internet en opsporing zijn gegaan, maar dat deze verwachtingen niet zijn uitgekomen, omdat men de stof al kende. De opleiding was meer basis dan men had verwacht.

144 Zie https://inteltechniques.com/book1.html

ten. Deze netwerken hebben een divers karakter, zoals netwerken die zijn ontstaan naar aanleiding van opleidingen (vaak geavanceerde methoden en technieken) en online netwerken van specialisten die via sociale media met elkaar zijn verbonden. In verschillende interviews hebben OGG-specialisten van de politie aangegeven dat zij via sociale media – vooral Twitter en LinkedIn – vooraanstaande (nationale en internationale) OSINT-specialisten volgen. Er is een (online) internationale gemeenschap waarin veel kennis wordt gedeeld.

> *'Bijna alles wat ik kan en ken, heb ik mezelf aangeleerd door contact te hebben met mensen die ervan afweten. In het OSINT-vakgebied wordt heel veel kennis gedeeld. Er zijn wereldwijd veel OSINT-specialisten die ik volg. (…) De gedachte bij OSINT is wel "je kunt het niet alleen".'* (21)

> *'Je moet zelf bijblijven, ik volg een aantal Twitter-accounts van mensen die op het vakgebied en specialisatie zitten. Daar pik ik een aantal dingen uit die relevant zijn voor de typen onderzoeken die ik doe. Ik probeer vooral bij te blijven in onderzoek van telefoonnummers, methodieken om personen te vinden, manieren hoe ik slim bij een account kan komen van iemand. Je kunt niet alles, moet bijblijven in je vakgebied. Het is een hoop zelfstudie.'* (25)

Er zijn daarnaast binnen de politie landelijke netwerken waarin vakontwikkeling plaatsvindt. Dit betreft onder andere de Landelijke Kenniskring OSINT voor wat betreft intelligence en de landelijke vakgroep internetonderzoek voor wat betreft opsporing.[145] Voor beide netwerken geldt dat er ook partners aan deelnemen, zoals de Fiscale Inlichtingen- en Opsporingsdienst en de KMar. De deelnemers aan deze vakgroepen komen (frequent) fysiek bij elkaar en hebben daarnaast ook een chatgroep waarin kennis wordt gedeeld.

> *'Ik leer veel van directe contacten en collega's landelijk. Van <naam> kan ik zeker veel leren. Zij is één van onze slimmeriken nationaal gezien.'* (28)

> *'Mensen zijn er bijna 24/7 mee bezig. Met een 9-5 mentaliteit red je het niet in de OSINT-business. Landelijk zie je dat ook. Zitten allemaal op Slack (soort Whatsapp, red.) en dergelijke. Maakt niet uit wanneer je een vraag post, eigenlijk heb je binnen een kwartier reactie. We hebben meerdere Slack-groepen, met rechercheurs, maar ook met partners erin. Dat gaat eigenlijk de hele dag door.'* (34)

Daarnaast vindt er professionalisering plaats door middel van landelijke hackathons op het gebied van OSINT (zie Lam & Kop, 2020a, 2020b, 2020c). Deze worden georga-

145 Er zijn daarnaast nog andere landelijke netwerken. Zo hebben cybercrimeteams een eigen OSINT-netwerk waarin vakontwikkelingen worden uitgewisseld. Er is tevens een landelijk netwerk financieel internet opsporen.

niseerd door Blue Movement (BlueM), een vernieuwingsbeweging binnen de politie.[146] Met deze hackathons worden zowel operationele resultaten behaald als leren & ontwikkelen gefaciliteerd. De landelijke hackathons hebben het karakter van publiek-private samenwerking.

Er zijn daarnaast netwerken – zoals expertgroepen – op eenheidsniveau. Hiervoor geldt dat men ten tijde van het veldwerk in diverse eenheden bezig was om deze op te zetten of uit te breiden met onder andere digitaal wijkagenten (zie ook paragraaf 3.5). In deze netwerken vinden vergelijkbare activiteiten plaats als in de landelijke netwerken: er worden tips & trucs uitgewisseld, afspraken gemaakt over onder andere software, overzicht gehouden op opleiding en ook hackathons georganiseerd. Ook de taakverdeling binnen de eenheid is veelal een gespreksonderwerp (zie paragraaf 3.5).

Kennis is noodzakelijk, maar niet voldoende. Kennis moet worden toegepast door nieuwe methoden, technieken en tools uit te proberen en er al doende vaardig in te worden. Het bijhouden van het vak kost tijd. Verschillende respondenten geven aan dat zij hiervoor tijd inruimen.

> *'Het is een kwestie van lezen en doen. Je moet een aparte telefoon voor jezelf hebben met daarop al die netwerken en daarop dingen uitproberen. Zo heb ik laatst Clubhouse (sociaal mediaplatform, red.) verkend, wat heel populair was geworden.'* (41)

> *'Doe veel in mijn vrije tijd, veel lezen in het nieuws en chatkanalen. Zo blijf ik bij. (…) Ik reserveer iedere vrijdagmiddag om mijn kennis op peil te houden.'* (24)

Bovenstaande respondent is geen uitzondering. Door uiteenlopende respondenten wordt opgemerkt dat zij in hun privétijd (veel) bezig zijn met het bijhouden van het vakgebied. Niet alleen of zozeer omdat het moet, maar ook en vooral omdat ze het leuk vinden. Dat is ook de indruk die wij in de gesprekken hebben gekregen: dit betreft een zeer gedreven groep professionals.

De dynamiek in het vakgebied en de daaruit voortvloeiende noodzaak om het voortdurend bij te houden, heeft voor degenen met een taakaccent een keerzijde. Zij – het gaat in dit onderzoek om de rechercheurs in de districtsrecherches – kunnen (zeer) beperkt tijd besteden aan OGG. Dit zorgt ervoor dat zij bestaande vaardigheden verleren en al helemaal niet toekomen aan het bijhouden van nieuwe ontwikkelingen in het vakgebied. Hun conclusie is dat OGG als taakaccent of deeltaak niet werkt. Zij ervaren dat hun leidinggevenden het niet belangrijk genoeg vinden (zie ook paragraaf 5.1).

146 BlueM is zich op OSINT hackathons gaan richten nadat zij een masterclass met Eliot Higgins – de oprichter van Bellingcat – hadden georganiseerd en hierdoor meer inzicht kregen in de mogelijkheden van OSINT. Zie voor verdere informatie over BlueM: https://www.politie.nl/woo/korpsstaf/2020-oprichting-bekostiging-blue-movement.html

'Donderdag moet ik met spoed iemand verhoren, omdat er niemand is. Maar die dag is mijn dag voor internetrechercheren. Dat is dan echt een belemmering. Als er andere dingen moeten gebeuren, dan gaan die vóór op internetrechercheren. Er is ook niet afgesproken hoeveel tijd ik mag besteden aan internetrechercheren. Voor de OE-s is alles belangrijker dan internetrechercheren. Ze snappen niet dat als je het weinig doet, je het weer kwijtraakt.' (14)

'We hebben nu een zaak van een overval waarin ik internetrechercheren toepas. Daarvóór heb ik een half jaar bijna niets gedaan. Het is echt een neventaak en dat maakt het lastig. Je bent er dan weer helemaal uit en je moet weer opstarten. Dan merk je dat OSINT weer helemaal veranderd is.' (18)

'Ik merk aan mezelf: als je het niet regelmatig doet, verleer je alle trucjes en kennis die je hebt. Daar lopen we al jaren tegenaan. De collega's die het dagelijks doen, kunnen toveren. Dat niveau heb ik niet. Dat is het grootste probleem bij de districtsrecherche. Je hebt geen continuïteit.' (19)

Mindset van OGG professionals

Tijdens het afnemen van de interviews met de OGG-professionals kwam voortdurend terug dat OGG een manier van denken is, een 'mindset'. Opleidingen, methoden, technieken, tools: het is allemaal van belang, maar uiteindelijk ondergeschikt aan de 'mindset', aldus de respondenten. Voor goed politiewerk in dit vakgebied is de mindset essentieel. Dit punt hebben we in deze paragraaf al eerder aangeraakt toen het ging over het begrijpen van de werking van het internet. Dit is een aspect van de bedoelde mindset, maar respondenten wijzen ook en vooral op een aantal eigenschappen of algemene vaardigheden waarover de OGG-professional *zou moeten* beschikken.

'Het gaat erom dat je herkent welke informatiewaarde in 'dingen' zit, zoals een foto of een Facebook-account. Bijvoorbeeld via felicitaties op Facebook kun je de geboortedatum van iemand achterhalen. Die geboortedatum kun je weer gebruiken om in de politiesystemen te zoeken. Om de informatiewaarde van 'dingen' te leren inschatten, moet je dagelijks met open bronnen bezig zijn, niet één keer per maand.' (23)

'OSINT is niet alleen trucjes kennen van internet leegtrekken, maar ook een manier van denken. Het is een puzzel: ik vind nu niets, hoe kan ik het wel vinden, wat moet ik toevoegen of veranderen om het wel te vinden? Ik heb ook altijd gezegd dat een goede OSINT-er creatief moet kunnen denken.' (30)

'Het is meer een soort mindset die je moet hebben. Je moet analytisch vermogen hebben, dat je dingen aan elkaar weet te verbinden. Je moet nieuwsgierig zijn. Het is een bepaalde persoonlijkheid die je moet hebben, dat je niet zomaar stopt, dat je wel getriggerd bent om door te gaan. Per situatie gebruik je andere software, onderzoeks-

technieken, platformen. Je moet op een bepaalde manier een mindset hebben en niet stoppen bij het antwoord "nee, er is niets".' (24)

De bovenstaande respondenten wijzen op verschillende kenmerken van de OGG-mindset: nieuwsgierigheid, creativiteit, analytisch vermogen, vasthoudendheid. De OGG-professional werkt van datapunt naar datapunt of van 'haakje naar haakje' en doet dit met veel oog voor detail (zie ook Higgens, 2021). Ook kritisch denken wordt geregeld als een wezenlijk onderdeel van de OGG-mindset genoemd, zeker in een tijd van steeds meer desinformatie.[147]

6.2 Hardware & software

Hardware
Het online vergaren van gegevens is werk dat met een computer wordt verricht. Computer moet hierbij breed worden opgevat: het gaat om een elektronisch apparaat voor informatieverwerking. De smartphone is dus niet alleen een telefoon, maar ook een computer. De computer is voor de OGG-professional een belangrijk onderdeel van het gereedschap. Met wat voor computers werken zij?

Het online vergaren van gegevens door politiemensen vindt van oudsher plaats op een iRN-computer. Het iRN is – zoals eerder aangegeven (zie paragraaf 3.1) – in 2004 ontwikkeld door het regiokorps Gelderland-Zuid en vervolgens uitgegroeid tot een netwerk met een groot aantal gebruikers binnen zowel de politie als andere overheden. Door gebruik te maken van een iRN-computer wordt er verbinding met het internet gemaakt via een gesloten infrastructuur. Het is te beschouwen als een internetprovider van en voor de overheid. Op een iRN-computer kunnen politiemensen veilig en anoniem gebruikmaken van het internet. De computers zijn ook van software voorzien om automatisch gegevens van het internet te vergaren (iColombo) en om automatisch vast te leggen wat de gebruiker doet, zodat dit eventueel later kan worden gebruikt voor de verslaglegging in een proces-verbaal (zie ook paragraaf 5.2).

Uit de interviews komt naar voren dat vrijwel alle respondenten (soms) gebruikmaken van een iRN-computer of hiervan gebruik hebben gemaakt. Het gebruik biedt veiligheid, maar gaat ook gepaard met diverse beperkingen. Deze beperkingen zijn vooral aangedragen door internetrechercheurs van de districtsrecherche, omdat zij in de regel minder andere middelen tot hun beschikking hebben en daarmee (meer) zijn aangewezen op het iRN. Een eerste beperking is het geringe aantal iRN-computers waarover een afdeling beschikt[148] (zie ook Zuurveen & Stol, 2020).

147 Zie ook https://medium.com/secjuice/osint-as-a-mindset-7d42ad72113d
148 Basisteams kunnen ook over een iRN-computer beschikken. De digitaal wijkagent is hier in de regel niet afhankelijk van, omdat die beschikt over een laptop (zie vervolg).

'We gebruiken een IRN-computer, maar we hebben er te weinig, een stuk of vijf. Als ik bezig ben en een collega wil iets opzoeken op Facebook, dan moet die wachten tot ik klaar ben.' (14)

Een tweede beperking is de beperkte mobiliteit: een iRN-computer heeft een vaste plek en alleen op die plek kun je er gebruik van maken. Kortom: je kunt er niet op de eigen werkplek of thuis gebruik van maken. Een derde punt heeft te maken met de beperkingen in de software die op een iRN kan worden gezet. Zo werkt de iRN met Firefox als webbrowser, terwijl voor een deel van de applicaties (volgens respondenten) een andere browser nodig is (Google Chrome). Je kunt er dus allerlei tools niet op gebruiken (zie ook het deel over software). Er wordt tot slot op gewezen dat het netwerk sterk is verouderd. Er zou in de afgelopen jaren te weinig zijn geïnvesteerd in de doorontwikkeling.[149]

'Een iRN-PC is beperkt bruikbaar, het datanetwerk is al ver over de uiterste houdbaarheidsdatum. Dit is een route die al is ingeslagen met de dienst ICT, maar is nog niet tot een project geworden.' (27)

Naast een 'vaste' iRN-computer maken veel OGG-professionals gebruik van een of meer laptops. Dit betreft in de eerste plaats de specialisten van de diensten. Ook veel digitaal wijkagenten hebben een eigen laptop. Het type laptop verschilt. Verschillende regionale specialisten geven aan dat zij een (Apple) Macbook hebben, terwijl digitaal wijkagenten (voor zover zij een laptop hebben) gebruikmaken van een (Google) Chromebook. Niet iedereen is tevreden met de Chromebook. Het scherm zou te klein zijn om prettig mee te werken. Deze digitaal wijkagenten hebben behoefte aan een 'normale laptop'. Zoals eerder aangegeven: een groot deel van de internetrechercheurs van de (geïnterviewde) districtsrecherche heeft geen (eigen) laptop. Dit zorgt er bij sommigen voor dat zij wel eens gebruikmaken van een privélaptop die zij naar eigen zeggen hebben ingericht (virtuele machine of een VPN) om veilig online gegevens mee te vergaren.

Het derde apparaat is de smartphone. Deze is volgens veel respondenten nodig, omdat bepaalde sociale mediaplatformen – zoals Snapchat, Whatsapp of Telegram – alleen via de smartphone kunnen worden gebruikt. Een smartphone is dus nodig om in (een deel van de) besloten groepen te kunnen komen. Een groot deel van de (uitvoerende) respondenten kan gebruikmaken van een telefoon die is geprepareerd voor online gegevensvergaring. Specialisten op regionaal niveau hebben veelal een eigen telefoon voor OGG en maken soms ook gebruik van een mobiele WiFi router waarmee de veiligheid verder wordt vergroot. Ook de meeste digitaal wijkagenten, die wij hebben geïnterviewd, hebben een eigen OGG-telefoon. Bij districtsrecherches is het beeld wisselender.

149 Hierbij moet worden opgemerkt dat het iRN op korte termijn vervangen wordt door een nieuw platform.

Met betrekking tot de hardware is een aantal aanvullende opmerkingen van belang. De eerste opmerking is dat veel respondenten enigszins kritisch zijn op de eigen organisatie. Het verkrijgen van de juiste hardware kost volgens hen 'bloed, zweet en tranen'.

> *'Ik wil er geen klaagzang van maken, want het gaat bij ons echt wel goed. Maar je moet wel een jaar en zeven maanden gillen en schreeuwen om een laptop te krijgen. En ieder jaar als de VPN verloopt, is het weer gedoe om dit te krijgen.'* (21)

> *'Omdat we best vroeg zijn begonnen met OSINT hebben we veel gepionierd. Heeft pijn en moeite gekost als het ging om laptops, VPN en software.'* (37)

De tweede opmerking is dat er naast verschillen tussen disciplines/organisatieonderdelen ook verschillen tussen eenheden en individuen bestaan voor wat betreft de hardware (en software) waarover zijn beschikken. Om die reden wordt er vanuit de portefeuille intelligence gewerkt aan een landelijke standaard voor de OGG-niveaus 3 en 4 (die een specifieke behoefte hebben).

> *'We willen een strakkere lijn zetten landelijk voor de DRIO's en DLIO. Nu is het per eigen eenheid afhankelijk hoe ze een werkplek inrichten voor medewerkers. We willen het uniformeren. Dat is eenduidiger, kosten-efficiënter en ook effectiever in de samenwerking.'* (26)

Ten derde kan worden opgemerkt dat respondenten ook 'andere geluiden' geven. Een enkele respondent benadrukt dat de collega's die actief zijn op het gebied van online gegevensvergaring te snel denken en vinden dat zij niet de juiste middelen hebben. Deze (twee) respondenten twijfelen of alle collega's die de middelen willen hebben wel kundig genoeg zijn om er veilig mee te werken.

> *'Mensen zeggen al snel "Ik kan mijn werk niet doen want heb de middelen niet". Terwijl ik vind: er zitten meer risico's aan het geven van mobiele telefoon en laptop dan vaak wordt erkend. Internetrechercheren is iets heel anders dan gewoon je mobiel gebruiken of internetten. Wat geef ik prijs? Bijvoorbeeld: in meerdere onderzoeken hetzelfde profiel gebruiken, is een probleem, maar mensen houden er te weinig rekening mee.'* (29)

Software

De twee voorgaande hoofdstukken hebben laten zien dat er bij het online vergaren van gegevens regelmatig gebruik wordt gemaakt van tools: software. Op deze plek geven we een overzicht van de tools die door respondenten zijn benoemd en maken we een aantal meer algemene opmerkingen.

Tabel 6.2. Software genoemd door respondenten

Programma	Beschrijving
Add-ons/extensies	Add-ons zijn een verzamelterm voor allerlei uitbreidingen op de internet browser (zijn allemaal stukjes software). Deze uitbreidingen worden gebruikt om informatie te verzamelen en te verwerken, zoals internetgeschiedenis, data-extractie van afbeeldingen, IP-, domein- en beheerinformatie, en tekst, screenshot en video-opnames.
Echosec[150]	Echosec is software waarmee dreigingen/risico's op het internet kunnen worden gedetecteerd, waaronder op sociale media en dark web. De software beschikt over datamining-technologie om berichten/gegevens te vinden op basis van zoektermen of geografie (geo metadata). Door middel van machine learning (artificiële intelligentie) wordt geselecteerd aan welke gegevens/berichten aandacht moet worden besteed.
FiveCast ONYX151	FiveCast ONYX is software waarmee grote hoeveelheden gegevens uit open bronnen kunnen worden doorzocht/gemonitord. Dit betreft een variëteit aan gegevens, zoals tekst, afbeeldingen en video's. Gegevens worden van kenmerken voorzien die vervolgens worden gebruikt voor het analyseren van patronen/relaties. Wordt vooral gebruikt in het kader van CTER en georganiseerde criminaliteit.
Google software	Google beschikt over diverse tools die door OGG-professionals worden gebruikt, waaronder Google Maps en Google Dorks.
Hunchly[152]	Hunchly verzamelt, documenteert en annoteert automatisch elke webpagina die de gebruiker bezoekt. Wordt gebruikt om bij te houden welke stappen worden gezet, o.a. om in een P-V te verwerken. Is een add-on op de browsersoftware.
Maltego[153]	Maltego is software ten behoeve van data mining (zie paragraaf 2.7) en analyse. Er kunnen in het kader van analyse verschillende databronnen worden gebruikt/toegevoegd. De patronen in de data kunnen op verschillende manieren worden gevisualiseerd, waaronder in (sociale) netwerkanalyse.
NexusXplore[154]	NexusXplore is software voor het (geavanceerd) geautomatiseerd online vergaren van gegevens (surface, deep & dark web) en analyseren van die gegevens. Vergaarde gegevens kunnen onder andere geografisch worden weergegeven en met de software kan ook sociale netwerkanalyse worden uitgevoerd.
PublicSonar[155]	PublicSonar is software om real-time sociale media te monitoren. Met gebruik van algoritmen worden relevante berichten/signalen herkend. Die worden met elkaar in verband gebracht om zodoende een beeld van de situatie te kunnen krijgen. De software biedt de mogelijkheid tot gepersonaliseerde alerts via sms of email, zodat de gebruiker weet wanneer een bepaalde situatie (bijv. een opruiende tweet) zich voordoet.
SpiderFoot[156]	SpiderFoot is software voor het geautomatiseerd vergaren van gegevens uit open online bronnen. De software vergaart gegevens over onder andere IP-adressen, domeinnamen en usernames. Het heeft geen analysefunctionaliteit.
Virtual Private Network	Een Virtual Private Network (de software) legt een versleutelde verbinding tussen het apparaat van de gebruik en een VPN-server. Al het internetverkeer gaat langs die server. De VPN koppelt je aan een nieuw, ander IP-adres, dat ook geregeld wisselt. De internet-activiteiten van de gebruiker zijn zo moeilijker te herleiden.

Met betrekking tot het gebruik van software is een negental aanvullende opmerkingen van belang.

150 Intuitive OSINT Tools | Echosec Systems
151 Home — Fivecast
152 Hunchly - OSINT Software for Cybersecurity, Law Enforcement, Journalists, Private Investigators and more
153 Homepage - Maltego
154 Open Source Intelligence | NexusXplore | Australia
155 Homepage - PublicSonar
156 Home - SpiderFoot

De eerste opmerking heeft direct betrekking op de tabel: het overzicht is gebaseerd op wat respondenten in de interviews hebben genoemd. Het is vermoedelijk geen volledig overzicht. De betreffende software wordt niet in alle eenheden gebruikt en er zijn verschillen tussen eenheden. Sommige software wordt in alle eenheden gebruikt – bijvoorbeeld PublicSonar – terwijl er ook software is die in één of enkele eenheden wordt gebruikt, bijvoorbeeld NexusXplore.

De tweede opmerking is dat de software voor verschillende functionaliteiten wordt gebruikt: 1) veilig werken (OPSEC), 2) automatisch vergaren van gegevens, 3) (geavanceerd) analyseren van gegevens en 4) ondersteunen van verslaglegging. OPSEC is van belang voor zowel intelligence als opsporing. Het automatisch vergaren van gegevens vindt meer – of in ieder geval breder – plaats in het intelligenceproces dan in het opsporingsproces.[157] Voor het analyseren van gegevens maken beide disciplines gebruik van software. Hierbij wordt (sociale) netwerkanalyse relatief vaak als methode genoemd. Software ten behoeve van verslaglegging – in het bijzonder Hunchly – wordt meer gebruikt in het opsporingsproces dan in het intelligenceproces. Deze verschillen met betrekking tot welke software in welk proces wordt gebruikt, hangen onder andere samen met het gegeven dat het intelligenceproces draait om sturingsinformatie en het opsporingsproces om bewijs.

De derde opmerking is dat er, naast software van commerciële aanbieders, ook software binnen de politie wordt ontwikkeld.[158] Dit betreft vooral allerlei programma's of scripts die door politiemensen worden geprogrammeerd om specifieke taken te automatiseren, bijvoorbeeld het dagelijks vergaren van eventueel nieuwe gegevens van een bepaald profiel. Bij het programmeren wordt onder andere gebruikgemaakt van open source software (voorbeeld: Python).

> *'De OS-B van TDO doet programmeerwerk. Dus als wij bepaalde tooltjes nodig hebben, dan kan hij die snel schrijven (...) Er worden ook veel programma's aangeboden. Die passen we vaak wat aan of we halen de code eruit en herschrijven het programma compleet. Dat zijn eigenlijk de tools die we add-ons noemen. Die maken we vaak zelf.'* (34)

De vierde opmerking heeft betrekking op de kenmerken van de 'off the shelf' software. Het betreft over het algemeen geavanceerde softwareprogramma's die ten behoeve van het vergaren en analyseren van gegevens gebruikmaken van artificiële-intelligentietechnologieën, zoals machine learning en natural language processing[159](zie ook Landman, 2022). Wij hebben geen beeld verkregen over de mate waarin de gebruikers van deze software inzicht hebben in de werking van deze technologieën en software kun-

157 PublicSonar is bijvoorbeeld software die uitsluitend ten behoeve van intelligence mag worden gebruikt.
158 Die staat dus niet in tabel 6.2.
159 Dit betreft overigens aanbieders uit diverse landen. PublicSonar is bijvoorbeeld een Nederlands product, Echosec en NexusXplorer zijn ontwikkeld in Australië en Maltego in Zuid-Afrika.

nen configureren op een manier die aansluit bij het doel dat wordt beoogd en de bevoegdheid die hiervoor wordt ingezet. Dit is wel een belangrijk aspect in relatie tot de inbreuk dat het gebruik van softwareprogramma's met algoritmen maakt op de persoonlijke levenssfeer van de burgers die in beeld komen (zie paragraaf 2.7).

De vijfde opmerking is dat er veel ontwikkeling is in software voor het online vergaren van gegevens (zie ook CTIVD, 2021). Het bijhouden hiervan is volgens respondenten een onderdeel van het vakonderhoud (zie paragraaf 6.1). Zij benutten hun netwerk(en) om op de hoogte te worden gebracht van tools die zij nog niet kennen en die mogelijk interessant zijn.

> *'Ik heb toevallig een collega die de landelijke OSINT-nieuwsbrief verzorgt en die heeft verschillende pagina's waar zij haar tools bijhoudt. Daar zit altijd wel wat tussen om te gebruiken. Het is wel handig dat je iemand hebt die dat heeft.' (17)*

De zesde opmerking is dat de beschikbaarheid van geavanceerde software in de markt (vanzelfsprekend) niet wil zeggen dat de politie hierover ook de beschikking heeft. Geavanceerde software voor het online vergaren en analyseren van gegevens is kostbaar, zo geven respondenten aan.[160] Diverse respondenten zijn van mening dat het online vergaren van gegevens inmiddels zo belangrijk en omvangrijk is geworden dat de politieleiding meer zou moeten investeren in software die dit werk gemakkelijker en efficiënter maakt.

> *'Eenheidsleidingen zijn vaak enthousiast over de resultaten. Dan is het hosanna en dan hoor je "Hier moeten we iets mee". Dan zeg ik "Put your money where your mouth is" en dan wordt het stil. Dan gaat het over geld (…) Voor het vergaren van informatie hebben wij geen tooling, dus dat vergt soms gewoon heel veel tijd. Bijvoorbeeld handmatig filmpjes aanklikken, downloaden, in een mapje doen. Terwijl daar gewoon tooling voor bestaat waarmee je dat in twee klikken kunt doen. De coronarellen hebben wel voor versnelling gezorgd.'* (21)

De zevende opmerking is dat veel respondenten kritisch zijn over de snelheid en het gemak waarmee de politieorganisatie over nieuwe software kan beschikken. Het vakgebied ontwikkelt zich snel en daarin wil men meebewegen. Dit wordt nu bemoeilijkt doordat het in de praktijk – onder andere door aanbestedingen – veel tijd en moeite kost om mee te bewegen.

> *'Als ik het (NexusXplore, red.) landelijk ga aanvragen, dan weet ik zeker dat ik het niet heb voor 2023. Er gaan 48 mensen en diensten iets van vinden. Dus ik heb het regionaal aangevraagd.'* (28)

160 Er kunnen overigens ook andere redenen dan de kosten zijn om bepaalde software niet te gebruiken. Hierbij kan onder andere worden gedacht aan het perspectief van ethiek en privacy.

'Als je eerst voor twaalf medewerkers tien A4-tjes moet invullen voor een tool van 46 euro, dan gaat dat natuurlijk nergens over. En uiteindelijk krijg je een streep door je verzoek, omdat de tool niet op een lijst staat.' (34)

De achtste opmerking is dat de respondenten die wij hebben gesproken vaker handmatig dan automatisch online gegevens vergaren en analyseren. Het gebruik van software voor het automatiseren van activiteiten wordt door velen weliswaar als een onmisbaar onderdeel van het werk beschouwd, maar er zijn ook veel handelingen die simpelweg niet kunnen worden geautomatiseerd. Niet alleen vanwege technische beperkingen, maar ook en vooral vanwege de aard van het politiewerk (vooral in geval van waarheidsvinding).

'Ik heb zelf geen bijzondere software zoals Public Sonar, dus ik doe alles met de hand. Maltego heb ik wel, maar gebruik ik niet, het lastige daaraan voor ons werk is dat wij zo dicht mogelijk tegen de originele bron moeten zitten als we antwoord willen hebben op de vraag.' (24)

De negende en laatste opmerking borduurt hierop voort: in veel interviews is erop gewezen dat de meerwaarde van software niet moet worden overschat.[161] Het is volgens veel respondenten onderdeel van het gereedschap van de professional – een aanvulling – maar de professional zelf maakt het verschil. Hiermee komen we terug op wat we eerder hebben beschreven over de mindset van de professional (paragraaf 6.1).

'Ik hoop wel dat mensen beseffen waarmee ze bezig zijn. Het is prima om terug te vallen op tools, maar je moet wel begrijpen wat je doet.' (29)

'Je kunt het nooit door een computer laten doen, software is een hulpmiddel, je doet het met je hoofd. Het is toch een stuk gevoel, in het hoofd kruipen van degene die je aan het zoeken bent.' (38)

Kortom: in online gegevensvergaring is de politiemens van doorslaggevend belang.

161 Een nuancerende opmerking hierbij is dat er bij handmatige online gegevensvergaring ook gebruik wordt gemaakt van software, namelijk minimaal een browser. De nadruk in deze paragraaf ligt echter op software voor de eerdergenoemde functionaliteiten en dan in het bijzonder op software voor geautomatiseerd vergaren en analyseren.

7 Conclusies en toekomstperspectief

In dit slothoofdstuk worden de voornaamste bevindingen samengevat onder de noemer van conclusies. We geven daarnaast enkele aandachtspunten mee voor de verdere ontwikkeling van OGG als vakgebied binnen de politie. We gaan ten derde in op de beperkingen van het onderzoek en ronden af met een slotopmerking.

7.1 Een verkennend onderzoek naar online gegevensvergaring

De opkomst en doorontwikkeling van het internet heeft veel consequenties gehad voor het politiewerk. Het betreft onder andere de digitalisering van criminaliteit, het ontstaan van allerlei andere vormen van online immoreel gedrag,[162] het vergroten van het organisatievermogen onder burgers[163] en het ontstaan van nieuwe manieren van communiceren en samenwerken tussen politie en burgers. Naar deze fenomenen wordt in toenemende mate wetenschappelijk onderzoek verricht. De opkomst en doorontwikkeling van het internet heeft voor de politie echter ook een consequentie gehad die in empirisch onderzoek vooralsnog minder aandacht heeft gekregen: er is een bron van intelligence en sporen c.q. bewijs bijgekomen. Vooral de ontwikkeling van het internet van een passief, informatiegevend medium (Web 1.0) naar een interactief medium (Web 2.0, sociale media) heeft ervoor gezorgd dat er op het internet steeds meer gegevens beschikbaar zijn gekomen die voor de politie interessant kunnen zijn (zie Feenstra, 2018; Koops, 2013; Stol & Strikwerda, 2018; Trottier, 2015a). Binnen politieorganisaties wereldwijd is in de afgelopen tien jaar dan ook het besef gegroeid dat het internet qua gegevens een bron met potentie is die moet worden benut (Ramwell et al., 2016).

Voor de politie in Nederland is politiewerk op het web een van de strategische ontwikkelthema's. Om die reden hebben wij – in lijn met de onderzoeksagenda van de politie – voorgesteld om empirisch onderzoek naar online gegevensvergaring te verrichten. Dit voorstel is gehonoreerd en dit geeft geleid tot voorliggend onderzoek. Dit onderzoek heeft een verkennend karakter en vertrekt vanuit de volgende globale onderzoeksvraag:

> *Op welke wijze maakt de politie gebruik van het online vergaren van gegevens ten behoeve van intelligence en opsporing?*

162 Denk aan doxing, haatzaaien en cyberpesten. Zie Rathenau Instituut (2021).
163 Denk aan online opruiing. Zie Stol (2021).

Deze onderzoeksvraag is (enigszins) geconcretiseerd door verschillende aspecten te benoemen waarop het onderzoek is gericht:
- organisatie van online gegevensvergaring;
- samenwerking op het gebied van online gegevensvergaring;
- inzet en opbrengsten van OGG in het politiewerk;
- gebruik van bevoegdheden in het kader van online gegevensvergaring;
- professionalisering op het gebied van online gegevensvergaring;
- gebruik van technologie in het kader van online gegevensvergaring;
- opbrengsten van OGG voor het politiewerk.

We hebben gekozen voor een kwalitatieve opzet waarin interviews met politiemensen die uitvoering geven aan OGG centraal staan. We hebben 41 respondenten geïnterviewd die werkzaam zijn in basisteams, districtsrecherches, informatieorganisaties en regionale recherches. Alle eenheden van de politie hebben deelgenomen aan het onderzoek. Hieronder worden de conclusies beschreven.

Terminologie
De interviews met respondenten maken duidelijk dat er in de praktijk verschillende begrippen in omloop zijn voor het online vergaren van gegevens. Deze diversiteit hangt vooral, maar niet uitsluitend, samen met het gegeven dat binnen de politie online gegevens worden vergaard ten behoeve van intelligence én opsporing. Respondenten benadrukken dat het onderscheid tussen intelligence en opsporing vooral betrekking heeft op het doel waarvoor gegevens worden verzameld en in mindere mate op de methoden en technieken die hiervoor worden gebruikt.

Online gegevensvergaring ten behoeve van intelligence is gericht op sturingsinformatie voor het politiewerk. Online gegevens worden onder andere gebruikt voor het in kaart brengen van trends & ontwikkelingen, dreigingen en dergelijke. Er is dan (nog) geen sprake van specifieke strafbare feiten die worden onderzocht; het gaat om de bijdrage aan het creëren van een informatiepositie die inzicht geeft in wat er gebeurt en eventueel kan gaan gebeuren. Opsporing vindt plaats in het kader van een verdenking van een gepleegd strafbaar feit en is gericht op het verzamelen van (steun)bewijs ten behoeve van waarheidsvinding. Respondenten benadrukken dat intelligence en opsporing in de praktijk in elkaar kunnen overvloeien. Dit deed zich onder andere voor bij de avondklokrellen: op het ene moment monitor je op sociale media het sentiment en de tendens rondom de avondklok in een bepaalde stad en op het andere moment lees je een bericht van een persoon dat neigt naar opruiing. Op het moment dat een persoon nader wordt onderzocht, gaat intelligence over in opsporing.

Wij hebben ervoor gekozen om het onderscheid tussen intelligence en opsporing tot uitdrukking te brengen in de terminologie die we in dit rapport gebruiken. We hanteren drie begrippen:

- online vergaren van gegevens (OGG) voor de overkoepelende activiteit en het vakgebied;
- OSINT[164] voor het online vergaren van gegevens ten behoeve van intelligence;
- internetrechercheren voor het online vergaren van gegevens ten behoeve van opsporing.

Organisatie van OGG binnen de politie

Online gegevensvergaring vindt vooral plaats binnen de informatieorganisatie en de rechercheorganisatie en in mindere – maar toenemende – mate in de basisteams.

Binnen de informatieorganisatie is OSINT breed ingebed. Dit wil zeggen dat relatief veel medewerkers in uiteenlopende afdelingen OSINT-werkzaamheden uitvoeren. Deze breedte heeft betrekking op eenvoudige OSINT-werkzaamheden (basisniveau). Daarnaast zijn er in iedere eenheid specialisten die meer complexe OSINT-werkzaamheden uitvoeren. Van oudsher ondersteunt de informatieorganisatie de recherche met OGG-werkzaamheden in opsporingsonderzoeken. Enkele eenheden hebben deze manier van organiseren beëindigd en een strakker onderscheid gemaakt tussen OGG ten behoeve van intelligence, dat wordt uitgevoerd door de informatieorganisatie, en OGG ten behoeve van opsporing, dat wordt uitgevoerd door de rechercheorganisatie.

Binnen de rechercheorganisatie is OGG minder breed ingebed dan binnen de informatieorganisatie. Ook zijn de verschillen tussen eenheden groter. Binnen de onderzochte districtsrecherches is internetrechercheren vooral georganiseerd als een taakaccent. Dit wil zeggen dat er enkele rechercheurs zijn die op niet-structurele basis activiteiten uitvoeren op het gebied van internetrechercheren. De mate waarin zij zich hiermee bezighouden is divers en afhankelijk van allerlei omstandigheden. Er zijn ook districtsrecherches die over een fulltime internetrechercheur beschikken, maar dit komt veel minder vaak voor dan het model van een taakaccent.

Binnen de regionale recherche is expertise op het gebied van internetrechercheren vooral verankerd bij het Team Digitale Opsporing van de afdeling Specialistische Opsporing. Dit wil zeggen dat er enkele (fulltime) internetrechercheurs werkzaam zijn, die worden ingezet in (omvangrijke) opsporingsonderzoeken en hun collega's van andere afdelingen en teams coachen en adviseren. De verschillen tussen eenheden zijn groot: van vijf-zeven fulltime specialisten tot een-twee met een taakaccent. Binnen de thematische opsporingsteams is de verankering van internetrechercheren divers. Er zijn verschillen tussen thema's. De cybercrimeteams hebben bijvoorbeeld allemaal mi-

164 OSINT verwijst naar open source intelligence. Hierbij moet worden opgemerkt dat intelligence ook wordt vergaard in afgeschermde bronnen. Zie hoofdstuk 4.

nimaal één specialist, terwijl het op andere thema's minder gebruikelijk is. Voor de andere thema's geldt dat de aanwezigheid van expertise niet vanzelfsprekend is en er verschillen tussen eenheden zijn.[165] Ook binnen de generieke opsporingsteams is de aanwezigheid van expertise niet vanzelfsprekend. Er zijn in het verleden in diverse eenheden tactische rechercheurs opgeleid, maar dit heeft niet geleid tot een breed basisniveau binnen de regionale recherche dat ook wordt onderhouden.

In het kader van OGG binnen de rechercheorganisatie moet tot slot worden gewezen op het team Observatie & Techniek van de afdeling Specialistische Opsporing. In dit team zijn 'virtual agents' werkzaam die onder dekmantel werken en heimelijk gegevens inwinnen op het internet. Deze werkzaamheden vallen wel onder het vakgebied OGG, maar zijn te beschouwen als een aparte (sub)discipline binnen de politie. Anders dan de andere OGG-specialisten interfereren zij in het leven van betrokken burgers door actief met hen de interactie aan te gaan. Deze virtual agents zijn in dit onderzoek niet meegenomen, maar voor het algehele beeld wel van belang.

Tot slot de basisteams. Een toenemend aantal basisteams verricht werkzaamheden op het gebied van OGG. Deze werkzaamheden worden vooral uitgevoerd door digitaal wijkagenten. Deze rol is in 2017 in het basisteam van Roosendaal ontstaan en heeft zich sindsdien als een olievlek verspreid over de basisteams (zie Boelens & Landman, 2021). In september 2021 had ongeveer een derde van de basisteams een digitaal wijkagent en was het aantal nog steeds groeiende. Digitaal wijkagenten houden zich, naast andere taken, vooral bezig met OSINT. Hierbij moet worden opgemerkt dat er verschillen tussen basisteams zijn voor wat betreft de rolinvulling van de digitaal wijkagent en de OSINT-taken. Er kunnen in een basisteam ook andere politiefunctionarissen zijn die OSINT-taken verrichten (taakaccent). Dit komt nog beperkt, maar wel in toenemende mate voor. Voor internetrechercheren geldt dat het rechercheteam binnen het basisteam dit kan inzetten. Hiernaar hebben we geen onderzoek gedaan.

Samenwerking op het gebied van OGG
Samenwerking op het gebied van OGG is een actueel en relevant vraagstuk binnen de politie. Dit komt doordat het aantal organisatieonderdelen en politiemensen dat zich in de afgelopen periode is gaan bezighouden met OGG is toegenomen. Dit roept de vraag op wie wat doet in het kader van OGG.

Met betrekking tot de afstemming over 'wie doet wat' lijken de specialisten binnen de eigen sectoren – informatie, recherche, district – elkaar redelijk goed te kunnen vinden. Er zijn veelal netwerken en overleggen waarin die afstemming wordt gerealiseerd. Tussen de sectoren is dit in mindere mate het geval en zijn de verschillen tussen een-

165 Dit geldt ook voor het team Migratiecriminaliteit en Mensenhandel dat onderdeel is van de Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel (van de regionale recherche) en vergelijkbaar is met een thematisch opsporingsteam.

heden groter. Er zijn eenheden waar de specialisten van de afdeling RI en TDO structureel overleg hebben en er zijn eenheden waar dit niet het geval is. Zeker in eenheden waar zowel RI als TDO grootschalige opsporingsonderzoeken ondersteunen met OGG-expertise kan er (soms) sprake zijn van overlap en concurrentie. Met betrekking tot de samenwerking tussen de diensten en districten geldt dat vooral de opkomst van de digitaal wijkagent in het basisteam een behoefte tot afstemming creëert, in het bijzonder voor wat betreft OSINT. In diverse eenheden zijn of worden netwerken gecreëerd om de samenwerking te intensiveren. Deze ontwikkeling bevindt zich in veel eenheden nog in een pril stadium.

De behoefte aan afstemming over 'wie doet wat' heeft ook een landelijke dimensie. Het gaat dan vooral over OSINT en dan in het bijzonder: het monitoren van maatschappelijk ongenoegen (boerenprotesten, corona en dergelijke). Er is volgens respondenten op dit moment weinig afstemming over de verdeling van de taken, terwijl er wel in alle eenheden min of meer gelijktijdig monitoring plaatsvindt met vermoedelijke overlap in werkzaamheden, bijvoorbeeld in de vorm van aanwezigheid in dezelfde (besloten) groepen zonder dit van elkaar te weten. Dit is volgens hen een aandachtspunt voor de toekomst.

Inzet en opbrengsten van OGG
Zoals eerder aangegeven: intelligence is sturingsinformatie en OSINT is een bron van gegevens voor deze sturingsinformatie. Internetgegevens bestaan naast allerlei gegevens die door de politie zelf worden verzameld in het kader van handhaving, opsporing en inlichtingen. In de informatieorganisatie wordt OSINT in de eerste plaats ingezet voor het opbouwen en onderhouden van thematische informatie- of intelligenceposities. Uit dit onderzoek komt naar voren dat de mate waarin OSINT hierin een rol speelt tussen thema's verschilt. Bij een thema als openbare orde is het aandeel OSINT relatief groot, terwijl dit bij het thema drugs minder groot is. OSINT wordt daarnaast ingezet voor andere (deels overlappende) doeleinden, zoals dreigingsinschattingen in het kader van bewaken & beveiligen, het verrijken van informatie over meldingen (in het RTIC) en het opstellen van situatierapporten of informatiebeelden in het kader van grootschalig en bijzonder optreden (zoals bij het SGBO Corona).

Intelligencemedewerkers vergaren op het internet op zowel handmatige als geautomatiseerde wijze gegevens. Bij het handmatig vergaren maakt men gebruik van onderzoeksprofielen (accounts onder een pseudoniem). Hierbij doen zich tussen eenheden verschillen voor wat betreft aanwezigheid in besloten groepen. De meeste informatieorganisaties doen dit wel. Voor de automatische vergaring wordt door alle informatieorganisaties gebruikgemaakt van het softwareprogramma PublicSonar. Deze software kan op verschillende manieren worden gebruikt, waaronder het monitoren van relevante berichten/signalen op sociale mediaplatformen.

In een deel van de basisteams vinden – zoals eerder aangegeven – eveneens OSINT-werkzaamheden plaats. De digitaal wijkagenten spelen hierin veelal een belangrijke rol. In het basisteam wordt OSINT ook gebruikt voor het opbouwen en onderhouden van een informatiepositie. Hierbij is een geografische oriëntatie logischerwijs dominant. Hierin schuilt ook een deel van de meerwaarde ten opzichte van wat de informatieorganisatie doet. In het basisteam monitort men vooral in het kader van de openbare orde. Daarnaast is er aandacht voor lokale netwerken, zoals jeugdgroepen of outlaw motorgangs. Onze indruk is dat de OSINT-werkzaamheden in de basisteams mondjesmaat en nog weinig gestructureerd plaatsvinden (zie ook Terpstra et al., 2021).

OGG wordt daarnaast ingezet in het kader van opsporing: internetrechercheren. Internetrechercheren is een opsporingsmethode. Uit dit onderzoek komt naar voren dat deze methode in een opsporingsonderzoek niet standaard of als vanzelfsprekend wordt overwogen. Hierbij doen zich verschillen voor tussen typen onderzoeken. Bijvoorbeeld: in sommige eenheden wordt de methode bij een TGO wel standaard overwogen, terwijl dit bij ondermijningsonderzoeken in mindere mate het geval is. Verschillende respondenten zijn van mening dat de methode te weinig wordt benut. Hierbij spelen volgens respondenten diverse factoren een rol, waaronder de aard en omstandigheden van een delict en de oriëntatie van recherchemensen en in het bijzonder leidinggevenden (al dan niet 'traditioneel' georiënteerd). Bij de 'onderbenutting' wordt opgemerkt dat er een kentering gaande is: de methode zou in toenemende mate worden ingezet.

Internetrechercheren begint – overigens net als OSINT – met een onderzoeksvraag die voortvloeit uit het opsporingsonderzoek. Om goed aan te kunnen sluiten bij het opsporingsonderzoek is (enige) inbedding in het onderzoeksteam van belang, zodat de internetrechercheur kan meelezen in het onderzoek en een goede onderzoeksvraag kan formuleren. Het beantwoorden van onderzoeksvragen op afstand van het onderzoeksteam werkt minder goed volgens respondenten. Met de onderzoeksvraag als uitgangspunt werkt de internetrechercheur van datapunt naar datapunt: je ontdekt bijvoorbeeld via sociale media dat de verdachte kinderen heeft, je vindt een van de kinderen op Snapchat, via Snapchat ontdek je waar het kind op school zit en op de website van de school vind je het rooster voor de tienminutengesprekken. In de omgeving van de school kan de verdachte worden aangehouden. De internetrechercheur gebruikt hierbij, naast het internet, ook andere bronnen om zo weer nieuwe 'haakjes' te vinden. Internetrechercheurs werken veel handmatig en gebruiken daarnaast software voor specifieke taken, waaronder het vastleggen welke handelingen worden verricht. Dit is van belang voor het geval er een proces-verbaal moet worden opgemaakt.

De opbrengsten van internetrechercheren zijn volgens respondenten wisselend: de ene keer heeft het veel opbrengsten voor het onderzoek en andere keer weinig tot niets. De opbrengsten hebben vooral betrekking op het identificeren van verdachten en slachtoffers, het verrijken van het beeld van verdachten en andere betrokkenen, het relateren van personen aan elkaar en het lokaliseren van zowel verdachten als voortvluchtigen.

Gebruik van bevoegdheden in het kader van OGG
Hoofdstuk 2 behandelt het juridisch kader voor OGG door de politie. Dit is een gebrekkig juridisch kader. De gebrekkigheid wordt vooral veroorzaakt doordat wetgeving die oorspronkelijk was bedoeld voor politiewerk in de fysieke wereld wordt toegepast op politiewerk op het web. Deze toepassing of vertaling gaat gepaard met obstakels. In het juridisch kader zijn verschillende vraagstukken geïdentificeerd waarover in meer of mindere mate onduidelijkheid bestaat.

In de politiepraktijk moet men omgaan met deze onduidelijkheden. In het kader van online intelligencevergaring gaat het dan in de eerste plaats over de grenzen van art. 3 Pw. Om relevante online gegevens te vergaren, is het volgens respondenten in toenemende mate nodig om aanwezig te zijn in besloten omgevingen, bijvoorbeeld Telegram-groepen. De vraag is echter wat zij op basis van art. 3 Pw mogen. Op basis van het juridisch kader kan worden aangenomen dat zij op basis van art. 3 Pw onderzoeksprofielen mogen gebruiken. De vraag of zij met deze onderzoeksprofielen naar binnen mogen gaan in afgeschermde omgevingen met toegangsbeleid is minder eenduidig te beantwoorden. Duidelijk is in ieder geval wel dat men in dat geval veel eerder dan in open bronnen een meer dan geringe inbreuk maakt op de privacy van betrokkenen. De grens van art. 3 Pw komt dus veel sneller in zicht, maar de precieze omstandigheden (bijvoorbeeld aard en grootte van een besloten groep) zijn van belang. In de praktijk biedt dit weinig houvast. Er doen zich dan ook verschillen voor tussen informatieorganisaties van de eenheden voor wat betreft aanwezigheid in besloten groepen.

Een tweede vraagstuk met betrekking tot intelligence gaat over wie het gezag is op het gebied van online gegevensvergaring in het domein van openbare orde. Met wie kan de politie bijvoorbeeld afstemmen over de grenzen van art. 3 Pw? Het juridisch kader geeft daarop geen eenduidig antwoord, al kan worden aangenomen dat de burgemeester de meest waarschijnlijke kandidaat is. In de politiepraktijk zijn er onduidelijkheden en verschillen. Er zijn eenheden waar wordt afgestemd met de informatieofficier van het OM en er zijn (minder) eenheden waar wordt afgestemd met de burgemeester. Een deel van de respondenten geeft aan dat zij op dit moment met de informatieofficier afstemmen, terwijl zij vinden dat de burgemeester het aangewezen gezag is. De burgemeester herkent volgens respondenten deze rol – op het gebied van online gegevensvergaring – echter niet en er zijn praktische bezwaren vanwege de grenzeloosheid van het internet (zie ook Bantema et al., 2018).

Ten behoeve van de opsporing is er (veel) meer een juridisch kader dan ten behoeve van intelligence. In de opsporing staat het vraagstuk van stelselmatigheid centraal. Stelselmatige online gegevensvergaring wil zeggen dat er een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands leven en er dus een meer dan geringe inbreuk op iemands privacy wordt gemaakt. In dat geval zijn algemeen taakstellende bepalingen (art. 3 Pw of art. 141/142 Sv) niet meer toereikend en is een bijzondere opsporingsbevoegdheid nodig. Uit dit onderzoek komt naar voren dat er in-

ternetrechercheurs zijn die stelselmatigheid onjuist interpreteren c.q. operationaliseren en daarmee het risico lopen onrechtmatig te handelen. Zij denken dat stelselmatigheid vooral gaat over de duur of frequentie van online gegevensvergaring – bijvoorbeeld vaker hetzelfde Facebookprofiel raadplegen – terwijl het gaat over het beeld dat wordt verkregen van iemands leven. Daarnaast worstelt men met de onduidelijkheden in het juridisch kader. Het centrale vraagstuk is hetzelfde als in het kader van intelligence: als er met een onderzoeksprofiel toegang wordt verkregen tot een afgeschermde bron, is er dan (per definitie) sprake van stelselmatigheid of kan dit ook nog op basis van een algemeen taakstellende bepaling? De respondenten ervaren dat officieren van justitie geregeld verschillend oordelen over stelselmatigheid, al wordt het eenduidiger naarmate online gegevensvergaring gangbaarder wordt.

Professionalisering van OGG professionals
De respondenten die uitvoering geven aan OGG-werkzaamheden hebben hier in de regel een meer of minder uitgebreide opleiding voor gevolgd. Deze opleidingen worden vooral aangeboden door private aanbieders, al merken respondenten op dat de Politieacademie in dit domein een inhaalslag heeft gemaakt. De Politieacademie is vooral toegerust voor het aanleren van de basisvaardigheden. Voor de meer geavanceerde – deels technische – vaardigheden (waaronder scripts programmeren) wordt per definitie gebruikgemaakt van private aanbieders, zoals data-expert en SANS. Het onderwijs door de Politieacademie wordt door veel respondenten belangrijk gevonden, omdat het onderwijs van private aanbieders in de regel geen politiespecifiek onderwijs is.[166] Dit heeft in sommige gevallen als gevolg dat er weinig aandacht wordt besteed aan de juridische kaders die voor het politiewerk gelden en de daarmee samenhangende afwegingen met betrekking tot het gebruik van bevoegdheden.

Respondenten zijn behoorlijk eensgezind: opleidingen zijn (veelal) nuttig, maar je wordt 'goed' in OGG door het te doen en door het vak bij te houden. Het bijhouden van het vak vraagt voortdurend aandacht, omdat er in het vak veel ontwikkeling is: het internet verandert – bijvoorbeeld nieuwe socialemediaplatformen die hun intrede doen – en methoden, technieken en tools op het gebied van OGG ontwikkelen door. Fulltime specialisten besteden veelal de nodige (privé)tijd aan het bijhouden van het vak. Zij volgen (inter)nationale OSINT-experts[167] via sociale media, zijn lid van landelijke netwerken binnen de politie (fysiek en via chatgroepen) en nemen veelal ook deel aan netwerken binnen de eenheid. Voor politiemensen met een taakaccent is het bijhouden van het vak nagenoeg onmogelijk. Zij kunnen beperkt tijd besteden aan OGG. Zij verleren de bestaande (basis)vaardigheden eerder dan dat zij zich verder kunnen ontwikkelen met nieuwe methoden, technieken en/of tools.

166 In geval van een samenwerkingscontract (als gevolg van een aanbesteding) tussen de Politieacademie en een private aanbieder kan het onderwijs wel een politiespecifiek karakter hebben.
167 OSINT is internationaal gezien de meest voorkomende aanduiding van het vakgebied.

Gebruik van technologie bij OGG werkzaamheden
De 'uitrusting' van OGG-professionals bestaat uit hard- en software. Het werk wordt met een computer verricht: een personal computer, laptop en/of smartphone (zie verder paragraaf 6.2). Daarnaast is software voor (een deel van) de OGG-professionals van belang. Software wordt gebruikt voor 1) veilig/anoniem werken, 2) automatisch zoeken en overnemen van gegevens, 3) analyseren van gegevens, en 4) ondersteuning van verslaglegging. De relevantie van deze functionaliteiten verschilt tussen intelligence en opsporing. Veilig werken is voor beide disciplines van belang, terwijl automatisch zoeken en overnemen relevanter is voor intelligence en ondersteuning voor verslaglegging relevanter is voor opsporing. Er wordt gebruikgemaakt van software van commerciële aanbieders en daarnaast worden ook eigen softwareprogramma's of scripts geprogrammeerd.

De respondenten die wij hebben gesproken geven aan dat zij vaker handmatig dan geautomatiseerd online gegevens vergaren en analyseren. Zij benadrukken daarnaast dat de meerwaarde van geavanceerde software niet moet worden overschat. Het is volgens veel respondenten onderdeel van het gereedschap van de professional, maar de professional zelf maakt het verschil. In interviews werd geregeld verwezen naar de 'mindset' van de professional. OGG is een manier van denken. Je moet begrijpen hoe het internet – onder de motorkap – werkt. De OGG-professional is een 'puzzelaar' die van datapunt naar datapunt werkt. Dit vraagt volgens respondenten nieuwsgierigheid, creativiteit, analytisch en kritisch vermogen, vasthoudendheid en veel oog voor detail.

7.2 Aandachtspunten voor de toekomst

In deze paragraaf richten we de blik naar voren en formuleren we aandachtspunten voor de toekomst van online gegevensvergaring binnen de politie. Hierbij maken we gebruik van eigen inzichten naar aanleiding van dit onderzoek én van wat respondenten ons hebben meegegeven.[168] De aandachtspunten zijn geordend in enkele thema's.

Digitaal fitte leidinggevenden
De verdere ontwikkeling van OGG als vakgebied binnen de politie heeft baat bij leidinggevenden die het belang ervan inzien voor het politiewerk. De respondenten in dit onderzoek hebben gemerkt dat de maatschappelijke onrust in het algemeen en de avondklokrellen in het bijzonder voor meer urgentie op strategisch niveau hebben gezorgd. Zij vragen zich echter af wat maakt dat hiervoor dergelijke incidenten en omstandigheden nodig zijn. De noodzaak van aanwezigheid van politie op het web is volgens hen evident als je kijkt naar de digitalisering van de samenleving. Zij signaleren daarnaast een verschil tussen woorden en daden. Dit wil zeggen dat het belang dat leidinggevenden op strategisch niveau aan online gegevensvergaring toekennen zich

168 We hebben hen hier expliciet naar gevraagd.

niet altijd vertaalt in de investeringen in mensen en middelen en onze respondenten – de OGG professionals – hebben daar juist behoefte aan.

Naast leidinggevenden op strategisch niveau gaat het ook om leidinggevenden op tactisch en operationeel niveau. Op tactisch niveau maken teamchefs keuzes met betrekking tot de personele inrichting van hun afdeling of team. Bijvoorbeeld: wel of geen digitaal wijkagent in ons basisteam? Wel of geen fulltime specialist in onze districtsrecherche of in onze Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel? Op operationeel niveau betreft het vooral de inzet van OGG in de uitvoering van politiewerk. Vooral in de opsporing wordt internetrechercheren nu soms niet ingezet, omdat degenen die onderzoeken leiden/coördineren de methode onvoldoende kennen en/of het belang er niet van inzien en voorkeur geven aan wat zij wel kennen.

Kortom: een politie die aanwezig wil zijn in wijk en web moet aandacht hebben voor de digitale fitheid van leidinggevenden die op verschillende niveaus keuzes maken.[169] De verwachting is dat leidinggevenden die begrip hebben van de digitale transformatie in de samenleving en begrijpen wat de meerwaarde of misschien wel noodzaak van online gegevensvergaring is, eerder keuzes maken die ten goede komen aan de verdere ontwikkeling van OGG binnen de politie.

Een breed basisniveau

Dit onderzoek maakt duidelijk dat online gegevensvergaring op dit moment alleen binnen de informatieorganisatie behoorlijk breed is ingebed. Dit wil zeggen dat er relatief veel medewerkers zijn die OGG-werkzaamheden uitvoeren. Hierbij is er een onderscheid tussen eenvoudige werkzaamheden (generalisten, grotere groep) en meer complexe werkzaamheden (specialisten, kleinere groep). Binnen de rechercheonderdelen en basisteams is van een dergelijke brede inbedding geen sprake. Volgens veel van onze respondenten is dit wel nodig voor een politie die aanwezig wil zijn in wijk en web. Zij pleiten voor verankering van de basisvaardigheden (OGG niveau 1-2, zie paragraaf 3.3) in het politieonderwijs[170] ten behoeve van de basispolitiezorg en de recherche, zodat alle politiemensen die via deze weg instromen de basis – waaronder veilig werken op het internet – meekrijgen.

> *'Ik denk dat OSINT een basisding moet worden. Wijk en web wil zeggen dat je ook fatsoenlijk moet kunnen OSINT-en. De basisvaardigheden zijn geen specialisme.'* (35)

Een brede(re) inbedding van het basisniveau is onder andere nodig om voor de specialisten ruimte te creëren, zodat zij zich kunnen richten op de meer complexe werkzaamheden. Dit is vooral nodig in de opsporing, waar specialisten soms worden ge-

169 Voor een uitwerking van digitale fitheid verwijzen we naar Aslander et al. (2022).

170 Hierbij moet worden opgemerkt dat het ook op andere manieren kan. Binnen de informatieorganisatie speelt de Intel Academie bijvoorbeeld een belangrijke rol in het basisniveau.

vraagd voor activiteiten die (tactisch) rechercheurs idealiter zelf zouden moeten (kunnen) verrichten. Voor het definiëren van de basis op het gebied online gegevensvergaring kan een beroep worden gedaan op de OGG-niveaus (zie paragraaf 3.4), maar ook op het onderzoek *Level-Up* van Jansen et al. (2020).

Verankering in de recherche
Het is volgens ons van belang om aandacht te besteden aan de verankering van online gegevensvergaring (internetrechercheren) binnen de recherche. Dit onderzoek maakt onder andere duidelijk dat expertise ontbreekt op plekken waar je dit wel zou verwachten én dat een taakaccent internetrechercheren een kwetsbare manier van organiseren is. Op basis hiervan denken wij dat er (bewuster) moet worden gekeken naar waar binnen de recherche de aanwezigheid van een of meer specialisten wenselijk is. Hierbij kan in het bijzonder worden gedacht aan de digitale platformen van de thematische opsporingsteams – hier rekenen we het Team Migratiecriminaliteit en Mensenhandel voor het gemak ook toe – en generieke opsporingsteams. Inbedding in de betreffende teams is ook een optie. In alle gevallen moet worden beseft dat het onderhouden van het specialisme – het gaat hier vooral om de meer complexe OGG-werkzaamheden – om toewijding vraagt. Deze toewijding kan door middel van een taakaccent in de regel niet worden bereikt.

> *'Je moet het als specialist 100% van je tijd doen. Anders kun je de fake accounts niet bijhouden, tools en platformen veranderen de hele tijd (…) Meer mensen moeten fulltime OSINT doen, zeker binnen de opsporing.'* (32)

Taakverdeling tussen disciplines en eenheden
Uit dit onderzoek komt naar voren dat de taakverdeling tussen de verschillende disciplines dan wel organisatieonderdelen binnen veel eenheden steeds meer aandacht krijgt. De noodzaak hiertoe is helder: steeds meer organisatieonderdelen verrichten OGG-werkzaamheden. Dit roept – zoals gezegd – de vraag 'Wie doet wat?' op. Op dit moment wordt deze vraag vooral op eenheidsniveau beantwoord. Het lijkt ons wenselijk dit naar landelijk niveau 'op te tillen'. Een van de respondenten heeft hierover het volgende opgemerkt:

> *'Wij snappen niet dat er landelijk geen portefeuille is voor OGG, dat er geen centraal beleid is waar ook bevoegd gezag en kennisinstituten in participeren. Waar kaders worden bepaald. De juridische kaders, de techniek, waar leg je de grens, hoe spreek je dit met elkaar af. Er worden per discipline wel wat afspraken gemaakt, maar de afstemming met andere disciplines is er niet.'* (37)

Met betrekking tot de afstemming tussen disciplines vraagt naar ons idee vooral de afstemming tussen de informatieorganisatie en het basisteam aandacht. Wie doet wat in het kader van OSINT? Hoe 'ver' reikt de OSINT-taak van het basisteam? Dit onderzoek maakt duidelijk dat er bij respondenten zorgen zijn over de werkzaamheden bin-

nen de basisteams. Gaat men niet te ver met aanwezigheid in besloten groepen? Heeft men voldoende oog voor de grenzen van art. 3 Pw? Een deel van de respondenten uit de basisteams heeft ook behoefte aan duidelijkheid met betrekking tot taken en bevoegdheden. Een landelijk antwoord hierop is gewenst.

Er is daarnaast aandacht nodig voor de landelijke operationele samenwerking op het gebied van OSINT, of anders gezegd: landelijke informatiecoördinatie. Het gaat dan in het bijzonder om het monitoren van maatschappelijk ongenoegen in al haar varianten. Zonder operationele afstemming is de kans op overlap in werkzaamheden groot, aangezien een deel van de groeperingen/online groepen beperkt territoriaal gebonden is. Eenheidsgrenzen hebben dan weinig betekenis.

Verduidelijken van het juridisch kader intelligence
In hoofdstuk 2 is aangegeven dat er voor online gegevensvergaring met een niet-strafvorderlijk doel – waaronder intelligence – vrijwel geen rechtsregels zijn. Er is inmiddels wel een groeiende praktijk van online gegevensvergaring ten behoeve van intelligence. Aandacht voor een normenkader lijkt daarom wenselijk (zie ook Commissie Koops, 2018). In de politiepraktijk ervaart men op dit moment onduidelijkheid ten aanzien van wat mag op basis van art. 3 Pw en er doen zich verschillen voor ten aanzien van hoe de grens van art. 3 Pw wordt geïnterpreteerd. Het gaat dan vooral om het gebruik van onderzoeksprofielen ten behoeve van toegang tot afgeschermde bronnen. Dit gebruik gaat op dit moment vermoedelijk soms over de grens van wat is toegestaan op basis van art. 3 Pw. Voor de intelligencepositie is toegang tot afgeschermde bronnen geregeld wel van belang, bijvoorbeeld in het kader van dreigende verstoringen van de openbare orde. Een normenkader kan meer duidelijkheid en eventueel ook mogelijkheden bieden.[171] De Commissie Koops adviseert om hierbij zoveel mogelijk aan te sluiten bij de terminologie – waaronder stelselmatigheid – en voorwaarden die binnen strafvordering worden gehanteerd.[172]

Een tweede aspect dat aandacht verdient, is geautomatiseerde online gegevensvergaring ten behoeve van intelligence. We mogen aannemen dat de voortschrijdende technologisering – in het bijzonder voor wat betreft kunstmatige intelligentie – leidt tot een verdere toename van het gebruik van geavanceerde software voor OSINT (zie ook CTIVD, 2021). Door middel van software kunnen tegelijkertijd honderden bronnen worden geraadpleegd. Dit kan – in geval van (overnemen van) persoonsgegevens – op

171 We pleiten hier zeker niet voor onbegrensde mogelijkheden. Een surveillancemaatschappij waarin steeds meer onschuldige burgers onderwerp van (enig) onderzoek worden, ligt op de loer (zie ook Landman, 2022).
172 Zie ook Stevens et al. (2021) voor een vergelijkbaar perspectief naar aanleiding van de casus 'Sensingproject Outlet Roermond'.

gespannen voet staan met het recht op privacy.[173] Dit roept de vraag op of er ten opzichte van de huidige situatie meer regulering nodig is. Op basis van dit onderzoek en onze expertise hebben wij hierover geen uitgesproken opvatting. Het gaat ons hier om de agendering van het thema.

Het is tot slot van belang dat er meer duidelijkheid wordt gegeven over het gezag bij online gegevensvergaring in het kader van openbare-orde-intelligence. Er is op dit moment een diverse praktijk – de een benadert de informatieofficier en de ander de burgemeester – en dit is onwenselijk. Indien de burgemeester het aangewezen gezag is, is het van belang om de praktische consequenties hiervan te verduidelijken. Een verstoring van de openbare orde in de fysieke wereld is immers territoriaal bepaald – die vindt ergens plaats – maar dit geldt niet of in veel mindere mate voor het online aanjagen van een dergelijke verstoring (zie o.a. Bantema et al., 2018). Hoe moet hiermee worden omgegaan indien de burgemeester het aangewezen gezag is?

Verduidelijken van het juridisch kader opsporing
Met betrekking tot online gegevensvergaring ten behoeve van de opsporing moet het gemoderniseerde Wetboek van Sv een antwoord zijn op de gebreken in het huidige juridisch kader. In het gemoderniseerde wetboek komt een nieuwe, specifieke grondslag voor stelselmatige online gegevensvergaring uit open bronnen[174] (zie hoofdstuk 2). Bij de inwerkingtreding ontstaat er hierdoor een juridisch kader met de volgende driedeling:[175]

- niet-stelselmatige online gegevensvergaring: de bestaande algemeen taakstellende bepalingen (art. 3 Pw of conceptart. 2.1.8 Sv).
- stelselmatige online gegevensvergaring uit open bronnen: de nieuwe bevoegdheid tot het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen (conceptart. 2.8.8 Sv).
- stelselmatige online gegevensvergaring uit afgeschermde bronnen (inclusief interactie met subjecten): de bestaande bevoegdheid tot het stelselmatig inwinnen van informatie (art. 126j Sv, conceptart. 2.8.11 Sv).

Bij de bevoegdheid tot het stelselmatig inwinnen van informatie is in de MvT aangegeven dat deze bevoegdheid moet worden gebruikt als een opsporingsambtenaar onder

173 Dit geldt des te meer wanneer softwareleveranciers ook data toevoegen aan de software. Dit kunnen gelekte data zijn van gebruikers van socialemediaplatformen of data die via data brokers zijn aangeschaft. Het raadplegen van deze (al aanwezige) persoonsgegevens kan een meer dan geringe inbreuk maken op de privacy van betrokken personen. Zie ook CTIVD (2021). Het is ons niet bekend of de politie ook gebruikmaakt van software van leveranciers die hier ook data aan hebben toegevoegd. Dit is in ieder geval wel een aandachtspunt voor de politie in het kader van zowel intelligence als opsporing.

174 Conceptart. 2.8.8. Dit artikel geeft de mogelijkheid om op bevel van de Officier van Justitie, bij een verdenking van een strafbaar feit waarop in de wet een jaar of meer gevangenisstraf is gesteld, stelselmatig gegevens uit publiek toegankelijke bronnen over te nemen.

175 Hierbij baseren we ons op het wetsvoorstel van juli 2020, de MvT hierop en beschouwingen op (eerdere versies van) het wetsvoorstel.

een valse naam toegang wil krijgen tot een afgesloten Facebook- of Twitter-account of tot een andere afgesloten vorm van sociale media, waarin hij als het ware onderdeel gaat uitmaken van dat online maatschappelijk verband, én hiermee een meer dan geringe inbreuk op de persoonlijke levenssfeer van een persoon maakt.

Deze driedeling heeft als consequentie dat de definitie en reikwijdte van open – de formele term is publiek toegankelijke – bron belangrijker wordt dan in de huidige situatie. In de huidige situatie draait alles in essentie om de vraag naar stelselmatigheid (zie hoofdstuk 2). In de MvT is uitgewerkt wat onder 'publiek toegankelijke bron' moet worden verstaan. Hierbij heeft men zich vooral gebaseerd op het advies van de Commissie Koops (2018). In de uitwerking valt echter op dat er beperkt wordt ingegaan op wat een afgeschermde bron is. De opsporingspraktijk moet het doen met de bovenstaande alinea en met de opmerking dat online vrienden worden van verdachte personen (met een nep-account) niet kan plaatsvinden op basis van de bevoegdheid tot het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Dit geeft de opsporingspraktijk naar ons idee te weinig houvast.[176] Ook de spelregel 'een afgeschermde bron betreft alle bronnen die niet publiek toegankelijk zijn' biedt weinig soelaas, want de operationalisering van de term 'publiek toegankelijke bron' biedt nog de nodige interpretatieruimte (zie ook Berends, 2020). Het lijkt ons wenselijk om het nieuwe juridisch kader te verduidelijken aan de hand van veelvoorkomende praktijkvoorbeelden, waarin wordt ingegaan op de vraag of het een afgeschermde bron betreft gecombineerd met de vraag of er sprake is van stelselmatigheid in de vergaring. De praktijkvoorbeelden zouden vooral betrekking moeten hebben op uiteenlopende besloten groepen.

Tot slot: ook in het kader van de opsporing is het van belang oog te hebben voor geautomatiseerde online gegevensvergaring en de juridische grondslag hiervoor (zie onder andere Lodder & Schuilenburg, 2016; Oerlemans, 2017; Stol & Strikwerda, 2018). Met de inwerkingtreding van het gemoderniseerde Wetboek van Sv verandert er in de kern niets ten opzichte van de huidige situatie: de juridische grondslag voor het gebruik van software wordt bepaald door de vraag naar stelselmatigheid. De operationalisering van stelselmatigheid – en het meenemen van geautomatiseerde vergaring – is een verbetering ten opzichte van de huidige situatie. Maar wederom geldt: de opsporingsambtenaar heeft beperkt houvast bij het beantwoorden van de vraag wanneer het gebruik van software leidt tot stelselmatigheid (zie Klaar, 2022). Meer houvast is gewenst. De uitwerking van Klaar (2022) kan in dit verband als een eerste stap worden beschouwd.

Kennis van het juridisch kader/bevoegdheden
Dat politiemensen in de huidige situatie te maken hebben met onduidelijkheden in het juridisch kader neemt niet weg dat sommigen ook een gebrek aan kennis hebben van wat op basis van welke bevoegdheid is toegestaan (zie ook Jansen et al., 2020). Hier-

176 Het gaat dan om de internetrechercheurs en niet zozeer om virtual agents.

voor is binnen de politie aandacht nodig, omdat het waarschijnlijk is dat politiemensen op dit moment op basis van algemeen taakstellende bepalingen activiteiten verrichten die een meer dan geringe inbreuk maken op de privacy van burgers. Dat is (dus) onrechtmatig. Het risico hierop is het grootst bij degenen die niet of beperkt zijn opgeleid voor online gegevensvergaring en zich hier niet dagelijks mee bezighouden.

Opleiden doet ertoe (zie ook Jansen et al., 2020). Het is essentieel dat het juridisch kader en gebruik van bevoegdheden een prominente plek hebben in de opleidingen op het gebied van OGG. Dit geldt in het bijzonder voor de basisopleidingen, die de opstap zijn naar meer geavanceerde opleidingen (zie paragraaf 6.1). Voor deze basis is de Politieacademie van belang, want de Politieacademie verzorgt politie-specifiek onderwijs. OGG kan weliswaar worden beschouwd als een vakgebied dat in uiteenlopende beroepen kan worden benut, maar in het politiewerk heeft het specifieke kenmerken die vooral te maken hebben met het juridisch kader. Voor de toekomst is het naar ons idee wenselijk dat alle politiemensen die OGG-werkzaamheden uitvoeren een basisopleiding bij of via de Politieacademie hebben gevolgd.[177] Dit waarborgt dat er voldoende aandacht is voor het gebruik van bevoegdheden.

Waarderen en faciliteren van OGG-professionals
Online gegevensvergaring – internationaal vooral bekend als OSINT – is (zoals gezegd) een vakgebied dat in diverse sectoren en beroepen een plek heeft gekregen. De specialisten die zich hiermee bezighouden zijn schaars.[178] Men kan op allerlei plekken aan de slag. Dit geldt ook voor de OGG-specialisten van de politie. Hoewel maatschappelijke betrokkenheid voor onze respondenten zwaar weegt, heeft men ook behoefte aan (financiële) waardering en ontwikkel- en doorgroeimogelijkheden. Dit wordt door sommigen gemist. Daarnaast zijn sommigen kritisch op de wijze waarop 'de' politieorganisatie hen faciliteert met middelen. De traagheid in procedures maakt dat zij moeizaam kunnen meebewegen met nieuwe ontwikkelingen in het vakgebied (zie ook paragraaf 6.2). Wij denken dat er aandacht nodig is voor het waarderen en faciliteren van de OGG-professionals binnen de politie, want zij maken in dit vakgebied binnen de politie het verschil.

Samenwerking in nieuwe veiligheidscoalities
Vaardigheden op het gebied van online gegevensvergaring zijn zeker niet alleen binnen intelligence- en opsporingsdiensten aanwezig. In een column in het *NRC* wijst Piet van Reenen op de opmars van onderzoekscollectieven van burgers die gebruikmaken van online gegevensvergaring. Hij definieert het als een beweging: het goede doen op het

177 In geval van 'via de Politieacademie' is het vanzelfsprekend van belang dat er toezicht is op de kwaliteit van de opleidingen die door externe partijen worden gegeven, in het bijzonder voor wat betreft het gebruik van bevoegdheden.
178 We baseren ons hier op respondenten.

internet, ongebonden en integer.[179] Deze ontwikkeling biedt de politie kansen op nieuwe veiligheidscoalities, ook een van haar strategische ontwikkelthema's. Deze kansen worden op dit moment voorzichtig benut, bijvoorbeeld door middel van de OSINT hackathons waaraan burgers deelnemen en door gebruik te maken van het werk van Bellingcat in het MH17-onderzoek (zie ook paragraaf 7.4). We delen de opvatting van Piet van Reenen dat er meer mogelijk is. Het is voor de politie (en het OM) van belang om de komende jaren te verkennen hoe zij in voorkomende gevallen kunnen aansluiten bij – en samenwerken met – burgernetwerken die over hoogwaardige expertise op het gebied van online gegevensvergaring beschikken.

7.3 Beperkingen van dit onderzoek

Dit onderzoek kent een aantal beperkingen. De eerste en voornaamste beperking is dat we het onderzoek breed hebben ingestoken. Dit komt tot uiting in de oriëntatie op zowel intelligence als opsporing en in de diverse aspecten van online gegevensvergaring die aan bod komen.[180] Hierdoor mist het onderzoek – in ieder geval op onderdelen, zoals intelligence – diepgang. Op bepaalde thema's is niet of nauwelijks ingegaan, zoals op het verifiëren van online vergaarde gegevens, aangezien er op het internet ook veel desinformatie te vergaren is. Het gebrek aan diepgang kwam ook in de feedback van de leescommissie naar voren. Een enkel lid had liever gezien dat we het onderzoek meer hadden afgebakend, zodat we het van meer diepgang hadden kunnen voorzien.

De tweede beperking is dat we respondenten hebben geïnterviewd die bezig zijn met – en enthousiast zijn over – OGG.[181] Hun perspectief staat centraal. We hebben bijvoorbeeld geen teamleiders van opsporingsonderzoeken geïnterviewd om hen te vragen naar onder andere de meerwaarde van OGG in opsporingsonderzoek. Dit had een breder, minder eenzijdig, perspectief kunnen opleveren, bijvoorbeeld voor wat betreft de opbrengsten van OGG.

De derde beperking heeft niet zozeer te maken met wie we hebben geïnterviewd, maar met het gegeven dat we hebben geïnterviewd. Het empirisch inzicht in online gegevensvergaring door de politie is gebaseerd op wat respondenten hierover zeggen. We hebben de werkzaamheden van OGG-professionals niet geobserveerd en we hebben ook geen casusonderzoek verricht naar bijvoorbeeld specifieke opsporingsonderzoeken waarin OGG is toegepast. Er kan een verschil zijn tussen wat mensen zeggen te doen en feitelijk doen. Daarnaast hebben de interviews niet geleid tot een gedetailleerd

179 https://www.nrc.nl/nieuws/2021/06/30/bellingcat-wijst-de-weg-naar-nieuwe-vormen-van-politie-a4049359?t=1652016191

180 Hierbij moet worden opgemerkt dat we geen aandacht hebben besteed aan de verdere verwerking van online vergaarde gegevens. We gaan daarnaast beperkt in op de duiding of analyse, in het bijzonder voor wat betreft intelligence.

181 Hierbij moet worden opgemerkt dat we niet van alle organisatieonderdelen OGG-professionals hebben geïnterviewd (zie ook par. 3.4). De nadruk lag op de afdeling RI van de DRIO, TDO van de DRR, de DR en het BT.

inzicht in hoe men te werk gaat: de methoden en technieken van de vergaring. Hierbij speelt vanzelfsprekend ook mee dat de interviews een brede insteek hadden.

7.4 *De inzet van de 'gekkies'*

> *'In het hoofdbureau van de politie van Leicester leidde een agent me naar een apart vertrek, waar twee onderzoekers uit Nederland en één uit Australië op me wachtten. Er waren ook een paar Britse politiemensen aanwezig die me verzekerden dat dit helemaal volgens protocol was. "Kun je alsjeblieft beginnen, Eliot, met uit te leggen wat je hebt gevonden", zei de Nederlandse leider van de groep. "Kun je, als je het niet erg vindt, heel belangrijk, ook vertellen hoe?" Hoe meer ik zei en hoe meer reacties ik van ze hoorde, hoe meer ik een duizeligmakend gevoel kreeg: wij waren de enigen die dit deden. De onderzoekers zagen in dat ze dit gedoe met open bronnen serieus moesten gaan nemen.'* (Higgins, 2021: 78)

Bovenstaand citaat is van Eliot Higgins – de oprichter van Bellingcat – en gaat over het opsporingsonderzoek naar het neerstorten van de MH17 waaraan Bellingcat een cruciale bijdrage heeft geleverd door gebruik te maken van online gegevensvergaring. Higgins zijn gevoel dat zij de enigen waren die dit deden, klopte niet helemaal, maar voorliggend onderzoek laat wel zien dat het even heeft geduurd voordat de politie 'dit gedoe met open bronnen' echt serieus is gaan nemen. In de afgelopen jaren is het vakgebied OGG binnen de politie echter zichtbaar en merkbaar gegroeid. Hoewel beleidsimpulsen hier ongetwijfeld een bijdrage aan hebben geleverd, zijn wij ervan overtuigd dat de inzet van de OGG-professionals binnen de politie – de 'gekkies' zoals zij zichzelf ook wel noemen – van doorslaggevend belang is (geweest). Wij hopen dat dit onderzoek recht doet aan hun praktijk en aanknopingspunten biedt voor de verdere doorontwikkeling van het vakgebied binnen de politie.

Literatuurlijst

Adang, O. (2013), *Er is geen feest. De overheidsreactie op project X Haren*. Den Haag: Commissie project X Haren.

Aslander, M., A. Broere & M. Meinema (2022), *Ons werk is stuk. Tips en inzichten voor onderhoud en reparatie*. Den Haag: Uitgeverij Publiek Denken BV.

Bacon, M. (2016), *Taking care of business. Police detectives, drug law enforcement and proactive investigation*. Oxford: Oxford University Press.

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

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

Bantema, W., S. Westers, M. Hoekstra, R. Herregodts & S.A.J. Munneke (2021*), Black box van gemeentelijke online. Een wankel fundament onder een stevige praktijk*. Den Haag: Sdu.

Baricco, A. (2018), *The game*. Amsterdam: De Bezige Bij.

Bazzell, M. (2022), *Open source intelligence techniques. Resources for searching and analyzing online information* (ninth edition).

Berends, T. (2020), *Publiek toegankelijke bronnen onderzoek door opsporingsinstanties. Strafvordering en privacy*. Open Universiteit.

Berkel, J.J. van, A. van Uden & C.J. Poot (2020), *Evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering. De wet 'vastleggen en bewaren van kentekengegevens door de politie' geëvalueerd*. Den Haag: WODC.

Beugelsdijk, S. (2021), *De verdeelde Nederlanden. Hoe een perfecte storm een klein land dreigt te splijten (en wat we daaraan kunnen doen*). Amsterdam: Uitgeverij Balans.

Bielska, A., N.R. Kurz Y. Baumgartner & V. Benetis (2020), *Open source intelligence tools and resources handbook*. Zurich: I-Intelligence.

Boelens, M. & W. Landman (2021), *Pionieren in gebiedsgebonden politiewerk. Een onderzoek naar de digitaal wijkagent in het basisteam*. Horn: Moduliprint.

Boer, W. de & C. van den Berg (2017), 'Real-time intelligence (RTI)'. In: M. den Hengst, T. ten Brink & J. ter Mors (red.), *Informatiegestuurd politiewerk in de praktijk* (241-248). Deventer: Vakmedianet.

Borgers, M.J. (2015), 'De normering van 'lichte' opsporingshandelingen', *Delikt en Delinkwent*, *15*(3), 143-155.

Brinkhoff, S. (2017), 'Datamining in een veranderende wereld van opsporing en vervolging', *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, *3*(4), 224-227.

Commissariaat voor de Media (2021), *Digital news report Nederland 2021*. Hilversum: Commissariaat voor de Media.

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops) (2018), *Regulering van opsporingsbevoegdheden in een digitale omgeving*. Den Haag.

COT (2021a), *Ongekende ongeregeldheden Leerevaluatie naar aanleiding van de ongeregeldheden in Eindhoven van 24 januari 2021*. Den Haag: COT.

COT (2021b), *Een machteloos gevoel. Leerevaluatie naar aanleiding van de ongeregeldheden in Den Bosch op 25 januari 2021*. Den Haag: COT.

CTIVD (2021), *Automated OSINT: tools en bronnen voor openbronnenonderzoek*. Den Haag: Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.

Dijk, A. van, P. De Baets, L. Gunther Moor, E. Devroe & S, Zouridis (2022), 'Politie en rechtsstaat in een gedigitaliseerde samenleving'. In: A. van Dijk, P. De Baets, L. Gunther Moor, E. Devroe & S. Zouridis (red.), *Politie en rechtsstaat in een gedigitaliseerde samenleving* (7-14). Antwerpen/'s-Hertogenbosch: Gompel & Svacina.

Doorn, M. van, S. Duivestein & T. Pepping (2021), *Echt nep. Spelen met de realiteit in tijden van AI, deepfakes en de Metaverse*. Voorschoten: Bot Uitgevers.

Dubberley, S., A. Koenig & D. Murray (2020), Introduction: the emergence of digital witnesses. In: S. Dubberley, A. Koenig, & D. Murray (eds.), *Digital Witness. Using open*

source information for human rights investigation, documentation and accountability (3-11). Oxford: Oxford University Press.

Duijn, P. (2011), Intelligence en recherchestrategieën. In: N. Kop, R. van der Wal & G. Snel (red.), *Opsporing belicht: over strategieën in de opsporingspraktijk* (63-94). Apeldoorn: Politieacademie.

Eeden, C.A.J. van den, J.J. van Berkel, C.C. Lankhaar & C.J. de Poot (2021), *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*. Den Haag: WODC.

Egmond, S.A. van (2017), *De digitale wijkagent. Een onderzoek naar de grenzen van het virtuele politiebureau*. Open Universiteit.

Feenstra, M. (2018), 'Opsporingsmiddelen in ontwikkeling. Open-bronnenonderzoek als nieuwe "tap"', *Proces*, *97*(6), 367-375.

Ferwerda, N.C. (2022), *Closing cases through open sources. Het gebruik van openbronnenonderzoek bij de Nederlandse opsporing en vervolging van internationale misdrijven*. Apeldoorn: Politieacademie.

Galič, M. (2022), 'Bulkbevoegdheden en strafrechtelijk onderzoek. Lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse', *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, *10*(2), 130-137.

Gritter, E. (2018), 'De rechtmatigheid van datamining door de politie', *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, *4*(2), 113-115.

Higgins, E. (2021), *Wij zijn bellingcat. Hoe gewone mensen de onderzoeksjournalisten van de toekomst werden*. Amsterdam: Spectrum.

Inspectie Justitie & Veiligheid (2018), *Intelligence in de opsporing. Over de bijdrage van de informatieorganisatie van de politie aan de opsporing door de recherche*. Den Haag: Inspectie J&V.

Inspectie Justitie & Veiligheid (2019), *Selectie en toewijzing in de opsporing*. Den Haag: Inspectie J&V.

Jansen, J., T. van Valkengoed, S. Veenstra & W. Stol (2020), *Level-Up! Kennis voor politiewerk in een digitale samenleving*. Leeuwarden/Apeldoorn: NHL Stenden Hogeschool/Politieacademie.

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.

Kop, N. & P. Klerks (2009), *Doctrine intelligencegestuurd politiewerk*. Apeldoorn: Politieacademie.

Koops, B.J. (2012), 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *Tijdschrift voor Veiligheid*, *11*(2), 30-46.

Koops, B.J. (2013), 'Police investigations in internet open sources: procedural-law issues', *Computer Law & Security Review*, 29, 654-665.

Lam, J. & N. Kop (2020a), *Evaluatie coldcase hackathon.* Apeldoorn: Politieacademie.

Lam, J. & N. Kop (2020b), *Evaluatie FASTNL hackathon*. Apeldoorn: Politieacademie.

Lam, J. & N. Kop (2020c), *Evaluatie vuurwerk hackathon*. Apeldoorn: Politieacademie.

Landman, W. (2022), *Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk*. Den Haag: Sdu (wordt nog gepubliceerd).

Landman, W., R.M. Kouwenhoven & M. Brussen (2020), *Kijk naar het systeem. Begrijpen en beïnvloeden van opsporingspraktijken*. Den Haag: Sdu.

Lassche, H. (2021), *Digitalisering en de opsporingspraktijk. Juridische aspecten*. Apeldoorn: Politieacademie.

Lodder, A.R. & M.B. Schuilenburg (2016), 'Politie web-crawlers en predictive policing', *Computerrecht*, *81*(3), 150-154.

Mehlbaum, S., R. van Steden & M. van Dijk (2018), *Doe-het-zelf-surveillance. Een onderzoek naar de werking en effecten van WhatsApp-buurtgroepen*. Den Haag: Sdu.

Meijer, A.J., S.G. Grimmelikhuijsen, D. Fictorie, M. Thaens & P. Sien (2013), *Politie & sociale media. Van hype naar onderbouwde keuzen*. Amsterdam: Reed Business.

Miller, B.H. (2018), 'Open Source Intelligence (OSINT): an oxymoron?', *International Journal of Intelligence and CounterIntelligence*, *31*(4), 702-719.

Oerlemans, J.J. (2017), *Normering van digitale opsporingsmethoden*. Breda: Nederlandse Defensie Academie.

Oerlemans, J.J. (2018a), 'Facebookvrienden worden met de verdachte. Over undercoverbevoegdheden op internet', *Justitiële Verkenningen*, *44*(5), 83-99.

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

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* (195-258). Den Haag: Boom Criminologie.

Oerlemans, J.J. & B.J. Koops (2012), 'Surveilleren en opsporen in een internetomgeving', *Justitiële Verkenningen*, *38*(5), 35-49

Oosterhoff, M. (2016), *Opsporing op social media. Afstudeerscriptie masteropleiding Rechtsgeleerdheid*. Amsterdam: Open Universiteit.

Openbaar Ministerie & Politie (2016), *Leidraad Bevoegdheden informatievergaring op het internet – opsporing*. Den Haag.

Politie (2012), *Inrichtingsplan Nationale Politie*. Den Haag: Politie.

Politie (2015), *Open source intelligence (OSINT) in de informatieorganisatie. Position paper*. Den Haag: Politie.

Politie (2016), *Positionpaper social media in de opsporing*. Den Haag: Politie.

Poot, C.J. de, R.J. Bokhorst, P.J. Koppen & E.R. Muller (2004), *Rechercheportret. Over dilemma's in de opsporing*. Alphen aan den Rijn: Kluwer.

Princen, M. (2015), *De gekooide recherche. Het ware verhaal achter de matige prestaties van de Nederlandse opsporing*. Amsterdam: Prometheus Bert Bakker

Ramwell, S., T. Day & H. Gibson (2016), 'Use cases and best practices for LEA's'. In: B. Akhgar, P.S. Bayerl & F. Sampson (eds.), *Open source intelligence investigation: from strategy to implementation* (197-212). Cham: Springer International Publishing.

Ratcliffe, J. (2008), *Intelligence-led policing*. New York: Routledge.

Rathenau Instituut (2021), *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland*. Den Haag.

Rosema, S.W. (2020), *De voorgestelde opsporingsbevoegdheid: het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen*. Open Universiteit.

Salet, R. (2015), *Opsporing, tegenspraak en veranderende frames. Een onderzoek naar tegenspraak in grootschalige rechercheonderzoeken*. Den Haag: Boom Lemma Uitgevers.

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., M. den Hengst & R. Waterreus (2016), *Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie*. Amsterdam: Reed Business.

Smilda, F. & A. de Vries (2017), 'Sociale media'. In: M. den Hengst, T. ten Brink & J. ter Mors (red.), *Informatiegestuurd politiewerk in de praktijk* (193-206). Deventer: Vakmedianet.

Smulders, I. (2017), *#Politie: twittergebruik door wijkagenten & de veiligheidsbeleving van de burger*. Open Universiteit.

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* (21-32). Cham: Springer International Publishing.

Stevens, L., M. Hirsch Ballin, M. Galič, S.S. Buisman, B. Groothoff, Y. Hamelzky, C. Lucas, K. Rasul & S. Verijdt (2021), 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling. Een analyse aan de hand van de casus "Sensingproject Outlet Roermond"', *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, *9*(4), 234-245.

Stol, W. (2021), 'Digitalisering en de maatschappelijke rol van de politie. Naar politie als "autoriteit fatsoenlijke rechthandhaving"'. In: G. Meershoek, J. Nap & L. van Spijk (red.), *In naam der wat? Reflecties op politie en politiewerk* (29-38). Den Haag: Boom criminologie.

Stol, W. & L. Strikwerda (2018), 'Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving', *Tijdschrift voor Veiligheid*, *17*(1-2), 8-22.

Streefkerk, M (2012), 'Onuitputtelijke bron', *Blauw*, *8*(23), 20-23.

Terpstra, J., R. Salet, I. van Duijneveldt & T. Havinga (2021), *Gebiedsgebonden politiewerk in ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving*. Den Haag: Sdu.

Trottier, D. (2015a), 'Coming to terms with social media monitoring: uptake and early assessment', *Crime Media Culture*, *11*(3), 317-333.

Trottier, D. (2015b), 'Open source intelligence, social media and law enforcement: visions, constraints and critiques', *European Journal of Cultural Studies*, *18*(4-5), 530-547.

Treeck, R. van & W.Ph. Stol (2000), 'Betrouwbare open bronnen', *Algemeen Politieblad*, 20, 11-13.

Verhoeven, N. (2020), *Thematische analyse. Patronen vinden bij kwalitatief onderzoek*. Amsterdam: Boom Uitgevers.

Vries, S. de & W. Bantema (2022), *Aanpak in kaart. Inzicht in een regionale aanpak van online aangejaagde ordeverstoringen*. Leeuwarden: NHL stenden.

Wermeskerken, H. van (2016), 'Privacy op Facebook', *Blauw*, *12*(5), 16-19.

Zuurveen, R. & W. Stol (2020), *Benutten van digitale sporen*. Den Haag: Sdu.

Bijlage 1 **Respondentenlijst**

Respondentnummer	Functie/rol en organisatieonderdeel
1	Senior GGP/Digitaal wijkagent, basisteam
2	Senior tactische opsporing, basisteam
3	Senior GGP/Digitaal wijkagent, basisteam
4	Senior GGP/Digitaal wijkagent, basisteam
5	Senior GGP/Digitaal wijkagent, basisteam
6	Senior GGP/Digitaal wijkagent, basisteam
7	Senior GGP/Digitaal wijkagent, basisteam
8	Senior GGP/Digitaal wijkagent, basisteam
9	Senior GGP/Digitaal wijkagent, basisteam
10	Senior GGP/Digitaal wijkagent, basisteam
11	Senior GGP/Digitaal wijkagent, basisteam
12	Senior GGP/Digitaal wijkagent, basisteam
13	Generalist tactische opsporing, districtsrecherche
14	Generalist tactische opsporing, districtsrecherche
15	Senior tactische opsporing, districtsrecherche
16	Senior tactische opsporing, districtsrecherche
17	Generalist tactische opsporing, districtsrecherche
18	Generalist tactische opsporing, districtsrecherche
19	Generalist tactische opsporing, districtsrecherche
20	Assistent Intake & Service B, districtsrecherche
21	Operationeel Specialist A, districtsrecherche
22	Operationeel Specialist B, regionale recherche
23	Operationeel Specialist B, regionale informatieorganisatie
24	Operationeel Specialist B, regionale recherche
25	Operationeel Specialist A, regionale recherche
26	Projectleider, politiedienstencentrum
27	Bedrijfsvoeringsspecialist, politiedienstencentrum
28	Operationeel Specialist A, regionale recherche
29	Operationeel Specialist D, regionale recherche
30	Operationeel Specialist A, regionale recherche
31	Operationeel Specialist B, regionale informatieorganisatie

Respondentnummer	Functie/rol en organisatieonderdeel
32	Operationeel Specialist A, regionale informatieorganisatie
33	Operationeel Specialist B, regionale informatieorganisatie
34	Operationeel Specialist A, regionale informatieorganisatie
35	Operationeel Specialist A, regionale recherche
36	Sectorhoofd/portefeuillehouder OSINT, regionale informatieorganisatie
37	Operationeel Specialist C, regionale informatieorganisatie
38	Operationeel Specialist B, landelijke informatieorganisatie
39	Operationeel Specialist B, regionale informatieorganisatie
40	Operationeel Specialist D, regionale recherche
41	Operationeel Specialist B, regionale recherche

Leden Redactieraad Programma Politie & Wetenschap

Voorzitter	prof. em. dr. ir. J.B. Terpstra Radboud Universiteit Nijmegen
Leden	mr. drs. C. Bangma Politie, Eenheid Midden-Nederland
	mw. mr. W.M. de Jongste Projectbegeleider Wetenschappelijk Onderzoek- en Documentatiecentrum Ministerie van Justitie en Veiligheid
	dr. P.P.H.M. Klerks Raadadviseur Parket-Generaal, Openbaar Ministerie
	mr. drs. C. Loef Adviseur Gemeente Amsterdam
	mw. J. Overeem Politie, Eenheid Midden-Nederland
	prof. em. dr. P. van Reenen Van Reenen-Russel Consultancy b.v. Studie- en Informatiecentrum Mensenrechten (SIM) Universiteit Utrecht
	mw. drs. M.H.M. van Tankeren Operational auditor/onderzoeker, Politie, Eenheid Den Haag

Secretariaat	Programmabureau Politie & Wetenschap Politieonderwijsraad Koninginnegracht 62 2514 AG Den Haag Postbus 25842 2502 HV Den Haag www.politieenwetenschap.nl

Uitgaven in de reeks Politiewetenschap

1. ***Kerntaken van de politie. Een inventarisatie van heersende opvattingen***
   C.D. van der Vijver, A.J. Meershoek & D.F. Slobbe, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2001
2. ***Bevoegdheden overd(r)acht. Een onderzoek naar delegatie en mandaat van beheersbevoegdheden in de politiepraktijk***
   H.B. Winter & N. Struiksma, Pro Facto B.V., Universiteit Groningen, 2002
3. ***Sturing van politie en politiewerk. Een verkennend onderzoek tegen de achtergrond van een veranderende sturingscontext en sturingsstijl***
   J. Terpstra, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2002
4. ***Woninginbrekers en zware jongens. Daders vanuit het voormalig Joegoslavië aan het woord***
   M. van San, E. Snel & R. Boers, Risbo, Erasmus Universiteit Rotterdam, 2002
5. ***Zeg me wie je vrienden zijn. Allochtone jongeren en criminaliteit***
   F.M.H.M. Driessen, B.G.M. Völker, H.M. Op den Kamp, A.M.C. Roest & R.J.M. Molenaar, Bureau Driessen, Utrecht, 2002
6. ***Op deugdelijke grondslag. Een explorerende studie naar private forensische accountancy***
   J. van Wijk, W. Huisman, T. Feuth & H.G. van de Bunt, Vrije Universiteit, Amsterdam, 2002
7. ***Voorbij de dogmatiek. Publiek-private samenwerking in de veiligheidszorg***
   A.B. Hoogenboom & E.R. Muller, COT, Den Haag, 2003
8. ***Hennepteelt in Nederland. Het probleem van de criminaliteit en haar bestrijding***
   F. Bovenkerk, W.I.M. Hogewind, D. Korf & N. Milani, Willem Pompe Instituut, Universiteit Utrecht, 2003
9. ***Politiekennis in ontwikkeling. Een onderzoek naar het verzamelen en veredelen van informatie voor het Politie Kennis Net***
   I. Bakker & C.D. van der Vijver, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2003

10a. ***Politie en geweld. Een verkenning van politiereacties op geweldsincidenten in vier Nederlandse regiokorpsen***
C.J.E. In 't Velt, W.Ph. Stol, P.P.H.M. Klerks, H.K.B. Fobler, R.J. van Treeck & M. de Vries, NPA-Politie Onderwijs- en Kenniscentrum, LSOP, Apeldoorn, 2003

10b. ***Geweldige informatie? Onderzoek naar de informatiehuishouding van geweldsmeldingen bij de politie***
R. van Overbeeke, O. Nauta, A. Beerepoot, S. Flight & M. Rietveld, DSP-groep, Amsterdam, 2003

11. ***Blauwe Bazen. Het leiderschap van korpschefs***
R.A. Boin, P. 't Hart & E.J. van der Torre, Departement Bestuurskunde, Universiteit Leiden/COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2003

12. ***Over de grens. Een verkenning van projecten voor probleemjeugd in Duitsland, Engeland en Zweden***
I. van Leiden, G. Verhagen & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2003

13. ***Integriteit in het dagelijkse politiewerk. Meningen en ervaringen van politiemensen***
J. Naeyé, L.W.J.C Huberts, C. van Zweden, V. Busato & B. Berger, Centrum voor Politiewetenschappen, VU Amsterdam, 2004

14. ***Politiestraatwerk in Nederland. Noodhulp en gebiedswerk: inhoud, samenhang, verandering en sturing***
W. Ph. Stol, A.Ph. van Wijk, G. Vogel, B. Foederer & L. van Heel, Nederlandse Politieacademie, Onderzoeksgroep, LSOP, Apeldoorn, 2004

15. ***De kern van de taak. Kerncompetenties van de politie als criterium voor de afbakening van kerntaken in de praktijk***
A. Mein, A. Schutte & A. van Sluis, ES&E, Den Haag, 2004

16. ***Professionele dienstverlening en georganiseerde criminaliteit. Hedendaagse integriteitsdilemma's van advocaten en notarissen***
F. Lankhorst & J.M. Nelen, Vrije Universiteit Amsterdam, Faculteit der Rechtsgeleerdheid, Sectie Criminologie, Amsterdam, 2004

17. ***Paradoxaal Politiebestel. Burgemeesters, Openbaar Ministerie en Politiechefs over de sturing van de politie***
L.W.J.C. Huberts, S. Verberk, K. Lasthuizen & J.H.J. van den Heuvel, Vrije Universiteit Amsterdam/B&A Groep, 's-Gravenhage, 2004

18. ***Illegale vuurwapens in Nederland: smokkel en handel***
A.C. Spapens & M.Y. Bruinsma, IVA, Tilburg, 2004

19. ***Samenwerking en netwerken in de lokale veiligheidszorg***
J. Terpstra & R. Kouwenhoven, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2004

20. ***Uit balans: politie en bestel in de knel. State-of-the-art: bundeling van kennis en inzicht***
H.G. van de Bunt, A.B. Hoogenboom, LW.J.C. Huberts, E.R Muller, J. Terpstra, C.D. van der Vijver & C. Wiebrens, 2004 Redactie: G.C.K. Vlek, C. Bangma, C. Loef & E.R. Muller

21. ***Politie en media. Feiten, fictie en imagopolitiek***
H. Beunders & E.R. Muller, Erasmus Universiteit Rotterdam/COT, Instituut voor Veiligheids- en Crisismanagement, Leiden, 2005 (2e druk 2009)

22. ***Integriteit van de politie. State-of-the-art: wat we weten op basis van Nederlands onderzoek***
L.W.J.C. Huberts & J. Naeyé, Centrum voor Politie- en Veiligheidswetenschappen/ Vrije Universiteit, Amsterdam, 2005

23. ***De sociale organisatie van mensensmokkel***
R. Staring, G. Engbersen, H. Moerland, N. de Lange, D. Verburg, E. Vermeulen & A. Weltevrede; m.m.v. E. Heyl, N. Hoek, L. Jacobs, M. Kanis & W. van Vliet, Erasmus Universiteit Rotterdam: Criminologie – Sociologie – Risbo, 2005

24. ***In elkaars verlengde? Publieke en private speurders in Nederland en België***
U. Rosenthal, L. Schaap J.C. van Riessen, P. Ponsaers & A.H.S. Verhage, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Universiteit Gent, 2005

25. ***De strafrechtelijke rechtshulpverlening van Nederland aan de lidstaten van de Europese Unie. De politieke discussie, het juridische kader, de landelijke organisatie en de feitelijke werking***
C.J.C.F. Fijnaut, A.C. Spapens & D. van Daele, Universiteit van Tilburg, Vakgroep Strafrechtwetenschappen, 2005

26. ***Niet zonder slag of stoot. De geweldsbevoegdheid en doorzettingskracht van de Nederlandse politie***
J. Naeyé, Faculteit der Rechtsgeleerdheid, Vrije Universiteit Amsterdam, 2005

27. ***Preventief fouilleren. Een analyse van het proces en de externe effecten in tien gemeenten***
E.J. van der Torre & H.B. Ferwerda, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Advies- en Onderzoeksgroep Beke, Arnhem, 2005

28. ***Zedenmisdrijven in Nederland. Aangiften- en verdachtenanalyses op basis van HKS-gegevens***
A.Ph. van Wijk, S.R.F. Mali, R.A.R. Bullens, L. Prins & P.P.H.M. Klerks, Politieacademie Onderzoeksgroep, Apeldoorn, Vrije Universiteit Amsterdam. KLPD, 2005

29. ***Groepszedenmisdrijven onder minderjarigen. Een analyse van een Rotterdamse casus***
I. van Leiden & J. Jakobs, Advies- en Onderzoeksgroep Beke, Arnhem, 2005

30. ***Omgaan met conflictsituaties: op zoek naar goede werkwijzen bij de politie***
O. Adang, N. Kop, H.B. Ferwerda, J. Heijnemans, W. Olde Nordkamp, P. de Paauw & K. van Woerkom, Onderzoeksgroep Politieacademie, Apeldoorn/ Advies en Onderzoeksgroep Beke, Arnhem, 2006

31. ***De strategische analyse van harddrugsscenes. Hoofdlijnen voor politie en beleid***
E.J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2006

32a. ***Cijfers en stakeholders. Prestatiesturing en de gevolgen voor de maatschappelijke en politiekbestuurlijke relaties van de politie***
A. van Sluis, L. Cachet, L. de Jong, C. Nieuwenhuyzen & A. Ringeling, Centre for Local Democracy, Erasmus Universiteit Rotterdam, 2006

32b. ***Operationele betrokkenheid. Prestatiesturing en bedrijfsvoering Nederlandse politie***
A.B. Hoogenboom, Nivra-Nyenrode, Breukelen, 2006

32c. ***Op prestaties gericht. Over de gevolgen van prestatiesturing en prestatieconvenanten voor sturing en uitvoering van het politiewerk***
M.P.C.M. Jochoms, F. van der Laan, W. Landman, P.S. Nijmeijer & A. Sey, Politieacademie, Apeldoorn/Twynstra Gudde, Amersfoort/Universiteit van Amsterdam, 2006

33. ***Het nieuwe bedrijfsmatig denken bij de politie. Analyse van een culturele formatie in ontwikkeling***
J. Terpstra & W. Trommel, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente, 2006

34. ***De legitimiteit van de politie onder druk? Beschouwingen over grondslagen en ontwikkelingen van legitimiteit en legitimiteitstoekenning***
Bundel onder redactie van C.D. van der Vijver & G.C.K. Vlek, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente/ Politie & Wetenschap, 2006

35. ***Naar beginselen van behoorlijke politiezorg***
M.J. Dubelaar, E.R. Muller & C.P.M. Cleiren, Faculteit der Rechtsgeleerdheid, Universteit Leiden, 2006

36a. ***Asielmigratie en criminaliteit***
J. de Boom, G. Engbersen & A. Leerkes, Risbo Contractresearch BV/Erasmus Universiteit, Rotterdam, 2006

36b. ***Criminaliteitspatronen en criminele carrières van asielzoekers***
M. Althoff & W.J.M. de Haan, m.m.v. S. Miedema, Vakgroep Strafrecht en Criminologie, Faculteit der Rechtsgeleerdheid, Rijksuniversiteit Groningen, 2006

36c. ***'Ik probeer alleen maar mijn leven te leven'. Uitgeprocedeerde asielzoekers en criminaliteit***
A. Leerkes, Risbo Contractresearch BV/Erasmus Universiteit, Rotterdam; Amsterdamse School voor Sociaal Wetenschappelijk Onderzoek/Universiteit van Amsterdam, Amsterdam, 2006

37. ***Positie en expertise van de allochtone politiemedewerker***
J. Broekhuizen, J. Raven & F.M.H.M. Driessen, Bureau Driessen, Utrecht, 2007

38. ***Lokale politiechefs. Het middenkader van de basispolitiezorg***
E. J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2007

39. ***Niet verschenen***

40. ***Conflict op straat: strijden of mijden? Marokkaanse en Antilliaanse jongeren in interactie met de politie***
N. Kop, Martin Euwema, m.m.v. H.B. Ferwerda, E. Giebels, W. Olde Nordkamp & P. de Paauw, Politieacademie, Apeldoorn, Universiteit Utrecht, 2007

41. ***Opsporing onder druk***
C. Liedenbaum & M. Kruijsen, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

42. ***Symbolen van orde en wanorde. Broken windows policing en de bestrijding van overlast en buurtverval***
B. van Stokkom, Centrum voor Ethiek, Radboud Universiteit Nijmegen, 2008

43. ***Verkeershandhaving: prestaties leveren, problemen aanpakken***
G. Meershoek & M. Krommendijk, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

44. ***De frontlinie van opsporing en handhaving. Stelselmatige bedreigingen door burgers als contrastrategie***
M.J.G. Jacobs, M.Y. Bruinsma & J.W.M.J. van Poppel, IVA Tilburg, 2008

45a. ***'Kracht van meer dan geringe betekenis'. Deel A: Politiegeweld in de basispolitiezorg***
R. Bleijendaal, J. Naeyé, P. Chattellon & G. Drenth, Vrije Universiteit, Amsterdam, 2008

45b. ***'Kracht van meer dan geringe betekenis'. Deel B: Sturing en toetsing van de politiële geweldsbevoegdheid***
G. Drenth, J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45c. ***Agressie en geweld tegen politiemensen. Beledigen, bedreigen, tegenwerken en vechten***
J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45d. ***Belediging en bedreiging van politiemensen***
J. Naeyé, m.m.v. M. Bakker & C. Grijsen, Vrije Universiteit Amsterdam, 2009

45e. ***Uitgangspunten voor politieoptreden in agressie- en geweldssituaties***
J. Naeyé, Vrije Universiteit Amsterdam, 2010

46. ***Wijkagenten en hun dagelijks werk. Een onderzoek naar de uitvoering van gebiedsgebonden politiewerk***
J. Terpstra, 2008

47. ***Bijzonder zijn ze allemaal! Vergelijkend onderzoek naar reguliere en bijzondere opsporing***
W. Faber, A.A.A. van Nunen & C. la Roi, Faber Organisatievernieuwing, Oss, 2009

48. ***Gouden bergen. Een verkennend onderzoek naar Nigeriaanse 419-fraude: achtergronden, daderkenmerken en aanpak***
Y.M.M. Schoenmakers, E. de Vries Robbé & A.Ph. van Wijk, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2009

49. ***Het betwiste politiebestel. Een vergelijkend onderzoek naar de ontwikkeling van het politiebestel in Nederland, België, Denemarken, Duitsland, Engeland & Wales***
A. Cachet, A. van Sluis, Th. Jochoms, A. Sey & A. Ringeling, Erasmus Universiteit Rotterdam/Politieacademie, Apeldoorn/Korps landelijke politiediensten, Driebergen, 2009

50. ***Leven met bedreiging. Achtergronden bij aangiften van bedreiging van burgers***
B. Bieleman, W.J.M. de Haan, J.A. Nijboer & N. Tromp, Intraval & Rijksuniversiteit Groningen, 2010

51a. ***Het publieke belang bij private preventie. Een economische analyse van inbraakpreventiebeleid***
B.A. Vollaard, TILEC/Universiteit van Tilburg, 2009

51b. ***Het effect van langdurige opsluiting van veelplegers op de maatschappelijke veiligheid***
B.A. Vollaard, TILEC/Universiteit van Tilburg, 2010

52. ***Lokale politiek over politie***
T.B.W.M. van der Torre-Eilert, H. Bergsma & M.J. van Duin, met medewerking van R. Eilert, LokaleZaken, Rotterdam, 2010

53a. ***Trainen onder stress. Effecten op de schietvaardigheid van politieambtenaren***
R.R.D. Oudejans, A. Nieuwenhuys & G.P.T. Willemsen, Vrije Universiteit Amsterdam, 2010

53b. ***Schieten of niet schieten? Effecten van stress op schietbeslissingen van politieambtenaren***
A. Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2012

53c. ***Politievaardigheden onder stress. Het optimaliseren van aanhouding en zelfverdediging in de praktijk***
P.G. Renden, A. Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

53d. ***Effectief omgaan met acute stress. Effecten van aanleg en trainingservaring op de schietprestatie onder druk***
A. Landman, A. Nieuwenhuys & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

54. ***Politie en publiek. Een onderzoek naar de communicatievormen tussen burgers en blauw***
H.J.G. Beunders, M.D. Abraham, A.G. van Dijk & A.J.E. van Hoek, DSP-groep, Amsterdam/Erasmus Universiteit, Rotterdam, 2011

55. ***Managing collective violence around public events: an international comparison***
O.M.J. Adang with cooperation from: S.E. Bierman, E.B. Brown, J. Dietermann, C. Putz, M. Schreiber, R. van der Wal, J. Zeitner, Police Science & Research Programme, Apeldoorn, 2011

56. ***Stads- en regioscan in de grootste Brabantse gemeenten. De achtergronden van onveilige GVI-scores***
B.M.W.A. Beke, E.J. van der Torre, M.J. van Duin, COT, Den Haag; LokaleZaken, Rotterdam & Beke Advies, Arnhem, 2011

57. ***De mythe ontrafeld? Wat we weten over een goed politieleiderschap***
W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2011

58. ***Proactief handhaven en gelijk behandelen***
J. Svensson, H. Sollie & S. Saharso, Vakgroep Maatschappelijke Risico's en Veiligheid, Institute of Governance Studies, Universiteit Twente, Enschede, 2011

59a. ***De sterkte van de arm: feiten en mythes***
J.H. Haagsma, T.M. Rumke, I. Smits, E. van der Veer & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

59b. ***Blauw, hier en daar. Onderzoek naar de sterkte van de politie in Nederland, België, Denemarken, Engeland & Wales en Nordrhein-Westfalen***
J.H. Haagsma, I. Smits, H. Waarsing & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

60. ***De nachtdienst 'verlicht'***
M.C.M. Gordijn, Rijksuniversiteit Groningen, 2012

61. ***Opsporing Verzocht. Een quasi-experimentele studie naar de bijdrage van het programma Opsporing Verzocht aan de oplossing van delicten***
J.G. van Erp, F. van Gastel & H.D. Webbink, Erasmus Universiteit, Rotterdam, 2012

62. ***Jeugdige zedendelinquenten en recidive. Een onderzoek bij jeugdige zedendelinquenten naar de voorspellende waarde van psychiatrische stoornissen en psychosociale problemen voor (zeden)recidive***
C. Boonmann, L.M.C. Nauta-Jansen, L.A. 't Hart-Kerkhoffs, Th.A.H. Doreleijers & R.R.J.M. Vermeiren, VUmc De Bascule, Duivendrecht, 2012

63. ***Hoe een angsthaas een jokkebrok herkent***
J. Jolij, Rijksuniversiteit Groningen, 2012

64. ***Politie en sociale media. Van hype naar onderbouwde keuzen***
A. Meijer, S. Grimmelikhuijsen, D. Fictorie, M. Thaens, P. Siep, Universiteit Utrecht, Center for Public Innovation, Rotterdam, 2013

65. ***Wapengebruik. Van inzicht in modus operandi naar een effectieve aanpak***
M.S. de Vries, Universiteit Twente, Enschede, 2013

66. ***Politieverhalen. Een etnografie van een belangrijk aspect van politieculturen***
M.J. van Hulst, Tilburg University, Tilburg, 2013

67. ***Recherchebazen. Een empirisch onderzoek naar justitieel politieleiderschap***
E.J. van der Torre, M.J. van Duin & E. Bervoets, LokaleZaken, Rotterdam, 2013

68. ***Driehoeken: overleg en verhoudingen. Van lokaal tot nationaal***
E.J. van der Torre & T.B.W.M. van der Torre-Eilert, m.m.v. E. Bervoets & D. Keijzer, LokaleZaken, Rotterdam, 2013

69. ***Overvallen vanuit daderperspectief. Situationele aspecten van gewelddadige, niet-gewelddadige en afgeblazen overvallen***
W. Bernasco, M.R. Lindegaard & S. Jacques, NSCR, Amsterdam, 2013

70. ***Geweld tegen de politie. De rol van mentale processen van de politieambtenaar***
L. van Reemst, T. Fischer & B. Zwirs, Erasmus Universiteit, Rotterdam, 2013

71. ***Vertrouwen in de politie: trends en verklaringen***
L. van der Veer, A. van Sluis, S. Van de Walle & A. Ringeling, Erasmus Universiteit, Rotterdam, 2013

72. ***Mobiel banditisme. Oost- en Centraal-Europese rondtrekkende criminele groepen in Nederland***
D. Siegel, i.s.m. R. Koenraadt, D. Lyubenova, N. Sovre & A. Troscianczuk, Universiteit Utrecht, 2013

73. ***De ontwikkeling van de criminaliteit van Rotterdamse autochtone en allochtone jongeren van 12 tot 18 jaar. De rol van achterstanden, ouders, normen en vrienden***
F.M.H.M. Driessen, F. Duursma & J. Broekhuizen, Bureau Driessen, Utrecht, 2014

74. ***Speciaal blauw. Verschijningsvormen en overwegingen van specialisatie en despecialisatie binnen de Nederlandse politieorganisatie***
R.J. Morée, W. Landman & A.C. Bos, Twynstra Gudde, Amersfoort, 2014

75. ***Gevangene van het verleden. Crisissituaties na de terugkeer van zedendelinquenten in de samenleving***
M.H. Boone, H.G. van de Bunt & D. Spiegel, m.m.v. K. van de Ven, Erasmus Universiteit, Rotterdam, Universiteit Utrecht, 2014

76. ***Brandstichters onder vuur. Een empirisch onderzoek naar zaken van brandstichting en hun daders***
L. Dalhuisen & F. Koenraadt, Universiteit Utrecht, 2014

77. ***Van stadswacht naar nieuwe gemeentepolitie? Gemeentelijk toezicht en handhaving in de openbare ruimte***
T. Eikenaar & B. van Stokkom, Radboud Universiteit, Nijmegen, 2014

78. ***Politiemensen over het strafrecht***
J. Kort, M.I. Fedorova & J.B. Terpstra, Radboud Universiteit, Nijmegen, 2014

79. ***Kijken, luisteren, lezen. De invloed van beeld, geluid en schrift op het oordeel over verdachtenverhoren***
M. Malsch, R. Kranendonk, J. de Keijser, H. Elffers, M. Konter & M. de Boer, NSCR, Amsterdam, 2015

80. ***De mentale gesteldheid van de familierechercheur. Een onderzoek naar werkgerelateerde stress en secundaire posttraumatische groei binnen een bijzondere groep politieambtenaren***
L.J.A. Bollen, M.C. Saan, M.J.J. Kunst, B.W.C. Zwirs & K.F. Kuijpers, Universiteit Leiden, 2015

81. ***Na de vrijlating. Een exploratieve studie naar recidive en re-integratie van jihadistische exgedetineerden***
D.J. Weggemans & B.A. de Graaf, Universiteit Leiden, Universiteit Utrecht, 2015

82. ***Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland***
L. Paulissen & J. van Wilsem, Universiteit Leiden, 2015

83. ***Demonstratieve kampementen***
B. Roorda, Rijksuniversiteit Groningen, 2015

84. ***Private ordebewaarders bij betogingen***
B. Roorda, Rijksuniversiteit Groningen, 2015

85. ***Spelen met weerbarstigheid. Belemmerende patronen en doorbrekende handelingsperspectieven bij het ontwikkelen van basisteams***
W. Landman, R. Kouwenhoven & M. Brussen, Twynstra Gudde, Amersfoort, 2015

86. ***'Onnodige' bureaucratie binnen het basispolitiewerk. Onderzoek naar de achtergronden van een hardnekkig verschijnsel***
J. Kort & J.B. Terpstra, Radboud Universiteit Nijmegen, 2015

87. ***Politie en GHB-problematiek op het platteland***
T. Nabben & D.J. Korf, Universiteit van Amsterdam, 2016

88. ***Basisteams in de Nationale Politie. Organisatie, taakuitvoering en gebiedsgebonden werk***
J. Terpstra, I. van Duijneveldt, T. Eikenaar, T. Havinga & B. van Stokkom, Radboud Universiteit Nijmegen, 2016

89. ***Samen of apart. De invloed van overleg tussen agenten bij het opstellen van het proces-verbaal***
A. Vredeveldt, L. Kesteloo & P.J. van Koppen, Vrije Universiteit Amsterdam, 2016

90. ***Overvallen in beeld. Gedrag van daders, slachtoffers en omstanders***
M.R. Lindegaard, W. Bernasco & T. de Vries, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2016

91. ***Boeven vangen. Een onderzoek naar proactief politieoptreden***
W. Landman & L. Kleijer-Kool, Twynstra Gudde, Amersfoort, 2016

92. ***VVC onder de aandacht. Een onderzoek naar ZSM en de gevolgen voor het politiewerk***
R. Salet & J. Terpstra, m.m.v. P. Frielink, Radboud Universiteit Nijmegen, 2017

93. ***De mogelijke meerwaarde van bodycams voor politiewerk. Een internationaal literatuuronderzoek***
S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2017

93A ***Focus. Evaluatie pilot bodycams Politie Eenheid Amsterdam 2017-2018***
S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2019

93b ***Evaluatie bodycams Landelijke Eenheid; Proeftuin bodycams Dienst Infrastructuur 2018***
S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2019

94. ***Criminele families in Noord-Brabant. Een verkenning van generatie-effecten in de georganiseerde misdaad***
H. Moors & T. Spapens, EMMA, Den Haag; Tilburg University, Tilburg, 2017

94a. ***Interveniëren in criminele families***
A. Boer, R. Ceulen, H. Moors, T. Spapens, EMMA/Tilburg University, 2020

95. ***Effectiviteit van het verdachtenverhoor. Een veldstudie naar de relatie tussen verhoortechnieken, de verklaring van verdachten en de aanwezigheid van de advocaat in zware zaken***
W.J. Verhoeven & E. Duinhof, Erasmus Universiteit, Rotterdam, 2017

96. ***Van meerdere markten thuis? Overlap in markten van zware en georganiseerde misdaad en de consequenties voor de opsporing***
T. Spapens, m.m.v. M. Bruinsma, Tilburg University, Tilburg, 2017

97. ***Horen, zien en zwijgen. Opsporing in dorpen en stadsbuurten met een gesloten leefgemeenschap***
E. Bervoets & M. Bruinsma, Bureau Bervoets, Amersfoort, 2017

98. ***Geweld tegen hulpverleners in de psychiatrie. Aard, omvang en aangifte bij de politie***
J.M. Harte, I. van Houwelingen & M.E. van Leeuwen, Vrije Universiteit, Amsterdam, 2017

99. ***Geëiste en opgelegde straffen bij de strafrechtelijke afhandeling van georganiseerde criminaliteit. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit***
C.G. van Wingerde & H.G. van de Bunt, Erasmus School of Law, Rotterdam, 2017

100. ***Doorgroeiers in de misdaad. De criminele carrières en achtergrondkenmerken van jonge daders van een zwaar delict***
V. van Koppen, V. van der Geest & E.R. Kleemans, Vrije Universiteit, Amsterdam, 2017

101. ***Profielen van Nederlandse outlawbikers en Nederlandse outlawbikerclubs***
A. Blokland, W. van der Leest & M. Soudijn (m.m.v. E. Kleinheerenbrink & I. van Die), Leiden Law School, Leiden, 2017

102. ***Verdachten van terrorisme in beeld. Achtergrondkenmerken, 'triggers' en eerdere politiecontacten***
F. Thijs, E. Rodermond & F. Weerman, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2018

103. ***Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld***
W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.Ph. Stol, NHL Stenden Hogeschool, Leeuwarden; Rijksuniversiteit Groningen, Groningen, 2018

104. ***Een bittere pil. Het fenomeen en de aanpak van illegale medicijnenhandel***
I. van Leiden, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem, 2018

105. ***Vastzitten zonder straf. Over inverzekeringstellingen en schadevergoedingen op basis van artikel 89 Sv***
P. Kruize & P. Gruter, Bureau Ateno, Amsterdam, 2018

106. ***'Ik hou het hier wel uit, hoor'. Mentale weerbaarheid binnen de districtsrecherche***
H. Sollie, Twynstra Gudde, Amersfoort, 2018

107. ***Bestuurlijke bevoegdheden, politie en de lokale aanpak van onveiligheid***
R. Salet & H. Sackers, Radboud Universiteit, Nijmegen, 2019

108. ***Politie en actief burgerschap: een veilig verbond? Een onderzoek naar samenwerking, controle en (neven)effecten***
V. Lub & T. de Leeuw, m.m.v. A.S. Leerkes & R.J. Kleinhans, Bureau voor Sociale Argumentatie, Rotterdam; Erasmus Universiteit, Rotterdam; Bureau voor Maatschappij, Veiligheid & Deviantie, Rotterdam, 2019

109. ***Wijkagenten en veranderingen in hun dagelijks werk. Verslag van een onderzoek***
J. Terpstra, m.m.v. A. Evers, Radboud Universiteit, Nijmegen, 2019

110. ***Naar een efficiëntere noodhulp? Een verkennend actieonderzoek***
A. Scholtens & I. Helsloot, m.m.v. S. Kraaijenbrink, J. Vlagsma, M. Jürgens, D. Mouris & M. Eising, Crisislab, Renswoude, 2019

111. ***Bestrijding van Outlaw Motorcycle Gangs. Een rechtsvergelijkende studie naar de aanpak van onrechtmatige organisaties in rechtsstatelijk perspectief.***
J. Koornstra, B. Roorda, M. Vols & J.G. Brouwer, Rijksuniversiteit Groningen, 2019

112. ***Politiestraatgezag en (on)gehoorzaam burgergedrag***
A. Scholtens, M. Helsloot, I. Helsloot, Crisislab, Renswoude, 2019

113. ***Verkeershandhaving op Nederlandse autosnelwegen; Evaluatie van de werkwijze van het Team EVT, de effecten en de acceptatie van politiecontroles***
Ch. Goldenbeld, A. Stelling-Kończak, S. van der Kint, SWOV, Den Haag, 2019

114. ***Virtual reality als onderzoeksmethode om inbrekers te doorgronden***
I. van Sintemaartensdijk, J.L. van Gelder, P.A.M. van Lange, M. Otte, J.W. van Prooijen, Vrije Universiteit Amsterdam, 2019

115. ***Wanneer blaffende honden bijten. Een vergelijking tussen fataal en niet-fataal huiselijk geweld***
P. Aarten, C. Boelema Robertus, L. Alink, M. Liem, Universiteit Leiden, 2020

116. ***Kijk naar het systeem. Begrijpen en beïnvloeden van opsporingspraktijken***
W. Landman, R. Kouwenhoven, M. Brussen, Twynstra Gudde, Amersfoort, 2020

117 ***Verbeelding in de verhoorkamer. De invloed van het gebruik van beeldmateriaal in het verhoor op verhoortechnieken en proceshouding***
W.J. Verhoeven, G. Vanderveen, L. van Dillen, S. Kruit, Erasmus Universiteit, Universiteit Leiden, 2020

118 ***Met gepast geweld. Politiegeweld in Nederland in 2016***
M. Kuin, F. Kriek, J. Timmer, m.m.v. Y. Bleeker en E. Verbeek, Regioplan, Amsterdam en Vrije Universiteit Amsterdam, 2020

119 ***De rol van bodycambeelden in de opsporing en bewijsvoering***
A. Vredeveldt, L. Kesteloo, A. Hildebrandt, Vrije Universiteit Amsterdam, 2020

120 ***Slachtoffer van onlinecriminaliteit, wat nu?***
S.G.A. van de Weijer, E.R. Leukfeldt, S. van der Zee, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2020

121 ***Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right***
J.A.M. Schiks, M.S. van 't Hoff-de Goede, E.R. Leukfeldt. De Haagse Hogeschool, Centre of Expertise Cybersecurity, Den Haag; Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2021

122 ***Criminaliteit en huiselijk geweld: twee kanten van dezelfde medaille? De relatie tussen criminaliteit en huiselijk geweld***
S. van Deuren, J. Kroese, M. van Dijk, V. Eichelsheim, A. Blokland, S. van de Weijer. Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2021

123 ***Oververtegenwoordiging verder ontcijferd. Een kwantitatief onderzoek naar sociale verschillen in verdenkingskans en zelfgerapporteerd crimineel gedrag onder jongeren in Nederland***
W. Bezemer, A. Leerkes. Erasmus Universiteit, Rotterdam, 2021

124 ***Gebiedsgebonden politiewerk in ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving***
J. Terpstra, R. Salet, I. van Duijneveldt, T. Havinga, Radboud Universiteit 2021

125 ***Slimme(re) opsporing, Een verslag van de ontwikkeling en pogingen tot implementatie van een handreiking voor efficiënte opsporing door de politie***
I. Helsloot, P. van Lochem, C. Kijne, Crisislab, Renswoude 2022