Publiek toegankelijke bronnen, ontoegankelijk voor opsporingsambtenaren ten behoeve van intelligence?

Suggesties ter verbetering van het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen

Vrije Universiteit Amsterdam, Faculteit der Rechtsgeleerdheid
Masterscriptie Rechtsgeleerdheid, afstudeerrichting Internet, Intellectuele eigendom en ICT
Begeleidster: dr. mr. A. de Hingh

Naam: Sigrid van Holland
Inleverdatum: 16 augustus 2023
Aantal woorden: 19.388

VU UNIVERSITY AMSTERDAM

Voorwoord

Voor u ligt de masterscriptie 'Publiek toegankelijke bronnen, ontoegankelijk voor opsporingsambtenaren ten behoeve van intelligence? Suggesties ter verbetering van het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen'. Deze scriptie is geschreven in het kader van mijn afstuderen aan de master Rechtsgeleerdheid, afstudeerrichting Internet, Intellectuele eigendom en ICT aan de Vrije Universiteit te Amsterdam.

Het onderzoek strekt zich tot verbetering van het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence. De keuze voor dit onderwerp heb ik te danken aan mijn stageperiode bij Team Xplore (een samenwerking tussen het FP en de FIOD). Hier heb ik geleerd dat het gebruik van data (waaronder publiek toegankelijke bronnen) en intelligence een actueel onderwerp is met daarin de nodige vraagstukken. Tijdens deze stage heb ik de kans gekregen om hierover mee te denken en bij te dragen aan de uitvoering in de praktijk.

Graag maak ik van de gelegenheid gebruik om een woord van dank uit te spreken. Ten eerste wil ik graag mijn begeleidster, Anne de Hingh, bedanken voor de begeleiding. Daarnaast wil ik mijn collega's bij Team Xplore, met in het bijzonder Tex Dissen, bedanken voor de leerzame tijd. Ook wil ik mijn dank uitspreken aan de respondenten die de tijd hebben genomen om deel te nemen aan de interviews. Hun inzichten, expertise en ervaringen hebben bijgedragen aan de totstandkoming van deze scriptie.

Ik wens u veel leesplezier toe.

Sigrid van Holland

Amsterdam, 20 juli 2023

Inhoudsopgave

Lijst van gebruikte afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMvB	Algemene maatregel van bestuur
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BOB	Bijzondere opsporingsbevoegdheden
CTIVD	Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
MvT	Memorie van toelichting
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
OM	Openbaar Ministerie
PIA	Privacy Impact Assessment
Pw	Politiewet
TCI	Team Criminele Inlichtingen
TIB	Toetsingscommissie Inzet Bevoegdheden
TOOI	Team Openbare Orde Inlichtingen
Wet BOD	Wet op de bijzondere opsporingsdiensten
Wiv	Wet op de inlichtingen- en veiligheidsdiensten 2017
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wpg	Wet politiegegevens
WvSv	Wetboek van Strafvordering

Hoofdstuk 1 – Inleiding

1.1 Aanleiding

Het aantal mensen dat informatie op het internet publiceert of waarover informatie op het internet wordt gepubliceerd is de afgelopen jaren sterk toegenomen. Het internet biedt hierdoor een schat aan informatie en aangezien het internet niet makkelijk vergeet, zal dit in de toekomst alleen maar meer worden.[1] Een groot gedeelte van de informatie op het internet is publiek toegankelijk, wat inhoudt dat deze informatie voor iedereen beschikbaar is. De afgelopen tien jaar zijn opsporingsinstanties dit ook steeds meer gaan beseffen. Het verzamelen van gegevens uit publiek toegankelijke bronnen op het internet is snel, efficiënt en laag in kosten.[2] De politie maakt tegenwoordig dan ook uitvoerig gebruik van online gegevensvergaring ten behoeve van intelligence en opsporing. Zo erkent ook Reinder Doeleman, programmadirecteur Intelligence binnen de politie: "Onlinegegevens verzamelen is nu al een belangrijk onderdeel van de politietaak en dat zal alleen maar toenemen.".[3] De politie beweegt dus mee met de digitalisering van de samenleving.

Dit geldt daarentegen niet voor de wetgever. Reinder Doeleman vervolgt: "Er wordt veel van ons gevraagd en daarbij hebben we een helder (juridisch) kader nodig. We werken nu veelal op basis van het taakstellend artikel 3 van de Politiewet. Die is echter heel algemeen en niet gericht op online informatievergaring".[4] Hoewel opsporingsambtenaren steeds meer onlinegegevens uit publiek toegankelijke bronnen verzamelen, ontbreekt dus een specifieke juridische grondslag. Wetgeving die voor de fysieke wereld was bedoeld, wordt nu bij gebrek aan beter ook toegepast op de digitale wereld.[5]

Momenteel vindt online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van een opsporingsonderzoek plaats op grond van de algemeen taakstellende bevoegdheid uit artikel 3 Politiewet (hierna: Pw), voor zover sprake is van een geringe inbreuk op de privacy. Indien een meer dan geringe inbreuk op de privacy plaatsvindt, wordt gebruik gemaakt van twee bijzondere opsporingsbevoegdheden (hierna: BOB) die hier eigenlijk niet voor zijn bedoeld: stelselmatige informatie-inwinning of stelselmatige observatie.[6] Dat deze BOB-middelen niet goed aansluiten op online gegevensvergaring uit publiek toegankelijke bronnen, erkent ook de moderniseringswetgever. Het gemoderniseerde Wetboek van Strafvordering (hierna: WvSv) bevat dan ook een nieuw BOB-middel in artikel 2.8.8, dat specifiek ziet op het stelselmatig overnemen van gegevens uit publiek toegankelijke internetbronnen.[7] Deze nieuwe regeling treedt waarschijnlijk in 2026 in werking.

---

[1] Rapport Commissie-Koops 2018, p. 12.
[2] Ramwell, Day & Gibson 2016, p. 198.
[3] 'Onduidelijkheid over online gegevensvergaring', politie.nl 27 september 2022, geraadpleegd op 13 maart 2023.
[4] 'Onduidelijkheid over online gegevensvergaring', politie.nl 27 september 2022, geraadpleegd op 13 maart 2023.
[5] Groothuis & Landman 2022, p. 21.
[6] Respectievelijk art. 126j WvSv en art. 126g WvSv.
[7] Klaar 2022, p. 2.

Online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van intelligence kan echter alleen plaatsvinden op grond van de algemeen taakstellende bevoegdheid uit artikel 3 Pw. Dit komt doordat BOB-middelen alleen ingezet mogen worden ten behoeve van opsporing en vervolging en niet louter met het doel om een betere informatiepositie te verkrijgen.[8] Bij online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van intelligence ligt de focus juist op het versterken van de informatiepositie om zo inzicht te verkrijgen in wat er momenteel gebeurt en kan gebeuren. Zo worden bijvoorbeeld trends en ontwikkelingen ten aanzien van specifieke veiligheidsthema's gemonitord, zodat er informatierapporten of veiligheidsbeelden gemaakt kunnen worden. Dit dient als sturingsinformatie en is dus niet gericht op opsporing en vervolging.[9] Het nieuwe artikel in het gemoderniseerde WvSv biedt dan ook geen uitkomst voor online gegevensvergaring in het kader van intelligence. De politie kent geen bevoegdheid om opsporingsmiddelen in te zetten puur ter verbetering van de informatiepositie, zoals inlichtingen- en veiligheidsdiensten die wel kennen.[10]

Op dit moment heerst er veel onduidelijkheid over wat mag op grond van artikel 3 Pw en waar de grens van een geringe inbreuk ligt.[11] Vanwege de groeiende praktijk van online gegevensvergaring uit publiek toegankelijke bronnen lijkt een duidelijk wettelijk kader dat ook specifiek ziet op intelligencedoeleinden daarom wenselijk. Onder andere de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (hierna: Commissie-Koops) adviseerde de wetgever om ook voor andere taken van de politie die niet onder strafvordering vallen, waaronder dus intelligence, een regeling te treffen voor het vergaren van persoonsgegevens uit publiek toegankelijke bronnen. Hierbij zou zo veel mogelijk moeten worden aangesloten bij de terminologie en voorwaarden uit de strafvorderlijke regeling. Daarnaast adviseerde de Commissie-Koops om met beide regelingen niet te wachten tot de inwerkingtreding in 2026, maar om dit zo snel mogelijk tot stand te brengen.[12]

Aangezien dit tot op heden nog niet is gebeurd, is het in navolging van dit advies relevant om te onderzoeken in welk opzicht het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence verbeterd zou moeten worden. Dit zal onderzocht worden aan de hand van de strafvorderlijke regelingen die gelden bij het opsporingsonderzoek, zoals geadviseerd door de Commissie-Koops. Daarnaast zal gekeken worden naar het juridisch kader dat geldt voor de inlichtingen- en veiligheidsdiensten, omdat intelligence daar ook tot de doelen behoort. Zowel het (gemoderniseerde) WvSv als de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Hierna: Wiv) bevatten bovendien artikelen die specifiek zien op het gebruik van publiek toegankelijke bronnen.

[8] Van den Eeden e.a. 2021, p 85-86.
[9] Groothuis & Landman 2022, p. 44.
[10] Van den Eeden e.a. 2021, p 85.
[11] Groothuis & Landman 2022, p. 134; Oerlemans 2018, p. 4.
[12] Rapport Commissie-Koops 2018, p. 151; Groothuis & Landman 2022, p. 134.

Dit onderzoek is wetenschappelijk relevant, omdat het probeert bij te dragen aan de al bestaande kennis op het gebied van publiek toegankelijke bronnen door specifiek in te zoomen op het gebruik door opsporingsambtenaren in het kader van intelligence. Daarnaast is het ook maatschappelijk relevant, omdat het zowel voor opsporingsdiensten als voor burgers van belang is om te weten waar de grenzen van de bevoegdheden liggen. Een verbeterd juridisch kader kan bijdragen aan een betere bescherming van de privacy, terwijl opsporingsambtenaren effectief hun werk kunnen blijven uitvoeren. Tot slot is dit onderzoek juridisch relevant, omdat getracht wordt het huidige juridische kader te verbeteren. Het komt de rechtszekerheid ten goede als ook de wet meebeweegt met de digitalisering.

1.2 Onderzoeksvraag en deelvragen

Het doel van dit onderzoek is dus om inzicht te verkrijgen in het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen om vervolgens suggesties te geven ter verbetering van dit juridisch kader op het gebied van intelligence. De onderzoeksvraag van deze masterscriptie luidt dan ook als volgt:

> *In welk opzicht zou het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence moeten worden verbeterd?*

Om een antwoord te formuleren op de onderzoeksvraag zijn de volgende deelvragen uitgewerkt:

1. Wat is het huidige juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence?
2. Wat zijn de knelpunten van het huidige juridische kader?
3. Hoe is online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek geregeld?
4. Hoe is online gegevensvergaring uit publiek toegankelijke bronnen voor de inlichtingen- en veiligheidsdiensten geregeld?
5. In welk opzicht zou, aan de hand van de regelingen in het (gemoderniseerde) WvSv en de Wiv, het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence moeten worden verbeterd?

1.3 Terminologie

Zowel in de praktijk als in de literatuur worden verschillende termen en/of reikwijdtes gehanteerd voor kernbegrippen uit de onderzoeksvraag. Om duidelijkheid te scheppen en verwarring te voorkomen, wordt hieronder kort toegelicht wat in deze masterscriptie wordt verstaan onder: gegevensvergaring, publiek toegankelijke bronnen en intelligence.

Gegevensvergaring

Het is van belang om het onderscheid tussen gegevensvergaring en gegevensverwerking helder te hebben. Gegevensvergaring ziet alleen op het verzamelen van de gegevens en wordt vooral genormeerd in de Pw en het (gemoderniseerde) WvSv. Gegevensverwerking is breder en ziet naast het verzamelen van gegevens onder andere op het bewaren, wijzigen, structureren, combineren, gebruiken en verspreiden van gegevens.[13] De reeds vergaarde gegevens worden hier dus ook verder gebruikt. Dit is grotendeels genormeerd in de Wet politiegegevens (hierna: Wpg) en de Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg).[14]

In dit onderzoek wordt alleen ingegaan op gegevensvergaring. De normering van gegevensvergaring hangt echter sterk samen met de normering van gegevensverwerking. Wanneer het mogelijk is om gegevens ruimer en indringender te verwerken, wordt het belangrijker om de gegevensvergaring te normeren (er dient dan rekening gehouden te worden met indringender gevolgen van ruimer gebruik). Het omgekeerde geldt ook: wanneer er strikte regels zijn voor het verwerken van de gegevens, kan dat een ruimere bevoegdheid voor het vergaren van de gegevens rechtvaardigen.[15] De twee kunnen dus niet geheel los van elkaar worden beschouwd.

Publiek toegankelijke bronnen

In de praktijk worden publiek toegankelijke bronnen vaak aangeduid als ‘open bronnen’ of ‘open source(s)’. Het gebruik van deze termen geeft echter de indruk dat deze bronnen vrij of onbeperkt te gebruiken zijn, wat niet terecht is. Uit het huidig juridisch kader blijkt immers dat de politie bevoegdheden nodig heeft om deze gegevens te vergaren en te verwerken.[16] Daarnaast zouden deze termen de suggestie kunnen wekken dat het bronnen betreft die open te raadplegen zijn, zonder bijvoorbeeld in te loggen. Dit is eveneens onjuist. Om deze redenen adviseren het Openbaar Ministerie (hierna: OM), de politie, de Nederlandse Orde van Advocaten en de Commissie-Koops om de term publiek toegankelijke bronnen te gebruiken. Deze term is passender, doordat het ziet op de feitelijke toegankelijkheid of beschikbaarheid van de gegevens en niet op het regelvrije gebruik van de gegevens. Bovendien sluit deze term aan bij de gebruikte terminologie in het Cybercrime-Verdrag.[17] Daar wordt als hoofdterm ‘publicly available’ gebruikt en niet ‘open source’.[18] In dit onderzoek wordt dan ook de term publiek toegankelijke bronnen gehanteerd.

Er is sprake van een publiek toegankelijke bron indien er geen effectieve toegangscontrole plaatsvindt en toegang kan worden verkregen zonder de server binnen te dringen.[19] Hiertoe behoren ook bronnen waarvoor je moet betalen (zoals de Kamer van

[13] Dit blijkt o.a. uit art. 4 lid 2 AVG en art. 1 sub c Wpg.
[14] Rapport Commissie-Koops 2018, p. 24.
[15] Rapport Commissie-Koops 2018, p. 24-25.
[16] Rapport Commissie-Koops 2018, p. 152.
[17] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 680-681; Rapport Commissie-Koops 2018, p. 152-153.
[18] Dit blijkt uit art. 32 sub a Cybercrime-Verdrag en de aanvullende Guidance Note.
[19] Klaar 2022, p. 3; *Kamerstukken II* 2022/23, 36327, nr. 3, p. 681-682; Rapport Commissie-Koops 2018, p. 153-155.

Koophandel), dient te registreren (zoals Facebook) of software moet downloaden (zoals de Tor-browser). Doordat iedereen in staat is om dit te doen, is er geen sprake van selectie. In het geval toegang pas kan worden verkregen na acceptatie van een vriendschapsverzoek, betreft het daarentegen wel een afgeschermde bron. Hier vindt immers selectie plaats. De gegevens zijn niet publiek toegankelijk, maar alleen voor vrienden. Een bron is dus publiek toegankelijk of afgeschermd, er bestaat geen 'tussencategorie'.[20]

Intelligence

Binnen de politie stamt het begrip intelligence af van het concept 'intelligence-led policing', wat in het Nederlands vertaald is naar intelligencegestuurd politiewerk.[21] Intelligence is hierbij door de Strategische Beleidsgroep Intelligence gedefinieerd als: "geanalyseerde informatie en kennis op grond waarvan beslissingen over de uitvoering van de politietaak worden genomen".[22] Dit wordt ook wel sturingsinformatie genoemd. Het is niet gericht op het verzamelen van bewijs voor een opsporingsonderzoek, want er is (nog) geen sprake van opsporing in de zin van artikel 132a WvSv. Het doel van intelligence is dus niet het nemen van strafvorderlijke beslissingen, maar het opbouwen van een informatiepositie.[23]

1.4 Onderzoeksmethoden

In deze masterscriptie is gebruik gemaakt van twee onderzoeksmethoden. Ten eerste is juridisch dogmatisch onderzoek verricht dat voornamelijk bestaat uit literatuuronderzoek.[24] Aan de hand hiervan wordt getracht het huidige juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen duidelijk in kaart te brengen. Daarnaast is als aanvulling een kleinschalig empirisch onderzoek verricht, waarbij zes semigestructureerde interviews zijn afgenomen, waarvan één dubbelinterview.[25] Zo wordt getracht te achterhalen hoe vanuit de praktijk tegen dit juridisch kader wordt aangekeken. Hier kunnen mogelijk nieuwe knelpunten en/of verbeterpunten aan het licht komen, die nog niet eerder bekend waren.

Om de eerste deelvraag te beantwoorden is onderzoek verricht naar de huidige wet- en regelgeving, jurisprudentie en literatuur over het gebruik van publiek toegankelijke bronnen door opsporingsambtenaren voor intelligencedoeleinden. Ter beantwoording van de tweede deelvraag is ook gekeken naar de huidige wet- en regelgeving, jurisprudentie en literatuur over het gebruik van publiek toegankelijke bronnen door opsporingsambtenaren voor intelligencedoeleinden. Daarnaast is aan de hand van semigestructureerde interviews informatie verzameld over de praktijkervaringen op dit gebied van OSINT-specialisten, juristen, een beleidsadviseur en een informatieofficier. Ter beantwoording van de derde deelvraag is gekeken naar de huidige en toekomstige wet- en regelgeving, jurisprudentie en

[20] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 681-682; Rapport Commissie-Koops 2018, p. 153-155.
[21] Kop & Klerks 2009, p. 9-10.
[22] SGBI 2008.
[23] Groothuis & Landman 2022, p. 44 en 61.
[24] Van Dijk, Snel & Van Golen 2018, p. 84.
[25] Van Dijk, Snel & Van Golen 2018, p. 90.

literatuur over het gebruik van publiek toegankelijke bronnen voor opsporingsdoeleinden. Hierbij is voornamelijk gebruik gemaakt van het (gemoderniseerde) WvSv en wetenschappelijke artikelen. Ter beantwoording van de vierde deelvraag is gekeken naar de huidige wet- en regelgeving, jurisprudentie en literatuur over het gebruik van publiek toegankelijke bronnen door de inlichtingen- en veiligheidsdiensten. Hierbij zijn vooral de Wiv en wetenschappelijke artikelen bestudeerd. Tot slot wordt de vijfde deelvraag beantwoord door de antwoorden van de eerste vier deelvragen in samenhang te bezien. Daarnaast worden hier ook de suggesties van de respondenten meegenomen. De beantwoording van deze deelvraag zal uiteindelijk leiden tot beantwoording van de onderzoeksvraag.

1.5 Leeswijzer

Het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen bestaat enerzijds uit wetgeving die ziet op de bescherming van de burgers en anderzijds uit wetgeving die ziet op de bevoegdheden van de opsporingsdiensten.[26] Dit geldt zowel voor online gegevensvergaring in het kader van intelligence als in het kader opsporing. Daarnaast geldt dit ook voor online gegevensvergaring door de inlichtingen- en veiligheidsdiensten. De wetgeving die ziet op de bevoegdheden verschilt per dienst en doel, maar de wetgeving die ziet op de bescherming van de burgers is hetzelfde en betreft in alle gevallen het recht op privacy. Zodoende begint deze masterscriptie met een algemeen hoofdstuk over het recht op privacy (hoofdstuk 2). Hier worden de eisen en waarborgen die van belang zijn bij online gegevensvergaring uit publiek toegankelijke bronnen uiteengezet.

De overige hoofdstukken corresponderen met de deelvragen. Dit betekent dat in hoofdstuk 3 wordt ingegaan op het huidige juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence. In Hoofdstuk 4 worden vervolgens de knelpunten van het huidige juridische kader behandeld. In hoofdstuk 5 wordt uiteengezet hoe online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek is geregeld. Naast dat hier wordt ingegaan op de huidige wet- en regelgeving, wordt ook het gemoderniseerde WvSv besproken. In hoofdstuk 6 wordt beschreven hoe online gegevensvergaring uit publiek toegankelijke bronnen voor de inlichtingen- en veiligheidsdiensten is geregeld. Aan de hand van de knelpunten en de in hoofdstuk 5 en 6 behandelde wet- en regelgeving wordt vervolgens in hoofdstuk 7 gekeken in welk opzicht het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence verbeterd zou moeten worden. Tot slot zal in hoofdstuk 8 de conclusie volgen.

[26] Groothuis & Landman 2022, p. 22.

Hoofdstuk 2 – Recht op privacy

2.1 Inleiding

In dit hoofdstuk wordt ingegaan op het recht op privacy. Wanneer een opsporingsambtenaar online gegevens vergaart uit publiek toegankelijke bronnen, kan worden gesproken van een inmenging in de privacy of het privéleven van een burger.[27] Het recht op privacy is een grondrecht dat burgers beschermt tegen een onrechtvaardige inmenging door de overheid en is vastgelegd in verschillende verdragen en wetten.[28] Deze masterscriptie beperkt zich tot het recht op privacy uit artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM). Hiervoor is gekozen vanwege de leidende rol die dit artikel heeft gekregen met betrekking tot het recht op privacy en de regulering van opsporingsbevoegdheden.[29]

Het doel van dit hoofdstuk is om de eisen en waarborgen die van belang zijn bij wetgeving over online gegevensvergaring uit publiek toegankelijke bronnen in kaart te brengen. Dit is van belang om de wetgeving in de volgende hoofdstukken in context te plaatsen. Daarnaast dient dit hoofdstuk als normatief referentiekader waarbinnen het verbeterde juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence moet worden ontwikkeld.

Eerst wordt ingegaan op artikel 8 EVRM en vervolgens wordt de relevante rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) ten aanzien van dit artikel en online gegevensvergaring besproken. Aangezien het EHRM veel aandacht besteedt aan het vereiste 'voorzien bij wet' om een inbreuk op artikel 8 EVRM te rechtvaardigen, zal dit in een afzonderlijke paragraaf worden behandeld. Tot slot volgt een korte tussenconclusie van dit hoofdstuk.

2.2 Artikel 8 EVRM

Het doel van artikel 8 EVRM is bescherming van het individu tegen een onrechtvaardige inmenging door de overheid in het privéleven en is in het Nederlands als volgt gedefinieerd:

> "1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."

[27] Groothuis & Landman 2022 p, 22.
[28] o.a. in art. 10 t/m 13 Gw; art. 12 UVRM; art. 8 EVRM; art. 7 en 8 Handvest Grondrechten EU.
[29] Rapport Commissie-Koops 2018, p. 34; Groothuis 2019, p. 23; Fedorova e.a. 2022, p. 35.

Het eerste lid waarborgt het recht op privacy. Het tweede lid geeft aan in welke gevallen een inbreuk op dit recht mag worden gemaakt en welke waarborgen hierbij gelden.[30] Hieruit blijkt dat het recht op privacy geen absoluut recht is. Een inbreuk op artikel 8 EVRM is gerechtvaardigd indien aan de drie cumulatieve vereisten uit het tweede lid is voldaan: de inbreuk moet (1) bij wet voorzien zijn, (2) een legitiem doel dienen en (3) noodzakelijk zijn in een democratische samenleving. Het tweede lid geeft een limitatieve opsomming van de legitieme doelen die een inbreuk kunnen rechtvaardigen.[31] De vereisten zijn verder uitgewerkt in de jurisprudentie van het EHRM en zullen in de volgende paragraaf besproken worden.

2.3 Rechtspraak EHRM

Het EHRM heeft zich nog niet specifiek uitgelaten over online gegevensvergaring uit publiek toegankelijke bronnen. Wel heeft het EHRM geoordeeld over offline gegevensvergaring uit publiek toegankelijke bronnen en over heimelijke methoden om gegevens te verzamelen in het algemeen. Wanneer overheidsinstanties heimelijke methoden gebruiken om informatie over mensen te verzamelen, spreekt het EHRM van 'geheime surveillance'. Hiermee wordt niet alleen surveillance bedoeld zoals wij dat in Nederlandse terminologie kennen, namelijk de meer algemene gegevensverzameling in het kader van openbare ordehandhaving, maar ook de meer gerichte gegevensverzameling ten behoeve van opsporing in het kader van de strafrechtelijke handhaving. Het EHRM maakt dus geen onderscheid tussen surveillance en opsporing en wijkt hiermee af van de Nederlandse terminologie.[32]

Het EHRM heeft zich over verschillende geheime surveillance methoden uitgesproken. Het EHRM heeft een vast toetsingskader en toetst zo per geval of sprake is van een inbreuk op artikel 8 EVRM en of deze inbreuk gerechtvaardigd is. Het EHRM heeft zo nader invulling gegeven aan de afbakening van artikel 8 EVRM evenals aan de eisen en waarborgen die hieruit voortvloeien.[33] Normaliter is de jurisprudentie van het EHRM casuïstisch van aard, maar de rechtspraak in het kader van geheime surveillance heeft een abstracter karakter. Meestal kunnen alleen slachtoffers van een vermeende verdragsschending klagen bij het EHRM. Bij de inzet van geheime surveillance methoden is slachtofferschap echter moeilijk aan te tonen vanwege het heimelijke karakter. Daarom is het in het kader van geheime surveillance niet alleen mogelijk om over de toepassing van een heimelijke methode in een concreet geval te klagen, maar ook over de wetgeving betreffende een methode. De wetgeving is immers niet heimelijk. Daarnaast abstraheert het EHRM bij klachten die wel gaan over de inzet van geheime surveillance methoden ook uitdrukkelijk van de omstandigheden van een concreet geval. Alles bij elkaar genomen, heeft dit gaandeweg geleid tot steeds algemenere principes over de inzet van geheime surveillance methoden.[34]

[30] De Vocht, in: T&C Sv, art 8 EVRM, aant. 1 (online, bijgewerkt 1 januari 2023).
[31] De Vocht, in: T&C Sv, art 8 EVRM, aant. 5 (online, bijgewerkt 1 januari 2023).
[32] Eskens, Van Daalen & Van Eijk 2016, p. 10.
[33] Fedorova e.a. 2022, p. 54.
[34] Eskens, Van Daalen & Van Eijk 2016, p. 11-12; Fedorova e.a. 2022, p. 54.

Wanneer burgers zich beroepen op een schending van artikel 8 EVRM, toetst het EVRM eerst of er sprake is van een inbreuk op het recht op privacy, zoals omschreven in het eerste lid. Het begrip privéleven wordt door het EHRM breed uitgelegd en omvat ook andere aspecten.[35] Een belangrijke uitspraak van het EHRM in het kader van dit onderzoek is Rotaru tegen Roemenië. In deze zaak oordeelde het EHRM dat het heimelijk verzamelen en opslaan van persoonsgegevens binnen het bereik van artikel 8 EVRM kan vallen. Bovendien bepaalde het EHRM in deze zaak dat publiek toegankelijke informatie eveneens onder de reikwijdte van dit artikel kan vallen.[36] Hierbij wordt een onderscheid gemaakt tussen gegevens uit publiek toegankelijke bronnen en afgeschermde bronnen. Het vergaren van gegevens uit afgeschermde bronnen impliceert altijd een inbreuk op artikel 8 EVRM, terwijl gegevensvergaring uit publiek toegankelijke bronnen niet altijd een schending van dit artikel oplevert. Er geldt dus geen absolute regel. Of sprake is van een inbreuk op artikel 8 EVRM hangt af van de omstandigheden van het geval.[37]

Bij de beoordeling of een inbreuk onder het toepassingsbereik van artikel 8 EVRM valt, let het EHRM op een drietal aanknopingspunten: het privacygevoelige karakter van de gegevens, de opslag van de gegevens en de manier waarop de gegevens zijn vergaard.[38] Hierbij kan, zeker in het geval van publiek toegankelijke bronnen, de 'reasonable expectation of privacy' een belangrijke, maar niet noodzakelijkerwijs doorslaggevende factor zijn.[39] De reasonable expectation of privacy gaat over de vraag of er bij de betrokkene een redelijke privacy verwachting bestond. Indien de betrokkene vooraf redelijkerwijs kon verwachten hoe de overheid zou kunnen handelen, heeft hij impliciet met dit overheidshandelen ingestemd door toch bepaald gedrag te vertonen.[40] Beargumenteerd zou kunnen worden dat de reasonable expectation of privacy van publiek toegankelijke bronnen lager is. De reasonable expectation of privacy kan overigens ook een rol spelen bij de vraag of een privacyinbreuk gerechtvaardigd is.

Indien sprake is van een inbreuk op artikel 8 EVRM, toetst het EHRM of deze inbreuk gerechtvaardigd is aan de hand van de vereisten uit het tweede lid. Het EHRM kijkt dus of de inbreuk (1) bij wet is voorzien, (2) een legitiem doel dient en (3) noodzakelijk is in een democratische samenleving.[41] Bij een toetsing in het kader van geheime surveillance besteed het EHRM vooral aandacht aan het eerste vereiste. Aan dit vereiste worden de meeste eisen en waarborgen gesteld en zal daarom worden besproken in de volgende paragraaf. Aan het tweede vereiste, of de inbreuk een legitiem doel dient, wordt doorgaans snel voldaan. De belangen zijn in het tweede lid ruim omschreven, waardoor het EHRM niet snel zal oordelen

[35] De Vocht, in: T&C Sv, art 8 EVRM, aant. 1 (online, bijgewerkt 1 januari 2023).
[36] EHRM 4 mei 2000, nr. 28341/95 (*Rotaru t. Roemenië*), par. 43.
[37] Veen 2019, p. 398.
[38] Kranenborg 2007, p. 119-121.
[39] EHRM 25 september 2001, nr. 44787/98 (*P.G en J.H. t. Verenigd Koninkrijk*), par. 57; Van Toor 2017, par III.6.2.2; De Vocht, in: T&C Sv, art 8 EVRM, aant. 3 (online, bijgewerkt 1 januari 2023).
[40] Kranenborg 2007, p. 122.
[41] De Vocht, in: T&C Sv, art 8 EVRM, aant. 1 (online, bijgewerkt 1 januari 2023).

dat hier niet aan is voldaan.[42] Bij het derde vereiste wordt een belangenafweging gemaakt tussen het individuele recht op privacy en het beoogde doel of het publieke belang. Deze belangenafweging maken de lidstaten zelf, zij hebben een zekere beoordelingsvrijheid.[43] De belangenafweging wordt beheerst door het proportionaliteits- en subsidiariteitsvereiste.[44] Mede gelet op het voorgaande en het feit dat het tweede en het derde vereiste een casuïstisch karakter hebben, is de relevantie van deze vereisten voor dit onderzoek beperkt.[45] Deze twee vereisten worden daarom niet verder behandeld.

Wat nog belangrijk is om te vermelden met betrekking tot het tweede vereiste, is dat het EHRM in het kader van geheime surveillance niet expliciet onderscheid maakt tussen het belang van het voorkomen van strafbare feiten en het belang van de nationale veiligheid. Dit kan worden verklaard door de verschillende manieren waarop lidstaten hun politie en inlichtingen- en veiligheidsdiensten hebben georganiseerd. In Europa zijn twee basismodellen te onderscheiden. Het eerste model kent een strikte scheiding tussen de politie en de inlichtingen- en veiligheidsdiensten. Het tweede model betreft een meer geïntegreerde organisatie, waarbij de bevoegdheden en taken van de verschillende diensten vaak in hetzelfde wetgevingsinstrument worden geregeld. Het EHRM maakt daarom bij de toetsing geen onderscheid tussen het gediende belang of autoriteit, maar onderzoekt enkel de gebruikte methoden. Nederland kent in beginsel een strikte scheiding tussen de politie en de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) of de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD). In de praktijk blijkt deze scheiding echter minder strikt.[46]

2.4 Voorzien bij wet

Waar het EHRM dus weinig aandacht besteedt aan de vraag welke autoriteit de gegevensverzameling uitvoert en in welk belang, besteedt het des te meer aandacht aan de vraag of de inbreuk bij wet is voorzien.[47] Naast dat de inbreuk een wettelijke grondslag moet hebben in het nationale recht, dient deze wettelijke grondslag ook aan bepaalde kwaliteitseisen te voldoen die voortvloeien uit de rechtstaatgedachte, ook wel de ‘rule of law’ genoemd. De rule of law houdt in dat ook de overheid zich aan de wet dient te houden en beschermt burgers zo dus tegen willekeurig overheidsoptreden. De kwaliteitseisen die hieruit voortvloeien zijn: (1) toegankelijkheid en (2) voorzienbaarheid. Het toegankelijkheidsvereiste houdt in dat burgers de mogelijkheid moeten hebben om kennis te nemen van de regelgeving, dit vereist in ieder geval dat de regelgeving gepubliceerd is. Het voorzienbaarheidsvereiste houdt in dat de regelgeving duidelijk en nauwkeurig geformuleerd moet zijn, zodat burgers

[42] De Vocht, in: T&C Sv, art 8 EVRM, aant. 5 (online, bijgewerkt 1 januari 2023).
[43] De Vocht, in: T&C Sv, art 8 EVRM, aant. 6 (online, bijgewerkt 1 januari 2023).
[44] Lassche 2023, p. 9.
[45] Veen 2019, p. 394; Oerlemans 2017b, p. 73.
[46] Eskens, Van Daalen & Van Eijk 2016, p. 12-13.
[47] Het vereiste dat een inbreuk op de privacy bij wet voorzien moet zijn, blijkt overigens ook uit artikel 10 lid 2 Gw.

kunnen voorzien wanneer een inbreuk op het recht op privacy mag worden gemaakt en in staat zijn hun gedrag te reguleren.[48] Dit ziet dus op de rechtszekerheid.

Het EHRM besteedt bij de toetsing of een geheime surveillance methoden bij wet is voorzien vooral aandacht aan het voorzienbaarheidsvereiste en aan de rule of law.[49] Ten aanzien van het voorzienbaarheidsvereiste in het kader van heimelijke bevoegdheden heeft het EHRM bepaald dat de wetgeving voldoende duidelijk aan burgers moet aangeven onder welke omstandigheden en voorwaarwaarden autoriteiten deze bevoegdheden mogen gebruiken.[50]

Het EHRM kijkt daarnaast of de wetgeving in lijn is met de rule of law. Vanwege het heimelijke karakter is er een verhoogd risico op willekeur. De wetgeving moet voldoende garanties bieden tegen machtsmisbruik. Dit houdt in dat er adequate en effectieve waarborgen tegen machtsmisbruik dienen te zijn.[51] Gezien het feit dat burgers de uitoefening van heimelijke bevoegdheden niet kunnen controleren, zou het niet in overeenstemming zijn met de rule of law wanneer de wetgeving ruime termen bevat die tot een grote beoordelingsruimte leiden. Om burgers voldoende tegen willekeurige inmenging te beschermen, moet de wet de reikwijdte van een dergelijke beoordelingsbevoegdheid die aan de bevoegde autoriteiten is toegekend en de wijze waarop deze wordt uitgeoefend, voldoende duidelijk aangeven.[52]

In de zaken Rotaru tegen Roemenië en Segerstedt Wiberg e.a. tegen Zweden heeft het EHRM zich uitgelaten over offline gegevensverzameling uit publiek toegankelijke bronnen. Het EHRM heeft in beide zaken een aantal voorwaarden gegeven waaraan de wettelijke grondslag moet voldoen. Samenvattend dient er een specifiek kader te zijn waarbinnen het verzamelen en opslaan van persoonsgegevens plaatsvindt, waarbij een vijftal punten van belang zijn. Ten eerste moet duidelijk zijn welk soort materiaal mag worden vastgelegd. Wat voor soort persoonsgegevens mogen vergaard worden en welke bronnen mogen daarvoor worden gebruikt? Het is hierbij belangrijk of de gegevens waarheidsgetrouw en actueel zijn. Ten tweede moet het onderwerp van het onderzoek worden vastgelegd. Tot welke categorieën van personen is de bevoegdheid gericht? Ten derde moet de context van het onderzoek worden vastgelegd. Onder welke omstandigheden kan en mag de bevoegdheid gebruikt worden? Ten vierde dient te worden vastgelegd hoe lang gegevens bewaard mogen worden en wanneer de gegevens gedateerd zijn. Tot slot dient er een objectieve en toezichthoudende autoriteit te zijn die toeziet op de werkzaamheden. Dit gebeurt bij voorkeur door een rechterlijke autoriteit.[53]

[48] De Vocht, in: T&C Sv, art 8 EVRM, aant. 4 (online, bijgewerkt 1 januari 2023).
[49] Veen 2019, p. 394; EHRM 4 mei 2000, nr. 28341/95 (*Rotaru t. Roemenië*); EHRM 6 juni 2006, nr. 6233/00 (*Segerstedt-Wiberg e.a. t. Zweden*).
[50] Veen 2019, p. 395.
[51] Veen 2019, p. 395.
[52] Veen 2019, p. 396.
[53] Veen 2019, p. 399-400; EHRM 4 mei 2000, nr. 28341/95 (*Rotaru t. Roemenië*); EHRM 6 juni 2006, nr. 6233/00 (*Segerstedt-Wiberg e.a. t. Zweden*).

Verder is de zwaarte van de privacyinbreuk van belang voor de kwaliteitseisen en waarborgen die worden gesteld aan de wetgeving. Hierbij geldt hoe ernstiger de privacyinbreuk des te hoger de kwaliteitseisen en des te zwaarder de waarborgen moeten zijn om burgers te beschermen tegen machtsmisbruik.[54] Daarnaast dient de wetgeving ook gedetailleerder te worden naarmate de inbreuk ernstiger wordt. Uit jurisprudentie van het EHRM volgt een driedeling voor de gedetailleerdheid van de wetgeving en de waarborgen: (1) een algemene rechtsgrondslag bij geringe inbreuken, (2) nadere regelgeving in de wet of richtlijnen met beperkingen voor de opsporingsmethoden bij meer dan geringe inbeuken en (3) nadere regelgeving in de wet met een procedurele waarborg van machtiging van een rechter-commissaris bij ingrijpende inbreuken.[55]

2.5 Tussenconclusie

In dit hoofdstuk is het recht op privacy uit artikel 8 EVRM behandeld. Uit jurisprudentie van het EHRM is gebleken dat informatie uit publiek toegankelijke bronnen onder de reikwijdte van dit artikel kan vallen. Of in een concreet geval sprake is van een inbreuk op artikel 8 EVRM hangt onder andere af van het privacygevoelige karakter van de gegevens, de opslag van de gegevens, de manier waarop de gegevens zijn vergaard en de reasonable expectation of privacy. Verder is gebleken dat een inbreuk op dit recht alleen gerechtvaardigd is indien aan de drie vereisten uit het tweede lid is voldaan: de inbreuk moet (1) bij wet voorzien zijn, (2) een legitiem doel dienen en (3) noodzakelijk zijn in een democratische samenleving.

Geconcludeerd kan worden dat bij een toetsing in het kader van geheime surveillance het EHRM met name aandacht besteed aan de vraag of de inbreuk bij wet is voorzien. Hierbij wordt vooral ingegaan op het voorzienbaarheidsvereiste en de rule of law. Het heimelijke karakter benadrukt het belang van adequate en effectieve waarborgen tegen machtsmisbruik. Hierbij geldt hoe ernstiger de privacyinbreuk, des te gedetailleerder de wetgeving en des te zwaarder de waarborgen moeten zijn. Het EHRM heeft daarnaast een aantal voorwaarden gegeven waaraan een wettelijke grondslag dient te voldoen. Er dient een specifiek kader te zijn waarbinnen het verzamelen en opslaan van persoonsgegevens plaatsvind, waarbij een vijftal punten van belang zijn: de aard van de gegevens, het onderwerp van het onderzoek, de context van het onderzoek, de bewaartermijnen van de gegevens en de aanwezigheid van een objectieve en toezichthoudende autoriteit.

Nu het recht op privacy en de daarbij behorende eisen en waarborgen die van belang zijn bij wetgeving over online gegevensvergaring uit publiek toegankelijke bronnen duidelijk zijn, wordt in de volgende hoofdstukken ingegaan op de wetgeving die ziet op de bevoegdheden van de opsporingsdiensten.

[54] Rapport Commissie-Koops 2018, p. 33-35; Oerlemans 2017b, p. 139.
[55] Oerlemans 2017b, p. 77-79.

Hoofdstuk 3 – Het huidige juridische kader

3.1 Inleiding

Uit hoofdstuk 2 is gebleken dat online gegevensvergaring uit publiek toegankelijke bronnen een inbreuk op het recht op privacy kan maken. Een belangrijke voorwaarde hierbij is dat de inbreuk bij wet voorzien moet zijn. Op dit moment is er nog geen specifieke wettelijke grondslag die ziet op het online vergaren van gegevens uit publiek toegankelijke bronnen. Opsporingsambtenaren zijn nu gebonden aan een juridisch kader dat niet specifiek voor online gegevensvergaring is bedoeld.[56]

In dit hoofdstuk wordt het huidige juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence in kaart gebracht. Het is van belang om het huidige juridische kader helder te hebben, teneinde de knelpunten die in het volgend hoofdstuk worden behandeld te begrijpen. Aan de hand van het huidige juridische kader en de knelpunten, is het vervolgens mogelijk om later in deze masterscriptie suggesties te geven ter verbetering van dit kader.

Het hoofdstuk begint met een toelichting van de algemene taakstelling. Vervolgens wordt de grens van een 'meer dan geringe inbreuk' die hierbij wordt gehanteerd behandeld. Daarnaast wordt in dit hoofdstuk ook kort ingegaan op de Wpg. Tot slot zal een korte tussenconclusie van dit hoofdstuk gegeven worden.

3.2 Algemene taakstellende artikelen

Online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence geschiedt nu op grond van de algemene taakstellende artikelen.[57] Artikel 3 Pw regelt de algemene taakstellende bevoegdheid voor opsporingsambtenaren van de politie en luidt als volgt:

> "De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven."

Voor opsporingsambtenaren van de bijzondere opsporingsdiensten wordt de algemene taakstellende bevoegdheid geregeld in artikel 3 Wet op de bijzondere opsporingsdiensten (hierna: Wet BOD). Dit artikel geeft een algemene taakstelling met betrekking tot de strafrechtelijke handhaving van de rechtsorde en is vergelijkbaar met artikel 3 Pw.[58]

Niet alle activiteiten die opsporingsambtenaren ter uitvoering van de algemene taak ondernemen, zijn wettelijk geregeld. Sommige methoden die een geringe inbreuk op de privacy maken zijn 'buitenwettelijk' en vinden hun basis in de algemene taakstelling,

[56] Groothuis & Landman 2022, p. 21.
[57] Groothuis & Landman 2022, p. 33; Rapport Commissie-Koops 2018, p. 151.
[58] *Kamerstukken II* 2004/05, 30182 nr. 3 p. 17.

waaronder online gegevensvergaring uit publiek toegankelijke bronnen.[59] De algemene taakstellende bevoegdheid wordt zo dus breed ingezet.[60] Een voordeel hiervan is dat nieuwe methoden die niet onder een bestaande grondslag vallen, gebaseerd kunnen worden op deze brede bepaling en dus geen nieuwe wetgeving vereisen. Deze flexibiliteit komt de effectiviteit van de rechtshandhaving ten goede. Een nadeel van een dergelijke brede bepaling is dat het ook een zekere mate van onzekerheid creëert, doordat het niet specifiek regelt welke handelingen wanneer zijn toegelaten.[61] De Hoge Raad heeft in 1995 in het Zwolsman-arrest een deel van deze onzekerheid weggenomen door te oordelen dat opsporingsambtenaren op grond van de algemene taakstelling uit artikel 3 Pw (destijds vastgelegd in artikel 2 Pw) een inbreuk mogen maken op de privacy van burgers voor zover dit een beperkte inbreuk betreft.[62] Dat deze norm ook geldt in het geval van online gegevensvergaring blijkt onder andere uit de memorie van toelichting (hierna: MvT) op de Wet computercriminaliteit II uit 1999:

> "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 (zie artikel 2 Politiewet 1993) (…) Verder geldt dat wanneer het onderzoek een stelselmatig karakter krijgt, het een aparte juridische legitimatie behoeft"[63]

Dat artikel 3 Pw gebruikt kan worden voor online gegevensvergaring is eveneens bevestigd in jurisprudentie. Zo oordeelde de Rechtbank Den Haag in 2015 in de Context-zaak dat artikel 3 Pw een toereikende wettelijke grondslag biedt voor gegevensvergaring via social media indien sprake is van een niet meer dan geringe inbreuk op de privacy.[64] In deze zaak was echter sprake van een meer dan geringe inbreuk, waardoor er een aparte wettelijke grondslag was vereist.

Aan de hand van het Zwolsman-arrest, de MvT op de Wet computercriminaliteiten en de Context-zaak kan geconcludeerd worden dat opsporingsambtenaren op grond van artikel 3 Pw online gegevens uit publiek toegankelijke bronnen mogen vergaren voor zover dit niet leidt tot een meer dan geringe inbreuk op de privacy van burgers.[65] Leidt het wel tot een meer dan geringe inbreuk en krijgt het onderzoek een stelselmatig karakter, dan volstaat artikel 3 Pw niet en is een specifieke wettelijke bepaling nodig. Voor online gegevensvergaring in het kader van een opsporingsonderzoek kan in deze gevallen gebruik gemaakt worden van BOB-

[59] Stol & Strikwerda 2018, p. 9.
[60] Groothuis & Landman 2022, p. 23.
[61] Borgers 2015, p. 143-144.
[62] HR 19 december 1995, ECLI:NL:HR:1995:ZD0328 (*Zwolsman*), r.o. 6.4.5.
[63] *Kamerstukken II* 1998/99, 26671, nr. 3, p. 35; Oerlemans 2017a, p. 18; Groothuis & Landman 2022, p. 23.
[64] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365 (*Context-zaak*), r.o. 5.15.
[65] Dit geld ook ten aanzien van andere grondrechten, maar voor deze masterscriptie is het recht op privacy het meest van belang. Daarnaast mag het geen risico vormen voor de integriteit van de opsporing.

wetgeving (dit wordt in hoofdstuk 5 nader uitgewerkt). Voor online gegevensvergaring in het kader van intelligence ontbreekt een dergelijke specifieke grondslag, waardoor het onderzoek uit publiek toegankelijke bronnen dient te worden beëindigd zodra het een meer dan geringe inbreuk op de privacy van burgers vormt.[66]

3.3 Geringe inbreuk op de privacy

De vraag die uit het bovenstaande logischerwijs voortvloeit is: wanneer is bij online gegevensvergaring de grens van een meer dan geringe inbreuk op de privacy van de burgers bereikt? Over het algemeen is sprake van een meer dan geringe inbreuk wanneer er een "min of meer compleet beeld van een of meer aspecten van het persoonlijk leven" ontstaat.[67] In het kader van strafvordering wordt het stelselmatigheidscriterium gehanteerd om het onderscheid tussen een geringe inbreuk en een meer dan geringe inbreuk te definiëren. Het begrip stelselmatig komt hierbij sterk overeen met een meer dan geringe inbreuk. De meer dan geringe inbreuk verwijst naar het resultaat en de term stelselmatig heeft betrekking op de manier van werken.[68] Stelselmatigheid in deze context is anders dan de term stelselmatig in het normale spraakgebruik. De term stelselmatig kan hier handelingen omvatten die normaal gesproken niet als stelselmatig worden gezien, maar in juridische zin wel als stelselmatig worden beschouwd, omdat ze een meer dan geringe inbreuk op de privacy veroorzaken.[69]

Het is niet eenvoudig om te bepalen wanneer bij online gegevensvergaring sprake is van stelselmatigheid. In de MvT bij de wet BOB worden vijf klassieke factoren genoemd die van belang zijn bij deze beoordeling: (1) de duur, (2) de plaats, (3) de intensiteit, (4) de frequentie en (5) de toepassing van een technisch hulpmiddel.[70] Het is echter de vraag in hoeverre deze factoren toepasbaar zijn op de online context. Uiteraard is het mogelijk om ook online deze factoren te gebruiken voor de beoordeling van stelselmatigheid, maar de uitwerking zal aanzienlijk verschillen ten aanzien van offline. Online is het (in tegenstelling tot offline) mogelijk om met één korte handeling grote hoeveelheden persoonsgegevens te vergaren, waardoor factoren als duur en frequentie hun betekenis verliezen.

Dit probleem wordt ook erkend in de MvT bij het gemoderniseerde WvSv. Hierin worden relevante factoren voor de invulling van het begrip stelselmatigheid in de online context gegeven en uitgewerkt. Deze factoren zijn deels aanbevolen door de Commissie-Koops, die bovendien heeft geadviseerd om ze te clusteren. Dit heeft geleid tot vier clusters relevante factoren betreffende: (1) de omvang en het type van de over te nemen gegevens, (2) de aard van de bron, (3) de wijze van zoeken en (4) de opslag en het gebruik van de gegevens en de mogelijke gevolgen voor de persoon. Bij de beoordeling van de factoren gaat

[66] Rapport Commissie-Koops 2018, p. 151.
[67] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27; Rapport Commissie-Koops 2018, p. 37; Ligthart 2019, p. 196; Groothuis & Landman 2022, p. 25.
[68] Rapport Commissie-Koops 2018, p. 37; Ligthart 2019, p. 196; Groothuis & Landman 2022, p. 25.
[69] Rapport Commissie-Koops 2018, p. 37
[70] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27.

het om de redelijke voorzienbaarheid vooraf.[71] Een compleet overzicht van de factoren is te vinden in Bijlage 1. Het gemoderniseerde WvSv treedt naar verwachting in 2026 in werking, niettemin zouden deze factoren nu al handvatten kunnen bieden bij de beoordeling van het stelselmatig karakter van online gegevensvergaring uit publiek toegankelijke bronnen.

Daarnaast bestaat de 'Leidraad bevoegdheden informatievergaring op internet' die is opgesteld door het OM en de politie. Deze leidraad is opgesteld voor opsporingsambtenaren en is niet (volledig) openbaar.[72] In de leidraad wordt ingegaan op stelselmatigheid en de grens tussen artikel 3 Pw en BOB-wetgeving.[73] De leidraad geeft opsporingsambtenaren richtlijnen om te beoordelen of een handeling zelfstandig uitgevoerd kan worden op grond van artikel 3 Pw of dat toestemming voor de inzet van een BOB-middel is vereist.[74] Stelselmatigheid dient daarnaast beoordeeld te worden op basis van de combinatie van handelingen. Individuele handelingen kunnen een geringe inbreuk vormen, maar wanneer ze worden gecombineerd kan dit een meer dan geringe inbreuk opleveren. Verder blijkt ook uit de leidraad dat stelselmatigheid vooraf moet worden beoordeeld.[75]

Ondanks de (nieuwe) factoren voor stelselmatigheid en de leidraad, kent online gegevensvergaring in het kader van intelligence nog steeds veel 'grijze gebieden'. Dit maakt afstemming met het gezag des te belangrijker. De vraag is echter wie in deze gevallen het gezag draagt. Opsporingsambtenaren kennen immers twee gezagsdragers: de officier van justitie en de burgemeester. De officier van justitie heeft gezag over de handhaving van de strafrechtelijke rechtsorde. In het geval van intelligence zal dit vaak een informatieofficier van justitie betreffen. De burgemeester heeft gezag over de handhaving van de openbare orde.[76]

Zoals al eerder opgemerkt, wordt het stelselmatigheidscriterium gebruikt in het kader van strafvordering. Voor online gegevensvergaring in het kader van intelligence is de term stelselmatigheid eigenlijk minder geschikt. Beargumenteerd kan worden dat in deze gevallen beter aangesloten kan worden bij het proportionaliteits- en subsidiariteitsvereiste. Het proportionaliteitsvereiste houdt in dat de inbreuk op de privacy in een redelijke verhouding tot het doel moet staan. Het subsidiariteitsvereiste houdt in dat de minst ingrijpende methode gebruikt moet worden om het doel te bereiken.[77] Zo vloeit uit het proportionaliteitsvereiste onder andere voort dat bij het vergaren van gegevens over onverdachte personen eerder sprake zal zijn van een meer dan geringe inbreuk op de privacy. Bij een inbreuk op de privacy van onverdachte personen weegt het algemene belang of het beoogde doel minder zwaar dan wanneer het gaat om een inbreuk op de privacy van verdachte personen.[78] Bij online

[71] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 684-685; Rapport Commissie-Koops 2018, p. 162-164.
[72] In een aantal artikelen, waaronder Stol & Strikwerda 2018, wordt kort wat beschreven over de leidraad en daarnaast is een Wob-verzoek (tegenwoordig Woo-verzoek) ingediend voor de leidraad waardoor kleine delen openbaar gemaakt zijn.
[73] Stol & Strikwerda 2018, p. 11; Groothuis & Landman 2022, p. 26.
[74] Stol & Strikwerda 2018, p. 11.
[75] Groothuis & Landman 2022, p. 26.
[76] Groothuis & Landman 2022, p. 34
[77] Groothuis & Landman 2022, p. 33-34.
[78] Groothuis & Landman 2022, p. 33-34.

gegevensvergaring in het kader van intelligence is veelal nog geen sprake van een verdachte, waardoor een inbreuk eerder als disproportioneel wordt beschouwd.

De vereisten van proportionaliteit en subsidiariteit komen voort uit het vereiste dat een inbreuk op de privacy noodzakelijk moet zijn (zoals benoemd in hoofdstuk 2). Deze vereisten komen sterk overeen met de huidige gegevensbeschermingsrechtelijke beginselen, zoals doelbinding, dataminimalisatie en opslagbeperking.[79] Deze beginselen zijn terug te vinden in de Wpg, die ook van toepassing is op het online vergaren van gegevens uit publiek toegankelijke bronnen.

3.4 Wet politiegegevens

De Wpg geeft geen bevoegdheden voor het vergaren van onlinegegevens aan opsporingsambtenaren voor intelligence-doeleinden. Die bevoegdheid volgt alleen uit de hierboven besproken taakstellende artikelen.[80] De Wpg beperkt daarentegen wel het online vergaren van gegevens uit publiek toegankelijke bronnen. De wet regelt kort gezegd hoe opsporingsambtenaren met persoonsgegevens moeten omgaan, ongeacht de manier waarop de gegevens zijn verkregen. De Wpg is niet slechts van toepassing bij de opslag van gegevens, maar bij de gehele verwerking van gegevens. De verwerking van persoonsgegevens vindt al plaats zodra de gegevens worden verzameld via een politiecomputer of door de systemen van de IT-infrastructuur van de politie stroomt.[81]

Artikel 2 Wpg bepaalt de reikwijdte van de wet en hieruit volgt dat de Wpg van toepassing is op de verwerking van politiegegevens die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen. Artikel 1 onder a Wpg definieert een politiegeven als 'elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet'.[82] Aangezien vergaren onderdeel uitmaakt van verwerken, is de Wpg dus ook van toepassing op het online vergaren van persoonsgegevens uit publiek toegankelijke bronnen.

In de Wpg wordt de verwerking van gegevens voornamelijk genormeerd door de zes algemene beginselen van gegevensverwerking: (1) rechtmatigheid, (2) doelbinding, (3) dataminimalisatie, (4) opslagbeperking, (5) juistheid en (6) integriteit en vertrouwelijkheid. De beginselen zijn terug te vinden in artikel 3 en 4 van de Wpg. Alle gegevensverwerkingen door opsporingsambtenaren moeten aan deze normen voldoen.[83] Daarnaast blijkt uit artikel 5 Wpg dat opsporingsambtenaren slechts bijzondere persoonsgegevens mogen verwerken indien dit onvermijdelijk is om het beoogde doel te bereiken. Bijzondere gegevens zijn onder andere gegevens over ras, etniciteit, religieuze overtuiging, gezondheid en politieke en seksuele voorkeur. Foto's van personen op social media zijn bijvoorbeeld bijzondere gegevens.[84]

[79] Fedorova e.a. 2022, p. 58.
[80] Schermer 2017, p. 209; Hirsch Ballin & Oerlemans 2023, p.25.
[81] Oerlemans 2017a, p. 19-20.
[82] Fedorova e.a. 2022, p. 16.
[83] Fedorova e.a. 2022, p. 21-22.
[84] Oerlemans 2017a, p. 19.

Toezicht op naleving van de Wpg vindt zowel intern (niet-onafhankelijk) als extern (onafhankelijk) plaats. Intern gebeurt dit door een privacyfunctionaris, dit is vaak een politiefunctionaris met kennis van het privacyrecht. Extern gebeurt dit door een functionaris gegevensbescherming en de Autoriteit Persoonsgegevens (hierna: AP). Daarnaast is ook een rol toegekend aan de officier van justitie. De officier van justitie heeft in een aantal gevallen zeggenschap, vanwege zijn gezag over de opsporing.[85]

3.5 Tussenconclusie

Geconcludeerd kan worden dat opsporingsambtenaren online gegevens uit publiek toegankelijke bronnen mogen vergaren op grond van artikel 3 Pw voor zover dit niet leidt tot een meer dan geringe inbreuk op de privacy van betrokkenen. Er is sprake van een meer dan geringe inbreuk wanneer er een "min of meer compleet beeld van een of meer aspecten van het persoonlijk leven" ontstaat. Om te beoordelen of dit het geval is, kunnen opsporingsambtenaren de (nieuwe) factoren voor stelselmatigheid en de leidraad bevoegdheden informatievergaring op internet raadplegen. Daarnaast dienen opsporingsambtenaren zich ook aan de algemene beginselen van gegevensverwerking en aan de overige eisen uit de Wpg te houden.

Verder is gebleken dat het huidige juridische kader nog veel grijze gebieden kent, waardoor afstemming met het gezag belangrijk is. In het volgend hoofdstuk worden de knelpunten van het huidige juridische kader behandeld en zal dieper worden ingegaan op deze grijze gebieden.

[85] Fedorova e.a. 2022, p. 25.

Hoofdstuk 4 – De knelpunten

4.1 Inleiding

Uit het vorig hoofdstuk is gebleken dat opsporingsambtenaren zijn gebonden aan een juridisch kader dat niet specifiek voor online gegevensvergaring is bedoeld. Het juridisch kader is niet berekend op de technologische mogelijkheden van de huidige tijd. Als gevolg hiervan, zijn er een aantal knelpunten ontstaan. In de literatuur waren met name knelpunten te vinden met betrekking tot de onduidelijkheid omtrent artikel 3 Pw, de onduidelijkheid aangaande gezagsdragers en over het toezicht op de Wpg. Vervolgens is aan de hand van interviews onderzocht of de geconstateerde knelpunten uit de literatuur daadwerkelijk voorkwamen in de praktijk en of er mogelijk andere knelpunten aanwezig waren. Tijdens de interviews zijn de knelpunten uit de literatuur bevestigd en zijn er ook nieuwe knelpunten naar boven gekomen. Zo ontstond in een aantal interviews een bredere discussie over wat nu precies het onderscheid is tussen intelligence en opsporing. De grens hiertussen blijkt vaak niet zo zwart-wit.

In dit hoofdstuk zal in elke paragraaf een ander knelpunt worden belicht. Respectievelijk zal worden ingegaan op de volgende vier knelpunten: (1) de onduidelijkheid over artikel 3 Pw, (2) de onduidelijkheid met betrekking tot de gezagsdragers, (3) het externe toezicht op de Wpg en (4) de bredere discussie over het onderscheid tussen intelligence en het opsporingsonderzoek. Tot slot zal een korte tussenconclusie volgen.

4.2 Onduidelijkheid over artikel 3 Pw

Het meest gehoorde knelpunt van het huidige juridische kader betreft de onduidelijkheid over de reikwijdte van artikel 3 Pw. Artikel 3 Pw regelt de algemene taakstellende bevoegdheid van opsporingsambtenaren en wordt zodoende gebruikt als grondslag voor veel ‘lichte’ opsporingshandelingen die niet op een specifieke wijze in de wet zijn geregeld. Enerzijds komt deze flexibele normering de effectiviteit van de rechtshandhaving ten goede. Anderzijds zorgt dit voor onzekerheid of een bepaalde handeling verricht mag worden, omdat het artikel niet specifiek regelt welke handelingen wanneer zijn toegelaten. Hierdoor zullen steeds discussies over de rechtmatigheid ontstaan. Zeker bij handelingen die in intensiteit kunnen verschillen, waaronder online gegevensvergaring uit publiek toegankelijke bronnen, waardoor de handeling in het ene geval wel gebaseerd kan worden op de algemene taakstelling en in het andere geval niet.[86]

Uit het vorig hoofdstuk is gebleken dat online gegevensvergaring uit publiek toegankelijke bronnen gebaseerd kan worden op artikel 3 Pw voor zover dit niet leidt tot een meer dan geringe inbreuk op de privacy van betrokkenen. Of sprake is van een meer dan geringe inbreuk wordt op dit moment bepaald aan de hand van de factoren voor stelselmatigheid en de leidraad bevoegdheden informatievergaring op internet. Desondanks ervaart men in de

[86] Borgers 2015, p. 143-145.

praktijk nog steeds onduidelijkheid over wat mag op grond van artikel 3 Pw en wordt de grens van een meer dan geringe inbreuk verschillend geïnterpreteerd.[87] Dit blijkt ook uit de interviews. Respondenten geven aan dat het onduidelijk is welke handelingen zij mogen verrichten op grond van artikel 3 Pw en dat collega's de reikwijdte van dit artikel soms anders interpreteren. Naast dat dit tot de nodige discussies leidt, kan deze onduidelijkheid op twee manieren een negatieve invloed hebben op het strafrechtelijke systeem.

Aan de ene kant kan deze onduidelijkheid leiden tot een 'chilling effect', doordat bepaalde handelingen worden vermeden vanwege twijfel over de toelaatbaarheid. Met name op het gebied van intelligence is dit het geval, omdat niet kan worden teruggegrepen op een specifieke wettelijke grondslag. Wanneer het zekere voor het onzekere wordt genomen, wordt ingeleverd op de effectiviteit van de rechtshandhaving.[88] Aan de andere kant bestaat het risico dat vanwege de onduidelijkheid meer wordt gedaan op basis van artikel 3 Pw dan is toegestaan. Dit risico wordt alleen maar groter vanwege de voortschrijdende technologische ontwikkelingen.[89] Wanneer de grenzen worden opgezocht en het risico dat een handeling onrechtmatig kan zijn bewust wordt aanvaardt, kan de burger het gevoel krijgen dat de overheid de wet niet serieus neemt.[90] Een aantal respondenten geeft aan dat zij soms inderdaad de grenzen opzoeken, terwijl andere respondenten aangeven liever het zekere voor het onzekere te nemen door bepaalde handelingen te vermijden.

De discussie over de reikwijdte van artikel 3 Pw beperkt zich niet alleen tot opsporingsambtenaren en juristen. Het heeft recentelijk ook bredere aandacht gekregen, doordat het opnieuw in het nieuws is gekomen in relatie tot het Team Openbare Orde Inlichtingen (hierna: TOOI). Het TOOI is een onderdeel van de politie dat heimelijk informatie vergaart, waaronder ook informatie uit publiek toegankelijke bronnen, ter handhaving van de openbare orde. Dit doen ze op grond van artikel 3 Pw.[91] Volgens de Minister van Veiligheid en Justitie biedt artikel 3 Pw hiervoor een voldoende grondslag, omdat het een geringe inbreuk op de persoonlijke levenssfeer betreft. Andere Kamerleden maken zich echter zorgen.[92] Ook hoogleraar strafrecht Sven Brinkhoff uit zijn zorgen: "Deze methodes grijpen echt diep in tegen de privacy van burgers, zonder dat dat in de wet is geregeld. Dat is heel intens".[93]

Ook hieruit blijkt dus dat de reikwijdte van artikel 3 Pw en de bijbehorende grens van een meer dan geringe inbreuk verschillend geïnterpreteerd wordt en zo tot discussies over de rechtmatigheid leidt. Eén respondent stelt zelfs dat artikel 3 Pw eigenlijk überhaupt geen grondslag biedt voor het inzetten van bevoegdheden. Het artikel stelt alleen de taak van de politie vast, maar verleent geen bevoegdheden aan de politie. Het is volgens de respondent

[87] Groothuis & Landman 2022, p. 134; Oerlemans 2018, p. 4.
[88] Borgers 2015, p. 144.
[89] Winter e.a. 2020, p. 27.
[90] Borgers 2015, p. 145.
[91] 'Minister: 'TOOI is geen inlichtingendienst'', vpngids.nl 17 mei 2023; 'Inlichtingendienst van politie bespioneert illegaal onschuldige burgers', rtlnieuws.nl 25 mei 2023.
[92] 'Minister: 'TOOI is geen inlichtingendienst'', vpngids.nl 17 mei 2023.
[93] 'Inlichtingendienst van politie bespioneert illegaal onschuldige burgers', rtlnieuws.nl 25 mei 2023, geraadpleegd op 3 juli 2023.

begrijpelijk dat bepaalde lichte bevoegdheden bij de taakuitoefening van de politie horen, maar artikel 3 gaat zo ver terug naar de basis van de politietaak dat het voor de praktijk geen enkel handvat biedt. Artikel 3 Pw wordt nu eigenlijk gebruikt als stoplap. Een andere respondent geeft nog aan dat er op dit moment een werkgroep loopt met het ministerie van Justitie en Veiligheid over de artikel 3 Pw discussie, waarbij ze aan het inventariseren zijn op welke vlakken welke vraagpunten spelen.

4.3 Onduidelijkheid ten aanzien van de gezagsdragers

Zoals uit het vorige hoofdstuk is gebleken, hebben opsporingsambtenaren van de politie twee gezagdragers. Wanneer de politie optreedt ter strafrechtelijke handhaving van de rechtsorde staat zij onder gezag van de officier van justitie en wanneer zij optreedt ter handhaving van de openbare orde staat zij onder gezag van de burgemeester. Dit blijkt ook uit artikel 11 en 12 Pw. Er vallen twee onduidelijkheden te onderscheiden met betrekking tot dit onderwerp.

Ten eerste is het niet altijd duidelijk tot welk gezag opsporingsambtenaren zich moeten richten bij online gegevensvergaring in het kader van intelligence. Enkele bevoegdheden die uitgeoefend worden op grond van de algemene taakstelling uit artikel 3 Pw, kunnen zowel betrekking hebben op de handhaving van de openbare orde als op de strafrechtelijke handhaving.[94] Dit geldt ook voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van intelligence. Dit heeft tot gevolg dat er in de praktijk op verschillende manieren wordt gehandeld. Zo zijn er eenheden die zich wenden tot de burgemeester, maar er zijn ook eenheden die zich richten tot de officier van justitie. Dit is een ongewenste situatie.[95] Daarnaast zijn er eenheden die zich bij openbare orde intelligence richten tot de officier van justitie in plaats van de burgermeester.[96] Deze praktijk hangt samen met de tweede onduidelijkheid.

De tweede onduidelijkheid betreft de rol van de burgemeester ten aanzien van online gegevensvergaring in het kader van de openbare orde intelligence. Burgemeesters zijn zich niet altijd bewust van het feit dat zij verantwoordelijk zijn voor online gegevensvergaring ten behoeve van openbare orde intelligence.[97] Dit is ook bevestigd in de interviews. Het heeft waarschijnlijk te maken met de bredere zoektocht naar de rol van de burgemeester in de online context.[98] Beargumenteerd kan worden dat de bevoegdheden van de burgemeesters niet geschikt zijn voor de online context. Burgemeesters beschikken vaak niet over de relevante kennis en zij zijn daarnaast gebonden aan gemeentegrenzen.[99] De fenomenen en groepen waarover online gegevens worden vergaard, houden zich echter niet aan de grenzen van de gemeenten. De vraag is dan welke burgemeester het gezag heeft.[100]

[94] Hirsch Ballin 2022, p. 21.
[95] Groothuis & Landman 2022, p. 75 & 135.
[96] Groothuis & Landman 2022, p. 75.
[97] Groothuis & Landman 2022, p. 75.
[98] Groothuis & Landman 2022, p. 34 & 75; Bantema e.a. 2018, p. 85-119.
[99] Bantema e.a. 2018, p. 86-92.
[100] Groothuis & Landman 2022, p. 75.

Zo staat ook het in het vorige knelpunt besproken TOOI onder gezag van de lokale burgemeester. De landelijk portefeuillehouder TOOI erkent dat de controle en het toezicht van de burgemeesters op het TOOI beter georganiseerd moet worden. Hij geeft echter ook aan dat dit lastig is gezien het feit dat het gezag van burgemeesters gebonden is aan gemeentegrenzen. Samen met het ministerie en de burgemeesters zijn ze dit nu beter aan het afstemmen.[101]

4.4 Extern toezicht op de Wpg

De normering van online gegevensvergaring uit publiek toegankelijke bronnen kan niet los worden gezien van het toezicht hierop. Door effectief toezicht wordt de norm bevestigd, afgedwongen en waar nodig uitgelegd. Effectief toezicht kan zo eventuele onduidelijkheden in het juridisch kader ondervangen.[102] Gezien de aanwezige onduidelijkheden in het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence lijkt effectief toezicht hierop van belang, om zo de onduidelijkheden te ondervangen. Op dit moment houden verschillende organen toezicht (zowel onafhankelijk als niet-onafhankelijk), maar kan niet van effectief toezicht worden gesproken.[103]

Het vorige hoofdstuk heeft aangetoond dat opsporingsambtenaren bij het vergaren van gegevens uit publiek toegankelijke bronnen ook de bepalingen uit de Wpg in acht dienen te nemen. De AP is het belangrijkste toezichthoudende orgaan en houdt extern toezicht op de naleving van de Wpg. Een groot gedeelte van de verantwoordelijkheid voor de naleving van de Wpg ligt hierbij in handen van de betrokkenen zelf. Onrechtmatigheden in de naleving van de Wpg kunnen aan het licht worden gebracht doordat betrokkenen klachten indienen. Betrokkenen kunnen dit echter moeilijk vaststellen, doordat zij vaak niet weten dat zij onderwerp van onderzoek zijn of doordat zij geen toegang tot de benodigde informatie hebben.[104] Daarnaast is de klachtprocedure onduidelijk en kent deze lange doorlooptijden.[105] Dit heeft tot gevolg dat het toezicht op naleving van het gegevensbeschermingsrecht grotendeels afhangt van een proactieve houding van de AP.[106] Uit onderzoeken en interviews blijkt echter dat de AP onvoldoende personeel en middelen heeft om dit toezicht effectief uit te voeren.[107] Uit informatie die op de website van de AP is gepubliceerd, blijkt ook dat de AP maar weinig inspanningen heeft geleverd wanneer het gaat om onderzoek naar gegevensverwerkingen door de politie.[108]

[101] 'Tooi probeert relschoppers een stap voor te zijn', politie.nl 19 mei 2023.
[102] Fedorova e.a. 2022, p. 167-168.
[103] Fedorova e.a. 2022, p. 168
[104] Stevens e.a. 2021, p. 240-241.
[105] Fedorova e.a. 2022, p. 33.
[106] Stevens e.a. 2021, p. 240-241.
[107] Hirsch Ballin & Oerlemans 2023, p. 34; Winter e.a. 2020, p. 26.
[108] Hirsch Ballin & Oerlemans 2023, p. 34

Effectief toezicht door de AP is juist in het geval van intelligence heel belangrijk, vanwege de beperkte rol van de strafrechter. In veel gevallen zal gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van intelligence namelijk niet gecontroleerd worden door een rechter.[109] Het doel van intelligence is immers niet het nemen van strafvorderlijke beslissingen (zoals bij opsporing) en leidt zodoende niet vaak tot een zaak bij de rechter. Bij intelligence gaat het om het opbouwen van een informatiepositie, wat eventueel kan leiden tot het starten van een opsporingsonderzoek. Overigens leidt ook niet ieder opsporingsonderzoek tot een strafzaak bij de rechter.[110] Indien het wel tot een strafzaak komt, is de strafrechter terughoudend met het verbinden van rechtsgevolgen aan privacy schendingen. Het gevolg hiervan is dat in de praktijk meestal niet grondig gecontroleerd wordt of de Wpg wordt nageleefd, aangezien een schending toch dikwijls niet tot een rechtsgevolg leidt.[111]

Bovendien raakt online gegevensvergaring ten behoeve van intelligence de privacyrechten van een veel grotere groep personen (waaronder ook niet-verdachten) dan bij een klassiek opsporingsonderzoek waar het alleen gaat om de verdachte(n).[112] Dit benadrukt de noodzaak van een zorgvuldige omgang met gegevens, zeker in het geval van niet-verdachten, en het belang van effectief toezicht hierop.[113]

Tot slot vindt het toezicht door de AP vooral achteraf plaats en is de toetsing vooraf beperkt.[114] Wat momenteel vooral ontbreekt, is een onafhankelijke toezichthouder die tijdens de inzet van digitale opsporingsbevoegdheden meekijkt en indien nodig kan ingrijpen.[115] In de interviews is ook de wens geuit voor een externe toezichthouder die niet alleen vooraf of achteraf controleert, maar juist ook toezicht houdt tijdens het vergaren van onlinegegevens.

4.5 Het onderscheid tussen intelligence en het opsporingsonderzoek

Het laatste knelpunt betreft het onderscheid tussen intelligence en het opsporingsonderzoek. Hoewel in de inleiding al een beknopte uitleg is gegeven, vereist dit onderwerp een meer uitvoerige behandeling. Uit de interviews is namelijk gebleken dat het onderscheid tussen intelligence en opsporing in de praktijk niet altijd helder is. Het is voor opsporingsambtenaren soms moeilijk om te bepalen of zij nog in de intelligencefase zitten of al in het opsporingsonderzoek. Het is echter van essentieel belang om dit te weten, aangezien de fase bepaalt welk juridisch kader van toepassing is en welke mogelijkheden er zijn om gegevens te vergaren.[116] Zo kunnen bij het opsporingsonderzoek (na toestemming van de officier van justitie) BOB-middelen worden toegepast, maar BOB-middelen kunnen niet louter ten

[109] Rapport Commissie-Koops 2018, p. 30; Oerlemans 2018, p. 18-19; Hirsch Ballin & Oerlemans 2023, p. 33.
[110] Rapport Commissie-Koops 2018, p. 30
[111] Fedorova e.a. 2022, p. 168-169.
[112] Hirsch Ballin & Oerlemans 2023, p. 27-26; Rapport Commissie-Koops 2018, p. 30.
[113] Rapport Commissie-Koops 2018, p. 30.
[114] Winter e.a. 2020, p. 26.
[115] Fedorova e.a. 2022, p. 171; Hirsch Ballin & Oerlemans 2023, p. 36.
[116] Schermer 2017, p. 209.

behoeve van intelligence worden ingezet.[117] Voordat dit knelpunt verder wordt uitgewerkt, wordt eerst het verschil tussen intelligence en opsporing nader uitgelegd.

Het onderscheid tussen online gegevensvergaring ten behoeve van intelligence en online gegevensvergaring ten behoeve van het opsporingsonderzoek heeft vooral betrekking op het doel waarvoor de gegevens vergaard worden.[118] Het doel van het opsporingsonderzoek volgt uit artikel 132a WvSv. Dit artikel definieert het opsporingsonderzoek en luidt als volgt:

> "Onder opsporing wordt verstaan het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen."

Het doel van het opsporingsonderzoek is dus het nemen van strafvorderlijke beslissingen. Online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van een opsporingsonderzoek is gericht op waarheidsvinding en het verzamelen van bewijs zodat er uiteindelijk strafvorderlijke beslissingen genomen kunnen worden.[119] Activiteiten van opsporingsambtenaren die hier niet op zijn gericht, vallen dus niet onder het opsporingsonderzoek. Zo valt het verkennend onderzoek uit artikel 126gg WvSv niet onder het opsporingsonderzoek.[120] Het doel van het verkennend onderzoek is namelijk niet het nemen van specifieke in de wet omschreven strafvorderlijke beslissingen, maar de voorbereiding van opsporing in concrete strafzaken.[121]

Ook intelligence wordt niet tot het opsporingsonderzoek gerekend, nu dit niet gericht is op het nemen van strafvorderlijke beslissingen maar op het opbouwen van een informatiepositie. Bij het online vergaren van gegevens uit publiek toegankelijke bronnen ten behoeve van intelligence ligt de focus op het monitoren van trends en ontwikkelingen ten aanzien van specifieke veiligheidsthema's. Op dit moment worden er (nog) geen specifieke strafbare feiten onderzocht, maar wordt een informatiepositie gecreëerd om zo inzicht te verkrijgen in wat er momenteel gebeurt en mogelijk kan gebeuren. Dit dient als sturingsinformatie en wordt opgenomen in informatieproducten zoals een informatierapport of een veiligheidsbeeld.[122]

Toch blijkt dit onderscheid in de praktijk niet altijd even helder. Dit kan ten eerste komen doordat intelligence een fase is in het opsporingsproces. Intelligence fungeert doorgaans als een voorbereidende stap voor het concrete opsporingsonderzoek.[123] Op zichzelf genomen maakt het dus geen onderdeel uit van het opsporingsonderzoek, maar intelligence kan wel

[117] Groothuis & Landman 2022, p. 45; Schermer 2017, p. 209; Van den Eeden e.a. 2021, p 85-86.
[118] Groothuis & Landman 2022, p. 124.
[119] Groothuis & Landman 2022, p. 44.
[120] Van der Meij, in: T&C Sv, art. 132a Sv, aant. 4 (online, bijgewerkt 1 januari 2023).
[121] *Kamerstukken II* 2004/05, 30164, nr. 3, p. 17.
[122] Groothuis & Landman 2022, p. 44.
[123] Schermer 2017, p. 209.

overvloeien in een opsporingsonderzoek.[124] Wanneer dit precies het geval is, is vaak moeilijk te bepalen. Het opsporingsbegrip uit artikel 132a WvSv voorziet namelijk niet in een duidelijk startpunt vanaf welk moment het onderzoek als opsporing wordt beschouwd. Het feit dat het opsporingsonderzoek gericht moet zijn op het nemen van strafvorderlijke beslissingen duidt meer op een punt in de toekomst, dan dat het een daadwerkelijk startpunt aangeeft voor het begin van het opsporingsonderzoek.[125] Hierdoor is het soms moeilijk voor opsporingsambtenaren om te bepalen of zijn nog in de intelligencefase zitten of al in het opsporingsonderzoek.

Ten tweede kan dit komen doordat het opsporingsbegrip uit artikel 132a WvSv een bredere reikwijdte heeft gekregen.[126] Tegenwoordig omvat het opsporingsbegrip een breed scala aan onderzoek "in verband met strafbare feiten", zonder dat een aanwijzing of een redelijk vermoeden van schuld is vereist. Daarnaast wordt "het nemen van strafvorderlijke beslissingen" breed uitgelegd. Hierdoor sluit het opsporingsbegrip beter aan bij het bredere karakter van strafvorderlijke reacties, dat in de praktijk niet meer beperkt is tot het hoofddoel, namelijk materiële waarheidsvinding door het verzamelen van bewijs voor de vervolging van de daadwerkelijke schuldige. Het opsporingsbegrip geeft zo de ruimte om tevens andere doelen en reacties na te streven, zoals het verstoren strafbare feiten en het versterken van de informatiepositie.[127] Bij een opsporingsonderzoek wordt dus niet meer uitsluitend reactief opgetreden (dus na een strafbaar feit). Steeds vaker wordt een proactieve aanpak toegepast, waarbij al beschikbare informatie uit andere opsporingsonderzoeken en overige bronnen, waaronder publiek toegankelijke bronnen, wordt geanalyseerd. Het voornaamste doel van deze aanpak is om de beperkte middelen voor toezicht en opsporing efficiënter te kunnen inzetten door het maken van betere keuzes.[128] De opsporingspraktijk raakt zo steeds meer verweven met de intelligencepraktijk.[129] Voor zover een proactieve aanpak niet hoofdzakelijk is gericht op het opsporen en vervolgen van individuen, maar (mede) op andere doelen (zoals bijvoorbeeld intelligence), ontstaat de vraag of dit binnen het opsporingsbegrip valt en of er opsporingsbevoegdheden ingezet kunnen worden.[130]

4.6 Tussenconclusie

Het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence kent dus een aantal knelpunten. Ten eerste heerst er onduidelijkheid over de reikwijdte van artikel 3 Pw en de bijbehorende grens van een meer dan geringe inbreuk. Ondanks de factoren voor stelselmatigheid en de leidraad, wordt de reikwijdte van artikel 3 Pw verschillend geïnterpreteerd. Dit leidt tot discussies over de rechtmatigheid. Ten tweede is het onduidelijke wie het gezag uitoefent bij online

[124] Groothuis & Landman 2022, p. 45; Schermer 2017, p. 209.
[125] Crijns e.a. 2021, p. 143; Hirsch Ballin 2022, p. 21.
[126] Hirsch Ballin & Oerlemans 2023, p. 29; Hirsch Ballin 2022, p. 10 & 35.
[127] Hirsch Ballin & Oerlemans 2023, p. 29-30.
[128] Rapport Commissie-Koops 2018, p. 22;
[129] Hirsch Ballin & Oerlemans 2023, p. 37.
[130] Rapport Commissie-Koops 2018, p. 22;

gegevensvergaring in het kader van intelligence. Er zijn eenheden die zich wenden tot de burgemeester, maar er zijn ook eenheden die zich richten tot de officier van justitie. Daarnaast heerst de vraag of een burgemeesters überhaupt geschikt is als gezagdrager van online gegevensvergaring in het kader van de openbare orde intelligence. Ten derde is er geen effectief extern toezicht op naleving van de Wpg. Terwijl dit juist in het geval van intelligence heel belangrijk is. Tot slot is het voor opsporingsambtenaren niet altijd duidelijk of zij zich in de intelligencefase bevinden of in een opsporingsonderzoek. Terwijl dit wel van belang is om te weten, aangezien de fase bepaalt welk juridisch kader van toepassing is en welke mogelijkheden er zijn om gegevens te vergaren.

In de volgende twee hoofdstukken wordt respectievelijk ingegaan op het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek en het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door de inlichtingen- en veiligheidsdiensten. Deze juridische kaders bieden mogelijk oplossingen voor de in dit hoofdstuk besproken knelpunten.

Hoofdstuk 5 – Online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek

5.1 Inleiding

Uit het vorig hoofdstuk is gebleken dat het voor opsporingsambtenaren moeilijk is om te bepalen of zij zich in de intelligencefase bevinden of in het opsporingsonderzoek, terwijl dit wel van belang is om te weten aangezien de juridische kaders verschillen. In dit hoofdstuk wordt het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek uiteengezet. Hierdoor worden in de eerste plaats de verschillen tussen de twee juridische kaders duidelijk. Belangrijker nog is dat het juridische kader voor het opsporingsonderzoek mogelijk waardevolle inzichten biedt die kunnen bijdragen aan de verbetering van het juridische kader op het gebied van intelligence. Dit sluit tevens aan bij het advies van Commissie-Koops om bij de normering van online gegevensvergaring ten behoeve van andere, niet-strafvorderlijke, taken zo veel mogelijk aan te haken bij de terminologie en voorwaarden die binnen de strafvordering gelden.[131]

In dit hoofdstuk wordt eerst ingegaan op het huidige juridische kader. Aangezien dit bij een geringe inbreuk grotendeels overlapt met het juridische kader voor intelligence-doeleinden uit hoofdstuk 3, wordt hier vooral ingegaan op het juridische kader dat geldt bij een meer dan geringe inbreuk op de privacy. Vervolgens wordt het gemoderniseerde WvSv behandeld. Hierbij wordt vooral ingegaan op het nieuwe artikel 2.8.8 dat specifiek ziet op het stelselmatig overnemen van gegevens uit publieke toegankelijke bronnen. Tot slot zal een korte tussenconclusie volgen.

5.2 Juridisch kader

Het juridisch kader voor online gegevensvergaring ten behoeve van het opsporingsonderzoek komt deels overeen met het in hoofdstuk 3 besproken juridisch kader voor online gegevensvergaring ten behoeve van intelligence. Het voornaamste verschil is dat de wettelijke grondslag voor online gegevensvergaring ten behoeve van intelligence alleen te vinden is in de Pw. Terwijl online gegevensvergaring ten behoeve van het opsporingsonderzoek zijn wettelijke grondslag vindt in zowel de Pw als in het WvSv.[132] Eerst zal kort worden ingegaan op het juridisch kader dat geldt bij een geringe inbreuk. Vervolgens wordt het juridisch kader dat geldt bij een meer dan geringe inbreuk behandeld.

5.2.1 Geringe inbreuk

Bij een geringe inbreuk op de privacy is het juridische kader dat geldt voor opsporing vrijwel hetzelfde als het juridisch kader dat geldt voor intelligence, zoals reeds besproken in hoofdstuk 3. Ten behoeve van het opsporingsonderzoek kan online gegevensvergaring uit publiek toegankelijke bronnen namelijk ook gebaseerd worden op artikel 3 Pw, dan wel artikel

[131] Rapport Commissie-Koops 2018, p. 151; Groothuis & Landman 2022, p. 134.
[132] Groothuis & Landman 2022, p. 23.

3 Wet BOD, voor zover dit uiteraard niet leidt tot een meer dan geringe inbreuk op de privacy van betrokkenen. Daarnaast kunnen opsporingsambtenaren die online gegevens vergaren voor strafvorderlijke doeleinden zich ook baseren op de algemene taakstellende bevoegdheden uit het WvSv. Op grond van artikel 141 en 142 WvSv mogen opsporingsambtenaren hetzelfde als op grond van artikel 3 Pw.[133]

Verder zijn de in hoofdstuk 3 besproken factoren voor stelselmatigheid, de leidraad bevoegdheden informatievergaring op internet en de Wpg eveneens van toepassing op online gegevensvergaring in het kader van een opsporingsonderzoek.[134] Het stelselmatigheidscriterium en de leidraad vinden zelfs hun oorsprong in het strafvorderlijke kader. Het enige verschil is dat online gegevensvergaring ten behoeve van het opsporingsonderzoek slechts één gezagdrager kent, namelijk de officier van justitie. Aangezien bij een geringe inbreuk de kaders verder overeenkomen, wordt dit onderdeel hier niet opnieuw behandeld.

5.2.2 Meer dan geringe inbreuk

Zodra sprake is van een meer dan geringe inbreuk verschillen de juridische kaders aanzienlijk. Uit de vorige hoofdstukken is gebleken dat bij een meer dan geringe inbreuk de taakstellende artikelen niet langer volstaan en een specifieke wettelijke grondslag is vereist. Dit blijkt overigens ook uit het strafvorderlijk legaliteitsbeginsel dat te vinden is in artikel 1 WvSv.[135] In tegenstelling tot (online) gegevensvergaring in het kader van intelligence, kent gegevensvergaring in het kader van het opsporingsonderzoek wel een dergelijk specifieke grondslag. Deze grondslag is te vinden in titel IVa van het WvSv, hier staan de bijzondere bevoegdheden tot opsporing beschreven. BOB-middelen vereisen een bevel van de officier van justitie en bieden zo meer rechtsbescherming dan de taakstellende artikelen.

Ook ten aanzien van BOB-middelen is het weinig concreet gemaakt in de wet hoe deze kunnen worden ingezet in de online context.[136] Dit heeft ertoe geleid dat op dit moment twee verschillende BOB-middelen gebruikt worden bij stelselmatige online gegevensvergaring ten behoeve van het opsporingsonderzoek, namelijk: stelselmatige observatie en stelselmatige informatie-inwinning.[137] De bevoegdheid tot stelselmatige observatie volgt uit artikel 126g WvSv, het eerste lid luidt als volgt:

> "In geval van verdenking van een misdrijf, kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar stelselmatig een persoon volgt of stelselmatig diens aanwezigheid of gedrag waarneemt."

[133] Groothuis & Landman 2022, p. 24.
[134] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 684-685; Rapport Commissie-Koops 2018, p. 162-164; Stol & Strikwerda 2018, p. 11; Groothuis & Landman 2022, p. 26; Oerlemans 2017a, p. 19-20.
[135] Groothuis & Landman 2022, p. 27; Stol & Strikwerda 2018, p. 9.
[136] Groothuis & Landman 2022, p. 24.
[137] Lassche 2023, p. 11; Klaar 2022, p. 2; Stol & Strikwerda 2018, p. 13; Groothuis & Landman 2022, p. 27

De bevoegdheid tot stelselmatige informatie-inwinning volgt uit artikel 126j WvSv, het eerste lid luidt als volgt:

> "In geval van verdenking van een misdrijf kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar als bedoeld in artikel 141, onderdeel b, Sv zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar, stelselmatig informatie inwint over de verdachte."

Beide bevoegdheden zijn niet geheel passend in het kader van stelselmatige online gegevensvergaring en kennen dan ook hun eigen problemen en tekortkomingen. Uit de interviews is gebleken dat de toepassing van deze artikelen afhankelijk is van de interpretatie van de opsporingsambtenaar en de officier van justitie. Over het algemeen wordt stelselmatige informatie-inwinning uit artikel 126j WvSv beschouwd als de best passende bevoegdheid.[138] Deze opvatting vindt steun in jurisprudentie van de Rechtbank Den Haag. In de Context-zaak oordeelde de Rechtbank dat voor het aanmaken van een Facebookaccount en de activiteiten die de politie daarmee uitvoerden een bevel van de officier van justitie was vereist op grond van artikel 126j WvSv, omdat deze activiteiten aangemerkt moeten worden als het stelselmatig inwinnen van informatie. Over een bevel voor stelselmatige observatie is in deze zaak niet gesproken.[139] Daarnaast blijkt uit de Leidraad bevoegdheden informatievergaring op internet ook dat stelselmatige informatie-inwinning over het algemeen de voorkeur verdient boven stelselmatige observatie.[140]

Ook de moderniseringswetgever erkent dat stelselmatige observatie en stelselmatige informatie-inwinning wezenlijk verschillen van stelselmatige gegevensvergaring uit publiek toegankelijke bronnen. Het gemoderniseerde WvSv introduceert daarom in artikel 2.8.8 een nieuw BOB-middel dat specifiek ziet op het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen.[141]

5.3 Het gemoderniseerde WvSv

Het wetsvoorstel voor het gemoderniseerde WvSv is op 20 maart 2023 naar de Tweede Kamer gestuurd, maar naar verwachting treedt het pas in 2026 in werking. Tot die tijd moeten opsporingsambtenaren dus gegevens vergaren uit publiek toegankelijke bronnen op grond van het juridische kader uit de vorige paragraaf. Het gemoderniseerde WvSv introduceert een nieuwe algemene bevoegdheidsbepaling en een specifieke bepaling voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek. Eerst zal kort worden ingegaan op de veranderingen die het gemoderniseerde WvSv met zich meebrengt voor het juridisch kader dat geldt bij een geringe

[138] Lassche 2023, p. 12; Groothuis & Landman 2022, p. 28; Stol & Strikwerda 2018, p. 13-14.
[139] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365 (*Context-zaak*), r.o. 5.25-5.27; Lassche 2023, p. 12.
[140] Stol & Strikwerda 2018, p. 13-14.
[141] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 677-679; Klaar 2022, p. 2

inbreuk. Vervolgens wordt dit gedaan voor het juridisch kader dat geldt bij een meer dan geringe inbreuk.

5.3.1 Geringe inbreuk

Met betrekking tot de algemene taakstellende bevoegdheden is er in het gemoderniseerde WvSv niets veranderd. Artikel 141 en 142 WvSv zijn in het gemoderniseerde WvSv overgenomen in artikel 1.3.10 en 1.3.11.[142] In aanvulling hierop bevat het gemoderniseerde WvSv een nieuwe algemene bevoegdheidsbepaling, deze is te vinden in artikel 2.1.9 en luidt als volgt:

> "Opsporingsambtenaren zijn ter uitvoering van hun taak bevoegd om in overeenstemming met de geldende rechtsregels onderzoekshandelingen te verrichten."[143]

Dit artikel bouwt voort op de vaste rechtspraak inzake de ruimte die bestaat om opsporingshandelingen te verrichten zonder specifieke wettelijke basis.[144] Zoals uit het eerder besproken Zwolsman-arrest en de Context-zaak is gebleken, kunnen opsporingshandelingen die een geringe inbreuk op de privacy maken, gebaseerd worden op de algemene taakstellende artikelen.[145] Dit artikel expliciteert en codificeert dus als het ware wat in de rechtspraak al werd aangenomen op basis van de algemene taakstellende artikelen, namelijk dat bij de uitvoering van de opsporingstaak de nodige onderzoekshandelingen kunnen en mogen worden verricht. Artikel 2.1.9 heeft overigens geen gevolgen voor de mogelijkheden die artikel 3 Pw (en artikel 3 wet BOB) biedt. Onderzoekshandelingen die een geringe inbreuk op de privacy maken, kunnen zowel op artikel 3 Pw als op artikel 2.1.9 gemoderniseerde WvSv worden gebaseerd.[146]

5.3.2 Meer dan geringe inbreuk

De noodzaak om de huidige strafvorderlijke bevoegdheden uit te breiden is voortgekomen vanuit praktijkbehoeften en de nieuwe mogelijkheden die zijn ontstaan door technologische ontwikkelingen.[147] Persoonsgegevens uit publiek toegankelijke bronnen worden steeds vaker gebruikt voor de opsporing en vervolging van strafbare feiten. Door nieuwe technologieën vindt dit bovendien steeds sneller, geavanceerder en op grotere schaal plaats. Hierdoor ontstaat veel eerder een min of meer compleet beeld van bepaalde aspecten van iemands privéleven. Om die reden is het volgens de wetgever van belang dat er een specifieke wettelijke grondslag is met voldoende waarborgen die een transparante, zorgvuldige en

[142] *Kamerstukken II* 2022/23, 36327, nr. 2, p. 14.
[143] *Kamerstukken II* 2022/23, 36327, nr. 2, p. 47.
[144] Stevens & Koops 2021, p. 708.
[145] HR 19 december 1995, ECLI:NL:HR:1995:ZD0328 (*Zwolsman*), r.o. 6.4.5; Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365 (*Context-zaak*), r.o. 5.15.
[146] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 365-366.
[147] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 677.

afgewogen inzet verzekeren.[148] Artikel 2.8.8 (stelselmatig overnemen persoonsgegevens uit publiek toegankelijke bronnen) uit het gemoderniseerde WvSv voorziet daarin en luidt als volgt:

> "1. In geval van verdenking van een misdrijf kan de officier van justitie bevelen dat een opsporingsambtenaar stelselmatig, al dan niet op geautomatiseerde wijze, persoonsgegevens uit publiek toegankelijke bronnen overneemt.
> 2. Het bevel wordt gegeven voor een periode van ten hoogste drie maanden. De geldigheidsduur kan telkens voor een periode van ten hoogste drie maanden worden verlengd.
> 3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de geautomatiseerde wijze van overnemen van gegevens."[149]

Doordat een bevel van de officier van justitie is vereist, de bevoegdheid ten hoogste drie maanden kan worden ingezet (met mogelijkheid tot verlenging) en er bij algemene maatregel van bestuur (hierna: AMvB) regels gesteld worden over de geautomatiseerde wijze van overnemen, is de regeling volgens de wetgever voldoende precies en wordt een zorgvuldige toepassing gewaarborgd. Daarnaast kan de bevoegdheid alleen worden ingezet in het belang van het onderzoek en met inachtneming van het proportionaliteits- en subsidiariteitsbeginsel.[150] Het artikel vereist niet dat aan het 'verdachtebegrip' moet worden voldaan. Hierdoor kunnen niet alleen persoonsgegevens van de verdachte overgenomen worden, maar ook van andere personen.[151]

In de MvT wordt het artikel verder toegelicht en worden de verschillende leden en bestanddelen verduidelijkt. Vooral de begrippen 'publiek toegankelijke bronnen' en 'stelselmatig' worden uitgebreid behandeld. Hierbij zijn de meeste adviezen en aanbevelingen van de Commissie-Koops zorgvuldig meegenomen. Zoals al eerder vermeld worden hier relevante factoren voor de invulling van het begrip stelselmatigheid in de online context gegeven en uitgewerkt.[152] Een compleet overzicht van deze factoren is te vinden in Bijlage 1. De gehanteerde definitie van publiek toegankelijke bron in deze masterscriptie is gebaseerd op de MvT en het advies van de Commissie-Koops, waardoor de definities en reikwijdtes overeenkomen.

Wat opvalt is dat het door Commissie-Koops aanbevolen algemene normeringscriterium, een getrapt stelsel van toestemmingsvereisten, in dit artikel niet is terug te vinden, ook niet in de MvT. De Commissie-Koops heeft (met name om redenen van consistentie) een driedeling voor de normering van het overnemen van persoonsgegevens uit publiek toegankelijke bronnen voorgesteld. (1) Het niet-stelselmatig overnemen van persoonsgegevens vereist geen toestemming en kan dus uitgevoerd worden door een

[148] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 678.
[149] *Kamerstukken II* 2022/23, 36327, nr. 2, p. 108.
[150] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 678-679.
[151] Veen 2019, p. 401.
[152] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 677-686.

opsporingsambtenaar op basis van de algemene taakstelling. (2) Voor het stelselmatig overnemen van persoonsgegevens is een bevel van een officier van justitie vereist. (3) Voor het ingrijpend stelselmatig overnemen van persoonsgegevens is een machtiging van een rechter-commissaris vereist. Het overnemen is ingrijpend stelselmatig wanneer "op voorhand redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van een wezenlijk deel van iemands privéleven kan ontstaan (diep), dan wel een min of meer volledig beeld op verscheidene aspecten van iemands privéleven (breed)". De Commissie-Koops benadrukt wel dat ingrijpend stelselmatig bij deze bevoegdheid een uitzondering zal zijn, vanwege het publiek toegankelijke karakter van de persoonsgegevens. Dit betekent echter niet dat het uitgesloten kan worden, zeker niet gezien het grote aantal gegevens dat nu al, maar zeker over een aantal jaar, online te vinden is.[153] De derde stap in de driedeling, ingrijpend stelselmatig, is in het gemoderniseerde WvSv alleen terug te vinden bij het stelselmatig onderzoek van gegevens in een digitale-gegevensdrager of geautomatiseerd werk uit artikel 2.7.38.

Wanneer een opsporingsambtenaar twijfelt of het overnemen van persoonsgegevens uit publiek toegankelijke bronnen een stelselmatig karakter heeft en dus een meer dan geringe inbreuk maakt, ligt het volgens de MvT voor de hand om de bevoegdheid uit artikel 2.8.8 als grondslag te gebruiken en niet de algemene bevoegdheidsbepaling uit artikel 2.1.9.[154]

Tot slot geeft het gemoderniseerde WvSv ook een specifieke grondslag om in het kader van het verkennend onderzoek (thans geregeld in artikel 126gg WvSv) stelselmatig persoonsgegevens uit publiek toegankelijke bronnen over te nemen. Deze bevoegdheid is terug te vinden in artikel 2.9.1 lid 2 onderdeel a van het gemoderniseerde WvSv. In dit kader is wel een machtiging van een rechter-commissaris vereist.[155]

5.4 Tussenconclusie

Geconcludeerd kan worden dat online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek gebaseerd kan worden op zowel de Pw als het WvSv. Wanneer sprake is van een geringe inbreuk op de privacy kunnen opsporingsambtenaren online gegevens vergaren op grond van de taakstellende artikelen, te weten: artikel 3 Pw, artikel 3 Wet BOD of artikel 141 en 142 WvSv (en over een aantal jaar artikel 2.1.9 uit het gemoderniseerde WvSv).

Wanneer sprake is van een meer dan geringe inbreuk op de privacy is een bevel van de officier van justitie vereist voor stelselmatige observatie (artikel 126g WvSv) of stelselmatige informatie-inwinning (artikel 126j WvSv). Waarbij stelselmatige informatie-inwinning beschouwd wordt als de best passende bevoegdheid. Het gemoderniseerde WvSv introduceert een nieuw BOB-middel dat specifiek ziet op het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Zodra dit gemoderniseerde WvSv van

[153] Rapport Commissie-Koops 2018, p. 165-166.
[154] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 679.
[155] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 726; *Kamerstukken II* 2022/23, 36327, nr. 2, p. 115.

kracht is, kunnen opsporingsambtenaren na een bevel van de officier van justitie stelselmatig gegevens overnemen uit publiek toegankelijke bronnen op grond van artikel 2.8.8 gemoderniseerde WvSv.

Om te bepalen wanneer sprake is van een meer dan geringe inbreuk kunnen opsporingsambtenaren de (nieuwe) factoren voor stelselmatigheid en de leidraad bevoegdheden informatievergaring op internet raadplegen. Daarnaast dienen opsporingsambtenaren zich ook aan de algemene beginselen van gegevensverwerking en aan de overige eisen uit de Wpg te houden.

Voor online gegevensvergaring ten behoeve van opsporing bestaan dus meer en specifiekere regels dan op het gebied van intelligence, zeker met de komst van het gemoderniseerde WvSv. Bij een geringe inbreuk op de privacy zijn de juridische kaders vrijwel hetzelfde, maar zodra er sprake is van een meer dan geringe inbreuk verschillen de kaders aanzienlijk.

Hoofdstuk 6 – Online gegevensvergaring uit publiek toegankelijke bronnen door de inlichtingen- en veiligheidsdiensten

6.1 Inleiding

In dit hoofdstuk wordt het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door de inlichtingen- en veiligheidsdiensten, bestaande uit de AIVD en de MIVD, uiteengezet. De inlichtingen- en veiligheidsdiensten verzamelen inlichtingen met als doel het versterken van hun informatiepositie en het verkrijgen van inzicht in ernstige risico's en bedreigingen voor de nationale veiligheid. De AIVD houdt zich bezig met bedreigingen en ernstige risico's voor de samenleving en de MIVD richt zich op zaken die defensie raken. Ondanks de verschillende taken, hebben de diensten een vergelijkbare werkwijze en werken ze beide op grond van de Wiv. De Wiv normeert zowel de vergaring als de verdere verwerking van gegevens. Ambtenaren van de AIVD en de MIVD hebben ruime bevoegdheden ter bescherming van de nationale veiligheid, maar ze hebben geen opsporingsbevoegdheid zoals opsporingsambtenaren van de politie en de bijzonder opsporingsdiensten die wel hebben.[156]

Hoewel de diensten en opsporingsambtenaren zich in gescheiden sferen bevinden met eigen wettelijke taken en bevoegdheden, groeien hun werkzaamheden steeds meer naar elkaar toe doordat opsporingsambtenaren de laatste jaren ook meer proactief en informatie-gestuurd zijn gaan werken. De AIVD en de MIVD verzamelen al langer grote hoeveelheden informatie en hebben dus meer ervaring op het gebied van intelligence.[157] Hierdoor biedt de Wiv mogelijk waardevolle inzichten die kunnen bijdragen aan de verbetering van het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence. Zeker gezien het feit de Wiv al een aantal keer is herzien en onlangs nog is geëvalueerd.[158]

Het hoofdstuk zal beginnen met een uiteenzetting van het juridische kader. Hierbij wordt eerst ingegaan op het juridische kader dat geldt in geval van een geringe inbreuk en vervolgens op het juridisch kader dat geldt bij een meer dan geringe inbreuk. Daarna worden de algemene bepalingen omtrent gegevensverwerking besproken. Tot slot wordt ingegaan op het toezichtstelsel. Het hoofdstuk zal eindigen met een korte tussenconclusie.

6.2 Juridisch kader

De AIVD en de MIVD kunnen op grond van de Wiv online gegevens uit publiek toegankelijke bronnen vergaren. In tegenstelling tot de hiervoor besproken juridische kaders, bevat de Wiv wel artikelen die specifiek zien op gegevensvergaring uit publiek toegankelijke bronnen. Wanneer sprake is van een geringe inbreuk op de privacy kunnen gegevens uit publiek toegankelijke bronnen verzameld worden op grond artikel 25 Wiv. Wanneer sprake is van een meer dan geringe inbreuk kunnen stelselmatig gegevens uit publiek toegankelijke bronnen

[156] Fedorova e.a. 2022, p. 89.
[157] Fedorova e.a. 2022, p. 90.
[158] Fedorova e.a. 2022, p. 90.

verzameld worden op grond van artikel 38 Wiv.[159] In de volgende paragrafen zal dieper worden ingegaan op deze bevoegdheden.

In beide gevallen betreft het een algemene bevoegdheid. Dit houdt in dat gegevens uit publiek toegankelijke bronnen verwerkt kunnen worden voor elke taak van de AIVD en de MIVD. De taken zijn terug te vinden in respectievelijk artikel 8 en artikel 10 Wiv.[160] Een algemene bevoegdheid kent minder zware waarborgen dan een bijzondere bevoegdheid. De wetgever ziet gegevensvergaring uit publiek toegankelijke bronnen hier dus niet als een ernstige inbreuk op het recht van privacy.[161]

6.2.1 Geringe inbreuk

Artikel 25 Wiv geeft in algemene zin bevoegdheden aan de diensten om verschillende soorten gegevens te verzamelen.[162] In het eerste lid onder a wordt de bevoegdheid gegeven om gegevens uit voor een ieder toegankelijke informatiebronnen te verzamelen:

> "1. De diensten zijn, met inachtneming van het bepaalde bij of krachtens deze wet, in ieder geval bevoegd tot het verzamelen van gegevens:
> a. uit voor een ieder toegankelijke informatiebronnen"

In de Wiv wordt dus niet de term publiek toegankelijke bronnen gehanteerd, maar 'een voor een ieder toegankelijke informatiebron'. Volgens de MvT zijn dit "alle bronnen (traditionele media, internet e.d.) die zonder meer kunnen worden geraadpleegd en waarvoor geen drempels bestaan".[163] Uit de wetsgeschiedenis en de MvT blijkt dat dit ook bronnen omvat waarvoor registratie of betaling is vereist. Zo zijn de diensten bevoegd om een social media profiel aan te maken en gegevens uit publiek toegankelijke delen te verzamelen. Voor een nadere inkadering van een voor een ieder toegankelijke informatiebron moet volgens de Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten (hierna: CTIVD) aansluiting worden gezocht bij het gemoderniseerde WvSv.[164] Dit zorgt er dus voor dat de twee termen, publiek toegankelijke bronnen en een voor een ieder toegankelijke informatiebron, worden gelijkgesteld.

Het enige verschil is de grondslag voor het verzamelen van commercieel beschikbaar gestelde gegevens, waarbij men slechts tegen betaling toegang toe krijgt (zoals bijvoorbeeld gegevens van de Kamer van Koophandel). In de Wiv is dit geregeld in artikel 25 lid 1 sub b en valt het dus niet onder voor een ieder toegankelijke informatiebronnen, terwijl dit in het gemoderniseerde WvSv wel onder publiek toegankelijke bronnen valt. Desondanks heeft het

[159] Toezichtsrapport CTIVD 2021, p. 7-8.
[160] Toetsingskader CTIVD 2021, p. 4
[161] Toetsingskader CTIVD 2021, p. 7.
[162] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55.
[163] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38.
[164] Toetsingskader CTIVD 2021, p. 4-5.

verschil in wettelijke grondslag geen juridische consequenties, doordat zowel artikel 25 lid 1 sub a als sub b Wiv een algemene bevoegdheid betreft.[165]

Verder moet bij het verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen worden voldaan aan de vereisten van proportionaliteit, subsidiariteit en gerichtheid uit artikel 26 Wiv. Deze eisen gelden expliciet voor deze vorm van gegevensverzameling naast de algemene normen van gegevensverwerking (die in paragraaf 6.2.3 worden besproken).[166]

Artikel 25 Wiv geeft dus een specifieke grondslag voor het vergaren van gegevens uit publiek toegankelijke bronnen voor zover dit niet leidt tot een meer dan geringe inbreuk op de privacy. Hiermee is voldaan aan de wens uit de Privacy Impact Assessment (Hierna: PIA) die is uitgevoerd op de Wiv om vanuit het oogpunt van kenbaarheid en voorzienbaarheid een specifieke grondslag te creëren voor gegevensverwerking uit publiek toegankelijke bronnen. Dit is veel duidelijker voor burgers dan wanneer zij een impliciete bevoegdheid moeten afleiden uit de algemene taakstelling van de diensten, zoals beschreven in artikel 8 en 10 Wiv.[167] De AIVD en de MIVD hoeven dus niet net zoals opsporingsambtenaren te werken op grond van de taakstellende artikelen.

6.2.2 Meer dan geringe inbreuk

Het onderscheid tussen gegevensverzameling uit publiek toegankelijke bronnen en stelselmatige gegevensverzameling uit publiek toegankelijke bronnen in de Wiv is ontstaan naar aanleiding van de PIA die is uitgevoerd op de Wiv. Daar werd benadrukt dat bij stelselmatige gegevensverzameling uit publiek toegankelijke bronnen een meer dan geringe inbreuk op de privacy kan plaatsvinden en dus nader genormeerd dient te worden.[168] Artikel 38 Wiv bevat daarom een bevoegdheid om stelselmatig gegevens uit voor een ieder toegankelijke informatiebronnen te verzamelen. Dit artikel luidt als volgt:

> "1. De diensten zijn bevoegd tot het al dan niet met gebruikmaking van een technisch hulpmiddel stelselmatig verzamelen van gegevens omtrent personen uit voor een ieder toegankelijke informatiebronnen.
> 2. De uitoefening van de bevoegdheid, bedoeld in het eerste lid, is slechts toegestaan, indien Onze betrokken Minister of namens deze het hoofd van een dienst daarvoor toestemming heeft verleend. Het hoofd van een dienst kan aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die de toestemming, bedoeld in de eerste volzin, namens hem verlenen. Onze betrokken Minister wordt een afschrift van het besluit, bedoeld in de tweede volzin, gezonden. Artikel 29 is van overeenkomstige toepassing."

[165] Toetsingskader CTIVD 2021, p. 6; *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38.
[166] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55.
[167] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55.
[168] Toezichtsrapport CTIVD 2021, p. 8; Oerlemans & Hagens 2018, p. 137

De term stelselmatig wordt noch in de MvT noch in de wetsgeschiedenis van de Wiv verder toegelicht of gedefinieerd. Voor de invulling van de term stelselmatig wordt daarom door de CTIVD aansluiting gezocht bij het stelselmatigheidscriterium uit de strafvorderlijke context. Het gaat hier dus weer om de vraag of op voorhand redelijkerwijs voorzienbaar is dat een "min of meer compleet beeld van een of meer aspecten van het persoonlijk leven" ontstaat.[169] In Bijlage 1 is een compleet overzicht te vinden van de relevante factoren voor de invulling van het begrip stelselmatigheid in de online context. Deze factoren kunnen ook bijdragen aan de invulling van het stelselmatigheidscriterium in de Wiv.[170]

Uit het tweede lid volgt dat voor de inzet van de bevoegdheid toestemming is vereist van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Defensie of het hoofd van een van de diensten. Het hoofd van de AIVD of de MIVD kan het geven van toestemming echter ook mandateren aan medewerkers.[171] Hierdoor rijst de vraag of de vereiste toestemming werkelijk bijdraagt aan een verbeterde rechtsbescherming. Verder is artikel 29 Wiv van overeenkomstige toepassing. Hieruit volgt dat de bevoegdheid wordt verleend voor ten hoogste drie maanden (met mogelijkheid tot verlenging).

Verder moet ook bij het stelselmatig verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen worden voldaan aan de vereisten van proportionaliteit, subsidiariteit en gerichtheid uit artikel 26 Wiv.[172]

Ook het stelselmatig verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen betreft dus een algemene bevoegdheid. In de PIA die is uitgevoerd op de Wiv is echter aangeraden om er een bijzondere bevoegdheid van te maken, vanwege de grotere privacyinbreuk die kan plaatsvinden. De wetgever heeft hier desondanks geen gehoor aan gegeven, omdat het dan niet mogelijk zou zijn om de bevoegdheid uit te voeren in het kader van bijvoorbeeld veiligheidsonderzoeken en dreigings- en risicoanalyses. Bijzondere bevoegdheden zijn slechts mogelijk bij een beperkt aantal taken van de diensten, dit blijkt uit artikel 28 Wiv.[173] Doordat het nu een algemene bevoegdheid betreft, is het mogelijk om gegevens te verzamelen uit voor een ieder toegankelijke informatiebronnen in het kader van alle taken van de diensten (en niet slechts de taken als bedoeld in artikel 28).[174] De Wiv verschilt op dit punt dus van het (gemoderniseerde) WvSv, waar het stelselmatig overnemen

[169] Toetsingskader CTIVD 2021, p. 8.
[170] Toetsingskader CTIVD 2021, p. 9.
[171] Toetsingskader CTIVD 2021, p. 8.
[172] Toetsingskader CTIVD 2021, p. 8.
[173] De AIVD kan bijzondere bevoegdheden uitoefenen bij het verrichten van onderzoek m.b.t. organisaties en personen die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat en bij het verrichten van onderzoek betreffende andere landen. De MIVD kan kort gezegd bijzondere bevoegdheden uitoefenen bij het verrichten van onderzoek ten aanzien van onderwerpen met een militaire relevantie.
[174] Oerlemans & Hagens 2018, p. 137; *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55.

van persoonsgegevens uit publiek toegankelijke bronnen wel onder de bijzondere bevoegdheden valt.

Evenwel wordt met artikel 38 Wiv de bevoegdheid expliciet gemaakt en zo dus de kenbaarheid en de voorzienbaarheid van de bevoegdheden van de diensten vergroot. Daarnaast zijn belangrijke elementen van het normeringskader voor bijzondere bevoegdheden al van toepassing op het stelselmatig verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen, zoals de eisen van proportionaliteit en subsidiariteit uit artikel 26 Wiv en de vereiste toestemming uit het tweede lid van artikel 38 Wiv.[175]

6.2.3 Algemene bepalingen gegevensverwerking

Net zoals opsporingsambtenaren moeten ook de diensten zich bij het verzamelen van gegevens uit publiek toegankelijke bronnen houden aan algemene beginselen van gegevensverwerking. Hoofdstuk 3 van de Wiv ziet op de gegevensverwerking door de AIVD en de MIVD, dit hoofdstuk bevat ook de hierboven besproken artikelen 25 en 38. De verwerking van gegevens is dus geregeld in dezelfde wet en niet zoals bij opsporingsambtenaren in een aparte wet, te weten de Wpg.

Uit artikel 1 onderdeel f Wiv volgt de definitie van gegevensverwerking. Hieruit blijkt dat “elke handeling of geheel van handelingen met betrekking tot gegevens” valt onder de verwerking van gegevens, waaronder ook het verzamelen van gegevens. De verwerking van gegevens wordt net zoals in de Wpg, vooral genormeerd door de algemene beginselen van gegevensverwerking. Zo volgt uit artikel 18 Wiv het noodzakelijkheidsbeginsel, het doelbindingsbeginsel en dat de gegevensverwerking op ‘behoorlijke en zorgvuldige’ wijze moet plaatsvinden.[176] Daarnaast mogen gevoelige gegevens op grond van artikel 19 Wiv alleen onder strikte voorwaarden verwerkt worden. Slechts “in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is”. Gevoelige gegevens worden in het derde lid gedefinieerd als: persoonsgegevens over “iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven”. Dit komt dus overeen met de bijzondere persoonsgegevens uit de Wpg. Verder blijkt uit artikel 20 Wiv dat gegevens moeten worden verwijderd zodra ze geen betekenis meer hebben, gelet op het doel waarvoor ze zijn verwerkt. Tot slot hebben de hoofden van de diensten een zorgplicht voor de gegevensverwerking en de geheimhouding van gegevens, bronnen en medewerkers (artikel 23 en 24 Wiv).[177]

6.2.4 Toezichtstelsel

De diensten kennen een uitgebreid stelsel van toezicht en controle. Het niet-parlementaire toezicht op de AIVD en de MIVD is toegewezen aan twee onafhankelijke instanties, te weten de CTIVD en de Toetsingscommissie Inzet Bevoegdheden (hierna: TIB). Zij toetsen en

[175] Oerlemans & Hagens 2018, p. 137; *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55.
[176] Toetsingskader CTIVD 2021, p. 12; Fedorova e.a. 2022, p. 95.
[177] Toetsingskader CTIVD 2021, p. 12-13.

controleren de inzet van (bijzondere) bevoegdheden op meerdere momenten.[178] De wetgever heeft er bewust voor gekozen om het toezicht te verdelen over twee instanties, zodat het geen afbreuk doet aan de onafhankelijkheid van de toetsing.[179]

De TIB beoordeelt of de toestemming van de minister voor de inzet van specifieke bijzondere bevoegdheden rechtmatig is. Deze toetsing vindt plaats voorafgaand aan de inzet (ex ante) en heeft een bindend oordeel.[180] Nu het verzamelen van gegevens uit publiek toegankelijke bronnen in de Wiv algemene bevoegdheden betreft, vindt hierbij dus geen controle plaats door de TIB.

De CTIVD houdt toezicht tijdens de inzet van bevoegdheden (ex durante) en na afloop van de inzet (ex post). Daarnaast houdt de CTIVD ook toezicht op andere werkzaamheden van de diensten en heeft het naast de afdeling toezicht ook een afdeling klachtenbehandeling. De oordelen over de klachten zijn bindend, maar de oordelen in verband met de toezichtstaak zijn niet bindend.[181] Ter uitoefening van de toezichtstaak heeft de CTIVD vergaande bevoegdheden. Zo is iedereen verplicht om medewerking te verlenen aan onderzoeken. Uit het rapport van de evaluatiecommissie is gebleken dat de CTIVD zich de afgelopen jaren meer heeft gericht op het uitoefenen van dynamisch toezicht (ex durante). Hierbij wordt zoveel mogelijk geprobeerd om real-time mee te kijken met specifieke handelingen.[182]

Over de huidige inrichting van het toezichtstelsel bestaat veel discussie. Deze discussie staat nauw in verband met de normering zelf en kan dan ook niet los daarvan worden beschouwd. Het is moeilijk om de juiste balans te vinden tussen aan de ene kant normering en toetsing vooraf en aan de andere kant toezicht tijdens en achteraf.[183] Toch laat de ervaring met de Wiv zien dat een statische toets vooraf (ex ante) niet optimaal is voor het dynamische proces van gegevensverwerking ten behoeve van intelligence. De wetgever streeft in een nieuw voorgestelde regeling dan ook naar een versterking van het toezicht tijdens (ex durante) en achteraf (ex post) door de CTIVD.[184] Dit betekent echter niet dat het toezicht vooraf geheel kan komen te vervallen. De evaluatiecommissie beschouwt de voorafgaande toetsing door de TIB als een aanzienlijke meerwaarde. Dit zorgt ervoor dat de diensten scherp blijven bij de inzet van bijzondere bevoegdheden en dat er meer wordt nagedacht over de aanvraag voor de inzet van een bijzondere bevoegdheid.[185]

Het toezicht op de gegevensverwerking van de politie en bijzondere opsporingsdiensten is zeer beperkt in vergelijking met het uitgebreide toezichtstelsel in de Wiv. Dit kan deels gerechtvaardigd worden doordat de AIVD en de MIVD ingrijpendere bevoegdheden hebben dan opsporingsambtenaren. Daarnaast kennen de AIVD en de MIVD

[178] Fedorova e.a. 2022, p. 108.
[179] Fedorova e.a. 2022, p. 110.
[180] Fedorova e.a. 2022, p. 109; 'Toetsing, toezicht en controle', AIVD.nl.
[181] Fedorova e.a. 2022, p. 108. 'Toetsing, toezicht en controle', AIVD.nl.
[182] Fedorova e.a. 2022, p. 109. 'Toetsing, toezicht en controle', AIVD.nl.
[183] Fedorova e.a. 2022, p. 110-112.
[184] Fedorova e.a. 2022, p. 110-115.
[185] Federova e.a. 2022, p. 109-110.

geen rechterlijke toetsing achteraf.[186] Mogelijk komt dit uitgebreide systeem van toezicht, dat ook vooral toezicht houdt tijdens de inzet (ex durante), de politie en de bijzondere opsporingsdiensten ook ten goede. Zeker nu zij steeds pro-actiever gaan werken. Zo kan de privacy van (onschuldige) burgers doorlopend gewaarborgd worden en niet slechts vooraf of achteraf.

6.3 Tussenconclusie

Geconcludeerd kan worden dat de AIVD en de MIVD op grond van de Wiv online gegevens uit publiek toegankelijke bronnen kunnen vergaren. De Wiv kent twee algemene bevoegdheden die specifiek zien op gegevensvergaring uit publiek toegankelijke bronnen. Bij een geringe inbreuk op de privacy kunnen gegevens verzameld worden op grond artikel 25 Wiv en bij een meer dan geringe inbreuk kunnen na toestemming stelselmatig gegevens verzameld worden op grond van artikel 38 Wiv. Stelselmatigheid heeft hier dezelfde betekenis als het stelselmatigheidscriterium uit de strafvorderlijke context. De diensten moeten zich bij het verzamelen van gegevens uit publiek toegankelijke bronnen ook houden aan de algemene bepalingen omtrent gegevensverwerking die eveneens te vinden zijn in de Wiv.

Verder kennen de diensten een uitgebreid stelsel van toezicht en controle. De TIB toetst vooraf de inzet van specifieke bijzondere bevoegdheden en de CTIVD houdt toezicht tijdens de inzet van bevoegdheden en na afloop. Een statische toets vooraf blijkt niet optimaal voor het dynamische proces van gegevensverwerking ten behoeve van intelligence. Er wordt nu meer gefocust op versterking van het toezicht tijdens en achteraf.

In tegenstelling tot opsporingsambtenaren, kennen de diensten dus wel specifieke bevoegdheden om online gegevens te vergaren uit publiek toegankelijke bronnen. Daarnaast is het systeem van toezicht veel uitgebreider dan bij opsporingsambtenaren. Zo wordt ook tijdens de inzet van bevoegdheden toezicht gehouden op de diensten. Bovendien is alles geregeld in één wet. De Wiv normeert zowel de vergaring als de (verdere) verwerking van gegevens.

[186] Fedorova e.a. 2022, p. 115.

Hoofdstuk 7 – Suggesties voor verbeteringen van het huidige juridische kader

7.1 Inleiding

In dit hoofdstuk wordt gekeken in welk opzicht het huidige juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence verbeterd zou moeten worden. Aan de hand van de juridische kaders voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek en door de inlichtingen- en veiligheidsdiensten (respectievelijk hoofdstuk 5 en 6), worden een aantal suggesties gedaan ter verbetering van de knelpunten van het huidige juridische kader voor opsporingsambtenaren op het gebied van intelligence (hoofdstuk 4). Dit geschiedt uiteraard met inachtneming van de eisen en waarborgen die het EHRM heeft gesteld aan online gegevensvergaring uit publiek toegankelijke bronnen (hoofdstuk 2). Daarnaast worden ook de praktijkervaringen en de door respondenten aangedragen oplossingen meegenomen.

Dit hoofdstuk zal per behandeld knelpunt suggesties geven ter verbetering van het betreffende knelpunt. Achtereenvolgens worden dus suggesties gegeven ter verbetering van: de onduidelijkheid over de reikwijdte van artikel 3, de onduidelijkheid ten aanzien van gezagsdragers, het externe toezicht op de Wpg en het onderscheid tussen intelligence en het opsporingsonderzoek.

7.2 Onduidelijkheid over artikel 3 Pw

Het eerste knelpunt van het huidige juridische kader ging over de onduidelijkheid van artikel 3 Pw en de bijbehorende grens van een meer dan geringe inbreuk. De reikwijdte van dit artikel wordt verschillend geïnterpreteerd en leidt daarmee tot discussies over de rechtmatigheid.[187] Dit knelpunt kan opgelost worden door artikel 3 Pw nader te duiden. Dit kan op verschillende manieren worden gerealiseerd.

Allereerst zou de rechter meer helderheid kunnen verschaffen over de reikwijdte van artikel 3 Pw. Dit kan door duidelijk aan te geven onder welke omstandigheden opsporingshandelingen, waaronder dus online gegevensvergaring uit publiek toegankelijke bronnen, zijn toegestaan op grond van artikel 3 Pw. Een meer algemene benadering in plaats van een casuïstische benadering heeft hierbij de voorkeur.[188]

Eén respondent geeft aan dat op dit moment ook wordt geprobeerd dit te bewerkstelligen. Zo zijn er proefprocessen gestart die specifiek gaan over de reikwijdte van artikel 3 Pw met betrekking tot publiek toegankelijke bronnen. Van één proefproces is onlangs een uitspraak verschenen. Deze zaak betrof een mensenhandel zaak uit Oost-Nederland, waarin is gepoogd om de inzet van webcrawling technologie onder artikel 3 Pw getoetst te

[187] Groothuis & Landman 2022, p. 134; Oerlemans 2018, p. 4.
[188] Borgers 2015, p. 150.

krijgen. Het OM had de rechtbank specifiek gevraagd om zich uit te spreken over de juridische basis van de toepassing van de webcrawler (en de rechtmatigheid van het hierdoor verkregen bewijs). De Rechtbank Overijssel heeft echter geoordeeld dat er in deze zaak geen wettelijke basis bestond om zich uit te laten over de rechtmatigheid van de inzet van de webcrawler. Dit komt doordat het "redelijk vermoeden van schuld niet is gebaseerd op informatie die is verkregen met de webcrawltechniek en de rechtbank de met behulp van deze techniek verkregen informatie evenmin voor het bewijs zal bezigen".[189] Het OM is hierop in hoger beroep gegaan in de hoop dat het gerechtshof hier wel een oordeel over gaat vellen.

De rechter kan echter slechts in beperkte mate bijdragen aan het specifiek afbakenen van de voorwaarden waaronder opsporingshandelingen kunnen worden gebaseerd op artikel 3 Pw. Dit is ook niet primair de verantwoordelijkheid van de rechter. Het is aan de wetgever om de grenzen te bepalen. De wetgever is ook beter uitgerust om algemene voorwaarden te formuleren waaronder opsporingshandelingen kunnen worden gebaseerd op artikel 3 Pw.[190]

Naast de rechter kan dus ook de wetgever meer helderheid verschaffen over de reikwijdte van artikel 3 Pw en de bijbehorende grens van een meer dan geringe inbreuk. De wetgever zou dit op verschillende manieren kunnen verduidelijken.

Ten eerste zou de wetgever een specifieker artikel kunnen toevoegen aan de Pw dat de bevoegdheid geeft om (voor zo ver dit een geringe inbreuk betreft) online gegevens uit publiek toegankelijke bronnen te vergaren. Hierbij kan een voorbeeld worden genomen aan de nieuwe algemene bevoegdheidsbepaling in artikel 2.1.9 uit het gemoderniseerde WvSv. Dit artikel geeft opsporingsambtenaren de bevoegdheid om onderzoekshandelingen te verrichten ter uitvoering van hun taak. Indien een dergelijke algemene bevoegdheidsbepaling ook wordt opgenomen in de Pw ten behoeve van intelligence, hoeft de bevoegdheid om opsporingshandelingen te verrichten niet langer indirect afgeleid te worden uit het taakstellend artikel 3 Pw. Dit verduidelijkt dat de bevoegdheid om onderzoekshandelingen te verrichten niet beperkt is tot de handelingen waarvoor een specifieke wettelijke grondslag bestaat. [191]

Een dergelijke bepaling creëert duidelijkheid, maar beantwoordt nog steeds niet de vraag welke opsporingshandelingen zijn toegelaten.[192] Om deze vraag te beantwoorden, zou de Pw een vergelijkbare bepaling als artikel 25 uit de Wiv moeten bevatten. Dit artikel bevat een algemene bevoegdheid om verschillende soorten gegevens te verzamelen, waaronder gegevens uit publiek toegankelijke bronnen. Ondanks dat dit in de praktijk misschien niet voor veel verandering zorgt, maakt dit het wel meer kenbaar en voorzienbaar voor burgers.

Ten tweede kan de wetgever ook meer duidelijkheid verschaffen zonder een specifiek wettelijke grondslag toe te voegen, maar door een uitgebreide en richtinggevende MvT op te

[189] Rb. Overijssel 5 april 2022, ECLI:NL:RBOVE:2022:900, r.o. 4.3.
[190] Borgers 2015, p. 150-151.
[191] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 366.
[192] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 366.

stellen. Het gemoderniseerde WvSv heeft ook een redelijk uitgebreide en richtinggevende MvT, zie bijvoorbeeld de uitwerking van de relevante factoren voor de invulling van het begrip stelselmatigheid in de online context (Bijlage 1).

De MvT zou bijvoorbeeld uitleg kunnen bevatten over het doel van artikel 3 Pw, wat de voornaamste afweging moet zijn bij de interpretatie ervan en concrete voorbeelden benoemen die er in ieder geval wel of niet onder vallen.[193] Eén respondent geeft aan dat het hierbij ook van belang is dat dit niet alleen gericht is op algemene opsporing door de politie (wat nu vaak het geval is), maar juist ook op bijzondere opsporingsambtenaren en andere doeleinden.

Tot slot geeft één respondent nog aan dat er misschien een tussengelegen artikel kan komen. Nu moet bij de grondslag voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek gekozen worden tussen twee uitersten, namelijk de taakstellende artikelen of een bijzondere opsporingsbevoegdheid zoals stelselmatige observatie of stelselmatige informatie-inwinning. Hiertussen zit een groot grijs gebied, waardoor vaak twee kanten op geredeneerd kan worden. Nu BOB-middelen niet louter ingezet mogen worden voor intelligencedoeleinden, valt er op het gebied van intelligence niet te kiezen. Desondanks zou een tussengelegen artikel ook voor intelligencedoeleinden een uitkomst kunnen bieden (zolang dit geen BOB-middel betreft). De wetgever zou dus ook kunnen overwegen om voor intelligencedoeleinden een artikel tot stand te brengen dat de bevoegdheid geeft aan opsporingsambtenaren om ook bij een meer dan beperkte inbreuk op de privacy persoonsgegevens uit publiek toegankelijke bronnen te vergaren. In lijn met het gedachtegoed van het EHRM zou dit artikel gedetailleerder moeten zijn dan de hiervoor besproken artikelen bij een geringe inbreuk.

De vraag is echter in hoeverre dit wenselijk en noodzakelijk is. Ongeacht de vraag of dit wenselijk is in verband met mogelijke privacy zorgen, lijkt een specifieke wettelijke basis die hierop ziet niet noodzakelijk. Volgens Gritter is bij het ongericht vergaren van onlinegegevens uit publiek toegankelijke bronnen geen sprake van een meer dan beperkte inbreuk op de privacy (mits dit niet neerkomt op stelselmatige observatie van specifieke personen).[194] Ook niet indien er veel gegevens automatisch vergaard worden over mogelijk onschuldige personen. Volgens hem zit een inbreuk op de informationele privacy ‘ingebakken’ in de politie- of opsporingstaak, in verband met de noodzaak om een goede informatiepositie te kunnen opbouwen.[195] De bevestiging of dit daadwerkelijk onder artikel 3 Pw kan vallen, kan pas met zekerheid worden gegeven na de uitspraken van de proefprocessen. Indien artikel 3 geen voldoende grondslag biedt, lijkt een tussengelegen artikel een mogelijk geschikte oplossing.

[193] Stevens & Koops 2021, p. 711.
[194] Gritter 2018, p. 114-115.
[195] Gritter 2018, p. 114-115.

De laatste mogelijkheid om artikel 3 Pw nader te duiden, bevindt zich tussen de rechtspraak en de wetgevingspraktijk, namelijk de AMvB. Door middel van een AMvB kunnen algemene regels opgesteld worden in overleg met relevante adviesorganen.[196] Dit zou gerealiseerd kunnen worden door in de wet vast te leggen dat bij AMvB nadere regels gesteld kunnen worden over de invulling van de politietaak.[197]

Hoewel Borgers pleit om 'lichte opsporingshandelingen' (opsporingshandelingen die een geringe inbreuk op de privacy maken) te normeren door middel van de AMvB, stelt de MvT bij het gemoderniseerde WvSv dat deze benadering niet de voorkeur heeft.[198] Ten eerste is het ook door middel van AMvB's niet mogelijk om alle (lichte) opsporingshandelingen uitputtend te reguleren. Ten tweede heeft het de voorkeur om, naast de algemene bevoegdheidsbepaling, een specifieke bepaling op te nemen die ziet op een meer dan geringe inbreuk. Zodat bij twijfel de specifieke bepaling als grondslag gebuikt kan worden.[199] Dit laatste argument ziet dus niet op lichte opsporingshandelingen, waardoor dit argument niet opgaat voor online gegevensvergaring uit publiek toegankelijke bronnen.

Een combinatie van algemene taakstellende artikelen met een AMvB is een sterkere grondslag dan alleen de algemene taakstellende artikelen, maar zwakker dan een specifieke grondslag in een wet in formele zin.[200] Het is echter niet mogelijk om alle onderzoekshandelingen van een specifieke wettelijke basis te voorzien. Bij de keuze voor de oplossing van dit knelpunt is een goede combinatie van rechtszekerheid en toekomstbestendigheid van belang.[201] Daarnaast moeten ook de voorwaarden van het EHRM waaraan een wettelijke grondslag dient te voldoen in acht genomen worden.

7.3 Onduidelijkheid ten aanzien van gezagsdragers

Het tweede knelpunt van het huidige juridische kader ging over de onduidelijkheid ten aanzien van gezagsdragers. Het is soms onduidelijk of de officier van justitie of de burgemeester het gezag uitoefent bij online gegevensvergaring in het kader van intelligence.[202] Daarnaast heerst de vraag of een burgemeesters überhaupt geschikt is als gezagdrager van online gegevensvergaring in het kader van de openbare orde intelligence. [203]

Ondanks het feit dat een officier van justitie vaak meer afweet van online gegevensvergaring in het kader van openbare orde intelligence en bovendien niet gebonden is aan gemeentegrenzen, moet op grond van artikel 11 Pw geconcludeerd worden dat de

[196] Borgers 2015, p. 151.
[197] Borgers 2015, p. 154.
[198] Borgers 2015, p. 151-155.
[199] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 367-368.
[200] Borgers 2015, p. 152.
[201] Stevens & Koops 2021, p. 710.
[202] Groothuis & Landman 2022, p. 34 & 75;
[203] Bantema e.a. 2018, p. 85-92.

burgemeester het gezag uitoefent over de handhaving van de openbare orde.[204] Ook volgens Groothuis en Landman lijkt de burgemeester de meest waarschijnlijke optie.[205] Het is dan wel van belang dat de burgemeester zijn rol ook gaat erkennen en meer kennis over openbare orde intelligence opdoet. Bovendien moeten de praktische consequenties verduidelijkt worden, het internet en openbare orde intelligence kennen immers vaak geen grenzen.[206]

Daarnaast moet rekening gehouden worden met het feit dat intelligence (waaronder dus ook openbare orde intelligence) en opsporingsactiviteiten in elkaar kunnen overlopen. Indien dit het geval is, gaat het gezag dus van de burgemeester over op de officier van justitie.[207] Wanneer dit precies het geval is, valt vaak niet duidelijk te bepalen. Het opsporingsonderzoek kent geen duidelijk startpunt. Dit kan de wetgever oplossen door het opsporingsbegrip zo te formuleren dat het een duidelijker startpunt bevat. In paragraaf 5 van dit hoofdstuk wordt dieper ingegaan op dit onderwerp.

Verder bleek uit dit knelpunt dat de controle en het toezicht van de burgemeesters op het TOOI beter georganiseerd moet worden. Momenteel is er een leemte in de wet- en regelgeving voor het werk van het TOOI.[208] In de praktijk worden bij het TOOI landelijke werkafspraken gemodelleerd naar de regelgeving en werkafspraken van het Team Criminele Inlichtingen (hierna: TCI).[209] Het TCI is ook een onderdeel van de politie dat heimelijk informatie vergaart, maar dan met betrekking tot zware en georganiseerde misdaad. Dit gebeurt dus ook niet onder het gezag van een burgemeester maar onder het gezag van een (TCI) officier van justitie.[210] Het TCI kent wel wet- en regelgeving voor de inzet van bevoegdheden en de controle hierop.

Op dit moment wordt onder leiding van de landelijke portefeuillehouder intelligence gewerkt aan voorstellen om de rol van de burgemeester nadrukkelijker te positioneren, vooral met het doel om het toezicht op het TOOI te versterken.[211] Hierbij zou dus een voorbeeld genomen kunnen worden aan de wet- en regelgeving die al bestaat over het TCI.

7.4 Extern toezicht Wpg

Het derde knelpunt van het huidige juridische kader had te maken met het externe toezicht op de Wpg. Op dit moment oefent de AP geen effectief toezicht uit op naleving van de Wpg, terwijl dit juist in het geval van intelligence heel belangrijk is.[212] Een objectieve en toezichthoudende autoriteit is bovendien een van de voorwaarden van het EHRM waaraan de

[204] Bantema e.a. 2018, p. 86-92.
[205] Groothuis & Landman 2022, p. 129
[206] Groothuis & Landman 2022, p. 135.
[207] Groothuis & Landman 2022, p. 76.
[208] Van der Plas & Brown 2017, p. 181.
[209] Van der Plas & Brown 2017, p. 181.
[210] Van der Plas & Brown 2017, p. 180.
[211] Van der Plas & Brown 2017, p. 181.
[212] Fedorova e.a. 2022, p. 168; Hirsch Ballin & Oerlemans 2023, p. 34; Winter e.a. 2020, p. 26.

wettelijke grondslag moet voldoen. Dit knelpunt kan opgelost worden door het toezicht- en controlestelsel te herinrichten.

Dit zou gerealiseerd kunnen worden door een nieuw gespecialiseerd en onafhankelijk toezichtsorgaan op te richten dat ook vooral tijdens de inzet van digitale opsporingsbevoegdheden meekijkt en indien nodig kan ingrijpen.[213] Hierbij kan een voorbeeld worden genomen aan het uitgebreide stelsel van controle en toezicht dat de AIVD en de MIVD kennen. De CTIVD functioneert daar ook als een gespecialiseerd en onafhankelijk toezichtsorgaan dat toezicht houdt tijdens de inzet van bevoegdheden en na afloop van de inzet.

In de interviews is ook de wens geuit voor een externe toezichthouder en dan bij voorkeur niet de AP maar een orgaan met opsporingservaring. Eén respondent stelt voor dat dit toezichtsorgaan bijvoorbeeld kan worden samengesteld uit voormalige rechters of officieren met een expertise op dit onderwerp. De CTIVD kent ook een brede juridische basis, maar beschikt daarnaast over andere expertises. Zo is een technische expertise van belang om nieuwe technologische ontwikkelingen en mogelijkheden te doorgronden. Maar ook operationele expertise is noodzakelijk.[214] Daarnaast is het volgens de respondent ook van belang dat het toezichtsorgaan in het begin niet alleen toezicht houdt en handhaaft, maar ook actief meedenkt en helpt om het proces te verbeteren. Een gespecialiseerd toezichtsorgaan kan bovendien aan normprecisering doen.[215] Zeker voor online gegevensvergaring uit publiek toegankelijke bronnen op het gebied van intelligence lijkt dit gewenst, nu dit juridische kader veel grijze gebieden kent.

Een nieuw toezichtsorgaan zorgt echter voor verdere fragmentatie, doordat er al verschillende toezichtsorganen actief zijn. Indien dit goed wordt afgestemd, hoeft dit niet als een groot nadeel te worden beschouwd.[216] Bovendien zou het nieuwe toezichtsorgaan de AP kunnen vervangen voor wat betreft het toezicht op naleving van de Wpg. Hierdoor heeft de AP ook meer tijd om haar andere taken uit te voeren.

7.5 Het onderscheid tussen intelligence en het opsporingsonderzoek

Het laatste knelpunt betrof het onderscheid tussen intelligence en het opsporingsonderzoek. Ten eerste is het soms onduidelijk voor opsporingsambtenaren of zij zich in de intelligencefase of in het opsporingsonderzoek bevinden. Intelligence wordt überhaupt niet in de wet gedefinieerd en het opsporingsbegrip uit artikel 132a WvSv voorziet niet in een duidelijk startpunt vanaf welk moment het onderzoek als opsporing moet worden beschouwd.[217]

Dit knelpunt kan worden opgelost door het opsporingsbegrip zo te formuleren dat het een duidelijker startpunt bevat. Zo wordt het niet alleen voor opsporingsambtenaren maar

[213] Fedorova e.a. 2022, p. 171; Hirsch Ballin & Oerlemans 2023, p. 36.
[214] Jaarverslag CTIVD 2022, p. 16.
[215] Federova e.a. 2022, p. 169.
[216] Federova e.a. 2022, p. 169.
[217] Crijns e.a. 2021, p. 143; Hirsch Ballin 2022, p. 21.

ook voor de burgers meer kenbaar en voorzienbaar. Ook Crijns e.a. zijn van mening dat het opsporingsbegrip te weinig richting geeft en stellen een nieuw opsporingsbegrip voor.[218] Volgens hen begint het opsporingsonderzoek zodra één of meer bepaalde personen onderwerp van het onderzoek worden vanwege hun mogelijke betrokkenheid bij een strafbaar feit. Hierdoor komt de nadruk meer te liggen op de vraag wat opsporing is in plaats van waar het toe dient. Dit betekent echter niet dat er sprake moet zijn van een verdenking. Het gaat erom dat het onderzoek zich richt op bepaalde personen (in plaats van dat het ongericht wordt uitgevoerd op een onbepaalde groep). De vraag waarom, zoals in het klassieke opsporingsbegrip waar de verdenking centraal stond, is hierbij niet van belang.[219]

Een nieuwe definitie van het opsporingsonderzoek zou volgens Crijns e.a. als volgt kunnen luiden:

> "Opsporing is onderzoek door ambtenaren met opsporing belast dat zich richt op één of meer bepaalde personen in verband met hun mogelijke betrokkenheid bij een strafbaar feit met als doel het nemen van strafvorderlijke beslissingen."[220]

Een kanttekening die hierbij geplaatst moet worden, is dat Crijns e.a. met deze formulering van het opsporingsbegrip het onderscheid tussen opsporing en bestuurlijk toezicht proberen te verduidelijken. Toezicht is iets anders dan intelligence, maar volgens Crijns e.a. ligt de essentie van het onderscheid tussen opsporing en toezicht in het feit dat opsporing gericht is en toezicht ongericht is.[221] Beargumenteerd zou kunnen worden dat dit ook het geval is bij het onderscheid tussen opsporing en intelligence. Online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van intelligence is immers niet gericht op waarheidsvinding en het verzamelen van bewijs tegen bepaalde personen om vervolgens strafvorderlijke beslissingen te nemen. Maar op het opbouwen van een informatiepositie om zo inzicht te verkrijgen in trends en ontwikkelingen ten aanzien van specifieke veiligheidsthema's. Dit dient als sturingsinformatie en dit is veeleer niet gericht op specifieke personen.

Ten tweede is gebleken dat het opsporingsbegrip uit artikel 132a WvSv een bredere reikwijdte heeft gekregen. Het doel van het opsporingsonderzoek (het nemen van strafvorderlijke beslissingen) wordt breed uitgelegd, waardoor het mogelijk is om tevens andere doelen en reacties na te streven. De vraag die zich nu opdringt is of onderzoek dat niet hoofdzakelijk is gericht op het opsporen en vervolgen van individuen, maar (mede) op andere doelen (zoals intelligence) ook binnen het opsporingsbegrip valt en of er opsporingsbevoegdheden ingezet kunnen worden.[222]

---

[218] Crijns e.a. 2021, p. 142-143.
[219] Crijns e.a. 2021, p. 142-143.
[220] Crijns e.a. 2021, p. 143.
[221] Crijns e.a. 2021, p. 143.
[222] Rapport Commissie-Koops 2018, p. 22;

Dat het opsporingsbegrip ruimte geeft om andere doelen en reacties na te streven, neemt niet weg dat voor opsporingsbevoegdheden uit het WvSv nog altijd het doelbindingsprincipe geldt. Dit doelbindingsprincipe is beperkt tot het traditionele (hoofd)doel van strafvordering, namelijk materiële waarheidsvinding door het verzamelen van bewijs voor de vervolging van de daadwerkelijke schuldige.[223] Dit houdt dus in dat de inzet van bevoegdheden primair gericht moet zijn op het traditionele doel van strafvordering. Alternatieve doelen (zoals intelligence) kunnen soms echter belangrijker zijn, waardoor de vraag is ontstaan of deze doelen ook zelfstandig naast het traditionele doel of zelfs in de plaats van het traditionele doel kunnen komen te staan.[224]

Hirsch Ballin en Oerlemans menen dat andere doelstellingen, zoals het verstoren van strafbare feiten en het versterken van de informatiepositie, ook als zelfstandige doelen kunnen dienen bij de uitoefening van opsporingsbevoegdheden. Dit heeft volgens hen wel implicaties voor de normering van bevoegdheidsuitoefening.[225] Het is immers de vraag of het huidig systeem van waarborgen in het WvSv geschikt is voor bevoegdheidsuitoefening die niet primair gericht zijn op vervolging. Het systeem is ingericht met een balans tussen toezicht vooraf en toezicht achteraf. Het toezicht achteraf vindt voornamelijk plaats door de rechter tijdens het onderzoek ter terechtzitting. Bij het verstoren van strafbare feiten en het versterken van de informatiepositie ontbreekt echter het toezicht achteraf, waardoor een nieuwe balans nodig lijkt om een geschikt systeem van waarborgen te creëren voor de inzet van bevoegdheden die niet primair gericht zijn op vervolging.[226]

Uit het voorgaande blijkt dus dat andere doelen, waaronder intelligence, niet zomaar in de plaats van het traditionele doel van strafvordering kunnen komen te staan. Dit vereist eerst een verandering in de normering van bevoegdheidsuitoefeningen. Online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van intelligence valt nu dus alleen onder het opsporingsonderzoek wanneer dit primair gericht is op vervolging en niet op daadwerkelijk op intelligence. Zelfs als intelligence wel als zelfstandig doel van opsporing wordt beschouwd, kunnen de huidige bijzondere opsporingsbevoegdheden nog steeds niet ingezet worden, omdat deze een klassieke verdenking (in de zin van artikel 27 WvSv) vereisen. Zowel artikel 126g en 126j WvSv als het nieuwe artikel 2.8.8 in het gemoderniseerde WvSv beginnen namelijk met: “In geval van verdenking van een misdrijf” en dit is bij intelligence meestal niet het geval.

7.6 Tussenconclusie

In dit hoofdstuk zijn verschillende suggesties gegeven om de knelpunten uit het huidige juridische kader (deels) op te lossen. Ten eerste kan de reikwijdte van artikel 3 Pw verduidelijkt worden door de rechter, de wetgever of door middel van een AMvB. De wetgever heeft hierbij zelfs meerdere opties om artikel 3 nader te duiden. Zo kan er een algemene

[223] Hirsch Ballin & Oerlemans 2023, p. 29-30; Hirsch Ballin 2022, p. 9-10.
[224] Hirsch Ballin & Oerlemans 2023, p. 29-30; Hirsch Ballin 2022, p. 10 & 15.
[225] Hirsch Ballin & Oerlemans 2023, p. 30.
[226] Rapport Commissie-Koops 2018, p. 24.

bevoegdheidsbepaling of een specifiek artikel dat ziet op gegevensvergaring uit publiek toegankelijke bronnen toegevoegd worden (voor zover dit een geringe inbreuk op de privacy betreft). Daarnaast kan de wetgever ook een uitgebreide en richtinggevende MvT opstellen. Verder zou de wetgever ook een tussengelegen artikel kunnen toevoegen, indien uit de proefprocessen volgt dat artikel 3 geen voldoende grondslag biedt voor bijvoorbeeld de inzet van een webcrawler.

Ten tweede kan een burgemeester beter in staat worden gesteld om zijn gezag over openbare orde intelligence uit te oefenen. Op dit moment lopen er ook voorstellen om de rol van de burgemeester nadrukkelijker te positioneren. Het is hierbij ook van belang dat de burgemeester zijn eigen rol (h)erkent.

Ten derde kan er een gespecialiseerd en onafhankelijk toezichtsorgaan opgericht worden dat ook tijdens de inzet van digitale opsporingsbevoegdheden meekijkt en indien nodig kan ingrijpen. Hierbij kan een voorbeeld genomen worden aan de CTIVD.

Tot slot zou het verschil tussen intelligence en het opsporingsonderzoek verduidelijkt kunnen worden door het opsporingsbegrip zo te formuleren dat het een duidelijker startpunt bevat. Hierbij is ook gebleken dat andere doelen, waaronder intelligence, niet zomaar in de plaats van het traditionele doel van strafvordering kunnen komen te staan.

Er kan dus geconcludeerd worden dat het juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence in meerdere opzichten verbeterd kan worden.

Hoofdstuk 8 – Conclusie

8.1 Samenvatting

In deze masterscriptie stond de verbetering van het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence centraal. Aan de hand van een literatuuronderzoek en een kleinschalig empirisch onderzoek is getracht een antwoord te vormen op de volgende onderzoeksvraag:

> *In welk opzicht zou het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence moeten worden verbeterd?*

Om tot een antwoord op de onderzoeksvraag te komen, is eerst in hoofdstuk 2 het recht op privacy in uit artikel 8 EVRM behandeld. Met de eisen en waarborgen die het EHRM stelt aan wetgeving over online gegevensvergaring uit publiek toegankelijke bronnen in het achterhoofd, is vervolgens in hoofdstuk 3 gekeken naar het huidige juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence. Hieruit is gebleken dat het huidige juridische kader een aantal grijze gebieden kent. Deze grijze gebieden zijn samen met andere knelpunten van het huidige juridische kader nader uitgewerkt in hoofdstuk 4. De knelpunten van het huidige juridische kader zagen op: de onduidelijkheid over de reikwijdte van artikel 3, de onduidelijkheid ten aanzien van gezagsdragers, het externe toezicht op de Wpg en het onderscheid tussen intelligence en het opsporingsonderzoek.

Vervolgens is in hoofdstuk 5 en hoofdstuk 6 respectievelijk ingegaan op het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek en het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door de inlichtingen- en veiligheidsdiensten. Beide juridische kaders kennen meer en specifiekere regels dan het juridische kader voor opsporingsambtenaren op het gebied van intelligence. Daarnaast kent de Wiv een uitgebreid stelsel van toezicht en controle.

Tot slot zijn in hoofdstuk 7 suggesties gedaan ter verbetering van de knelpunten van het huidige juridische kader aan de hand van de juridische kaders voor online gegevensvergaring uit publiek toegankelijke bronnen ten behoeve van het opsporingsonderzoek en door de inlichtingen- en veiligheidsdiensten. Daarnaast zijn ook de praktijkervaringen en door respondenten aangedragen oplossingen meegenomen. Dit heeft geleid tot een aantal suggesties ter verbetering van het huidige juridische kader.

8.2 Conclusie

Geconcludeerd kan worden dat het juridische kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence in een

aantal opzichten verbeterd kan worden. Ten eerste kan de reikwijdte van artikel 3 Pw verduidelijkt worden door de rechter, de wetgever of door middel van een AMvB. De wetgever heeft hierbij meerdere opties om artikel 3 nader te duiden. Zo kan er een algemene bevoegdheidsbepaling of een specifiek artikel dat ziet op gegevensvergaring uit publiek toegankelijke bronnen toegevoegd worden (voor zover dit een geringe inbreuk op de privacy betreft). Daarnaast kan de wetgever een uitgebreide en richtinggevende MvT opstellen. Indien uit de proefprocessen volgt dat artikel 3 geen voldoende grondslag biedt voor bijvoorbeeld de inzet van een webcrawler, zou de wetgever ook een tussengelegen artikel kunnen toevoegen. Ten tweede kan een burgemeester beter in staat worden gesteld om zijn gezag over openbare orde intelligence uit te oefenen. Op dit moment lopen er ook voorstellen om de rol van de burgemeester nadrukkelijker te positioneren. Het is hierbij ook van belang dat de burgemeester zijn eigen rol (h)erkent. Ten derde kan er een gespecialiseerd en onafhankelijk toezichtsorgaan opgericht worden dat ook tijdens de inzet van digitale opsporingsbevoegdheden meekijkt en indien nodig kan ingrijpen. Hierbij kan een voorbeeld genomen worden aan de CTIVD. Tot slot zou het verschil tussen intelligence en het opsporingsonderzoek verduidelijkt kunnen worden door het opsporingsbegrip zo te formuleren dat het een duidelijker startpunt bevat.

8.3 Aanbevelingen

Voortvloeiend uit het bovenstaande, volgen in deze paragraaf kort vijf concrete aanbevelingen om het juridisch kader voor online gegevensvergaring uit publiek toegankelijke bronnen door opsporingsambtenaren op het gebied van intelligence te verbeteren.

Aanbeveling 1: De wetgever moet de reikwijdte van artikel 3 Pw nader duiden.
Artikel 3 Pw kan al nader geduid worden door een algemene bevoegdheidsbepaling (vergelijkbaar met artikel 2.1.9 gemoderniseerde WvSv) toe te voegen aan de Pw. Het zou echter beter zijn voor de rechtszekerheid om een specifiek artikel dat ziet op online gegevensvergaring uit publiek toegankelijke bronnen (verglijkbaar met artikel 25 Wiv) toe te voegen. Ook zou eventueel een tussengelegen artikel toegevoegd kunnen worden dat de bevoegdheid geeft om bij een meer dan beperkte inbreuk op de privacy persoonsgegevens uit publiek toegankelijke bronnen te vergaren. Daarnaast zou in de Pw vastgelegd kunnen worden dat bij AMvB nadere regels gesteld kunnen worden over de invulling van de politietaak. Tot slot kan de reikwijdte van artikel 3 Pw ook verduidelijkt worden in een uitgebreide en richtinggevende MvT.

Aanbeveling 2: **De rechter moet de reikwijdte van artikel 3 Pw nader duiden.**
De rechter kan de reikwijdte van artikel 3 Pw nader duiden door zich in de proefprocessen uit te spreken over de vraag of artikel 3 Pw een voldoende grondslag biedt voor online gegevensvergaring uit publiek toegankelijke bronnen.

Aanbeveling 3: De rol van de burgemeester bij openbare orde intelligence moet nadrukkelijker gepositioneerd worden.
Hierbij is het ook van belang dat de burgemeester zijn eigen rol (h)erkent. Ten aanzien van het toezicht op het TOOI zou een voorbeeld genomen kunnen worden aan de wet- en regelgeving die al bestaat over het TCI.

Aanbeveling 4: Richt een gespecialiseerd en onafhankelijk toezichtsorgaan op.
Hiervoor kan een soortgelijk toezichtsorgaan als de CTIVD worden opgericht dat zich richt op de inzet van online bevoegdheden door opsporingsambtenaren, waaronder dus online gegevensvergaring uit publiek toegankelijke bronnen. Het is hierbij van belang dat het toezichtsorgaan niet alleen vooraf of achteraf toezicht houdt, maar juist ook tijdens de inzet van digitale opsporingsbevoegdheden meekijkt en indien nodig ingrijpen.

Aanbeveling 5: De wetgever moet de reikwijdte van artikel 132a WvSv nader duiden.
Het startpunt van het opsporingsonderzoek uit artikel 132a WvSv kan verduidelijkt worden door dit artikel als volgt aan te passen: “Opsporing is onderzoek door ambtenaren met opsporing belast dat zich richt op één of meer bepaalde personen in verband met hun mogelijke betrokkenheid bij een strafbaar feit met als doel het nemen van strafvorderlijke beslissingen.” [227]

Hopelijk maken deze aanbevelingen het gebruik van publiek toegankelijke bronnen ook ten behoeve van intelligence toegankelijk voor opsporingsambtenaren.

[227] Crijns e.a. 2021, p. 143.

Literatuurlijst

Bantema e.a. 2018
W. Bantema e.a., *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*, Den Haag: SDU 2018.

Borgers 2015
M.J. Borgers, 'Normering van "lichte" opsporingshandelingen', *DD* 2015/15, p. 143-155.

Crijns e.a. 2021
J.H. Crijns, 'De verregaande lenigheid van het opsporingsbegrip: Verkenningen op het grensvlak van toezicht en opsporing', in: T. Kooijmans e.a. (red.), *Op zoek naar evenwicht. Liber amicorum Marc Groenhuijsen*, Deventer: Wolters Kluwer 2021, p. 133-147.

Van Dijk, Snel & Van Golen 2018
G. Van Dijck, M. Snel & T. Van Golen, *Methoden van rechtswetenschappelijk onderzoek*, Den Haag: Boom Juridisch 2018.

Van den Eeden e.a. 2021
C.A.J. van den Eeden e.a., *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*, Den Haag: WODC 2021.

Eskens, Van Daalen & Van Eijk 2016
S.J. Eskens, O.L van Daalen & N.A.N.M. van Eijk, *Geheime surveillance en opsporing: Richtsnoeren voor de inrichting van wetgeving* (diss. Amsterdam UvA), Amsterdam: IViR 2016.

Fedorova e.a. 2022
M.I Fedorova e.a., *Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Nijmegen: Radbound University Press 2022.

Gritter 2018
E. Gritter, 'De rechtmatigheid van datamining door de politie', *TBS&H* 2018/2 p. 113-115.

Groothuis 2019
M.M. Groothuis M.M, 'Commentaar op artikel 10 van de Grondwet (Eerbiediging en bescherming van de persoonlijke levenssfeer), in: E.M.H. Hirsch Ballin & G. Leenknegt (red.), *Artikelsgewijs commentaar op de Grondwet*, webeditie 2021 (nederlandrechtsstaat.nl).

Groothuis & Landman 2022

W. Groothuis & S. Landman, *Politiewerk op het web: een verkennend onderzoek naar online gegvensvergaring door de politie*, Den Haag: Sdu Uitgevers; Den Haag: Politie en Wetenschap; Amersfoort: TwynstraGudde 2022.

Hirsch Ballin 2022
M.F.H. Hirsch Ballin, *Responsief strafprocesrecht in een netwerk van rechtsbetrekkingen: Preadvies voor de Christen Juristen Vereniging*, Den Haag: Boom Juridisch 2022.

Hirsch Ballin & Oerlemans 2023
M.F.H. Hirsch Ballin & J.J. Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden', *DD* 2023/2, p. 18-38.

Klaar 2022
R.J.A. Klaar, 'De strafvordelijke normering van het geautomatiseerd overnemen van persoonsgegevens uit publiek toegankelijke bronnne met behulp van webcrawlers', *Platform Modernisering Strafvordering* maart 2022, p. 1-15, DOI: 10.5553/PMSV/258950952022005003001.

Kop & Klerks 2009
N. Kop & P. Klerks, *Doctrine intelligencegestuurd politiewerk*, Den Haag: OBT 2009.

Kranenborg 2007
H.R. Kranenborg, *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie*. Over de openbaarheid van persoonsgegevens, Deventer: Kluwer 2007.

Lassche 2023
H. Lassche, *Digitalisering en de opsporingspraktijk, juridische aspecten*, Apeldoorn: Politieacademie 2023.

Ligthart 2019
M.S. Ligthart, 'Het criterium van stelselmatigheid in het gemoderniseerde Wetboek van Strafvordering: redelijke voorzienbaarheid als voorwaarde voor meer dan geringe en ingrijpende privacy-inbreuken?', *RMThemis* 2019/5, p. 195-202.

Van der Meij, in: *T&C Sv*
P.P.J. Van der Meij, commentaar op art. 132a Sv, in: C.P.M Cleiren, J.H. Crijns & M.J.M Verpalen (red.), *Tekst & Commentaar Strafvordering*, Deventer: Wolters Kluwer (online).

Oerlemans 2017a
J.J. Oerlemans, *Normering van digitale opsporingsmethoden*, Breda: Nederlandse Defensie Academie 2017.

Oerlemans 2017b
J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017.

Oerlemans 2018
J.J. Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', *Platform Modernisering Strafvordering* november 2018, DOI: 10.5553/PMSV/258950952018001018001.

Oerlemans & Hagens 2018
J.J. Oerlemans & M. Hagens, 'De Wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018/111, p. 130-141.

Van der Plas & Brown 2017
A. van der Plas & C. Brown, 'Inwinning', in: M. den Hengst, T. ten Brink & J. ter Mors (red.), *Informatiegestuurd politiewerk in de praktijk*, Deventer: Vakmedianet 2017, p. 179-191.

Ramwell, Day & Gibson 2016
S. Ramwell, T. Day & H. Gibson, 'Use cases and best practices for LEA's', in: B. Akhgar, P.S. Bayerl & F. Sampson (red.), *Open source intelligence investigation: from strategy to implementation*, Cham: Springer International Publishing 2016, p. 197-212.

Rapport Commissie-Koops 2018
Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018.

SBGI 2008
SBGI, *Waakzaam tussen wijk en wereld. Nationaal Intelligence Model. Sturen op en met informatie*. Strategische Beleidsgroep Intelligence 2008.

Schermer 2017
B.W. Schermer, 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *TBS&H* 2017/4, p. 207-216.

Stevens 2021
L. Stevens e.a., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling', *TBS&H* 2021/4, p. 234-245.

Stevens & Koops 2021

L. Stevens & B-J. Koops, 'Naar een strafvordering 2030 and beyond', in: T. Kooijmans e.a. (red.), *Op zoek naar evenwicht. Liber amicorum Marc Groenhuijsen*, Deventer: Wolters Kluwer 2021, p. 701-713.

Stol & Strikwerda 2018
W. Stol & L. Strikwerda, 'Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving'. *TvV* 2018/17, p. 8-22.

Van Toor 2017
D.A.G. van Toor, 'Inbreuk op artikel 8 lid 1 EVRM', in: D.A.G. van Toor (red.), *Het schuldige geheugen? (SteR nr. 32)*, Deventer: Wolters Kluwer 2017.

Toetsingskader CTIVD 2021
CTIVD, *Toetsingskader* bijlage bij Toezichtsrapport 74: *Automated OSINT: tools en bronnen voor openbronnenonderzoek*, Den Haag: Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten 2021.

Toezichtsrapport CTIVD 2021
CTIVD, Toezichtsrapport 74: *Automated OSINT: tools en bronnen voor openbronnenonderzoek*, Den Haag: Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten 2021.

Jaarverslag CTIVD 2022
CTIVD, *Jaarverslag 2022*, Den Haag: Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten 2022.

Veen 2019
R. S. Veen, 'Digitale opsporing. Het EHRM en het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen', *DD* 2019/30, p. 386-404.

De Vocht, in: *T&C Sv*
D. de Vocht, commentaar op art. 8 EVRM, in: C.P.M Cleiren, J.H. Crijns & M.J.M Verpalen (red.), *Tekst & Commentaar Strafvordering*, Deventer: Wolters Kluwer (online).

Winter e.a. 2020
H. Winter e.a., *De verwerking van politiegegevens in vijf Europese landen*, Groningen/Den Haag: WODC 2020.

Jurisprudentielijst

EHRM 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*).
EHRM 25 september 2001, nr. 44787/98 (*P.G en J.H. t. Verenigd Koninkrijk*).
EHRM 6 juni 2006, nr. 6233/00 (*Segerstedt-Wiberg e.a. t. Zweden*).
HR 19 december 1995, ECLI:NL:HR:1995:ZD0328 (*Zwolsman*).
Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365 (*Context-zaak*).
Rb. Overijssel 5 april 2022, ECLI:NL:RBOVE:2022:900.

Regelgeving en parlementaire stukken

Kamerstukken II 1996/97, 25403, nr. 3.
Kamerstukken II 1998/99, 26671, nr. 3.
Kamerstukken II 2004/05, 30164, nr. 3.
Kamerstukken II 2004/05, 30182, nr. 3.
Kamerstukken II 2016/17, 34588, nr. 3.
Kamerstukken II 2022/23, 36327, nr. 2.
Kamerstukken II 2022/23, 36327, nr. 3.

Bijlage 1 – Factoren voor stelselmatigheid

In de MvT bij het gemoderniseerde WvSv worden enkele aanknopingspunten gegeven voor de relevante factoren voor de invulling van het begrip stelselmatigheid in de online context. Deze factoren zijn deels aanbevolen door de Commissie-Koops, die bovendien heeft geadviseerd om ze te clusteren.[228]

De eerste factor betreft de omvang en het type van de over te nemen gegevens:

- de hoeveelheid gegevens;
- de aard van de gegevens;
- de diversiteit van gegevens;
- Relevant is de mate waarin vooraf bekend is hoe vaak en hoe de persoon zich manifesteert in publiek toegankelijke bronnen.

De tweede factor is de aard van de bron. Te denken valt aan:

- de aard van de locatie waarop de gegevens te vinden zijn; sommige bronnen zijn naar hun aard zeer openbaar (de krant), andere helemaal niet (de inhoud van privé-opslagruimte die toevallig niet beveiligd was);
- de menselijke bron van de gegevens (heeft de betrokkene deze zelf op internet geplaatst, of hebben anderen dat gedaan?);
- het doel waarmee de gegevens in eerste instantie zijn vergaard of gepubliceerd; is bijvoorbeeld expliciet of, gezien de context, impliciet duidelijk dat de gegevens op internet zijn geplaatst met het oog op brede verspreiding, of juist niet met het oog op kennisneming door een brede of onbeperkte kring;
- de plaats van de gegevens (welke privacy-verwachting bestaat bij de locatie van de gegevens: staan ze direct zichtbaar op een platform met een breed publiek, of op een obscure webpagina?);
- de feitelijke bekendheid van de gegevens (zijn de gegevens in een brede groep verspreid? Is dit de eerste openbaarmaking? Of zijn er inmiddels vele bronnen die er mededeling over hebben gedaan?).

De derde factor betreft de wijze van zoeken. Te denken valt aan:

- de “geavanceerdheid” van het gebruikte technisch hulpmiddel (handmatig zoeken met een klassieke zoekmachine, of geautomatiseerd zoeken en combineren van gegevens, of geautomatiseerde veredeling van gegevens?);
- het doel van de zoekactie (gericht op het overnemen van enkele simpele gegevens, of breder, gericht op een specifiek feit of persoon of op feitencomplexen en meerdere al dan niet verdachte personen);

[228] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 684-686; Rapport Commissie-Koops 2018, p. 162-164.

- de specificiteit van de zoekvraag (wordt een algemene of heel specifieke vraag gesteld, wordt de zoekvraag op voorhand toegespitst aan de hand van al in een onderzoek bekende gegevens, en gaat het om “gesloten vragen” of om “open vragen”?
- de samenhang tussen de zoekvraag en het strafbare feit (is de zoekvraag direct en specifiek gericht op dit feit, of breder?).

De vierde factor betreft de opslag en het gebruik van de gegevens en de mogelijke gevolgen voor de persoon:

- de mate waarin (door een crawler of opsporingsambtenaar onderzochte) gegevens worden overgenomen en de selectiviteit die daarbij wordt gehanteerd (worden gegevens alleen beperkt en gericht overgenomen in politiesystemen, of is er juist sprake van een brede en weinig selectieve overneming van wat is aangetroffen?);
- de in het onderzoek al bekende informatie (hoeveel zal de zoekactie toevoegen aan het al bestaande beeld?);
- de combinatie van gegevens uit verschillende bronnen.

Deze veelheid van relevante aspecten en het brede spectrum van de mate van inbreuk in concrete gevallen is inherent aan de diversiteit van bronnen op het internet. Er is zoveel informatie over zoveel aspecten van de levens van zoveel personen, informatie die op zoveel verschillende wijzen te benaderen valt, dat dit zich niet laat vatten in een beperkte set aspecten die meegewogen moeten worden.

Zoals gezegd, gaat het bij al de genoemde factoren om de redelijke voorzienbaarheid vooraf. Niet alles is daarbij even goed te voorzien: de manier van zoeken kan vanzelfsprekend wel vooraf worden bepaald (en vervolgens weer aangepast afhankelijk van de uitkomsten van het begin van de zoekactie), maar de hoeveelheid, de plaats en de aard van gegevens die in beeld komen zullen niet altijd vooraf goed kunnen worden ingeschat. De opsporingsambtenaren zullen moeten afgaan op wat al bekend is over de persoon en over diens manifestatie op internet, en vervolgens op basis van algemene ervaringsregels moeten inschatten of de voorgenomen zoekvragen met enige waarschijnlijkheid kunnen leiden tot een min of meer volledig beeld van bepaalde aspecten van iemands privéleven. In twijfelgevallen zou het uitgangspunt moeten zijn dat aan de voorwaarden van stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen moet worden voldaan en een bevel worden aangevraagd. Een andere mogelijkheid is dat de opsporingsambtenaar ervoor kiest om eerst een oppervlakkige zoekslag te maken, om een eerste beeld te krijgen van wat een uitgebreide zoekslag op zou kunnen leveren. Hierbij zal hoe dan ook moeten worden geaccepteerd dat deze afweging – achteraf gezien – soms onjuist zal blijken te zijn geweest.[229]

[229] *Kamerstukken II* 2022/23, 36327, nr. 3, p. 684-686.