OPSPORING OP SOCIAL MEDIA

Marnix Oosterhoff

OpenUniversiteitNederland

www.ou.nl

OPSPORING OP SOCIAL MEDIA

Afstudeerscriptie Masteropleiding Rechtsgeleerdheid

Auteur: Marnix Oosterhoff

Studentnummer: 851528488

Opleiding: Master Rechtsgeleerdheid

Organisatie: Open Universiteit

Begeleider: prof. dr. W.Ph. Stol

Examinator: mr. dr. W.H.B. Dreissen

Januari 2016

Inhoud

Gebruikte afkortingen ii
1 Inleiding 1
1.1 Aanleiding 1
1.2 Onderwerp en doel van onderzoek 2
1.3 Onderzoeksvragen 2
1.4 Gehanteerde onderzoekmethoden 3
1.5 Opbouw 4
2 Politie en social media 5
2.1 Inleiding 5
2.2 Social media binnen de politie: de negen domeinen 6
2.3 Gebruik van social media binnen de opsporing 8
2.3.1 Methode van onderzoek 8
2.3.2 Resultaten 10
2.4 Conclusies 13
3 Privacy 16
3.1 Inleiding 16
3.2 Definities van privacy 16
3.3 Historie van de ontwikkeling van het recht op privacy 19
3.4 Actueel juridisch kader ten aanzien van privacy 21
3.4.1 Internationale en nationale wet- en regelgeving 21
3.4.2 Artikel 10 Grondwet 22
3.4.3 Artikel 8 EVRM 24
3.4.4 Recente ontwikkelingen 28
3.5 Conclusies 30
4 Opsporingsbevoegdheden op social media 32
4.1 Inleiding 32
4.2 Digitale IRT-affaire? 34
4.3 Opsporing: typering en normering 37
4.3.1 Definitie opsporing 37
4.3.2 Normering van de opsporing 38
4.4 Politiewet of BOB-middel? 41
4.5 Stelselmatige observatie 45
4.5.1 Artikel 126g Sv 45

4.5.2 Opsporing op social media als stelselmatige observatie? 47
4.5.3 Beoordeling 48
4.6 Stelselmatige informatie-inwinning 50
4.6.1 Artikel 126j Sv 50
4.6.2 Opsporing op social media als stelselmatige informatie-inwinning? 51
4.6.3 Beoordeling 53
4.7 Toetsing aan art. 8 EVRM 54
4.8 Conclusie 55
5 Conclusie en discussie 58
5.1 Inleiding 58
5.2 Antwoorden op de onderzoeksvragen en conclusies 58
5.3 Discussie 61
Verwijzingen 65
Geraadpleegde literatuur 65
Jurisprudentie 70
Bijlage 1 – Interviewvragen 72
Bijlage 2 - Gespreksverslag prof. Fijnaut 73

Gebruikte afkortingen

BOB	Bijzondere Opsporingsbevoegdheden
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
Gw	Grondwet
IRN	Internet Research Netwerk
IRT	Interregionaal Rechercheteam
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
MvT	Memorie van Toelichting
OSINT	Open Source Intelligence
OVC	Opnemen Vertrouwelijke Communicatie
PolW	Politiewet 2012
Sv	Wetboek van Strafvordering
TCI	Team Criminele Inlichtingen
TGO	Team Grootschalige Opsporing
UVRM	Universele Verklaring van de Rechten van de Mens
VEU	Verdrag betreffende de Europese Unie
Wbp	Wet bescherming persoonsgegevens
WPolG	Wet op de politiegegevens

1 Inleiding

1.1 Aanleiding

Het gebruik van social media heeft de afgelopen jaren een stormachtige ontwikkeling doorgemaakt. Veel mensen hebben de neiging om datgene wat hen bezighoudt of wat ze hebben gedaan, met anderen te delen via omgevingen als Facebook en Twitter. Social media zijn er naar hun aard op gericht om zoveel mogelijk informatie te delen. Het gevolg is dat veel gebruikers bewust of onbewust veel (vaak persoonlijke) informatie over zichzelf met vrienden delen maar soms ook in de openbaarheid brengen. Mede door de opkomst van social media speelt het sociale leven zich in toenemende mate online af.

Voor de informatie die burgers via social media naar buiten brengen bestaat vanuit opsporingsinstanties veel belangstelling omdat deze informatie van belang kan zijn voor de opsporing. Niet verwonderlijk dus dat de opsporing op allerlei manieren probeert om deze informatie te gebruiken. Echter, bij het gebruik van deze informatie binnen een rechercheonderzoek moet de opsporing plaatsvinden binnen wettelijke kaders, en van het bestaande wettelijke kader is niet altijd duidelijk hoe het moet worden toegepast in een online-omgeving.

Deze situatie roept herinneringen op aan het onderzoek van de parlementaire enquêtecommissie opsporingsmethoden (in de volksmond bekend als de commissie Van Traa) dat medio jaren 90 plaatsvond. In haar conclusies en aanbevelingen stelde de commissie dat er in de opsporing van georganiseerde criminaliteit in Nederland sprake was van een situatie van onvoldoende normstelling en van onduidelijkheid over wie waarvoor verantwoordelijk was. Het bracht de commissie tot het oordeel dat er sprake was van een crisis in de opsporing en concludeerde dat het hoog tijd was dat iedereen weer wist waar men aan toe was.[1] Dit heeft uiteindelijk geleid tot het stelsel van Bijzondere Opsporingsbevoegdheden (BOB) zoals gedefinieerd in de Wet BOB van 2000. In de literatuur worden van die bijzondere opsporingsbevoegdheden met name stelselmatige observatie (art. 126g Sv) en stelselmatige informatie-inwinning (art. 126j Sv) aangewezen als van toepassing zijnde bevoegdheid op de opsporing op social media, daarom concentreert dit masteronderzoek zich op die twee artikelen.

Nu is niet voor elk opsporingsonderzoek op social media de inzet van dergelijke bijzondere opsporingsbevoegdheden noodzakelijk. Op grond van de algemene taakomschrijving van de politie in art. 3 Politiewet (PolW) mag de politie bepaalde opsporingshandelingen verrichten. In de praktijk worstelen politie en Openbaar Ministerie echter regelmatig met de vraag welke politiehandelingen

[1] Inzake opsporing 1996

hun legitimering kunnen vinden in art. 3 PolW en op welk moment er sprake is van handelingen die dusdanig ingrijpend zijn ten aanzien van de grondrechten van betrokken burgers, dat zij een eigenstandige legitimering vereisen middels specifieke wetgeving, zoals de bijzondere opsporingsbevoegdheden uit het Wetboek van Strafvordering. Bij het beantwoorden van de vraag welke van die bijzondere opsporingsbevoegdheden bij opsporing op social media van toepassing zijn, moet ook de vraag worden meegenomen of de bevoegdheden die de wet op dit moment kent zonder meer gebruikt kunnen worden in de online wereld.

Daarnaast is de vraag relevant of het vanuit maatschappelijk oogpunt gewenst is dat alles wat kan ook mag. Organisaties als Bits of Freedom waarschuwen burgers voor de inbreuk die de digitale wereld maakt op de privacy van burgers zonder dat deze dat zelf doorhebben (zie bijvoorbeeld www.bof.nl). Bij de discussie over de toepasbaarheid van opsporingsbevoegdheden op social media is daarom de vraag naar de noodzakelijke begrenzing daarvan minstens zo relevant.

1.2 Onderwerp en doel van onderzoek

In dit onderzoek gaat het over opsporingsbevoegdheden op social media en dan met name op Facebook en Twitter vanwege hun marktaandeel.[2] Het doel van het onderzoek is het leveren van een bijdrage aan een "rechtmatige, effectieve en verantwoorde wijze van opsporing"[3] op social media waarbij een goede balans bestaat tussen de belangen van de opsporing en de grondrechten van burgers.

In het onderzoek wordt mede op basis van empirisch materiaal nagegaan of de bestaande wettelijke middelen die worden ingezet voor de regulering van politiewerk in een digitale omgeving in de praktijk voldoen. Met de uitkomsten wordt beoogd een bijdrage te leveren aan het wetenschappelijke debat met betrekking tot de vraag op welke wijze het werk van de politie ten aanzien van opsporing op social media op zodanige wijze genormeerd kan worden dat dit past binnen de beginselen van de democratische rechtsstaat.[4]

1.3 Onderzoeksvragen

De hoofdvraag in dit onderzoek is:

> Bieden de bijzondere opsporingsbevoegdheden stelselmatige observatie (126g) en stelselmatige informatie-inwinning (126j) in het Wetboek van Strafvordering voldoende

[2] In 2014 gebruiken 8,9 miljoen Nederlanders Facebook waarvan 6,1 miljoen dagelijks, en 3,5 miljoen Nederlanders gebruiken Twitter waarvan 1,5 miljoen dagelijks. (bron: Onderzoeksbureau Newcom, http://www.newcom.nl/social-media-onderzoek2014).

[3] Inzake opsporing 1996 (p. 5). De term verantwoord heeft daarbij betrekking op de eis dat de opsporingsinstantie verantwoording moet afleggen van de wijze waarop de opsporing heeft plaatsgevonden.

[4] Zie hierover bijvoorbeeld Meij 2010

mogelijkheden om binnen de grenzen van het strafvorderlijk legaliteitsbeginsel op rechtmatige, effectieve en verantwoorde wijze opsporingswerkzaamheden op social media uit te voeren in die situaties waarin art. 3 Politiewet onvoldoende grondslag vormt?

Deelvragen waarvan de beantwoording bijdraagt tot de beantwoording van de hoofdvraag zijn:

1. Op welke wijze is de politie actief op social media en hoe worden op dit moment informatievergarende werkzaamheden van de politie verantwoord?
2. Welke definitie van het recht op privacy is het meest geschikt in online omgevingen?
3. Hoe heeft het recht op privacy zich in de geschiedenis ontwikkeld en hoe is dit recht in de wet verankerd?
4. Welke informatievergarende werkzaamheden kan de politie uitvoeren op basis van art. 3 Politiewet en wanneer is de inbreuk op de privacy dusdanig groot dat hiervoor een eigenstandige bevoegdheid noodzakelijk is?
5. In hoeverre zijn de bevoegdheden stelselmatige observatie (126g) en stelselmatige informatie-inwinning (126j) van toepassing op informatievergarende werkzaamheden op social media en voldoen ze?

Het onderzoek richt zich verder niet op de effectiviteit van de opsporing.

1.4 Gehanteerde onderzoekmethoden

Voor de beantwoording van de deelvraag over de werkwijze van de politie zijn interviews afgenomen bij politiemensen die betrokken zijn bij de opsporing op social media. In deze interviews is volgens een semi-gestructureerde aanpak onderzocht op welke wijze de opsporing op social media plaatsvindt, welke rol de opsporingsbevoegdheden daarbij spelen en op welke wijze het onderzoek op social media wordt verantwoord. In paragraaf 2.3.1 wordt de gevolgde werkwijze gedetailleerd beschreven.

Omdat bij de informatievergaring op social media het recht op privacy van de burgers in het geding is, wordt vervolgens in hoofdstuk 3 door middel van literatuuronderzoek gereconstrueerd op welke wijze het recht op privacy zich in de geschiedenis heeft ontwikkeld en hoe dit recht in de loop van de geschiedenis is verankerd in nationale en internationale wet- en regelgeving. Omdat de wetenschappelijke discussie rondom het recht op privacy teruggaat tot in de 19^{e} eeuw, is gebruik gemaakt van diverse oudere bronnen, met name uit de Verenigde Staten. Daarnaast is literatuur verzameld met betrekking tot de herziening van de grondwet in de vorige eeuw, zoals de eindrapporten van de commissies die de regering over die herziening hebben geadviseerd. Gelet op

het toenemende belang van de Europese regelgeving ten aanzien van het recht op privacy is daarnaast literatuur bestudeerd over het EVRM.
In hoofdstuk 4 wordt vervolgens geanalyseerd wat deze discussie betekent voor de opsporing op social media. Door middel van bestudering van de berichtgeving rondom de IRT-affaire, de aanleiding tot de parlementaire enquêtecommissie opsporingsbevoegdheden, en het interviewen van de leider van de onderzoekscommissie naar de georganiseerde criminaliteit in Nederland, is onderzocht welke parallellen er bestaan tussen de tijd van de IRT-affaire en de huidige situatie ten aanzien van opsporingsbevoegdheden op social media. De beperkt beschikbare publicaties rondom online opsporingsbevoegdheden zijn onderzocht. Mede op basis van dit onderzoek is vastgesteld welke factoren bij de opsporings op social media bepalend zijn voor de mate van inbreuk op het recht op privacy. Vervolgens zijn de opsporingsbevoegdheden stelselmatige observatie en stelselmatige informatie-inwinning mede op basis van literatuurstudie juridisch geanalyseerd en is vastgesteld in hoeverre deze bevoegdheden gebruikt kunnen worden om de opsporing op social media te normeren.

1.5 Opbouw

In hoofdstuk 2 worden de resultaten van het veldwerk binnen de politie weergegeven en wordt een aantal conclusies getrokken over de bestaande situatie ten aanzien van informatievergaring op social media door de opsporing in de Nederland.
Vervolgens wordt in hoofdstuk 3 geschetst welke definities van privacy vanuit de literatuur bekend zijn, welke definitie het beste past ten aanzien van social media en hoe deze definitie zich verhoudt tot de wijze waarop het recht op privacy is gecodificeerd. De ontwikkeling van het privacybegrip wordt daarbij afgezet tegen de ontwikkelingen in de maatschappij.
Hoofdstuk 4 beschrijft wanneer bij opsporing op social media de inbreuk op het recht op privacy zo groot is dat deze een eigenstandige bevoegdheid in de wet vereist. Tevens wordt nagegaan in hoeverre de bestaande bijzondere opsporingsbevoegdheden stelselmatige observatie en stelselmatige informatie-inwinning voldoen aan de eisen die aan een dergelijke bevoegdheid gesteld kunnen worden vanuit de rechtmatigheid, de effectiviteit en de verantwoording.
In hoofdstuk 5 wordt antwoord gegeven op de geformuleerde onderzoeksvragen en wordt een aantal aanbevelingen gedaan voor eventueel vervolgonderzoek.

2 Politie en social media

2.1 Inleiding

In 2009, dus al meer dan zes jaar geleden, verstuurde de politie haar eerste officiële tweet. Het toenmalige korps Brabant-Zuidoost vroeg toen het publiek om hulp bij de opsporing van een woninginbreker door het signalement van de verdachte via haar Twitter-account te verspreiden. Naar eigen zeggen deed het korps dit omdat men niet zeker wist of de media het opgestelde officiële persbericht zouden overnemen. Dat het een memorabele actie betrof, bleek toen vijf minuten na het verzenden van de eerste tweet op Teletekst de kop “Politie op Twitter” verscheen en binnen de kortste keren de televisieploegen op de stoep stonden. Tegenwoordig is bijna niet meer voor te stellen dat dit zo groot nieuws was. Inmiddels heeft de politie namelijk meer dan tweeduizend officiële Twitteraccounts en zijn er honderden politiemensen en –teams actief op Facebook. Social media worden niet meer als hype gezien, maar maken in toenemende mate onderdeel uit van het dagelijkse politiewerk.

Maar de politie gebruikt social media niet alleen als kanaal om informatie te verzenden maar ook als bron van informatie om in te zoeken. Omdat het gebruik van social media in onze samenleving de afgelopen jaren een stormachtige ontwikkeling heeft doorgemaakt, is er een voor de politie bijzonder interessante bron van informatie ontstaan. Veel mensen hebben de neiging om datgene wat hen bezighoudt of wat ze hebben gedaan met anderen te delen. Hierdoor brengen ze bewust of onbewust veel (vaak persoonlijke) informatie over zichzelf in de openbaarheid. Daarnaast wijst Van de Broek er in zijn studie onder jongeren op dat het sociale leven van vooral jongeren zich steeds meer online afspeelt.[5] Veel van die informatie op social media kan voor de politie heel bruikbaar zijn in het kader van de openbare orde en de veiligheid. Social media zijn daarom ook een interessante onderzoeksomgeving voor opsporingsinstanties. Daaraan zijn echter wel vragen verbonden: wat mag, wat is ethisch en wat is effectief?

Nu denkt de politie al langer na over het gebruik van open bronnen bij de uitvoering van haar taak. In 1996 verscheen het rapport “Wat wil je weten?” van de werkgroep Open Bronnen van het Accacia-project.[6] In dat rapport wordt verslag gedaan van een inventarisatie naar het gebruik van open bronnen binnen de politie en de eventuele juridische implicaties van dat gebruik. Geconstateerd wordt dat het gebruik van open bronnen binnen de politie in 1996 nog geen gemeengoed was. Er werd breed gebruik gemaakt van databanken van bijvoorbeeld de Kamer van Koophandel, het Kadaster, de Telefoongids, de RDW en de Gemeentelijke BasisAdministratie. Maar een aansluiting op

[5] Zie http://www.trouw.nl/tr/nl/6704/Sociale-Vraagstukken/article/detail/3762144/2014/10/04/Straatcultuur-beweegt-zich-van-straathoek-naar-Facebook.dhtml

[6] “Wat wil je weten?”, Eindrapport werkgroep Open Bronnen, Accacia deelproject 6, december 1996

Internet was lang niet in elk toenmalig korps beschikbaar, zodat het dus vooral meer statische informatie betrof. Ten aanzien van de juridische implicaties was toen de conclusie, mede in het licht van de bevindingen van Van Traa, dat als informatie uit open bronnen gebruikt wordt, verantwoord moet worden waarom deze informatie gebruikt is en op welke wijze de informatie is verkregen.

In dit hoofdstuk wordt beschreven op welke wijze de politie sinds haar eerste tweet de inbedding van social media binnen het politiebestel heeft aangepakt. De politie doet dit aan de hand van een negen-domeinen strategie (zie paragraaf 2.2), waarin voor diverse onderdelen van het politiewerk wordt beschreven wat de verwachte impact is van social media op dat domein en op welke wijze de politieprestaties kunnen worden verbeterd met behulp van social media. Bij de daadwerkelijke implementatie van social media binnen die domeinen wordt onderscheid gemaakt tussen 'zenden' (social media als communicatiekanaal) en 'informatie verzamelen' (social media als informatiebron voor handhaving en opsporing).
Omdat het onderwerp van deze masterscriptie opsporing op social media is, wordt na de bespreking van de negen domeinen ingezoomd op de wijze waarop de politie omgaat met social media binnen het opsporingsproces. Aan de hand van de resultaten van een aantal interviews dat is afgenomen binnen diverse politie-eenheden, wordt een beeld geschetst van de wijze waarop de politie social media gebruikt bij de opsporing en de wijze waarop wordt omgegaan met de juridische aspecten van die wijze van onderzoek. Het hoofdstuk sluit af met een aantal conclusies (paragraaf 2.4).

2.2 Social media binnen de politie: de negen domeinen

De betekenis van social media in de maatschappij is de afgelopen jaren sterk toegenomen. Een steeds groter deel van de samenleving communiceert, informeert en organiseert via social media. Om de verbinding met de samenleving niet te verliezen, wil de politie meegaan in deze ontwikkeling. Daarom heeft de politie in een door de korpsleiding bekrachtigde beleidsnotitie het volgende in haar visie op social media uitgesproken:
"*Social media zijn een vast onderdeel binnen het politiewerk en dragen bij aan het behalen van de doelstellingen van de Nationale Politie. Social media-bewustzijn is gemeengoed en stelt ons in staat betekenisvolle* ***verbindingen*** *aan te gaan binnen en buiten de organisatie. Social media zien we als middel om* ***transparant, betrokken, verantwoordelijk*** *en* ***anticiperend,*** *direct en indirect bij te dragen aan* ***veiligheid***." [7]

[7] De Vries & Smilda 2014 die deze informatie ontlenen aan een interne beleidsnotitie van de politie uit 2013.

De visie en missie van Nationale Politie zijn samen met de kernwaarden die politie hanteert (verbinden, betrouwbaar, moedig en integer) vertaald naar doelstellingen, die centraal staan bij de inbedding van social media binnen de politieorganisatie.
De politie spreekt in haar visie dus uit dat ze social media zoveel mogelijk wil inzetten om haar operationele doelstellingen te realiseren. Daarbij wil ze gebruik maken van de toegevoegde waarde van social media en die koppelen aan de al bestaande doelstellingen van de politie. Om dit voornemen door te voeren binnen de politieorganisatie zijn negen domeinen gedefinieerd waarop de social media strategie van de politie gericht is. Deze strategie moet leiden tot betere operationele politieprestaties en betere communicatie:

1. Social media als mediakanaal (eenrichtingsverkeer)
2. Social media voor actieve wederkerigheid (tweerichtingsverkeer)
3. Social media als crisis watch en communicatiemiddel in crisissituaties
4. Social media als media watch en webcare
5. Social media als event watch crowd control
6. Social media als realtime intelligencetool
7. Social media als opsporingstool en als opsporingscommunicatie
8. Social media als kennisdeler
9. Social media als professioneel en privékanaal

Voor elk van deze domeinen heeft de politie maatregelen geformuleerd waarmee geprobeerd wordt om social media binnen dat domein op effectieve wijze te integreren in het politiewerk. Deze werkzaamheden zijn verdeeld over twee programma's: het gebruik van social media als communicatiemiddel valt onder het programma Integraal Mediabeleid (IMDM), de overige onderdelen onder het programma Social Media in Operationele Politieprocessen (SMPP).[8]
De politie heeft met deze aanpak drie hoofddoelstellingen:

1. Verbeteren van de politieprestaties
2. Bevorderen van het werken als één korps
3. Behouden en vergroten van de legitimiteit van en het vertrouwen in de politie

De urgentie ten aanzien van de inbedding van social media binnen de politie werd nog eens benadrukt door de commissie Cohen, de onderzoekscommissie die werd ingesteld naar aanleiding

[8] Recent (juli 2015) is besloten om beide programma's samen te voegen.

van Project X in Haren op 21 september 2012.[9] In haar eindrapport[10] adviseert de commissie om de aandacht voor en de strategie ten aanzien van social media binnen de politie hoog in de organisatie te beleggen, omdat het centrale strategische taken zijn geworden. Een en ander moet stevig verankerd worden binnen de inrichting van de Nationale Politie. De minister van Veiligheid en Justitie geeft in een brief van april 2013 aan dat "het bevoegde gezag over de politie stevig regie zal gaan voeren op inzet van social media bij zaken als uitgaansgeweld, evenementen en dreigende incidenten. Duidelijk is dat de alertheid en de snelheid van handelen van de politie in het digitale domein omhoog moet.".[11]

Op basis van het bovenstaande kan geconstateerd worden dat de politie een inhaalslag aan het maken is waar het gaat om het gebruik van social media. Deze inhaalslag vindt plaats over de hele breedte van het politiewerk en het alleen uitspreken van deze ambitie geeft niet veel richting. Deze ambitie zal voor de verschillende domeinen nader ingevuld moeten gaan worden met concrete maatregelen.

Door middel van dit masteronderzoek wordt geprobeerd om op één van de benoemde aspecten van het politiewerk, namelijk het gebruik van social media binnen de opsporing, een empirische en theoretische verdieping aan te brengen.

2.3 Gebruik van social media binnen de opsporing

2.3.1 Methode van onderzoek

Omdat het onderwerp van deze scriptie betrekking heeft op social media binnen de opsporing (grofweg de domeinen 6 en 7), is door middel van interviews met opsporingsambtenaren van de Nationale Politie onderzocht op welke wijze de opsporing op dit moment omgaat met social media als onderzoeksomgeving. Daarbij zijn drie elementen onderzocht:

1. Het doel van de opsporing op social media en de wijze waarop deze opsporing plaatsvindt
2. De rol van de opsporingsbevoegdheden bij het onderzoek op social media
3. De wijze waarop het uitgevoerde politieonderzoek wordt verantwoord en welke rol dit deel van het politieonderzoek op de terechtzitting speelt

De interviews vonden plaats aan de hand van een vragenlijst (zie

[9] Een 15-jarig meisje verstuurde via Facebook een uitnodiging voor haar verjaardagsfeestje naar een aantal vrienden, waarbij de optie "Openbaar" aangevinkt stond. Via een sneeuwbaleffect en een kwaadwillende Facebook-gebruiker uit Nieuw-Zeeland kwam de uitnodiging uiteindelijk bij meer dan 250.000 mensen terecht. Op de avond van 21 september kwamen duizenden mensen naar Haren, hetgeen uitliep op grootschalige rellen en vernielingen.

[10] *Kamerstukken II* 2012/13, 33 751, nr. 1

[11] *Kamerstukken II* 2012/13, 33 751, nr. 2

Bijlage 1 – Interviewvragen). Deze lijst werd niet in elk interview precies in de gegeven volgorde gevolgd, maar de aanpak was semi-gestructureerd, dat wil zeggen dat de interviews meer het karakter hadden van een gesprek over de ervaringen van de respondenten met betrekking tot social media. Wel werd ervoor gezorgd dat alle vragen uiteindelijk aan bod kwamen.
De geïnterviewden werden gekozen uit vijf eenheden, verspreid over het land. In totaal zijn er vijf interviews afgenomen. Elk interview vond plaats op de werkplek van de geïnterviewde en duurde ongeveer anderhalf uur. Van de interviews zijn aan de hand van aantekeningen gespreksverslagen gemaakt, die na afloop aan de geïnterviewden zijn voorgelegd ter controle op juistheid en volledigheid.
De namen van geschikte respondenten zijn verkregen van de projectleider van het SMPP-project (SMPP staat voor Social Media in operationele PolitieProcessen, een landelijk programma dat tot doel heeft om in alle eenheden het gebruik van social media binnen de operationele werkprocessen te faciliteren, stimuleren en harmoniseren), omdat hij deze mensen kende en wist welke mensen het meest representatieve beeld zouden kunnen schetsen van de stand van zaken binnen de politie. De respondenten werden geselecteerd op basis van hun ervaring met het gebruik van social media binnen de opsporing. Vaak betrof het pioniers binnen hun eigen eenheid.
Twee respondenten zijn werkzaam in de proactieve opsporing (dat wil zeggen dat er wel sprake is van (verdenking van) misdrijven maar nog niet van verdachten in de zin van art. 27 Sv), drie in de meer klassieke opsporing (als er wel sprake is van een concrete verdenking). De geïnterviewden zijn gekozen uit verschillende afdelingen/disciplines: een persoon die standaard meedraait in alle TGO's[12] van een eenheid, een persoon die betrokken is bij een team dat zich richt op pro-actief onderzoek naar een bepaalde doelgroep, een persoon die werkzaam is op een afdeling die zich specifiek richt op zogenaamde Open Source Intelligence (OSINT), een persoon die werkzaam is binnen de Informatieorganisatie en betrokken bij een langlopend onderzoek waarbinnen veel social media gebruikt worden en een medewerker van de Digitale Opsporing die op basis van zijn kennis van (de techniek van) social media vaak gevraagd wordt om als internetrechercheur een bijdrage te leveren aan onderzoeken.
Verschillende respondenten gaven aan dat de informatie die zij verstrekten dusdanig vertrouwelijk is (met name informatie over de gehanteerde werkwijze), dat het ongewenst zou zijn als deze

[12] TGO = Team Grootschalige Opsporing. Een TGO is een tijdelijke hulpstructuur die door politie en OM wordt ingericht bij de aanpak van complexe rechercheonderzoeken, die door de grote maatschappelijke impact en acute noodzaak tot inrichting van een omvangrijk team niet door de staande opsporingsafdeling(en) binnen een eenheid kunnen worden afgehandeld. Een TGO wordt in in principe alleen gestart in geval van een kapitaal misdrijf met te verwachten grote maatschappelijk impact waarbij geen ondubbelzinnig daderschap kan worden vastgesteld.

informatie op concrete personen en/of onderzoeksteams teruggevoerd zou kunnen worden. Om die reden is ervoor gekozen om de resultaten van de interviews anoniem in deze scriptie weer te geven.

2.3.2 Resultaten

Algemeen

Uit de afgenomen interviews blijkt dat de politie het belang van social media voor de opsporing duidelijk onderkent. In alle bezochte eenheden zijn opsporingsambtenaren aangesteld die zich specifiek richten op social media als onderzoeksomgeving. Soms zijn het complete afdelingen die volledig gericht zijn op opsporing op social media (het genoemde doelgroepteam en de afdeling OSINT), in de andere gevallen betreft het individuele rechercheurs die ondersteuning bieden aan de tactische opsporing. Rechercheurs worden daarbij geselecteerd uit de reguliere opsporing op basis van kennis, interesse of technische achtergrond, of uit de informatieorganisatie op basis van kennis en ervaring in (online) informatieverzameling.

Doel van de opsporing op social media en de wijze waarop deze opsporing plaatsvindt

De reden waarom op een bepaald moment wordt besloten om de opsporing (ook) op social media te doen, verschilt. Voor de genoemde gespecialiseerde afdelingen is opsporing op social media *core business*. De rechercheur van het doelgroepenteam geeft aan dat zij wel aanwezig móeten zijn op social media: "Het is bekend dat minimaal 90% van de communicatie tussen de doelgroep via social media plaatsvindt. Het is daarom van cruciaal belang om binnen die omgeving een goede informatiepositie te hebben."

Een van de geïnterviewden (de rechercheur die standaard wordt ingezet op TGO's) is in de praktijk ook full-time bezig met opsporing op social media. In zijn eenheid is ervoor gekozen om bij elk TGO zeker in de beginfase zoveel mogelijk informatie te verzamelen over de locatie van het incident, over het slachtoffer, over getuigen en over eventuele verdachten. Voor de rechercheurs die meer een ondersteunende rol hebben, bepaalt de aard van het onderzoek of ze worden ingezet. Daarbij speelt de wijze waarop het misdrijf is gepleegd vaak een rol: als er een bedreiging via social media heeft plaatsgevonden, ligt het voor de hand dat via social media wordt geprobeerd om de identiteit van de bedreiger te achterhalen. En ook bij zedenmisdrijven speelt tegenwoordig internet vaak een rol (denk bijvoorbeeld aan verspreiding van kinderporno, grooming, sexting en chantage met pikante foto's maar ook pedofielen die via internet onderling contact onderhouden). Ook dan wordt vaak (mede) via social media onderzoek gedaan.

Daarnaast wordt social media gebruikt om een completer beeld te construeren van betrokkenen bij een misdrijf (zowel slachtoffer(s) als mogelijke dader(s)). Het gaat dan om het in beeld brengen van wat iemand op bijvoorbeeld Facebook of Twitter publiceert, maar ook hoe zijn online netwerk eruit

ziet (volgers, vrienden, vrienden van vrienden), op welke plaatsen hij geweest is etc. Afhankelijk van de fase waarin het onderzoek zich bevindt, wordt de informatieverzameling van breed (bijvoorbeeld bij de start van een TGO) steeds gerichter.
Het soort informatie dat de politie verzamelt op social media wordt vooral bepaald door de concrete vraag vanuit de tactische opsporing. Soms gaat het om "alles wat je kunt vinden" bij bijvoorbeeld een TGO, soms wordt bij een bepaald soort misdrijf de hulp van een gespecialiseerde rechercheur ingeroepen (bijvoorbeeld online bedreigingen of zedenmisdrijven met een online-aspect). Ook komt het voor dat alle uitingen van iemand op social media bekeken worden om te kijken of hij/zij bepaalde uitlatingen doet die relevant zijn voor de opsporing.
De hulpmiddelen die gebruikt worden bij de opsporing op social media verschillen ook. Vaak wordt gebruik gemaakt van IRN-computers[13] om (redelijk) anoniem op internet te zoeken. Daarnaast wordt gebruik gemaakt van gespecialiseerde zoektools. Sommige geïnterviewden geven aan dat ze voor de opsporing een of meer fake-accounts op Facebook hebben. Deze accounts worden gebruikt om toegelaten te worden in bepaalde groepen en om "vrienden" te worden met verdachten of mensen daar omheen. Om de accounts geloofwaardig te houden, wordt af en toe iets geplaatst op de eigen Facebook-pagina of wordt gecommuniceerd met een andere Facebook-gebruiker. De meer gespecialiseerde afdelingen gaan hierin veel verder: zij gaan met hun account nadrukkelijk de interactie met hun subjecten aan. Wel geven zij zelf aan dat er wel een grens zit aan die interactie: "Een belangrijke grens bij de interactie met subjecten is dat er geen sprake mag zijn van (mede)plegen van strafbare feiten, ook al zou dat goed kunnen werken voor de geloofwaardigheid van het profiel.".

De rol van de opsporingsbevoegdheden bij het onderzoek op social media

Ten aanzien van het vraagstuk rondom de bevoegdheid tot opsporing op social media is ook een verschil te zien tussen de rechercheurs die door een team of een onderzoek worden ingeschakeld en de rechercheurs op de gespecialiseerde afdelingen (doelgroepteam en OSINT). De eerste groep werkt in opdracht van een ander en heeft geen rechtstreeks contact met de officier van justitie ten aanzien van de bevoegdheid. Het opdrachtgevende team geeft aan dat de officier instemt met het onderzoek en daarmee kan de internetrechercheur aan het werk. Als er dan door de internetrechercheur kritische vragen worden gesteld over bijvoorbeeld de stelselmatigheid van het onderzoek op social media, wordt daar door het opdrachtgevende team niet veel mee gedaan. In de woorden van een

[13] IRN = Internet Research Netwerk, een netwerkinfrastructuur die de gebruikers in staat stelt om (redelijk) anoniem onderzoek te doen op internet, waarbij de uitgevoerde handelingen worden vastgelegd in een logging. Daarmee is naderhand precies te reconstrueren hoe bepaalde informatie gevonden is. IRN is onder andere in gebruik bij de politie, de FIOD, de AFM en de SIOD

van de geïnterviewden: “De politie is goed doordrongen van de noodzaak om binnen de wettelijke bevoegdheden te opereren (dit besef leeft breed binnen de politie), maar in het opsporingsbelang worden uiteraard wel de grenzen opgezocht.”.
Anders is dat bij de tweede groep rechercheurs. Omdat zij zelf het hele opsporingsonderzoek uitvoeren, staan ze over het algemeen rechtstreeks in contact met de officier van justitie. In die situaties vindt wel het gesprek over de benodigde bevoegdheid plaats. Ook deze teams moeten wel eens “nee” verkopen, en dat wordt niet altijd even gemakkelijk geaccepteerd: “In de publieke opinie wordt van de politie verwacht dat zij hetzelfde kunnen en mogen als wat de burger kan en mag. Als je dan aangeeft dat dit gelet op het juridisch kader niet toegestaan is, wordt dat niet altijd geaccepteerd.”.
Beide teams geven aan dat aan de hand van de stelselmatigheid van de onderzoekshandelingen er vaak onder een bevel Stelselmatige Informatie-inwinning, Stelselmatige Observatie, Werken onder Dekmantel of Pseudokoop wordt gewerkt. Overigens konden de teams niet aangeven of basis van welke harde criteria wordt vastgesteld of de grens van de stelselmatigheid is bereikt. Het OSINT-team geeft aan dat zij onderzoeksverzoeken in beginsel afwijzen als het aanvragende team niet voor het benodigde bevel heeft gezorgd.

De wijze waarop het onderzoek op social media wordt verantwoord en welke rol dit deel van het onderzoek speelt op de terechtzitting

Veel van de geïnterviewden geven aan dat de informatie die zij verzameld hebben, beschikbaar gesteld wordt aan het tactische team dat het daadwerkelijke opsporingsonderzoek verricht in de vorm van een proces verbaal van bevindingen. De verantwoording van de wijze waarop het onderzoek op social media heeft plaatsgevonden, beperkt zich in het uiteindelijke procesdossier over het algemeen tot termen als “Uit onderzoek op social media is gebleken dat ….”. Soms wordt op uitdrukkelijk verzoek van de betrokken officier van justitie in het dossier weinig aandacht besteed aan de hulpmiddelen die bij het onderzoek zijn gebruikt (zoals gebruikte tools voor zoeken op internet en verzamelen van gegevens alsmede gehanteerde zoekvragen). Dat kan ook een tactische reden hebben: “Vaak wordt zo weinig mogelijk in het dossier beschreven welke middelen zijn gebruikt bij het onderzoek op social media om zo de opsporingsmethode niet prijs te geven.”.
Wel wordt soms vermeld dat het onderzoek via een IRN-computer heeft plaatsgevonden. Door de logfunctie in IRN is het indien gewenst mogelijk om na afloop van het onderzoek de uitgevoerde handelingen te reconstrueren. Voor het doelgroepenteam geldt dat zij hun informatie in de vorm van een kluisverbaal verstrekken aan het Team Criminele Inlichtingen (TCI).[14] Een kluisverbaal is een

[14] Voorheen bekend onder de naam Criminele Inlichten Eenheid (CIE)

proces verbaal dat niet in de politiesystemen wordt opgeslagen, maar in de kluis van het TCI. Het TCI kan deze informatie door middel van een verstrekking aan een tactisch team doen toekomen. Daarbij wordt dan de bron van de informatie en de wijze waarop de informatie is verkregen afgeschermd voor de ontvanger.

Alle geïnterviewden geven aan dat het nog nooit is voorgekomen dat op de terechtzitting de wijze van informatievergaring via social media ter sprake is gekomen. Naar de oorzaken hiervan blijft het gissen, maar sommige geïnterviewden geven aan dat dit waarschijnlijk mede veroorzaakt wordt door een gebrek aan kennis van deze materie bij zowel rechters als bij advocaten. Een van de geïnterviewden zegt daarover: “Het gevoel leeft dat de kennis op dit terrein bij ZM en advocatuur beperkt is.”.

2.4 Conclusies

De politie is sinds een aantal jaar bezig met een inhaalslag waar het gaat om het gebruik van social media binnen alle politieprocessen. Waar men begon met social media als een extra communicatiemiddel (denk aan de twitterende wijkagent), is het gebruik van social media in korte tijd binnengedrongen in heel veel aspecten van het politiewerk. Daarmee sluit de politie aan bij de ontwikkeling in de maatschappij waar het sociale leven van vooral jongeren zich steeds meer online afspeelt. De informatie die met vrij weinig moeite op social media gevonden kan worden, bevat vaak voor de politie interessante informatie. Elke eenheid van de politie beschikt inmiddels over een of meer gespecialiseerde rechercheurs die door hun diepgaande kennis van social media in staat zijn om met gespecialiseerde hulpmiddelen veel informatie op social media te vinden die voor de opsporing nuttig kan zijn. Sommige van deze specialisten zijn afkomstig uit de informatieorganisatie, anderen zijn vooral vanuit technische aanleg en interesse bij dit vakgebied gekomen. Ook zijn er eenheden die gespecialiseerde afdelingen voor het zoeken in zogenaamde open bronnen hebben ingericht (OSINT). In de praktijk worden dergelijke afdelingen vaak ingezet in de meer pro-actieve fase van de opsporing (zoals dreigingen en fenomeenonderzoek). Een enkele eenheid heeft een afdeling ingericht die heimelijk opereert binnen een bepaalde doelgroep. Om echt effectief te zijn in het gebruik van social media binnen de opsporing is het van belang dat dit niet beperkt blijft tot specialisten maar dat alle rechercheurs geschoold worden in het opsporen op social media.[15]

Voor wat betreft de vraag naar de benodigde bevoegdheid geven de geïnterviewde rechercheurs vrij unaniem aan dat dat wordt overgelaten aan het tactische team dat om het onderzoek op social media heeft gevraagd. Als dat team aangeeft dat het onderzoek is goedgekeurd door de officier van

[15] Zie ook Stol, Leukfeldt & Klap 2013

justitie, wordt het onderzoek op social media uitgevoerd en worden de resultaten aan het aanvragende team verstrekt in de vorm van een proces verbaal.
Anders is dat bij het OSINT-team en het doelgroepenteam. De onderzoeken die door deze teams worden uitgevoerd, zijn vaak zelfstandige onderzoeken. In die gevallen wordt de vraag naar de benodigde bevoegdheid wel rechtsreeks besproken met het Openbaar Ministerie. Deze teams hebben dan ook de meeste ervaring met vraagstukken rondom stelselmatigheid. Een eenduidige keuze over welke bevoegdheid voor welk soort onderzoekshandeling wordt ingezet is echter nog niet gemaakt.[16] Uit de interviews is niet duidelijk geworden op basis van welke criteria besloten wordt dat een opsporingshandeling niet op basis van art. 3 PolW kan worden uitgevoerd en aanvullende bevoegdheden noodzakelijk zijn. Het zou goed zijn als vanuit het OM concrete handvatten worden aangereikt aan de politie zodat de politie hier bewuster mee om kan gaan.

De verantwoording van de uitgevoerde onderzoekshandelingen op social media in het procesdossier zou de rechter en de verdediging in staat moeten stellen om de rechtmatigheid daarvan te beoordelen. Uit de interviews blijkt dat de wijze waarop het onderzoek op social media heeft plaatsgevonden over het algemeen vrij summier beschreven wordt, in termen als “Uit onderzoek op social media is gebleken dat…”. Vaak vormt de verzameling van informatie via social media ook niet de kern van het onderzoek maar is het ondersteunend aan de bewijzen die elders in het onderzoek zijn verzameld. Het is zeer de vraag of de beschrijving van de gevolgde werkwijze ten aanzien van het onderzoek op social media voldoende is voor rechters en advocaten om de bedoelde objectieve toetsing te doen. Tijdens de interviews zijn er vanuit de praktijk geen voorbeelden aangedragen waarbij dit onderwerp aan de orde is geweest in een terechtzitting.[17] Naar de reden daarvoor blijft het speculeren, maar onbekendheid ten aanzien van social media bij rechters en advocaten wordt door meedere mensen aangewezen als een van de oorzaken.[18] Om dit vast te stellen, zou nader onderzoek uitgevoerd moeten worden. Echter, het valt te verwachten dat binnen de Zittende Magistratuur en de advocatuur deze kennis in de loop van de tijd verder zal toenemen, zodat het een kwestie van tijd lijkt voordat dit onderwerp wel nadrukkelijk ter sprake zal komen tijdens een terechtzitting. Het lijkt niet onverstandig voor politie en OM om daarop voorbereid te zijn en over de opsporingsbevoegdheden op social media heldere regels vast te stellen. Daar komt bij dat vanuit het

[16] Wel is er een werkgroep actief waarin OM, politie en BOD’s gezamenlijk een pragmatisch juridisch kader op te stellen waarmee dergelijke vragen beantwoord kunnen worden. Op dit moment is het eindproduct van deze werkgroep nog niet beschikbaar.
[17] In een zeer recente zaak (zie http://www.nrc.nl/nieuws/2015/09/10/politie-raakt-cruciale-informatie-jihadproces-kwijt-op-internet/) werd door de verdediging wel het vermeend onrechtmatig gebruik van bepaalde opsporingsmethoden op Facebook aan de orde gesteld.
[18] Zie ook Veenstra, Leukfeldt & Boes 2013

oogpunt van rechtmatigheid van de opsporing het hoe dan ook ongewenst is als er onduidelijkheid bestaat over de bevoegdheid om bepaalde opsporingshandelingen te verrichten. Bovendien is de politie op basis van art. 152 Sv verplicht om zo spoedig mogelijk proces-verbaal op te maken van de door hen opgespoorde strafbare feiten en hetgeen door hen ter opsporing is verricht of bevonden (de zogenaamde verbaliseringsplicht).

3 Privacy

3.1 Inleiding

Bij opsporing op social media is het recht op privacy van de onderzochte persoon in het geding. Nu doet zich ten aanzien van privacyvraagstukken in elektronische omgevingen een merkwaardige paradox voor. Waar het privacyvraagstuk al in de beginfase van de ontwikkeling van elektronische netwerken gezien werd als een cruciaal ethisch vraagstuk, lijkt het erop dat burgers zich steeds minder gelegen laten liggen aan de steeds groter wordende inbreuk die er op hun privacy zou worden gemaakt.[19] Uit een onderzoek uit 2015, dat in opdracht van Kaspersky Lab is uitgevoerd onder ruim 1000 Nederlanders van 18 jaar of ouder, blijkt dat mensen weliswaar in het algemeen belang hechten aan privacy maar dat ze vaak bereid zijn om privacy in te leveren in ruil voor gemak, gezondheid of veiligheid.[20] En al in 1997 deed Stol met een aantal collega's een onderzoek naar wat weggebruikers vonden van de videocontrole die op de ringweg van Amsterdam zou gaan worden toegepast. Het vermoeden was dat men wel bezwaren zou hebben in verband met de privacy, maar het bleek dat men privacy vrij gemakkelijk opgaf in ruil voor (de suggestie van) veiligheid.[21]
Privacy is een containerbegrip, waarbij diverse morele vraagstukken een rol spelen. Als deze vraagstukken niet helder van elkaar worden onderscheiden, leidt dit onvermijdelijk tot begripsverwarring.
Daarom wordt in dit hoofdstuk allereerst een aantal definities van het begrip privacy beschreven (paragraaf 3.2). Daarbij geldt dat de begrippen persoonlijke levenssfeer en privacy qua betekenis niet echt van elkaar verschillen, zodat de begrippen door elkaar gebruikt kunnen worden. Vervolgens wordt in paragraaf 3.3 gekeken naar de historische ontwikkeling van het recht op privacy. Daarna wordt in paragraaf 3.4 aandacht besteed aan het juridisch kader rondom privacy waarbij ook wordt nagegaan hoe de bescherming van privacy in de jurisprudentie nader is ingevuld. Het hoofdstuk sluit af met een aantal conclusies (paragraaf 3.5).

3.2 Definities van privacy

Twee dominante denktradities die in Nederland aan de basis liggen van het politieke en morele leven zijn het liberalisme en het communitarisme. De eerste gaat vooral uit van de vrijheid en de autonomie van het individu, de andere staat daar kritisch tegenover en legt meer nadruk op de gemeenschap en het collectieve belang. Een definitie van privacy die uitgaat van het liberalisme besteedt vooral aandacht aan het recht van het individu om gevrijwaard te blijven van

[19] De Mul & Van der Ploeg 2001
[20] Rapportage onderzoek online privacy, Right Marktonderzoek in opdracht van Kaspersky Lab, 10 februari 2015
[21] Stol & Van Treeck 1997

overheidsbemoeienis, terwijl vanuit het communitarisme overheidsingrijpen in de persoonlijke levenssfeer gelegitimeerd wordt wanneer het collectieve belang dit noodzakelijk maakt.
In de literatuur gaat de discussie rondom het recht op privacy ver terug. Al in de 19e eeuw werd er vooral in de Verenigde Staten over geschreven. Privacy-pioniers Warren en Brandeis kiezen bij hun definitie van privacy de eerste invalshoek, door privacy te omschrijven als "het recht om met rust gelaten te worden".[22] Privacy maakt dan onderdeel uit van de afweerrechten die verwantschap vertonen met de klassieke grondrechten: vrijheidsrechten van de burger ten opzichte van de overheid. Toegespitst op de wereld van de ICT komt Westin tot de definitie: "de claim van het individu, de groep of de institutie, om zelf te bepalen wanneer, hoe en in welke mate informatie over hem of haar aan anderen wordt gegeven".[23] Fried zegt het korter en meer op het individu gericht: privacy is "controle van het individu over kennis over hem/haar zelf".[24] Van verlies aan privacy is dan sprake als anderen informatie verkrijgen over, aandacht besteden aan of toegang verkrijgen tot een individu.[25] Privacy in deze zin is meer een actierecht: de persoon zelf is degene die zijn eigen ruimte bewaakt en behoudt. Deze invalshoek ligt meer in de sfeer van de sociale grondrechten.[26] Wel kan van deze definitie gezegd worden dat hij wat instrumenteel van karakter is en weinig aandacht besteedt aan de emotie die gepaard gaat met privacy.
Bij Johnson wordt bij de duiding van privacy vooral aandacht besteed aan de relatie tussen betrokken actoren.[27] Privacy heeft bij hem betrekking op de bescherming van bepaalde aspecten van individuen tegen de (positieve of negatieve) evaluatieve oordelen van anderen. Daarmee wordt de betekenis en inhoud van privacy afhankelijk van de omstandigheden waarbinnen het begrip gebruikt wordt en is dan een dynamisch begrip. Bepaald gedrag kan de ene dag vanuit het oogpunt van privacy onaanvaardbaar zijn maar de volgende dag op basis van gewijzigde maatschappelijke omstandigheden maar bij een gelijkblijvend juridisch kader wel acceptabel.
Bij een dergelijke relatiegerichte visie op privacy is de betekenis en inhoud van privacy dus afhankelijk van de omstandigheden. Daarmee is dan ook interessant wat op een bepaald moment de dominante opvattingen van burgers over privacy zijn. In Nederland is niet veel onderzoek gedaan naar opvattingen van individuen over privacy en privacybedreigingen. In 1999 verscheen bij het Rathenau-instituut een studie onder de titel *Privacybeleving van burgers in de informatiemaatschappij* waarin de auteurs onderzoek doen naar waarden, normen en opvattingen

[22] Warren & Brandeis 1890
[23] Westin 1967
[24] Fried 1986
[25] Gavison 1980
[26] Azouz e.a. 2007
[27] Johnson 1989

achter privacy.[28] De auteurs constateren dat waarden achter privacy zijn: zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering, ongestoord leven, eigenwaarde, vrij blijven van manipulatie, integriteit en autonomie. Daarnaast komen ze tot de conclusie dat verschillende personen verschillende waardestelsels hanteren en daardoor verschillende waarden meer of minder belangrijk vinden. Het is dan wel mogelijk om in algemene zin iets te zeggen over privacy en de achterliggende waarden, maar het belang dat individuen toekennen aan die waarden verschilt van persoon tot persoon en van situatie tot situatie.

Nissenbaum gaat bij haar definitie van privacy nog een stap verder.[29] De definitie van privacy als een recht op geheimhouding is wat haar betreft veel te ongeraffineerd. “Volledige controle over jouw informatie kun je alleen bereiken als je in een grot gaat wonen. Het delen van persoonlijke informatie is een essentieel onderdeel van het leven. Als je de redenering doordenkt, betekent het dat iedere keer dat je de controle ook maar een beetje kwijtraakt, jouw privacy wordt geschonden. Dat is natuurlijk onzin. (…) Zo’n rigide definitie van privacy leidt tot een recht dat niet te verdedigen valt omdat er alleen maar uitzonderingen op bestaan.”, zei ze in een interview.[30] In haar opvatting kent privacy zowel een individuele als een sociale component. Enerzijds heeft het individu het recht om te bepalen wat er met zijn of haar gegevens gebeurt. Anderzijds heeft veel informatie die iemand deelt ook betrekking op anderen. Deze sociale component vormt de basis voor het door Nissenbaum geïntroduceerde begrip *contextual integrity*. Centraal in haar betoog staat de stelling dat mensen niet een privacyschending ervaren als zij het gevoel hebben de controle over de informatie kwijt te raken of als de geheimhouding wordt geschonden, maar wel als ze de desbetreffende informatiestroom niet gepast vinden. Daarmee introduceert Nissenbaum een normatief aspect in de definitie van privacy. Binnen een bepaalde context stroomt er informatie van zender naar ontvanger. De stroom heeft een onderwerp, is van een bepaald type en wordt onder bepaalde voorwaarden of met een bepaalde bedoeling verzonden. Als een of meer van deze elementen veranderen, zou de informatiestroom niet meer gepast kunnen zijn en dan wordt het gebruik van de informatie door de zender als privacyschending ervaren. Van belang is dat het doel van een bepaalde context sociaal gedefinieerd is: de samenleving bepaalt wat het doel van een informatiestroom is. Op basis van dat doel kan bepaald worden of een informatiestroom acceptabel is. Het recht op privacy houdt in de gedachtengang van Nissenbaum in dat iemand er recht op heeft dat de informatie in een informatiestroom die als ongepast wordt beschouwd, niet gebruikt wordt.

[28] Smink, Hamstra & Van Dijk 1999
[29] Nissenbaum 2010
[30] ‘Deze bevlogen professor helpt je doorgronden wat privacy is’, https://decorrespondent.nl/1998/Deze-bevlogen-professor-helpt-je-doorgronden-wat-privacy-is/61450488-b6ee8d9d

Op basis van de vooral in de EHRM-jurisprudentie ontwikkelde doctrine van de *reasonale expectation of privacy*[31] (zie paragraaf 3.4.3) zal bij de te hanteren definitie van privacy een subjectief element meegenomen moeten worden. Het elegante van de theorie van de *contextual integrity* is dat het dat subjectieve element verbindt met specifieke eigenschappen van social media. Door gebruik te maken van social media kiezen burgers ervoor om een deel van hun privacy op te geven: social media zijn er immers naar hun aard op gericht om informatie te delen. Daarmee geeft de gebruiker van social media impliciet aan de informatiestroom naar de ontvangers van die gegevens passend te vinden. Veel social media bieden ook mogelijkheden om gepubliceerde informatie af te schermen en daarmee zelf controle te voeren op welke informatiestromen passend gevonden worden. De "passendheid" van kennisname van informatie op social media door opsporingsinstanties kan vervolgens net als bij Johnson door de maatschappij gedefinieerd worden.

Omdat het in dit onderzoek gaat over overheidsoptreden dat in de wet wordt gereguleerd, zal de te hanteren definitie van privacy moeten aansluiten bij de definitie zoals de wetgever die heeft gebruikt. De notie van de contextualiteit zoals Nissenbaum die heeft geïntroduceerd combineert dit recht op een elegante manier met een meer subjectieve kijk op privacy, die ook goed aansluit bij de *reasonable exptectation of privacy*. Voor dit onderzoek wordt uitgegaan van de volgende definitie van privacy:

> *Privacy is het recht om onbevangen zichzelf te zijn, binnen de grenzen die door het betrokken individu en door de maatschappij als passend worden ervaren. De precieze ligging van deze grenzen wordt mede beïnvloed door de mate waarin het individu door zijn gedrag laat merken dit recht op te geven.*

3.3 Historie van de ontwikkeling van het recht op privacy

Om het belang dat burgers hechten aan privacy te duiden, is het goed om op deze plaats nader te beschouwen hoe het begrip privacy zich in de geschiedenis heeft ontwikkeld en waarin het zijn wortels vindt. De aandacht voor privacy heeft met name in de jaren 60 van de twintigste eeuw een grote impuls gekregen. In die tijd kwam er meer aandacht voor de Jodenvervolging in de Tweede Wereldoorlog en werd aangetoond dat een deugdelijke bevolkingsregistratie en efficiënte identificatieplicht bij die vervolging een grote rol hadden gespeeld. Deze constateringen waren koren

[31] Hierbij staat centraal de vraag of de betrokkene(n) gezien de omstandigheden van het geval een redelijke privacyverwachting mocht(en) hebben.

op de molen van het maatschappelijke protest tegen grootschalige verwerking van persoonsgegevens door de overheid.

De angst van burgers voor een alwetende overheid werd treffend verwoord in het boek *1984*[32] van George Orwell. Dit boek verscheen tijdens de Koude Oorlog (een term die als eerste gebruikt werd door diezelfde George Orwell), een periode die gekenmerkt werd door argwaan ten opzichte van regimes. De invloed van Orwell blijkt wel uit het feit dat de term *Big Brother* uit *1984* een staande uitdrukking is geworden in de Nederlandse taal.[33]

In de periode na de Tweede Wereldoorlog kwam in Nederland de verzorgingsstaat tot ontwikkeling. De groeiende welvaart zorgde ervoor dat er ruimte ontstond om een maatschappelijk vangnet op te zetten in de vorm van volks- en werknemersverzekeringen en de bijstand. De uitvoering van deze wetten en regelingen vereiste echter wel een aanzienlijke groei van het overheidsapparaat. Die groei ging gepaard met een enorme toename van de overheidsadministratie. Daarbij werd dankbaar gebruik gemaakt van de stormachtige ontwikkeling van de automatisering. Dit leidde onder andere tot een modernisering van de bevolkingsadministratie.

Deze ontwikkelingen zorgden ervoor dat er een brede bewustwording op gang kwam ten aanzien van privacyrisico's bij grootschalige verwerking van persoonsgegevens. Deze bewustwording leidde medio 1970 tot een besluit van de ministerraad om een algemene privacywet te ontwikkelen. Hiertoe werd in 1972 de Staatscommissie Koopmans ingesteld. In 1976 verscheen het eindrapport van deze commissie. Daarnaast werd een start gemaakt met de voorbereiding van een Wet op de Centrale Personenadministratie, wat overigens pas in 1989 leidde tot de invoering van de Wet bescherming persoonsregistraties. Tenslotte werd een traject gestart om het recht op privacy als grondrecht te verankeren in de Grondwet,[34] mede bedoeld om het vertrouwen tussen overheid en burgers te herstellen. Dat herstel werd noodzakelijk geacht om door te kunnen gaan met de modernisering van de overheidsadministratie. Uitkomst van dit traject was dat het recht op bescherming van de persoonlijke levenssfeer in de Grondwet is verankerd als een zelfstandig, algemeen geformuleerd grondrecht (zie hiervoor 3.4.2).

Een laatste relevante ontwikkeling rondom de ontwikkeling van het recht op privacy is de toenemende invloed van de Europese eenwording op dit onderwerp. Al in 1990 heeft de Europese Commissie een voorstel voor een richtlijn ingediend met betrekking tot de bescherming van de persoonsgegevens. Deze is in 1995 vastgesteld en in 1998 in werking getreden.[35] Van recenter datum is de afkondiging van het Handvest van de Grondrechten van de Europese Unie op 7 december

[32] Orwell 1949
[33] Zie ook Stol 2014 p. 242-244
[34] In het EVRM stond het recht op privacy al sinds 1950 in artikel 8, waarbij uiteraard aansluiting werd gezocht.
[35] Richtlijn 95/46/EG

2000.[36] Ook in dat handvest is het recht op eerbiediging van de persoonlijke levenssfeer vastgelegd. Met het Verdrag van Lissabon is in art. 6 lid 1 VEU aan dit Handvest dezelfde juridische waarde als de verdragen toegekend.

Overigens is met die wettelijke verankering van het recht op privacy de maatschappelijke discussie over dit onderwerp niet gesloten. In de uitingen van organisaties als Bits of Freedom[37] en Privacy First[38] klinkt nog steeds het oude wantrouwen ten opzichte van overheid en bedrijfsleven door. Gelet op de hiervoor (3.2) beschreven "definitie" van privacy zal deze maatschappelijke discussie ook moeten blijven doorgaan. Alleen zo kan blijvend een actueel beeld verkregen worden van wat in de maatschappij als passend gebruik van de informatie op social media door opsporingsinstanties wordt beschouwd. Bovendien is een dergelijke discussie noodzakelijk in het creëren van een goede balans tussen de belangen van de opsporing en de grondrechten van de burgers.

3.4 Actueel juridisch kader ten aanzien van privacy

3.4.1 Internationale en nationale wet- en regelgeving

In de vorige paragraaf is geschetst hoe het begrip privacy zich in de loop van de geschiedenis heeft ontwikkeld. Gelet op het belang dat in de maatschappij aan het recht op privacy gehecht wordt, is vervolgens aan de orde hoe dit recht is gecodificeerd.

Het recht op eerbiediging van de persoonlijke levenssfeer wordt in onze maatschappij vrij algemeen als een grondrecht beschouwd[39] en wordt in diverse verdragen en wetten beschermd:

- Art. 12 van de Universele Verklaring van de Rechten van de Mens (UVRM)
- Art. 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR)
- Art. 7 en 8 van het Handvest van de Grondrechten
- Art. 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM)
- Art. 10 t/m 13 van de Grondwet

Art. 17 IVBPR en art. 8 EVRM gaan beide terug op art. 12 UVRM. Overkleeft-Verburg geeft aan dat uit jurisprudentie-onderzoek blijkt dat art. 17 IVBPR in het nationale recht als toetsingskader niet of nauwelijks een rol speelt. De oorzaak hiervan is de inhoudelijke overlap met art. 8 EVRM gecombineerd met de gezaghebbendheid van de uitspraken van het Europees Hof voor de Rechten

[36] *PbEG* 2000, C 364/01
[37] www.bof.nl
[38] www.privacyfirst.nl
[39] Overkleeft-Verburg 2014 p. 13

van de Mens (EHRM).[40] Art. 7 van het Handvest is feitelijk een gemoderniseerde versie van art. 8 EVRM. In de toelichting bij het Handvest wordt ook aangegeven dat inhoud en reikwijdte van art. 7 dezelfde zijn als die van art. 8 EVRM. Art. 8 van het Handvest is volgens de toelichting geïnspireerd op Richtlijn 95/46/EG (bescherming persoonsgegevens door de lidstaten) en EG-verordening 45/2001 (verwerking persoonsgegevens door Europese instellingen). Beide artikelen uit het Handvest worden bij het EU Hof van Justitie regelmatig aangehaald en fungeren dan als belangrijke inspiratiebron. Vanwege de inhoudelijke overeenkomst tussen art. 17 IVBPR en art. 7 en 8 van het Handvest met art. 8 EVRM, zal de verdere bespreking voor wat betreft de internationale regelgeving in deze paragraaf over art. 8 EVRM gaan (3.4.3).

3.4.2 Artikel 10 Grondwet

Art. 10 van de Grondwet luidt als volgt:

1. *Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
2. *De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
3. *De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.*

Dit artikel kent een lange wordingsgeschiedenis. In 1966 werd het fundament gelegd in het ambtelijk rapport *Proeve van een nieuwe grondwet*. De opzet van deze proeve was om de grondrechten in de Grondwet te actualiseren, voor zover nodig in aanvulling op het EVRM. In dit geval ging het dus om aanpassingen op basis van art. 8 EVRM. De Staatscommissie Cals/Donner (1967-1971) schreef in haar tweede rapport in 1969 “dat de privacy in de huidige tijd bijzonder kwetsbaar is gebleken en uit dien hoofde behoefte bestaat aan nadere wettelijke bescherming”.[41] In het Eindrapport adviseert de commissie om een regelingsverplichting op te nemen (“De wet stelt regels ter bescherming van de persoonlijke levenssfeer”), omdat “het belang van de bescherming van de persoonlijke levenssfeer door deze bepaling erkenning vindt als te behoren tot de grondslagen van de rechtsorde”.[42]
In 1974 kwam het kabinet-den Uyl met een nota over de herziening van de Grondwet.[43] In die nota stelde het kabinet dat de Grondwet een bepaling diende te bevatten inzake het recht op inzage van

[40] Belinfante & de Reede 2009 p. 325 geven ook aan dat het belang de jurisprudentie van het EHRM ten aanzien van art. 8 EVRM steeds verder toeneemt
[41] *Tweede rapport van de Staatscommissie van advies inzake de Grondwet en de Kieswet* 1969
[42] *Eindrapport van de Staatscommissie van advies inzake de Grondwet en de Kieswet* 1971
[43] *Kamerstukken II* 1973/74, 12944, nr. 2

persoonlijke gegevens. Verder werd een nieuwe staatscommissie in het leven geroepen (de Staatscommissie Koopmans) die als opdracht kreeg om de regelingsverplichting concreet in te vullen. Het eindrapport van deze commissie verscheen in 1976.[44]

Uiteindelijk leidde deze voorgeschiedenis in 1976 tot een wetsvoorstel voor de herziening van de Grondwet. In de MvT[45] wordt het standpunt van het kabinet ten opzichte van privacy duidelijk: "Eerbiediging van de persoonlijke levenssfeer wordt in onze samenleving thans terecht beschouwd als een essentiële voorwaarde voor een menswaardig bestaan en als een van de grondslagen van onze rechtsorde". Het recht op privacy wordt daarmee ook formeel als grondrecht aangewezen en gecodificeerd in artikel 10 van de Grondwet.

Hoewel tijdens de invoering van de herziene Grondwet in 1983 er nog geen sprake was van internet in de huidige vorm, is de discussie rondom dit grondrecht nog steeds actueel. Net als toen staan ook nu de legitimiteit van het overheidshandelen in de democratische rechtsstaat en de noodzaak van een daarop toegesneden waarborgfunctie in de Grondwet centraal. Een nieuw element is sinds het begin de van de jaren negentig de toenemende invloed van de gespannen relatie tussen veiligheid en privacybescherming.

Privacy zoals opgenomen in art. 10 van de Grondwet is niet expliciet gedefinieerd. Wel wordt in de MvT[46] op een wat hoger abstractieniveau gedefinieerd wat onder persoonlijke levenssfeer moet worden verstaan: "het gebied waarbinnen elk individu vrij is en geen inmenging van anderen behoeft te dulden", "het recht zijn eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf" en "de reeks van situaties waarin de mens onbevangen zichzelf wil zijn". Nadere invulling van het begrip privacy wordt overgelaten aan wetgever en rechter.

Zoals hierboven geschetst was een van de redenen dat er meer aandacht kwam voor bescherming van privacy de toename van de verwerking van persoonsgegevens door de overheid. Ten aanzien van dat element van de persoonlijke levenssfeer wordt in de memorie van toelichting iets opgemerkt dat ook nu nog actueel is: "Doorslaggevend daarbij hoeft niet zozeer te zijn, dat al die gegevens intieme informatie zouden bevatten (…), maar de privacy-aantasting kan hierin gelegen zijn, dat over de individuele burger met al zijn hoedanigheden, gedragingen en kenmerken, welke zijn persoon en zijn leven vormen, op allerlei plaatsen gegevens worden vastgelegd en dat dit geheel van gegevens een steeds grotere invloed gaat krijgen op voor hem belangrijke zaken (…). Aldus kan een situatie ontstaan waarin de burger onvoldoende 'ruimte' overhoudt om zijn eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf". De wetgever kiest dus voor een privacy-begrip waarbij de

[44] *Eindrapport van de staatscommissie Koopmans* 1976
[45] *Kamerstukken II* 1975/76, 13872, nr. 3
[46] *Kamerstukken II* 1975/76, 13872, nr. 3

inbreuk op die privacy bepaald wordt door een combinatie van de hoeveelheid en de aard van de gegevens.

In lid 2 en 3 van art. 10 krijgt de wetgever een regelingsplicht om het recht op privacy te beschermen. Hieraan is uitvoering gegeven in een drietal wetten: de Wet persoonsregistraties[47] (per 1 september 2001 vervangen door de Wet bescherming persoonsgegevens, Wbp[48]), de Wet gemeentelijke basisadministratie persoonsgegevens[49] (per 6 januari 2014 vervangen door de Wet basisregistratie personen[50]) en de Wet politieregisters[51] (per 1 januari 2008 vervangen door de Wet politiegegevens[52]). De Wet bescherming persoonsgegevens en eerder de Wet persoonsregistraties fungeren als een algemeen kader om te bepalen of een bepaalde verwerking van persoonsgegevens rechtmatig is. Echter, dit kader was zo algemeen geformuleerd dat het in verschillende sectoren onvoldoende rechtszekerheid bood. Sinds het eind van de jaren tachtig is een ontwikkeling op gang gekomen om dit algemene kader in sectorwetgeving nader uit te werken en toe te passen. In de wetgeving is dit herkenbaar aan aparte informatieparagrafen. Zo kent bijvoorbeeld de Wet op de geneeskundige behandelingsovereenkomst (WGBO/BW) in artikel 457 en 458 een aantal voorschriften die specifiek gaan over de privacyrechten van de patiënt. Een ander voorbeeld is de nieuwe Jeugdwet. Ten aanzien van de privacy geldt dat in algemene zin de art. 8, 9 en 21 van de Wbp de grondslag voor de verwerking van persoonsgegevens zijn. Echter, in hoofdstuk 7 van de Jeugdwet worden deze normen nader toegespitst op het jeugdwerk.

Deze voorbeelden laten zien dat de Wbp niet de centrale positie heeft gekregen die de wetgever wel voorzien had.

3.4.3 Artikel 8 EVRM

Art. 8 EVRM luidt als volgt:

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.*

[47] Stb. 1988, 665
[48] Stb. 2000, 302
[49] Stb. 1994, 494
[50] Stb. 2013, 315
[51] Stb. 1990, 414
[52] Stb. 2007, 300

Zowel art. 8 EVRM als het voor de nationale context minder van belang zijnde art. 17 IVBPR gaan terug op art. 23 van de Universele verklaring van de rechten van de mens. Op grond van art. 93 en 94 van de Grondwet jo. art. 60 EVRM respectievelijk art. 5 lid 2 IVBPR zijn zowel art. 8 EVRM als art. 17 IVBPR ieder verbindende verdragsbepalingen en werken ze daarom rechtstreeks door in het nationale recht.

Waar het gaat om het beschermde belang zijn er geen significante verschillen tussen art. 8 EVRM en art. 10 Grondwet. Echter, als het gaat om de mogelijkheden om het grondrecht op privacy te beperken, is dat verschil er wel degelijk. Art. 10 Gw geeft in lid 1 aan dat de beperking van het recht op privacy alleen kan plaatsvinden op basis van een wet in formele zin. Art. 8 EVRM beschrijft de mogelijkheden om inbreuk te maken op het recht op privacy uitgebreider. Zoals bij meer grondrechten in het EVRM moet bij een geconstateerde inbreuk op een bepaald grondrecht worden vastgesteld of deze inbreuk rechtmatig is. En dat wordt weer bepaald aan de hand van de voorwaarden in lid 2 van datzelfde artikel. Daarin zijn drie elementen te onderkennen: (1) de beperking moet "in accordance with the law" zijn, (2) de beperking moet "necessary (zijn) in a democratic society" en (3) moet dienstbaar zijn aan een van de genoemde doelcriteria ("legitimate aim").[53]

In het eerste element wordt het begrip *law* ruim uitgelegd. Uit de EHRM-jurisprudentie blijkt dat ermee bedoeld wordt "een grondslag in het nationale recht". Oftewel: onder law wordt niet alleen de wet in formele zin verstaan, maar ook wetten in materiële zin alsmede jurisprudentie en beleidsregels.[54] Wel moet voldaan worden aan de vereisten van kenbaarheid en voorzienbaarheid.[55] Volgens de *Leidraad Wet bescherming persoonsgegevens* van het ministerie van Veiligheid en Justitie houdt het kenbaarheidsvereiste in dat de inmenging voor de burger in elk geval kenbaar moet zijn. Bij wetgeving, verdragen en besluiten van volkenrechtelijke organisaties wordt daaraan voldaan door deze bekend te maken in het Staatsblad, de Staatscourant, het Tractatenblad of het Publicatieblad van de Europese Unie. Aan de kenbaarheid van de motivering van wetsvoorstellen wordt voldaan door de publicatie van de Kamerstukken. Met betrekking tot de voorzienbaarheid geldt dat de inmenging voldoende nauwkeurig moet zijn geformuleerd zodat de burger in staat is om zijn gedrag af te stemmen op het geldende recht. Voor de bescherming van persoonsgegevens betekent dit dat de desbetreffende wet duidelijk moet aangeven met betrekking tot welke categorieën van personen gegevens mogen worden opgeslagen, maar ook onder welke omstandigheden gegevens mogen

[53] Zie voor een uitgebreide bespreking van art. 8 EVRM Rainey, Wicks & Ovey 2014. Zie ook Gerards 2014 voor een artikelsgewijze bespreking van de procedurele aspecten van het EVRM.
[54] Zie EHRM 2 augustus 1984, NJ 1988, 534 m.nt. P. van Dijk (Malone)
[55] Zie EHRM 26 april 1979, NJ 1980, 146 (Sunday Times); EHRM 2 augustus 1984, NJ 1988, 534 m.nt. P. van Dijk (Malone); EHRM 24 april 1990, NJ 1981, 523 m.nt. EJD (Huvig-Kruslin); EHRM 28 oktober 1994, NL 1995, 509 m.nt. Kn. (Murray v. Verenigd Koninkrijk); EHRM 29 augustus 1997, NJ 1999, 710 m.nt. EJD (Worm)

worden verzameld en hoe lang deze mogen worden bewaard. Ook moeten er voorzieningen zijn voor de transparantie en de controleerbaarheid van de opgeslagen informatie, zoals voorschriften voor verslaglegging. Dit heeft tot gevolg dat ruim geformuleerde discretionaire bevoegdheden in dit opzicht problematisch kunnen zijn. Verder moet duidelijk zijn welke sancties aan overtreders van deze voorschriften opgelegd kunnen worden.
Het tweede element (*noodzakelijk in democratische samenleving*) is bij het beoordelen van de rechtmatigheid van een inbreuk op de privacy veruit het belangrijkste. Hiervan is sprake als er een *pressing social need* is en dat de beperking evenredig is aan het daarmee beoogde doel (proportionaliteit).[56] Overkleeft-Verburg geeft aan dat uit de jurisprudentie van het EHRM blijkt dat dit vereiste tevens het subsidiariteitsbeginsel (inzetten van het minst ingrijpende middel) omvat.[57] In de zaak Lambert tegen Frankrijk[58] heeft het EHRM uitgesproken dat alle burgers effectief rechtsbescherming moeten hebben tegen privacy-inbreuken. Deze rechtsbescherming mag niet worden gemarginaliseerd door nationale wetgeving.
Aan het derde element (*legitimate aim*) worden over het algemeen weinig woorden vuil gemaakt. Over het algemeen wordt het belang van de opsporing als voldoende beschouwd om een opsporingsmethode als dienstbaar aan een genoemd doelcriterium aan te merken.

Eskens vraagt nog aandacht voor het feit dat er in de literatuur twijfel bestaat of de privacybescherming van art. 10 Gw ook moderne communicatiemiddelen omvat.[59] Zij verwijst daarbij onder andere naar Steenbruggen[60] en naar een aantal parlementaire stukken rondom de wijziging van de Grondwet.[61] Zij betoogt dat de bescherming van het recht op privacy door art. 8 EVRM wel het gebruik van moderne communicatiemiddelen zoals email en internet beschermt.[62] Omdat art. 8 EVRM in ons land het belangrijkste toetsingskader is ten aanzien van de privacy, levert dit verder geen complicaties op waar het gaat om de bescherming van de privacy in een online omgeving.

Uit bovenstaande beschrijving van de werking van art. 8 EVRM blijkt dat de beoordeling van privacyvraagstukken op basis van dit artikel casuïstisch van aard zal zijn. Immers, naast de formele vereisten (*in accordance with the law*) zal op basis van de concrete omstandigheden van het geval

[56] EHRM 26 april 1979, *NJ* 1980, m.nt. E.A. Alkema (*Sunday Times/Verenigd Koninkrijk*)
[57] Overkleeft-Verburg 2014
[58] EHRM 24 augustus 1998 (Lambert v. Frankrijk)
[59] Eskens 2015
[60] Steenbruggen 2009
[61] *Kamerstukken II* 1996/97, 25443, 3; *Kamerstukken II* 2000/01, 27460, 1; *Kamerstukken II* 2013/14,33989, 3
[62] Zie ook EHRM 3 april 2007, 62617/00 (Copland v. the UK), par. 41-42

moeten worden vastgesteld of een inbreuk die is geconstateerd noodzakelijk is in een democratische samenleving en de inbreuk een rechtmatig doel dient.

Bij het beoordelen van de vraag of er sprake is van een schending van art. 8 EVRM volgt het EHRM een vast stappenplan: allereerst wordt nagegaan of er sprake is van een inbreuk op het recht op privacy, daarna komen achtereenvolgens de hierboven gestelde vragen aan bod (namelijk of deze inbreuk *in accordance with the law* is, zo ja of er sprake was van een *legitimate aim*, zo ja of de inbreuk *necessary (was) in a democratic society*. Hoewel er in het geval van het optreden van de overheid ten opzichte van burgers al snel sprake is van een inbreuk op het recht op privacy,[63] is het recht op privacy niet onbeperkt. Zoals hiervoor gesteld is een schending van dat recht onder voorwaarden toelaatbaar. Om vast te stellen of de privacy is geschonden, wordt door het EHRM onder andere de doctrine van de *reasonable expectation of privacy* gehanteerd.[64] Hierbij staat centraal de vraag of de betrokkene(n) gezien de omstandigheden van het geval een redelijke privacyverwachting mocht(en) hebben.[65] In het concrete geval van het arrest-Lüdi werd bijvoorbeeld het optreden van een pseudo-koper niet in strijd geacht met art. 8 EVRM omdat de dader van een drugsdelict zich er wel van bewust móet zijn dat hij het risico loopt in handen te vallen van een undercover-agent. Daarmee werd de omvang van de persoonlijke levenssfeer van de dader restrictief uitgelegd. Het illegaal verkopen van drugs, en volgens Corstens meer in het algemeen het smeden van criminele plannen, viel daarmee buiten de privacybescherming.[66] Deze benadering sluit aan bij de Amerikaanse benadering.[67] Er zit echter wel een risico aan deze benadering: inbreuken op de privacy zijn eenvoudiger te rechtvaardigen. Eenzelfde handeling is dan bij een crimineel niet als schending aan te merken en bij een onschuldige burger wel. Corstens[68] is van mening dat deze redenering uitgaat van de overheid en niet vanuit de burger, hetgeen in zijn ogen een principieel verkeerd uitgangspunt is. Bovendien houdt het recht op privacy bescherming van de burgers tegen de overheid in. Het is dan niet juist om de overheid de omvang en de reikwijdte van die bescherming te laten bepalen. Dit leidt in de praktijk tot rechtsongelijkheid en rechtsonzekerheid. Bovendien kijkt deze benadering altijd achteraf. De bepaling van schuld en onschuld vindt immers plaats ná de privacy-inbreuk. Daarmee wordt volgens Corstens de bescherming van art. 8 EVRM ernstig ingeperkt. Hij ziet meer heil in het zoeken van de rechtvaardiging van de privacy-inbreuk in het

[63] In EHRM 16 februari 2000 (Amann v. Zwitserland) heeft het EHRM uitgesproken dat het enkel van staatswege opslaan van informatie die betrekking heeft op iemands (privé)leven reeds een inbreuk oplevert van het door art. 8 EVRM beschermde recht op privacy.

[64] EHRM 15 juni 1992 (Lüdi v. Zwitserland). Zie ook EHRM 23 november 1992 (Niemitz v. Germany); EHRM 27 maart 1997 (Halford v. the UK); EHRM 3 april 2007 (Copland v. the UK); EHRM 12 januari 2010 (Gillan and Quinton v. the UK)

[65] Blom 2001

[66] Corstens 2014

[67] Solove 2008

[68] Corstens 2014

opsporingsbelang. Daarbij gaat men uit van een schending waarvan achteraf wordt bepaald of deze gerechtvaardigd is. Het recht op privacy blijft daarmee niet onbeperkt, maar de valkuil van rechtsongelijkheid wordt daarmee vermeden.

Ook Knigge stelt de mogelijk onaanvaardbare gevolgen van de *reasonable expectation of privacy* doctrine aan de orde in zijn noot bij het arrest *Beslagen autoruiten.*[69] Hij geeft aan dat dit criterium normatief moet worden ingevuld. De gedachtegang moet verschuiven van wat objectief gezien verwacht *kan* worden naar de vraag waarop betrokkenen aanspraak kunnen maken. Hij geeft wel aan dat daarmee de doctrine zijn eigenlijke kracht verliest: hetgeen waar men aanspraak op kan maken op basis van art. 8 EVRM en art. 10 Gw is de bescherming van de persoonlijke levenssfeer en daarmee is de cirkel rond.

Ondanks deze bezwaren tegen de mogelijk ongewenste gevolgen van een te rigide uitleg van de *reasonable expectation of privacy* is het toch de heersende doctrine binnen de jurisprudentie van het EVRM. Zoals eerder gesteld (3.2) zal in de doorgaande maatschappelijke discussie de invulling van dit subjectieve begrip bepaald moeten worden.

Net als bij andere grondrechten hebben de lidstaten namelijk wel een zekere *margin of appreciation* waar het gaat om de wijze waarop het recht op privacy wordt geborgd in de nationale rechtsorde en de afweging tussen het belang van de privacy en het maatschappelijk belang, hoewel de observatie van Overkleeft-Verburg[70] is dat de rechtspraak van het EHRM over art. 8 EVRM een steeds meer rechtspolitieke inslag heeft gekregen met betrekking tot de waarborging van de persoonlijke autonomie. Door deze sterkere aandacht voor de persoonlijke autonomie is de *margin* substantieel verkleind. Met name vanuit het Verenigd Koninkrijk bestond veel bezwaar tegen deze verkleining van de *margin* en daarmee de zeggenschap van de lidstaten, hetgeen geresulteerd heeft in de vaststelling van Protocol no. 15 van 24 juni 2013, waarin in de preambule bij het EVRM nadrukkelijk de lidstaten worden aangewezen als *primary responsible* voor de bescherming van de grondrechten. Daarmee wordt uiteraard niet het EHRM terzijde geschoven, maar neemt de zeggenschap van de individuele lidstaten ten aanzien van de concrete invulling wel toe.

3.4.4 Recente ontwikkelingen

Op mondiaal niveau heeft met name de NSA-affaire[71] geleid tot een hernieuwde aandacht voor art. 17 IVBPR. De Algemene Vergadering van de Verenigde Naties heeft op 18 december 2013 een

[69] HR 19 maart 1996, NJ 1997, 85 (Beslagen Autoruiten) m.nt. Kn

[70] Overkleeft-Verburg 2014

[71] In 2013 werd door Edward Snowden onthuld dat de Amerikaanse National Security Agency (NSA) op grote schaal heimelijk gegevens van internetgebruikers had verzameld.

resolutie aangenomen over *The Right to privacy in the digital age*.[72] De resolutie wil dat het recht op privacy online op dezelfde wijze is beschermd als offline. Lidstaten wordt gevraagd om hun nationale wet- en regelgeving ten aanzien van de omgang met gegevens van de burgers (opnieuw) tegen het licht te houden om na te gaan of het recht op privacy voldoende is gewaarborgd. De Hoge Commissaris voor de mensenrechten wordt verzocht aan de Algemene Vergadering te rapporteren over de voortgang.

In Europa is in 2011 een begin gemaakt met het moderniseren van het Europees Dataverdrag uit 1981.[73] De inhoud van het verdrag moet in overeenstemming gebracht worden met de voorstellen die zijn gedaan ten aanzien van de herziening van de EG-Richtlijn bescherming persoonsgegevens.[74] Bij de inwerkingtreding van deze richtlijn in 1998 verschoof de regelverplichting van art. 10 lid 2 en 3 Gw naar Europa. Vanaf 2012 loopt het proces om deze richtlijn te vervangen door een Verordening algemeen kader bescherming persoonsgegevens[75] (ook bekend als de General Data Protection Regulation). Daarnaast wordt het kaderbesluit 2008/977/JBZ inzake de bescherming van persoonsgegevens bij politiële en justitiële samenwerking vervangen door de Richtlijn bescherming gebruik door politiële en justitiële autoriteiten.[76] Verordening en richtlijn zijn nog niet aangenomen, maar naar verwachting zullen de consequenties voor het nationale recht aanzienlijk zijn.

Een laatste ontwikkeling betreft het Europese Handvest van de Grondrechten. Sinds het Verdrag van Lissabon op 1 december 2009 heeft dit Handvest op grond van art. 6 lid 1 VEU rechtskracht gekregen, gelijk aan die van de verdragen. In art. 7 van het Handvest, dat inhoudelijk een gemoderniseerde versie van art. 8 EVRM is, wordt het recht op privacy gedefinieerd. Het Hof van Justitie gebruikte dit artikel al regelmatig als inspiratiebron, maar in een drietal recente arresten van het Hof is de doorwerking van de grondrechten in het nationale recht nadrukkelijk vastgelegd.

In het arrest-Meloni[77] spreekt het Hof uit: “Het is immers vaste rechtspraak dat krachtens het beginsel van voorrang van Unierecht, dat een wezenlijk kenmerk is van de rechtsorde van de Unie (…), de omstandigheid dat een lidstaat zich beroept op bepalingen van nationaal recht, ook zal zijn deze van constitutionele aard, niet kan afdoen aan de werking van het recht van de Unie op het grondgebied van die staat.” Daarbij mag de lidstaat de nationale grondrechtenbescherming toepassen, maar alleen als het beschermingsniveau van het Handvest daardoor niet in het gedrag komt.

---

[72] Resolutie 68/167 van de Algemene Vergadering van de Verenigde Naties (18 december 2013), *The right to privacy in the digital age*, *UN Doc* A/RES/68/167

[73] Verdrag bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatburg 28 januari 1981, Trb. 1988, 7 en 1993, 11

[74] Richtlijn 95/46/EG, 24 oktober 1995

[75] COM(2012) 11

[76] COM(2012) 10

[77] EU Hof van Justitie van 26 februari 2013, Melloni v. Mnisterio Fiscal, zaaknr. C-399/11

In het arrest-Aklagaren[78] is het oordeel van de het Hof: “Wat vervolgens de gevolgen betreft die de nationale rechter moet verbinden aan een conflict tussen bepalingen van zijn nationaal recht en door het Handvest gewaarborgde rechten is het vaste rechtspraak dat de nationale rechter die in het kader van zijn bevoegdheid belast is met de toepassing van de bepalingen van het Unierecht, zorg dient te dragen voor de volle werking van deze normen, en daarbij zo nodig, op eigen gezag, elke strijdige bepaling van de – zelfs latere – nationale wetgeving buiten toepassing moet laten, zonder dat hij hoeft te vragen of af te wachten dat deze eerst door de wetgever of door enige andere constitutionele procedure wordt ingetrokken.”
In het arrest-Romeo[79] spreekt het Hof uit dat het van belang is dat een eenduidige interpretatie van begrippen uit het Handvest met oog op het belang van Unie noodzakelijk is, “ongeacht de omstandigheden waaronder zij toepassing moeten vinden”. Er kan dus niet door nationale wetgeving gedifferentieerd worden.

3.5 Conclusies

Bij het onderzoeken van de verschillende definities van privacy bleek dat bij privacy zowel het individu als zijn omgeving een rol spelen. De betekenis van privacy is contextafhankelijk en de mate waarin bepaalde waarden een rol spelen bij het bepalen wat privacy inhoudt zijn afhankelijk van het individu omdat privacy ook een aantal subjectieve aspecten kent (denk aan de *reasonable expectation of privacy*). Met het begrip *contextual integrity* wordt bedoeld dat de mate waarin een bepaalde informatiestroom als ongepast wordt beschouwd, bepalend is voor de mate waarin die informatiestroom als privacy-inbreuk wordt ervaren. De wijze waarop in art. 8 EVRM het recht op privacy is gedefinieerd laat volop ruimte voor deze balans tussen individu en omgeving omdat ook gedefinieerd is welke inbreuken op de privacy toelaatbaar zijn in een democratische samenleving.

De historische ontwikkeling van het recht op privacy laat zien dat deze ontwikkeling zijn wortels vindt in een wantrouwen ten opzichte van de overheid. Door het recht op privacy als een grondrecht in de Grondwet op te nemen heeft de overheid een poging gedaan om het vertrouwen in de overheid te herstellen. Daarmee is de maatschappelijke discussie echter nog niet afgelopen.
Uit de geschiedenis van de codificatie van het recht op privacy in de Grondwet blijkt dat de overheid al in de jaren 60 was doordrongen van de fundamentele noodzaak om een dergelijk recht als grondrecht op te nemen. De formulering in art. 10 Gw focust vooral op de rechten van het individu

[78] EU Hof van Justitie van 26 februari 2013, Aklagaren v. Hans Akerberg Fransson, zaaknr. C-617/10
[79] EU Hof van Justitie van 7 november 2013, Romeo v. Regione Siciliana, zaaknr. C-313/12

en laat de concrete invulling over aan lagere wetgeving en rechtspraak. Aan de regelingsplicht uit art. 10 lid 2 en 3 is invulling gegeven door een aantal beschermingswetten.

Sinds het begin van de jaren 90 is de invloed van Europese recht op de Nederlandse rechtsorde steeds sterker geworden. Op grond van de rechtstreekse werking van het EVRM en het feit dat het Handvest van de grondrechten van de Europese Unie onderdeel uitmaakt van de Nederlandse rechtsorde,[80] valt de bescherming van het recht op privacy inmiddels volledig onder het beslag van de rechtspraak van het EHRM en het Hof van Justitie. Daarmee is ook het belang van de doctrine van de *reasonable expectation of privacy* toegenomen. Om tot een goede balans te komen tussen de belangen van de opsporing en de grondrechten van de burgers is een doorgaande maatschappelijke discussie over wat *reasonable* is cruciaal.

In dit hoofdstuk is aandacht besteed aan het grondrecht op privacy, in het volgende hoofdstuk wordt gedefinieerd op welke wijze de informatievergaring op social media genormeerd moet worden om dat grondrecht te beschermen.

[80] Barkhuysen & Bos 2011

4 Opsporingsbevoegdheden op social media

4.1 Inleiding

In hoofdstuk 3 is beschreven hoe het recht op privacy is verankerd in nationale en internationale wet- en regelgeving. Bij het normeren van de opsporing op social media vormt deze verankering de belangrijkste toetssteen. In het verleden is op pijnlijke wijze gebleken waartoe het niet of onvoldoende normeren van de opsporing kan leiden.

Op 7 december 1993 brachten burgemeester Van Thijn van Amsterdam, hoofdofficier van justitie Vrakking en korpschef Nordholt een persbericht uit waarin zij meedeelden dat het interregionale rechercheteam (IRT) Noord-Holland/Utrecht, dat was opgezet voor de bestrijding van de zware, georganiseerde misdaad, was opgeheven wegens een omstreden opsporingsmethode. Het was gebleken dat de Haarlemse politie gebruik had gemaakt van een informant die grote partijen softdrugs importeerde. De politie wilde deze informant laten "groeien" in de criminele organisatie en liet daarom containers vol verdovende middelen ongemoeid.

Nadat er in de eerste maanden van 1994 steeds meer nieuws naar buiten kwam, lieten (inmiddels) minister Van Thijn van Binnenlandse Zaken en Hirsch Ballin van Justitie een onderzoek instellen naar het IRT. De onderzoekscommissie kwam tot de conclusie dat niet de werkmethode, maar onderlinge ruzie tussen de betrokken politiekorpsen en het Openbaar Ministerie de voornaamste oorzaak waren geweest van het opheffen van het IRT. Hoewel de ministers na een debat met de Tweede Kamer aangaven met de betrokkenen een stevig gesprek te zullen voeren en dachten dat daarmee de kous af was, kwam er in de maanden die volgden via de pers steeds meer informatie over opsporingsmethoden naar buiten waarover in de wet niets was vastgelegd en die bovendien in de ogen van veel mensen moreel verwerpelijk waren. Zo bleken politiemensen in te breken in loodsen (inkijkoperaties) om te onderzoeken of een officiële huiszoeking succes zou opleveren. De IRT-affaire was geboren.
In het debat over deze nieuwe onthullingen traden zowel Hisch Ballin als Van Thijn af.

De IRT-affaire vormde het startschot voor een discussie over de toelaatbaarheid van opsporingsmethoden. Op dat moment bestond voor methoden als afluisteren, inkijken, infiltreren e.d. geen wettelijke basis. De Tweede Kamer wilde, voordat een eventueel wetgevingstraject zou worden opgestart, eerst inzicht krijgen in de praktijk van het opsporingswerk van de politie. Die wens leidde in de zomer van 1994 tot een onderzoek door een Kamercommissie onder leiding van de PvdA'er Maarten van Traa. De commissie oordeelde enkele maanden later dat er weliswaar veel

feiten over het opsporingswerk boven tafel waren gekomen, maar om een echt betrouwbaar beeld van de praktijk te krijgen het beter zou zijn om een parlementaire enquête uit te voeren.

Op 6 september 1995 begonnen, na bijna een jaar van onderzoeken en voorgesprekken, de openbare verhoren door de parlementaire enquêtecommissie opsporingsmethoden, beter bekend als de commissie Van Traa. De commissie hoorde meer dan tachtig functionarissen van politie en justitie, politici, onderzoekers en ambtenaren. Op 1 februari 1996 presenteerde de commissie het resultaat van haar onderzoek in het rapport *Inzake opsporing.*[81] Deze bevindingen waren de opmaat tot een *Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden)*[82] kortweg de Wet BOB. In de Wet BOB worden de bijzondere opsporingsmethoden beschreven die binnen de opsporing gebruikt mochten worden en onder welke voorwaarden.

In onze rechtsstaat is de politie de sterke arm van de overheid. Voor de uitvoering van haar taak heeft de politie vergaande bevoegdheden gekregen. In het licht van het model van *checks and balances* moeten burgers in een rechtsstaat tegen een machtige overheid beschermd worden. Hoe ingrijpender de aan de overheid gegeven bevoegdheid is, hoe sterker de bescherming voor de burger moet zijn.
De bijzondere opsporingsbevoegdheden, zoals die zijn opgenomen in het Wetboek van Strafvordering, geven de politie middelen in handen om haar opsporingstaak uit te voeren, maar verbinden aan het gebruik daarvan ook strenge voorwaarden. Daarmee wordt een rechtmatige, effectieve en verantwoorde wijze van opsporing mogelijk gemaakt.

Burgers worden op allerlei manieren beschermd tegen de overheid: bescherming van de lichamelijke integriteit (bescherming tegen lichamelijke dwang), bescherming van de geestelijke integriteit (bescherming tegen psychische dwang), bescherming van de identiteit (bescherming tegen een andere voorstelling van wat of wie iemand is dan de voorstelling die de desbetreffende persoon van zichzelf geeft) en bescherming van de anonimiteit (bescherming tegen het verwerven van en/of aan anderen bekend maken van informatie over die persoon). Informatievergaring op social media door opsporingsinstanties maakt inbreuk op die laatste twee grondrechten: het recht op identiteit en het recht op anonimiteit. Deze twee elementen komen terug in het recht op privacy, zoals gedefinieerd in 3.2. Vanuit de gedachte van bescherming van de burgers tegen een dergelijke inbreuk wordt in dit

[81] Inzake Opsporing 1996
[82] *Kamerstukken II* 1996/97, 25 403, nr. 1 en 2

hoofdstuk nagegaan op welke wijze die bescherming vorm moet krijgen binnen het bestaande wettelijk kader van Politiewet en Wetboek van Strafvordering.
In art. 3 PolW wordt de algemene taak van de politie beschreven. De politie mag bij de uitvoering van die taak bepaalde handelingen verrichten. In de praktijk worstelen politie en Openbaar Ministerie regelmatig met de vraag welke politiehandelingen hun legitimering kunnen vinden in de in art. 3 PolW algemeen geformuleerde politietaak, en op welk moment er sprake is van handelingen die dusdanig ingrijpend zijn ten aanzien van de grondrechten van betrokken burgers dat zij een eigenstandige legitimering vereisen middels specifieke wetgeving, zoals de bijzondere opsporingsbevoegdheden uit het Wetboek van Strafvordering. Voor alle opsporingshandelingen geldt bovendien dat ze moeten vallen binnen de grenzen die het EVRM aan de opsporing stelt.

In dit hoofdstuk wordt nagegaan waar de grens ligt tussen art. 3 PolW en de bijzondere opsporingsbevoegdheden als het gaat om opsporing op social media. Allereerst wordt vastgesteld wanneer de inbreuk op de privacy van de betrokken burger(s) zo groot is, dat een meer specifieke bevoegdheid dan art. 3 PolW noodzakelijk is. Daarbij wordt vervolgens van de twee artikelen uit de BOB-wetgeving die over het algemeen worden genoemd als het gaat om dit soort onderzoek (te weten stelselmatige observatie [art. 126g Sv] en stelselmatige informatie-inwinning [126j Sv]) nagegaan in hoeverre zij toepasbaar zijn en of het eventueel nodig is om voor dergelijke onderzoekshandelingen een nieuw soort bevoegdheid te formuleren.[83]

4.2 Digitale IRT-affaire?

Het gebruik van social media heeft de afgelopen jaren een stormachtige ontwikkeling doorgemaakt. Lang niet al die ontwikkelingen werden door de wetgever voorzien bij de introductie van de Wet BOB. Om toch te garanderen dat de opsporing op social media rechtmatig en verantwoord plaatsvindt, is het van belang om na te gaan in hoeverre de online-omgeving bijzondere eisen stelt aan de te hanteren opsporingsbevoegdheden.
Veel mensen hebben de neiging om datgene wat ze bezighoudt of wat ze hebben gedaan met anderen te delen. Hierdoor brengen veel mensen bewust of onbewust veel (vaak persoonlijke) informatie over zichzelf in de openbaarheid.

[83] Deze twee bevoegdheden zijn gekozen omdat op basis van literatuurstudie blijkt dat deze vaak genoemd worden in het kader van de strafvorderlijke aspecten van politieonderzoek in open bronnen, zie Koops 2012, Oerlemans & Koops 2012 maar ook in 'Procedure gegevensvergaring online communities', Landelijk Parket, cluster High Tech Crime en Telecom, september 2012

Opsporingsinstanties proberen deze informatie te gebruiken in opsporingsonderzoeken bijvoorbeeld door het netwerk van een verdachte op Facebook in beeld te brengen. Er bestaat echter op dit moment geen eenduidigheid over de daarbij te hanteren juridische kaders.
Deze situatie roept herinneringen op aan het onderzoek van de commissie Van Traa. De commissie concludeerde dat er in de opsporing in Nederland sprake was van onvoldoende normstelling en onduidelijkheid over wie waarvoor verantwoordelijk was. Er was sprake van een crisis in de opsporing en het was hoog tijd dat iedereen weer wist waar men aan toe was.[84]
Schermer stelt in een opinieartikel uit 2012 de vraag of er sprake is van een digitale IRT-affaire[85] omdat het juridisch kader voor opsporing op internet onvoldoende duidelijk is. De bij dergelijk onderzoek gehanteerde opsporingsmethoden kunnen soms erg diep ingrijpen in de persoonlijke levenssfeer van de burger en moeten daarom nauwkeurig omschreven zijn. Ook moeten er voldoende waarborgen zijn voor een zorgvuldige toepassing. En juist op die punten signaleert Schermer een achterstand in de bestaande wet- en regelgeving. Van een echte digitale IRT-affaire is volgens hem echter geen sprake, omdat OM en politie zich baseren op bestaande bevoegdheden en bovendien heel nadrukkelijk rekening houden met de privacybelangen van de burger. Wel vraagt hij aandacht voor het feit dat het huidige juridisch kader aan een opfrisbeurt toe is. Vaak worden de nieuwe opsporingsmethoden met enige moeite “geperst” in de omschrijving van de bestaande bevoegdheden, maar dat is niet altijd goed mogelijk. Bovendien is op deze manier voor de burger minder duidelijk wat de politie nu allemaal kan en mag.
Daar wringt de situatie wellicht ook waar het gaat om het EVRM. Dat verdrag stelt immers aan de toepassing van opsporingsmiddelen de eis dat ze voorzienbaar moeten zijn. Als voor de burger niet duidelijk is wat de opsporing kan en mag, is het maar zeer de vraag of aan die eis van voorzienbaarheid is voldaan.

De commissie Van Traa heeft ter voorbereiding op de openbare verhoren een viertal hoogleraren verzocht onderzoek te doen naar de aard en de omvang van de georganiseerde criminaliteit in Nederland. Een van hen was prof. dr. C.J.C.F Fijnaut. Vanwege zijn kennis rondom het hele IRT-dossier is Fijnaut in het kader van deze scriptie geïnterviewd. Hij geeft in dat interview[86] aan dat hij geen echte parallel ziet tussen de IRT-affaire en het vraagstuk rondom opsporingsbevoegdheden op internet. De IRT-affaire was het gevolg van een oorlog tussen OM en politie, aldus Fijnaut. Van een dergelijke verstoorde verhouding is rondom de opsporing op social media geen sprake. Door teveel te redeneren vanuit de gedachte dat nieuwe opsporingsmogelijkheden een bedreiging vormen voor

[84] Inzake Opsporing 1996, p. 5
[85] Schermer 2012
[86] Zie Bijlage 2 - Gespreksverslag prof. Fijnaut

een of meer grondrechten ontstaat een reactie vanuit het negatieve hetgeen gemakkelijk zal leiden tot gemiste kansen. Fijnaut ziet meer heil in de aanpak zoals die gevolgd wordt rondom technische ontwikkelingen in de forensische opsporing (denk aan DNA): het bestaande arsenaal aan onderzoeksmethoden en -technieken wordt enorm vergroot, met de bijbehorende toename aan kansen voor de opsporing. Wel is dan regulering en begrenzing noodzakelijk, maar met behoud van het goede van de ontwikkeling.

Koops is van mening dat social media een dusdanig andere omgeving voor informatievergaring is, dat het noodzakelijk is om na te denken over een nieuw soort opsporingsbevoegdheid.[87] Hij signaleert bij onderzoekers in open bronnen de neiging om te denken dat alles wat mensen zelf op internet hebben gezet zonder enige beperking gebruikt mag worden. Hij is van mening dat er ten aanzien van het gebruik van dergelijke gegevens door opsporingsambtenaren vanuit twee juridische invalshoeken beperkingen gelden: de bescherming van de privacy (geregeld in art. 8 EVRM en art. 10 Gw en verder uitgewerkt in de Wet bescherming persoonsgegevens en de Wet politiegegevens) en het intellectuele eigendomsrecht (onder andere geregeld in de Auteurswet). De beperkingen vanuit de Auteurswet vallen buiten het bestek van deze scriptie en worden hier niet verder uitgewerkt. Vanuit de Wet op de Politiegegevens leidt Koops af dat vanwege de vereiste doelbinding[88] opsporingsinstanties voorafgaand aan het onderzoek in open bronnen moeten vastleggen wat het doel van dat onderzoek is. Gevoelige gegevens (denk aan gegevens over ras, geloofsovertuiging, seksuele voorkeur) mogen alleen verzameld worden als dit vanuit de doelstelling van het onderzoek onvermijdelijk is.[89] Daarnaast vraagt hij aandacht voor het feit dat, hoewel vrij algemeen bekend is dat de politie internet raadpleegt, in de meeste gevallen vooral niet-verdachte mensen niet verwachten dat de informatie die zij op internet publiceren wordt gebruikt voor opsporingsdoeleinden.

Siemerink[90] stelt dat de Wet BOB voornamelijk is toegesneden op de fysieke wereld. Zij verwijst naar het uitgangspunt van de regering dat “wat «off line» geldt ook «on line» moet gelden”.[91] In de praktijk blijkt echter een aantal eigenschappen van de online-wereld de toepassing van dit uitgangspunt te compliceren. Specifiek gaat het om *dematerialisering* (dat op zijn beurt weer sterk samenhangt met *depersonificering*), *internationalisering* en *technologische (en maatschappelijke) turbulentie*. Dematerialisering is de ontwikkeling dat kennis, diensten en informatie niet meer fysiek

[87] Koops 2012
[88] Art. 3 WPolG
[89] Art. 5 WPolG
[90] Siemerink 2000
[91] Vgl. *Kamerstukken II* 1997/98, 25 880, nr. 1 en 2

maar digitaal zijn vastgelegd. Het daarmee samenhangende begrip depersonificering betreft dan het gegeven dat op internet het heel eenvoudig is om je als een ander voor te doen. Internationalisering heeft betrekking op het feit dat fysieke landsgrenzen op internet een minder grote rol spelen. En technologische turbulentie tenslotte is de beweging dat de ontwikkeling van de informatietechniek en alles wat daarmee samenhangt in hoge mate onvoorspelbaar is en een hoge doorloopsnelheid kent. Siemerink ziet vervolgens aan de hand van de bevoegdheden pseudokoop en infiltratie een probleem als geprobeerd wordt om deze bijzondere opsporingsbevoegdheden toe te passen in een digitale omgeving. Zo is Siemerink van mening dat het Talloncriterium (de verdachte niet tot andere handelingen brengen dan die waarop zijn opzet reeds was gericht) sneller wordt geschonden in een online omgeving, omdat er vanwege de dematerialisering en depersonificering eerder sprake is van misleiding. Daar komt bij dat het op Internet heel gebruikelijk is om onder een andere naam of identiteit aanwezig te zijn. Daardoor zal internetsurveillance (rondkijken) dat is toegestaan onder art. 3 PolW al snel kunnen ontaarden in infiltratie omdat er geen fysieke contacten plaatsvinden. Het werken door de politie onder een pseudoniem kan snel uitmonden in het aannemen van een andere identiteit (infiltratie). Dit zet volgens Siemerink de rechtsbescherming van internetgebruikers onder druk. Zij pleit dan ook voor specifieke regelgeving die dit probleem het hoofd biedt, waarbij het van groot belang is om die regels technologie-onafhankelijk te formuleren om daarmee te voorkomen dat bij een volgende ontwikkeling in de techniek de regelgeving opnieuw aangepast moet worden.

4.3 Opsporing: typering en normering

4.3.1 Definitie opsporing

De taak van de politie (art. 3 PolW) valt uiteen in twee onderdelen: handhaving en opsporing. De politie is op beide terreinen actief op social media. Omdat het onderwerp van de masterscriptie de opsporing betreft, wordt in deze paragraaf eerst het begrip opsporing afgebakend.

Het legaliteitsbeginsel voor het strafrecht vindt zijn basis in het EVRM: art. 6 beschrijft het recht op een eerlijk proces (formeel legaliteitsbeginsel) en art. 7 betreft het *nulla poena* beginsel. Voor het strafprocesrecht is dit verder uitgewerkt in art. 1 Sv. Met dat artikel wordt de bevoegdheid van de overheid om inbreuk te maken op rechten en vrijheden van burgers gebonden aan de wet.[92] Keulen en Knigge benadrukken dat dit geen exclusief strafvorderlijk beginsel is: elk overheidsoptreden dat belastend is voor burgers moet direct of indirect berusten op een wet in formele zin.[93] Het behoeft geen betoog dat opsporingsactiviteiten van de overheid regelmatig belastend zijn voor burgers: opsporingsmethoden grijpen vaak diep in in de rechten van burgers, het systematisch verzamelen en vastleggen van gegevens over burgers is op zichzelf al een privacygevoelige activiteit en tenslotte

[92] Cleiren, Crijns & Verpalen 2013
[93] Keulen & Knigge 2010

speelt ook een rol dat strafvordering gericht is op sanctionering. Het is daarom van belang dat bij de beoordeling van de toelaatbaarheid van nieuwe opsporingsmethoden het legaliteitsbeginsel een bepalende rol speelt.

In de klassieke opvatting, zoals de Hoge Raad die bijvoorbeeld koos in een tweetal arresten uit 1986,[94] begint de opsporing pas op het moment dat er sprake is van een vermoeden dat een strafbaar feit is begaan. Daarmee was het observeren, waar het in deze arresten om ging, niet terug te voeren op art. 1 Sv maar werd het toenmalige art. 2 PolW als wettelijke grondslag gehanteerd. Hiermee werd de politie in staat gesteld om zonder adequate rechterlijke controle allerlei activiteiten te ontplooien (dit werd door Corstens 'vroegsporing' genoemd[95]). En volgens Keulen en Knigge leidde dat tot wat de Commissie Van Traa een 'crisis in de opsporing' noemde.[96] Het gegeven dat er geen sprake was van opsporing bleek gebruikt te worden als rechtvaardiging om een groot deel van het onderzoek buiten het zicht en de controle van de rechter en het OM uit te voeren.[97]

Uiteindelijk werd in 2007 art. 132a ingevoegd in het Wetboek van Strafvordering:

> "*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 onderscheidende criterium is daarmee het *doel* geworden: zodra het doel van het onderzoek strafrechtelijk ingrijpen is, dan is er sprake van opsporing. Daarmee wordt afstand genomen van de hierboven beschreven klassieke opvatting.

4.3.2 Normering van de opsporing

Art. 1 Sv beschrijft het strafvorderlijk legaliteitsbeginsel:

> *"Strafvordering heeft alleen plaats op de wijze bij de wet voorzien."*

Dit legaliteitsbeginsel bindt de bevoegdheden van de overheid tot het maken van inbreuken op de rechten en vrijheden van de burger aan de wet.[98] Zoals in de vorige paragraaf aangegeven, is opsporing gericht op het nemen van strafvorderlijke beslissingen. Opsporing is dus strafvordering, en valt daarmee binnen de reikwijdte van het legaliteitsbeginsel van art. 1 Sv. Ook de opsporing moet daarom plaatsvinden op de wijze bij wet voorzien.

Zoals gezegd wordt de algemene taakstelling van de politie beschreven in art. 3 PolW:

> "*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.*"

---

[94] HR 14 oktober 1986, *NJ* 1987, 564 en HR 14 oktober 1986, *NJ* 1988, 511
[95] Corstens 1995
[96] Inzake Opsporing 1996
[97] Keulen & Knigge 2010, p. 269
[98] Cleiren, Crijns & Verpalen 2013

Voor wat betreft de normering van het politiewerk is de aanduiding *in overeenstemming met de geldende rechtsregels* van belang. Deze eis geldt ook voor de opsporingstaak van art. 141 en 142 Sv. Het is dus van belang om vast te stellen wanneer er sprake is van *rechtmatige* opsporing. Vanwege de term *rechtsregels* gaat het daarbij om meer dan alleen wetgeving.
Hoewel in het Wetboek van Strafvordering de nodige voorschriften zijn opgenomen met betrekking tot de normering van de opsporingstaak (denk aan regels voor het verhoor, voorwaarden voor toepassing van dwangmiddelen, verbaliseringsplicht), is er ook veel niet geregeld. Opsporing is, zeker sinds de invoering van art. 132a Sv, doelgericht. Het *hoe* van de opsporing is niet volledig in regels te vangen en zou de opsporing ook teveel beperken in het uitvoeren van haar taak. Ook is het niet doenlijk om de wet voortdurend aan te passen aan ontwikkelingen in de techniek of de wetenschap. De opsporing heeft dus de nodige speelruimte.
Om excessen te voorkomen is deze speelruimte wel beperkt. Opsporing is een overheidstaak die belastend is voor de burgers die het betreft. Daarom is het van belang dat die taak berust op een wettelijke bevoegdheid en door het publiekrecht wordt beheerst.[99] Dit houdt onder andere in dat het doel van de opsporing normerend werkt: alleen die activiteiten die bijdragen aan het bereiken van dat doel zijn toegelaten, anders is er sprake van *détournement de pouvoir*. Overigens mag hieruit niet geconcludeerd worden dat het doel de middelen heiligt: juist vanwege het belastende karakter van de opsporing moet het belang van de opsporing voortdurend worden afgewogen tegen de belangen van de burgers. Dus naast doelbinding zijn proportionaliteit en subsidiariteit sturende beginselen bij de normering van de opsporing.
Keulen en Knigge wijzen erop dat op basis hiervan de opvatting dat de politie alles mag wat gewone burgers ook mogen niet overeind kan blijven. De jurisprudentie van het EHRM wijst in diezelfde richting.[100] Overigens blijkt alleen al uit het feit dat er opsporingsbevoegdheden zijn die aan voorwaarden zijn gebonden, dat er voor opsporingsinstanties andere (en soms restrictievere) regels gelden dan voor burgers.

Zoals gezegd heeft de opsporing de nodige speelruimte bij de uitvoering van zijn taak: lang niet alle opsporingsactiviteiten zijn expliciet in de wet beschreven. De basis voor het gebruik van niet expliciet in de wet vastgelegde opsporingsbevoegdheden wordt gevonden in art. 141 en 142 Sv. Melai en Groenhuijsen betogen dat deze artikelen niet alleen een bevoegdheid maar ook een verplichting tot opsporing geven.[101] Art. 159 Sv borduurt daarop voort: van de opsporingsambtenaar wordt verwacht

[99] Knigge & Kwakman 2001. Zie ook Melai, Groenhuijsen e.a. 2013
[100] EHRM 8 april 2003, nr. 39339/98, (M.M. vs. Nederland) en EHRM 25 oktober 2007, nr. 38258/03 (Van Vondel vs. Nederland)
[101] Melai, Groenhuijsen e.a. 2013

dat hij de zaak probeert op te lossen, in spoedgevallen zelfs zonder vooraf de officier van justitie om instructies te vragen.

Dat art. 141 en 142 Sv in beginsel voldoende grondslag bieden om ook niet bij specifiek in de wet vastgelegde opsporingsbevoegdheden toe te passen, wordt bevestigd door de Hoge Raad. In het bekende Zwolsman-arrest[102] oordeelde de Hoge Raad dat bepaalde opsporingshandelingen, die niet expliciet in de wet geregeld waren, gebaseerd konden worden op art. 141 Sv. In datzelfde arrest wordt bepaald dat voor "verrichtingen, (waardoor, M.O.) een beperkte inbreuk op de persoonlijke levenssfeer zou worden gemaakt, de globale taakomschrijving van art. 2 Politiewet 1993 een toereikende wettelijke grondslag biedt".*[103]*

In de memorie van toelichting bij de Wet BOB[104] wordt apart aandacht besteed aan de vraag wanneer opsporingsmethoden een specifieke wettelijke regeling behoeven. De wetgever geeft daarin aan dat het niet de bedoeling van de opstellers is geweest om het opsporingsonderzoek systematisch en uitputtend te beschrijven. Uitgangspunt was dat voor bevoegdheden die ingrijpen op de vrijheid (de MvT geeft aan dat het bij de Wet BOB in het bijzonder om de bescherming van de persoonlijke levenssfeer gaat) of op andere grondrechten (zoals opgenomen in de Grondwet, in het EVRM of in het IVBPR) een specifieke regeling zou worden opgenomen, omdat in die wetten en verdragen de eis gesteld wordt dat een dergelijke inbreuk een wettelijke basis noodzakelijk maakt. In de MvT wordt expliciet aansluiting gezocht bij de doelcriteria van art. 8 lid 2 EVRM (zie 3.4.3):

1. Is er een *interference by a public authority*?
2. Zo ja, is deze *in accordance with the law*?
3. Zo ja, heeft de *interference* een *legitimate aim*?
4. Zo ja, is deze *interference necessary in a democratic society*?

Of een bepaalde opsporingsbevoegdheid aangemerkt kan worden als een *interference by a public authoriry* is volgens de MvT afhankelijk van de concrete omstandigheden van het geval. Daarnaast geeft de MvT aan dat het EHRM de doctrine van de *reasonable expectation of privacy* hanteert, zodat ook de verwachting van de betrokkene van invloed is op de vraag of er sprake is van een *interference*. Ten aanzien van de eis dat de *interference in accordance with the law* moet zijn, geldt tevens dat de desbetreffende regeling voldoende toegankelijk moet zijn en dat de burger aan de hand daarvan moet kunnen voorzien wat de gevolgen van een bepaalde handelwijze kunnen zijn. Geheime opsporingsbevoegdheden zijn op basis daarvan niet toegestaan, wel kan het gebruik van

[102] HR 19 december 1995, *NJ* 1996, 249

[103] HR 19 december 1995, *NJ* 1996, 249, paragraaf 6.4.5. Zie ook HR 1 juli 2014, ECLI:NL:HR:2014:1562 waarin de Hoge Raad oordeelt over de inzet van een IMSI-catcher.

[104] *Kamerstukken II* 1996/97, 25 403

bepaalde bevoegdheden onder omstandigheden geheim gehouden worden, als dit in het belang van het onderzoek is. Het moet voor de burger wel duidelijk zijn in welke omstandigheden en onder welke voorwaarden een bevoegdheid ingezet kan worden. Willekeurige inmenging door de overheid moet worden voorkomen. Ten aanzien van de vraag of een bevoegdheid een *legitimate aim* dient en *necessary is in a de democratic society* verwijst de MvT vooral naar het belang van de opsporing. Het zou gaan om bevoegdheden die bij de opsporing van criminaliteit niet gemist kunnen worden.
De bedoeling van de wetgever was om alle opsporingsmethoden die 'naar huidig inzicht' een inbreuk maakten een plaats te geven in de wet. Als er in de loop van de tijd andere buitenwettelijke opsporingsmethoden bij zouden komen, dan moet de rechter oordelen of deze methoden inbreuk maken op de privacy en is vervolgens de wetgever aan zet om deze in een wettelijke regeling op te nemen.[105]
Overigens zijn Cleiren, Crijns en Verpalen bijzonder kritisch over deze handelwijze van de wetgever. Zij vinden het bedenkelijk dat de wetgever zelfs geen poging heeft gedaan om het begrip "beperkte inbreuk" uit het Zwolsman-arrest[106] nader af te bakenen. In hun ogen ondergraaft de wetgever daarmee zijn eigen systematiek en laat onduidelijkheid bestaan waarover de rechter zich dan maar moet buigen. Daarmee schiet in hun ogen de wetgever tekort.[107]

4.4 Politiewet of BOB-middel?

De benodigde bevoegdheid voor de informatievergaring op social media is afhankelijk van de mate van inbreuk op de privacy. Als die inbreuk gering is, is art. 3 PolW jo. art. 141 en 142 Sv voldoende wettelijke grondslag, maar de vraag is nu vanaf welk moment een meer specifieke wettelijke grondslag noodzakelijk is.
Er moeten dus twee vragen beantwoord worden:

1. Wanneer is de inbreuk op de privacy meer dan gering?
2. Welk BOB-middel leent zich het beste als grondslag?

Koops[108] stelt allereerst dat de verwerking van persoonsgegevens in het algemeen onder art. 8 EVRM valt.[109] Dat geldt ook voor gegevens die uit zogenaamde open bronnen afkomstig zijn omdat ook daar tot op zekere hoogte een redelijke privacyverwachting bestaat.[110] Het feit dat het een openbaar

[105] Dat het in de praktijk inderdaad op deze manier gaat blijkt o.a. uit Rb. Rotterdam, 11 april 2012, LJN BW3105, waarin de rechtbank art. 126n Sv voldoende grondslag vindt voor de inzet van stealth-sms
[106] HR 19 december 1995, *NJ* 1996, 249, paragraaf 6.4.5.
[107] Cleiren, Crijns & Verpalen 2013
[108] Koops 2012
[109] De Hert & Gutwirth 2009 p. 27
[110] Zie bijvoorbeeld EHRM 24 juni 2004,.nr. 59320/00, §77 ((Hannover v. Duitsland) en EHRM 25 oktober 2007, nr. 38258/03 (Van Vondel v. Nederland)

toegankelijke bron betreft, betekent wel dat de aanspraak op privacy minder groot is dan in een afgesloten omgeving. Om nu te bepalen hoe groot die inbreuk is, kiest Koops aansluiting bij een van de kernbegrippen in de BOB-wetgeving, namelijk de stelselmatigheid. In de MvT bij de Wet BOB[111] wordt beschreven dat de toepassing van een opsporingsmiddel stelselmatig is als door die toepassing een min of meer compleet beeld wordt verkregen van bepaalde aspecten van iemands leven. Aanknopingspunten om dat begrip nader in te vullen zijn volgens diezelfde MvT:

> "de duur, de plaats, de intensiteit en het al dan niet toepassen van een technisch hulpmiddel dat meer biedt dan alleen versterking van de zintuigen."

De Hoge Raad heeft dit bevestigd door uit te spreken dat "voor de beantwoording van de vraag of bij het hanteren van de opsporingsmethode van observatie al dan niet sprake is van een beperkte inbreuk op de persoonlijke levenssfeer van de verdachte de omstandigheden bepalend zijn, zoals de duur, de intensiteit, de plaats, het doel van de observaties en de wijze waarop deze hebben plaatsgevonden".[112] Koops[113] en Cleiren, Crijns en Verpalen[114] geven, in navolging van de MvT, aan dat de plaats waar de observatie plaatsvindt van invloed is op de mate van inbreuk op de privacy. Naarmate die plaats intiemer is, is de kans groter dat een min of meer compleet beeld wordt verkregen. Daarmee is er dus eerder sprake van stelselmatige observatie. De Hoge Raad heeft daarover uitgesproken dat in situaties waarin verdachten niet mogen verwachten onbevangen zichzelf te zijn er geen sprake is van privacyschendende/stelselmatige observatie.[115] Ook tijdens de parlementaire behandeling van de Wet BOB werd al opgemerkt dat bijvoorbeeld een woning een meer privacygevoelige omgeving is dan een sportveld en dat daarmee de toepassing van een opsporingsmethode binnen een woning eerder stelselmatig zal zijn.[116]

Door systematisch en grootschalig gegevens te verzamelen, in het bijzonder als het gaat om een gerichte zoekactie op een bepaalde persoon, ontstaat al snel een min of meer compleet beeld van iemand. Zeker als daarbij bedacht wordt dat mensen tegenwoordig heel veel gegevens over zichzelf (maar ook over anderen) op internet plaatsen.

In de MvT bij de Wet Computercriminaliteit II[117] is een hoofdstuk gewijd aan opsporingsonderzoek op openbare computernetwerken waarbij de vraag gesteld wordt of bestaande opsporingsbevoegdheden (inclusief die uit de Wet BOB) kunnen en mogen worden gebruikt bij onderzoek op Internet en of ze eventueel aangepast zouden moeten worden. De MvT maakt daarbij

---

[111] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 27
[112] HR 21 maart 2000, ECLI:NL:HR:2000:AA5254, r.o. 3.5, vgl. HR 13 november 2012, ECLI:NL:HR:2012:BW9338
[113] Koops 2012
[114] Cleiren, Crijns & Verpalen 2013
[115] HR 20 april 2004, NJ 2004, 525
[116] *Kamerstukken II* 1998/99, 25 403, nr. 25, blz. 5
[117] *Kamerstukken II* 1998/99, 26 671 nr. 3,p.35

onderscheid tussen rondkijken op Internet en het verrichten van opsporingshandelingen. Opsporingsambtenaren mogen rondkijken, net als ieder ander, ook als er geen sprake is van een verdenking en ook zonder hun hoedanigheid als opsporingsambtenaar kenbaar te maken. De MvT maakt de vergelijking met surveilleren op straat. Wel moet het rondkijken gerekend kunnen worden tot de uitoefening van hun algemene politietaak ex. art. 3 PolW. Ze hoeven zelfs niet onder hun echte naam te opereren als het op dat deel van Internet niet ongebruikelijk is om onder een pseudoniem of alias actief te zijn. Het op deze manier opereren wordt pas als misleiding gezien als het zich afspeelt in een omgeving waar het wel gebruikelijk is om onder eigen naam te opereren. De MvT geeft verder aan dat als het onderzoek een stelselmatig karakter krijgt, het een aparte juridische legitimatie behoeft. Daarbij wordt verwezen naar art. 126j Sv (stelselmatig inwinnen van informatie), met dien verstande dat hier volgens de MvT pas sprake van is, als de opsporingsambtenaar actief deelneemt aan informatie-uitwisseling en op die manier probeert informatie los te krijgen, uiteraard zonder als opsporingsambtenaar herkenbaar te zijn. Het enkel kennis nemen van informatie die anderen hebben geplaatst, zonder dat de opsporingsambtenaar daarom gevraagd heeft, wordt niet als stelselmatige informatie-inwinning beschouwd maar als onderdeel van de politietaak zoals bedoeld in art. 3 Polw.

Overigens impliceert het vrij mogen rondkijken op internet niet dat daarbij ook stelselmatig gegevens van onverdachte personen mogen worden gedownload en opgeslagen in politieregisters. Dit mag alleen indien en voor zover dit noodzakelijk is voor de uitoefening van de politietaak. Uiteraard mogen in het kader van de opsporing van een bepaald strafbaar feit wel uiteenlopende persoonsgegevens worden gedownload en worden opgenomen in een tijdelijk register, om deze gegevens te kunnen analyseren en eventueel in verband te brengen met andere gegevens.

Uit de MvT kan worden afgeleid dat het opslaan, bewaren en later gebruiken van gevonden gegevens ook een factor is die de mate van inbreuk op de privacy beïnvloedt.[118]

Verder is het feit dat bij onderzoek op social media gebruik gemaakt wordt van technische hulpmiddelen (zoekmachines, analyseprogrammatuur e.d.) eveneens van invloed op de mate van inbreuk. Al bij de invoering van de Wet BOB is aangegeven:

> "Ook ingeval van gebruik van technische hulpmiddelen is voor de vraag of er al dan niet een expliciete wettelijke regeling noodzakelijk is, het stelselmatige van de observatie van personen beslissend. Al heel snel zal bij gebruik van technische hulpmiddelen sprake zijn van stelselmatige observatie, maar er zijn situaties denkbaar dat dat niet het geval is. Dan is geen toestemming van de officier van justitie vereist."[119]

[118] In diezelfde zin: Buruma 2001. Zie ook EHRM 28 oktober 1994, *NJ* 1995, 509 (Murray v. Verenigd Koninkrjk) en EHRM 4 december 2008, nr. 30562/04 en 30566/04 (S. en Marper vs. Verenigd Koninkrijk)

[119] *Kamerstukken II* 1997/98, 25 403, nr. 3, p. 110

Het bestuderen van wat er op social media staat door middel van geautomatiseerde hulpmiddelen (automatische zoekslagen e.d.) gaat verder en levert veel meer informatie op dan wanneer een opsporingsambtenaar gewoon rondkijkt op internet. Daarmee is dan ook de inbreuk op de privacy groter.

Ook de aard en de ernst van de verdenking spelen mee bij deze beoordeling. In een arrest uit 2002[120] oordeelde de Hoge Raad dat de ernst van de feiten van invloed zijn op de mate waarin een opsporingsmethode inbreuk maakt op de privacy. Hier sluit de Hoge Raad aan bij het EHRM en de doctrine van de *reasonable expectation of privacy*. In Lüdi v. Zwitserland[121] had ook het EHRM al uitgesproken dat iemand die vermoedelijk betrokken is bij zware misdrijven, een lagere privacyverwachting moet hebben. Dus ook proportionaliteit is een van factoren die de mate van inbreuk op de privacy bepalen.

Waar het gaat om de aard van de verkregen gegevens, valt te wijzen op art. 5 van de Wet politiegegevens. In dat artikel wordt een zwaarder beschermingsregime geïntroduceerd voor gegevens betreffende godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Verwerking van dergelijke gegevens is slechts toegestaan voor zover dit voor het doel van die verwerking onvermijdelijk is (waar dat voor andere gegevens is toegestaan als dit noodzakelijk is). Blijkbaar beoogt de wetgever voor dergelijke gevoelige gegevens een zwaarder privacyregime te hanteren. Daarmee is de gevoeligheid van de gegevens dus ook van invloed op de mate van inbreuk op de privacy.

Bij beoordeling van de stelselmatigheid van een opsporingsmethode gaat het, zoals hierboven al uitgewerkt, in zijn algemeenheid om het verkrijgen van een min of meer compleet beeld van bepaalde aspecten van iemands leven.[122] Daarbij geven Koops[123] en Cleiren, Crijns en Verpalen[124] aan dat er door het gebruik van technische hulpmiddelen waarmee geregistreerd kan worden over het algemeen eerder sprake is van stelselmatigheid.

Samenvattend: op de mate van inbreuk op de privacy door opsporing op social media zijn de volgende factoren van invloed:

- De duur
- De plaats

[120] HR 12 februari 2002, *LJN* AD7804
[121] EHRM 15 juni 1992, nr. 12433/86 (Lüdi v. Zwitserland)
[122] *Kamerstukken II* 1996/97, 25 403, nr. 3, blz. 26
[123] Koops 2012
[124] Cleiren, Crijns & Verpalen 2013

- De intensiteit
- De gevoelige aard van de gegevens
- Het doel van het onderzoek
- Het al dan niet toepassen van een technisch hulpmiddel
- Of de gevonden gegevens worden opgeslagen
- De proportionaliteit

Als op basis van de inschatting van deze factoren in een concreet geval bepaald wordt dat de mate van inbreuk op de privacy door het gebruik van een bepaalde opsporingsmethode meer dan gering is, moet vervolgens bepaald worden welke bevoegdheid dan noodzakelijk is om die methode toch toe te passen. Zoals in de inleiding is aangegeven, blijkt uit de literatuur (en de praktijk) dat met name stelselmatige observatie (art. 126g Sv) en stelselmatige informatie-inwinning (126j Sv) hiervoor gebruikt worden. In de volgende paragrafen wordt uitgewerkt in hoeverre beide bevoegdheden daadwerkelijk geschikt zijn als grondslag voor opsporing op social media.

4.5 Stelselmatige observatie

4.5.1 Artikel 126g Sv

Art. 126g Sv luidt als volgt:

1. *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.*
2. *Indien de verdenking een misdrijf betreft als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie in het belang van het onderzoek bepalen dat ter uitvoering van het bevel een besloten plaats, niet zijnde een woning, wordt betreden zonder toestemming van de rechthebbende.*
3. *De officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel wordt aangewend, voor zover daarmee geen vertrouwelijke communicatie wordt opgenomen. Een technisch hulpmiddel wordt niet op een persoon bevestigd, tenzij met diens toestemming.*
4. *Het bevel wordt gegeven voor een periode van ten hoogste drie maanden. Het kan telkens voor een termijn van ten hoogste drie maanden worden verlengd.*
5. *Het bevel tot observatie is schriftelijk en vermeldt:*
   a) *het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;*
   b) *de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;*

c) de naam of een zo nauwkeurig mogelijke aanduiding van de in het eerste lid bedoelde persoon;

d) bij toepassing van het tweede lid, de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in dat lid, zijn vervuld, alsmede de plaats die zal worden betreden;

e) de wijze waarop aan het bevel uitvoering wordt gegeven, en

f) de geldigheidsduur van het bevel.

6. *Bij dringende noodzaak kan het bevel mondeling worden gegeven. De officier van justitie stelt in dat geval het bevel binnen drie dagen op schrift.*
7. *Zodra niet meer wordt voldaan aan de voorwaarden, bedoeld in het eerste lid, bepaalt de officier van justitie dat de uitvoering van het bevel wordt beëindigd.*
8. *Het bevel kan schriftelijk en met redenen omkleed worden gewijzigd, aangevuld, verlengd of beëindigd. Bij dringende noodzaak kan de beslissing mondeling worden gegeven. De officier van justitie stelt deze in dat geval binnen drie dagen op schrift.*
9. *Een bevel als bedoeld in het eerste lid kan ook worden gegeven aan een persoon in de openbare dienst van een vreemde staat. Bij algemene maatregel van bestuur kunnen eisen worden gesteld aan deze personen. Het tweede tot en met achtste lid zijn van overeenkomstige toepassing.*

Stelselmatige observatie is een opsporingsmiddel dat kan worden ingezet als er sprake is van een verdenking van een misdrijf en de officier van justitie van mening is dat het inzetten van dit middel in het belang van het onderzoek is. Op grond hiervan is het niet noodzakelijk dat de persoon die stelselmatig geobserveerd wordt zelf een verdachte in de zin van art. 27 Sv is. Lid 1 spreekt immers over “een persoon” en niet over “de verdachte”. Ten aanzien van de persoon tegen wie het middel van observatie mag worden ingezet, geeft Buruma aan dat ook de Hoge Raad heeft uitgesproken dat het feit dat iemand niet een verdachte is in de zin van art. 27 Sv er op zichzelf niet aan in de weg staat dat de politie onder bepaalde omstandigheden systematisch en niet-incidenteel nagaat of bepaalde aanwijzingen juist zijn waardoor eventuele misdrijven kunnen worden voorkomen.[125] Ook in de MvT wordt onderstreept dat observatie ook kan worden ingezet als er geen sprake is van een verdachte.[126]

Lid 1 definieert observatie als het waarnemen van een persoon, diens aanwezigheid of gedrag. Buruma[127] interpreteert dit, in navolging van het rapport Inzake Opsporing,[128] als ”het direct, fysiek heimelijk gadeslaan en heimelijk volgen van een persoon of een object, al of niet met gebruikmaking van hulpmiddelen”. In art. 126g is de term heimelijk niet opgenomen, omdat ook niet-heimelijke observatie een inbreuk op het recht op privacy inhoudt. Daarbij wordt nog onderscheid gemaakt in dynamische observatie (het klassieke schaduwen) en statische observatie (vanuit een vast punt de

[125] HR 13 oktober 1998, NJB 1998, nr. 129
[126] *Kamerstukken II* 1997/98, 25 403, nr. 3, p. 11
[127] Buruma 2001, p. 38
[128] Inzake Opsporing 1996, p. 177

zaak in de gaten houden). Het feit dat het artikel spreekt over stelselmatige observatie impliceert dat er ook niet-stelselmatige observatie bestaat. Van der Meijde[129] geeft aan dat de Hoge Raad in het Zwolsman-arrest[130] heeft uitgesproken dat niet-stelselmatige observatie mag plaatsvinden op grond van art. 3 PolW jo. art. 141 en 142 Sv.

4.5.2 Opsporing op social media als stelselmatige observatie?

In de literatuur is door een aantal schrijvers aangegeven wat hun visie is op stelselmatige observatie in relatie tot informatievergaring op social media. Koops[131] komt, zonder dat diepgaand te onderbouwen, tot de conclusie dat het verzamelen van informatie over iemand in open bronnen valt onder observatie. Vervolgens beantwoordt hij de vraag wanneer een dergelijke observatie stelselmatig is, zoals bedoeld in art. 126g. Een argument dat daartegen pleit is de 'plaats' waar de observatie plaatsvindt. Koops legt vervolgens een verband tussen een open bron op internet en de openbare ruimte in de fysieke wereld. Op basis van een arrest van de Hoge Raad[132] geeft hij aan dat het feit dat de observatie 'in de openbare ruimte' plaatsvindt, zwaarder weegt dan de duur, de frequentie en de intensiteit van de observatie waar het gaat om de beoordeling van de stelselmatigheid.

Het opslaan van de gevonden gegevens[133] en het gebruik van technische hulpmiddelen (onderzoekstools) pleiten volgens Koops juist voor de kwalificatie stelselmatig. Al in de MvT wordt aangegeven dat bij het gebruik van technische hulpmiddelen al heel snel sprake zal zijn van stelselmatigheid.[134] Het geautomatiseerd zoeken in open bronnen gaat veel verder dan handmatig surfen op internet, waar de MvT over spreekt, en kan in korte tijd veel meer informatie verzamelen dan met handkracht gevonden kan worden.

Ook de frequentie en de intensiteit van de observatie zijn van invloed op de mate van stelselmatigheid. Koops vertaalt dat in het onderscheid tussen eenmalige en herhaalde zoekslagen, waarbij die laatste heel veel informatie over een persoon naar boven kunnen halen, zeker als op verschillende plaatsen tegelijkertijd wordt gezocht. Ook daarin verschilt onderzoek in open bronnen fundamenteel van het gebruik van bijvoorbeeld camera's, waar veel van de jurisprudentie bij dit artikel op is gericht. Met een dergelijke camera kan immers één plaats in de gaten worden gehouden, terwijl bij internetonderzoek veel verschillende plaatsen tegelijkertijd bekeken kunnen worden.

---

[129] Van der Meijde (*Handboek strafzaken)*, 16.2 Observatie
[130] HR 19 december 1995, *NJ* 1996, 249, r.o. 6.4.5. Zie ook HR 25 januari 2000, *NJ* 2000, 279
[131] Koops 2012
[132] HR 29 maart 2005, LJN AS2752
[133] Vgl. EHRM 28 oktober 1994, NJ 1995, 509 (Murray v. Verenigd Koninkrijk)
[134] *Kamerstukken II* 1997/98, 25 403, nr. 3, p. 110

Dit alles gecombineerd brengt Koops tot de conclusie dat onderzoek in open bronnen al snel het karakter van stelselmatigheid heeft en dat daarom voor dergelijk onderzoek de grondslag van art. 3 PolW onvoldoende is.
Oerlemans en Koops vragen in een andere publicatie[135] nog aandacht voor de verschillen tussen fysieke en online observatie. Dat verschil zit met name in het feit dat bij online observatie gegevens uit het verleden van iemand kunnen worden verzameld. Bij fysieke observatie wordt de informatie verzameld door de persoon te observeren gedurende een bepaalde tijd en daar conclusies uit te trekken of gegevens over dat gedrag te gebruiken in de bewijsvoering. Bij online observatie komt echter ook informatie over het verleden van de onderzochte persoon naar boven. Die informatie kan dan door die persoon zelf maar ook door een ander geplaatst zijn. Beide factoren kunnen ervoor zorgen dat er een niet actueel of zelfs onjuist beeld van de persoon ontstaat, met alle gevolgen van dien waar het het gebruik van die informatie in het opsporingsonderzoek betreft. Terecht vragen Oerlemans en Koops zich af of de wetgever met dit aspect van de terugwerkende kracht rekening heeft gehouden bij het opstellen van de Wet BOB.

4.5.3 Beoordeling

Is stelselmatige observatie nu te gebruiken als grondslag voor informatievergaring op social media? Observatie heeft te maken met het waarnemen van gedrag van de persoon die geobserveerd wordt. Hierdoor wordt een beeld verkregen van voor het desbetreffende opsporingsonderzoek relevante aspecten van het leven van de geobserveerde. Als dit een min of meer compleet beeld oplevert van een of meer aspecten van het leven van de geobserveerde, wordt dit stelselmatig genoemd. Waar dit nuttig is, kan bij die observatie gebruik gemaakt worden van technische hulpmiddelen, die er gelet op de aard van de observatie op gericht zijn om de zintuiglijke waarneming van de observant te versterken c.q. het waargenomen gedrag vast te leggen. De betrouwbaarheid van de observatie wordt gewaarborgd door de persoon van de observant: alleen een rechtsgeldig proces verbaal van de observatie wordt geaccepteerd als betrouwbaar verslag van het geobserveerde gedrag. Dit verslag kan eventueel ondersteund worden door bijvoorbeeld foto's en/of videobeelden.
Bij het verzamelen van gegevens op internet over een bepaald persoon is er echter geen sprake van waarnemen van gedrag, maar van kennisnemen van informatie. Oftewel: de rechercheur die informatie leest die door een persoon op social media is geplaatst, observeert niet het gedrag van die persoon maar ziet alleen het resultaat van dat gedrag. Dit pleit voor het standpunt dat stelselmatige observatie niet geschikt is als bevoegdheid voor het vergaren van informatie op social media. Bovendien blijkt uit de parlementaire behandeling van de Wet BOB dat het ook de bedoeling van de

[135] Oerlemans & Koops 2012

wetgever was om het vergaren van informatie niet onder de observatie te laten vallen. Op een vraag van een lid van de CDA-fractie over een mogelijke samenloop tussen observatie en opnemen van vertrouwelijke communicatie (bij een observatie waarbij zichtbaar is dat een gesprek gevoerd wordt en dat vervolgens door middel van liplezen vastgesteld wordt wat er gezegd wordt) is het antwoord: "Zo ook wanneer gesprekken worden opgenomen en daarbij tevens personen in beeld worden gebracht, tenzij geen geluid wordt opgenomen en de personen tevens niet zodanig in beeld worden gebracht dat door middel van liplezen de communicatie kan worden ontcijferd. Deze afgrenzing tussen observatie en het opnemen van vertrouwelijke communicatie is neergelegd in artikel 126g, derde lid, in het slot van de eerste volzin.".[136] Ook in de praktijk wordt voor de inzet van een observatieteam vaak op voorhand twee bevelen aangevraagd, namelijk een bevel stelselmatige observatie en een bevel OVC (opnemen vertrouwelijke communicatie).[137] Dit standpunt is in 2013 bevestigd door de rechtspraak. In een niet gepubliceerde uitspraak was de zaak aan de orde van een observatieteam dat op basis van een bevel stelselmatige observatie door middel van zeer geavanceerde camera's onder andere opnames had gemaakt van een subject dat een telefoongesprek voerde. Vervolgens werd door middel van liplezen vastgesteld wat het subject tijdens dat telefoongesprek had gezegd. De rechter was van mening dat dat te ver ging: de inhoud van het gesprek mocht niet worden vastgesteld op basis van het bevel stelselmatige observatie. De op deze wijze verkregen gegevens werden dan ook uitgesloten van het bewijs.
Bij het lezen van informatie die uit naam van een persoon op social media is geplaatst is verder ook niet door zintuiglijke waarneming van de observant te verifiëren dat dit daadwerkelijk door deze persoon is neergezet omdat er geen sprake is van waarneming van het gedrag.
Overigens is het standpunt verdedigbaar dat stelselmatige observatie op meer betrekking zou kunnen hebben dan alleen op fysiek gedrag, namelijk ook op bepaalde gevolgen van dat gedrag. Denk aan de observant die het huis van een verdachte observeert en ziet dat het licht aangaat. Het fysieke gedrag van de verdachte (of een andere persoon) is dan niet waarneembaar, maar wel wordt geobserveerd dat het licht aangaat en wordt geconstateerd dat iemand het licht heeft aangedaan zonder dat de veroorzakende handeling is waargenomen. Het betreft dan het observeren van artefacten die het gedrag van een persoon representeren. In een online omgeving is die grens tussen fysiek en virtueel waarnemen zo mogelijk nog lastiger te trekken, alleen al op basis van het feit dat de fysieke afstand tussen het gedrag van een persoon en het daardoor veroorzaakte gevolg heel groot kan zijn.[138] Op basis van het voorgaande kan betoogd worden dat informatie die waargenomen

[136] *Kamerstukken II* 1997/98, 25 403, nr. 7, blz. 60 (nota n.a.v. het verslag)
[137] Aldus een chef OT van de eenheid Rotterdam
[138] Zie ook Strikwerda 2014

wordt op social media als representatie van het gedrag van de geobserveerde persoon gezien kan worden en daarmee onder het beslag van de stelselmatige observatie gebracht kan worden. Hoewel het dus niet goed mogelijk lijkt om hier een strakke grens te trekken, blijft staan dat de wetgever bij de totstandkoming van de Wet BOB de intentie had om de reikwijdte van de stelselmatige observatie scherp af te bakenen. Alles overziend is dan toch de conclusie dat de bevoegdheid stelselmatige observatie niet toepasbaar is op informatievergaring op social media.

4.6 Stelselmatige informatie-inwinning

4.6.1 Artikel 126j Sv

Art. 126j Sv luidt als volgt:

1. *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, zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar, stelselmatig informatie inwint over de verdachte.*
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. *Het bevel tot het inwinnen van informatie is schriftelijk en vermeldt:*
   a) *het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke omschrijving van de verdachte;*
   b) *de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;*
   c) *de wijze waarop aan het bevel uitvoering wordt gegeven, en*
   d) *de geldigheidsduur van het bevel.*
4. *Een bevel als bedoeld het eerste lid kan ook worden gegeven aan:*
   a) *een persoon in de openbare dienst van een vreemde staat, die voldoet aan bij algemene maatregel van bestuur te stellen eisen;*
   b) *een opsporingsambtenaar als bedoeld in artikel 141, onderdelen c en d, of artikel 142, mits deze opsporingsambtenaar voldoet aan bij algemene maatregel van bestuur te stellen regels terzake van opleiding en samenwerking met opsporingsambtenaren als bedoeld in artikel 141, onderdeel b.*

   Het tweede en derde lid zijn van overeenkomstige toepassing.
5. *Artikel 126g, zesde tot en met achtste lid, is van overeenkomstige toepassing.*

In tegenstelling tot art. 126g Sv heeft stelselmatige informatie-inwinning volgens lid 1 altijd betrekking op informatie over de verdachte (in de zin van art. 27 Sv). Het moge duidelijk zijn dat deze verdachte dan verdacht is van het misdrijf dat in lid 1 wordt genoemd.

In navolging van de MvT[139] is voor Buruma[140] het feit dat bij de toepassing van deze bevoegdheid de opsporingsambtenaar niet als zodanig herkenbaar is, het onderscheidende element van stelselmatige informatie-inwinning. Voor Cleiren, Crijns en Verpalen[141] is dat aanleiding om te stellen dat er daarom altijd sprake is van misleiding. Die misleiding kan ingrijpende gevolgen hebben. Buruma[142] stelt de vraag aan de orde of toepassing van deze bevoegdheid niet op gespannen voet staat met het *nemo tenetur* beginsel (art. 6 EVRM) en/of het zwijgrecht (art. 29 Sv).[143]

Het doel van de bevoegdheid is volgens Cleiren, Crijs en Verpalen[144] om aanwezig te zijn in de omgeving van de verdachte en wel op een zodanige manier dat contacten kunnen worden aangeknoopt met de verdachte of met personen in diens omgeving. De opsporingsambtenaar interfereert actief in het leven van de verdachte, waarbij de MvT vooral voorbeelden geeft uit de fysieke wereld, zoals lid worden van dezelfde sportclub.

Van der Meijde[145] ziet daarin het grote verschil met stelselmatige observatie: bij stelselmatige informatie-inwinning gaat de informant bewust en actief verder dan alleen verkennen en luisteren zoals bij observatie: hij gaat de interactie aan.[146] Voor hem is informatie-inwinning een stap verder dan observatie. Als er sprake is van misleiding, dan is dit een belangrijke reden om te kiezen voor toepassing van de bevoegdheid informatie-inwinning, omdat de term 'zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar' (waarvan sprake is bij misleiding) ontbreekt bij art. 126g Sv. Dat is overigens niet verwonderlijk: observatie in de zin van art. 126g Sv is naar zijn aard heimelijk: leden van een observatieteam zullen er alles aan doen om niet herkenbaar te zijn als opsporingsambtenaar.

Cleiren, Crijns en Verpalen[147] wijzen er nog op dat het toepassen van deze bevoegdheid geen toestemming inhoudt om strafbare feiten te plegen. Dat is alleen zo bij infiltratie (art. 126h Sv).

4.6.2 Opsporing op social media als stelselmatige informatie-inwinning?

Ook over de verhouding tussen stelselmatige informatie-inwinning en informatievergaring op social media heeft een aantal schrijvers zich uitgelaten. Stol, Leukfeldt en Klap[148] zijn van mening dat art. 126j Sv een goede grondslag vormt voor de opsporing op social media. Zij nemen als uitgangspunt

[139] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 35
[140] Buruma 2001, p. 84
[141] Cleiren, Crijns & Verpalen 2013
[142] Buruma 2001, p. 85
[143] Volgens EHRM 5 november 2002, NJ 2004/262, m.nt. Kn (Allen) is hier alleen sprake van als er zeer grote druk is uitgegaan van de informant
[144] Cleiren, Crijns & Verpalen 2013
[145] Van der Meijde (*Handboek strafzaken)*, 16.5 Stelselmatig inwinnen van informatie
[146] In soortgelijke bewoordingen: Cleiren, Crijns & Verpalen 2013
[147] Cleiren, Crijns & Verpalen 2013
[148] Stol, Leukfeldt & Klap 2012

dat de politie bij het vergaren van informatie over personen net als ieder ander de openbare informatie van internet mag gebruiken, ook als die informatie over personen gaat. Wel is die bevoegdheid begrensd en wel op basis van de mate waarin de toepassing van die bevoegdheid inbreuk maakt op het recht op privacy. Wanneer die inbreuk meer dan gering is, is een wettelijke bevoegdheid nodig en die vinden Stol c.s. in art. 126j Sv. De reden waarom zij voor dit artikel kiezen wordt verder niet onderbouwd en lijkt vooral een tekstuele te zijn: het verzamelen van informatie uit open bronnen is inwinnen van informatie, art. 126j spreekt over informatie-inwinning en daarom is art. 126j Sv van toepassing op stelselmatig verzamelen van informatie uit open bronnen. Daarbij laten de auteurs de complicatie dat in de MvT bij de Wet BOB ten aanzien van dit artikel gesproken wordt over het actief interfereren in het leven van de verdachte onbesproken. Voor Koops[149] en Oerlemans[150] is juist die complicatie de doorslaggevende reden om te concluderen dat art. 126j Sv niet van toepassing is op opsporing in open bronnen. Het feit dat bij het verzamelen van informatie vanuit open bronnen niet actief om informatie *gevraagd* wordt, maakt voor hen dat art. 126j Sv niet op die manier van opsporen van toepassing is. Wel wijst Koops erop dat als de politie gebruik maakt van middelen om (min of meer) anoniem op internet aanwezig te zijn, er aansluiting gevonden kan worden bij lid 1: “zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar”. Deze toevoeging komt namelijk niet voor in art. 126g Sv. Oerlemans en Koops zien als enige mogelijke toepassing van art. 126j Sv het vrienden worden met de verdachte of iemand in diens omgeving op een netwerksite als Facebook.

Voor de beoordeling van de stelselmatigheid verwijzen Stol, Leukfeldt en Klap[151] naar de *Aanwijzing opsporingsbevoegdheden* van het College van Procureurs-generaal (d.d. 1 maart 2011). Daarin wordt, in navolging van de MvT, gesproken over stelselmatigheid als er een min of meer compleet beeld wordt verkregen van een of meer aspecten van iemands leven. Stol, Leukfeldt en Klap wijzen erop dat in de aanwijzing geen expliciete aandacht besteed wordt aan het inwinnen van informatie uit open bronnen. Het beoordelen of bepaalde opsporingshandelingen een stelselmatig karakter hebben, blijft daardoor casuïstisch. Ondanks dat de minister van Veiligheid en Justitie in een brief aan de Tweede Kamer van 26 juni 2009[152] aangeeft dat het hem bekend is dat er binnen de opsporing behoefte bestaat aan meer uitleg over de toepassing van opsporingsbevoegdheden op internet, heeft dit nog niet geleid tot nadere regelgeving vanuit de wetgever. Mogelijk wordt dit overgelaten aan het lopende herzieningstraject van het Wetboek van Strafvordering.

[149] Koops 2012
[150] Oerlemans en Koops 2012
[151] Stol, Leukfeldt & Klap 2012
[152] *Kamerstukken II* 2008/09, 28 684, nr. 232

Stol, Leukfeldt en Klap constateren dat de wijze van vergaren (bijvoorbeeld gebruik van tools of zoekmachines) niet bepaalt of het onderzoek stelselmatig is, maar het resultaat van het onderzoek daarvoor doorslaggevend is. Deze twee aspecten kunnen echter niet los van elkaar gezien worden. Juist het gebruik van (geautomatiseerde) tools zorgt ervoor dat het resultaat alleen al qua omvang van de verzamelde informatie al snel een min of meer volledig beeld oplevert.

4.6.3 Beoordeling

Is stelselmatige informatie-inwinning nu te gebruiken als grondslag voor de informatievergaring op social media? Opsporing op social media wordt gekenmerkt door het verzamelen (in termen van art. 126j Sv: 'inwinnen') van informatie. Over het algemeen probeert de opsporingsambtenaar om bij die activiteiten niet herkenbaar te zijn als opsporingsambtenaar. Al lang geleden bleken er websites te bestaan die er voor gebruikers die werkten vanaf een politiecomputer volstrekt anders uitzagen dan voor 'gewone' internetgebruikers. Mede daarom is het steeds gebruikelijker binnen de politie om bij dergelijk onderzoek anoniem te surfen door het gebruik van zogenaamde iRN-computers.[153] Hierdoor is de opsporingsambtenaar niet herkenbaar in zijn hoedanigheid, hetgeen een extra argument is om aansluiting te zoeken bij art. 126j Sv.

Het stelselmatig inwinnen van informatie is in de MvT bij dit artikel nader ingevuld als het actief interfereren in het leven van de verdachte: "Het onderscheid met de stelselmatige observatie is daarin gelegen dat de opsporingsambtenaar uitdrukkelijk tot opdracht heeft om op zodanige wijze aanwezig te zijn in de omgeving van de verdachte, dat de verdachte of personen uit de directe omgeving van de verdachte met hem contacten onderhouden zonder dat zij weten dat zij met een opsporingsambtenaar van doen hebben. De opsporingsambtenaar observeert dus niet alleen, maar interfereert actief in het leven van de verdachte. Hij gaat daarbij verder dan alleen waarnemen of luisteren.".[154] Dat kan niet gezegd worden van het ongemerkt verzamelen van informatie uit open bronnen, mogelijk met uitzondering van het sluiten van vriendschappen op netwerksites als Facebook. Op basis van het Tallon-criterium[155] is het echter de vraag in hoeverre dergelijke vriendschappen effectief zijn bij het in de omgeving van de verdachte komen, omdat de interactie met de verdachte beperkt moet zijn.

De *Aanwijzing opsporingsbevoegdheden* stelt over het verschil tussen stelselmatige observatie en stelselmatige informatie-inwinning: "De bevoegdheid tot het stelselmatig inwinnen van informatie onderscheidt zich van de bevoegdheid tot stelselmatige observatie doordat de opsporingsambtenaar

[153] iRN staat voor Internet Recherche Netwerk, een infrastructuur die erop gericht is om anoniem op internet aanwezig te kunnen zijn.
[154] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 34/35
[155] HR 4 december 1979, NJ 1980, 356 m.nt. ThWvV

zich niet beperkt tot het stelselmatig volgen of het waarnemen van het gedrag van een persoon, maar actief interfereert in het leven van de verdachte of de betrokkene van een georganiseerd verband. Een opsporingsambtenaar die stelselmatig informatie inwint, zal zich op een zodanige wijze in de directe omgeving van de verdachte of de betrokkene ophouden dat hij daardoor met personen contacten onderhoudt uit die directe omgeving. Terwijl een opsporingsambtenaar die stelselmatig observeert slechts heimelijk het gedrag van die personen waarneemt.”.[156]

Voor wat betreft het actief interfereren geldt dat dit in een online omgeving mogelijk een andere invulling moet krijgen. De bevoegdheid zoals beschreven in de Wet BOB ziet op fysieke situaties waarin informatie alleen verkregen kan worden door er actief om te vragen. Om de vertrouwenspositie te krijgen die nodig is om dat zonder argwaan te wekken te doen, is actieve interferentie in de omgeving van het subject nodig. Op social media is de informatie die wordt ingewonnen in veel gevallen ongevraagd beschikbaar. Het enkele aanwezig zijn in de virtuele omgeving van het subject om daar de informatie in te winnen, zou dan al gezien kunnen worden als actieve interferentie in diens omgeving.

Daarmee lijkt art. 126j Sv het beste te passen op de informatievergaring uit open bronnen.[157] Gelet op de complicaties die verschillende auteurs naar voren brengen, zou het goed zijn als bij de herziening van het Wetboek van Strafvordering er een aparte bevoegdheid gecreëerd voor het inwinnen van informatie in een niet-fysieke omgeving.[158] Het behoort ook tot de mogelijkheden om het bestaande artikel rondom stelselmatige informatie-inwinning zo uit te breiden dat ook helder is hoe een en ander geregeld is in een online omgeving.

4.7 Toetsing aan art. 8 EVRM

In paragraaf 3.4.3 is uiteengezet hoe de voorwaarden die art. 8 EVRM stelt aan een inbreuk op de privacy moeten worden toegepast op opsporingsmethoden: er moet sprake zijn van een beperking die *in accordance with the law* is, de beperking moet *necessary (zijn) in a democratic society* en moet een *legitimate aim* dienen.

Aan de eis dat een inbreuk *in accordance with the law* moet zijn, wordt in beginsel voldaan door vast te stellen welke bijzondere opsporingsbevoegdheid van toepassing is op opsporing op social media, zoals dat in de vorige paragrafen is gedaan. Bij toepassing van stelselmatige observatie of stelselmatige informatie-inwinning moet voldaan worden aan de voorwaarden in het desbetreffende wetsartikel. In de vorige paragraaf is aangegeven dat art. 126j Sv voor dit doel het beste toepasbaar is. Zoals in 3.4.3 is aangegeven, moet daarnaast echter ook voldaan zijn aan de eisen van

[156] Stcrt. 2014, 24442
[157] Zie voor een zeer recent voorbeeld ECLI:NL:RBDHA:2015:14365.
[158] Vgl. Oerlemans en Koops 2012

kenbaarheid en voorzienbaarheid. Kenbaarheid wordt in dezen opgevat als de eis dat de burger moet weten *dat* de opsporingsdiensten meelezen op social media. Hoewel hier in het kader van deze scriptie geen onderzoek naar is gedaan, is het tegenwoordig vrij algemeen bekend dat de politie ook online actief is. Bovendien maakt de politie er ook geen geheim van dat ze dit doet (zie 2.2). De eis van de voorzienbaarheid heeft betrekking op *hoe* de politie te werk gaat bij die online opsporing. Voor de burger is dit noodzakelijk omdat hij alleen dan op een adequate manier afwegen of hij informatie op social media wil publiceren, welke informatie en op welke wijze. In 3.4.3 is al aangegeven dat een te ruim geformuleerde discretionaire bevoegdheid problematisch kan zijn. Ten aanzien van art. 126j Sv is van belang dat van de opsporingsambtenaar die de bevoegdheid toepast gesteld wordt dat deze niet kenbaar is of hoeft te zijn als opsporingsambtenaar. Dit heimelijke karakter van deze bevoegdheid begrenst intrinsiek de voorzienbaarheid van de wijze waarop het onderzoek plaatsvindt. Bovendien kan het niet de bedoeling zijn om de opsporingsmethoden van de politie prijs te geven. Daarmee staat de voorzienbaarheid wel onder druk. De nadruk zal daarom moeten liggen op een adequate verslaglegging van de in concreto uitgevoerde opsporingshandelingen om de rechter in staat te stellen de rechtmatigheid daarvan achteraf vast te stellen.

De overige eisen die art. 8 EVRM stelt aan een inbreuk op de privacy (*necessary in a democratic society* en *legitimate aim*) worden volgens de memorie van toelichting bij de Wet BOB ingevuld door middel van het opsporingsbelang: het betreffen opsporingshandelingen die bij de bestrijding van de criminaliteit niet gemist zouden kunnen worden. Bij nieuwe opsporingsmethoden zoals opsporing op internet is het noodzakelijk dat de opsporing de ontwikkelingen in de maatschappij en de techniek volgt en indien nodig de gehanteerde opsporingsmethoden daarop aanpast. Dit is niet anders dan bij andere ontwikkelingen in de techniek zoals de ontwikkelingen rondom DNA. Omdat deze nieuwe manieren van opsporing niet voorzien waren bij de totstandkoming van de Wet BOB, is het aan de rechter om in voorkomende gevallen te beoordelen of de desbetreffende onderzoekshandelingen rechtmatig zijn toegepast. Op zeker moment is dan de wetgever aan zet om de wet te moderniseren.

4.8 Conclusie

Een van de oorzaken van de IRT-affaire was dat de opsporing gebruik maakte van opsporingsmethoden die niet in de wet geregeld waren en die men probeerde geheim te houden waardoor er geen democratisch toezicht mogelijk was. Met de komst van de Wet BOB naar aanleiding van het onderzoek van de commissie Van Traa zijn de op dat moment noodzakelijk geachte bijzondere opsporingsmethoden gedefinieerd en is tevens vastgelegd in welke gevallen en onder welke voorwaarden deze methoden gebruikt mogen worden. Een van de cruciale criteria is ‘stelselmatigheid’: als de inbreuk op de rechten van de verdachte meer dan gering is, vormen art. 3

PolW in combinatie met art. 141 en 142 Sv onvoldoende grondslag voor deze wijze van opsporen en moet voldaan worden aan de eisen die in de Wet BOB zijn opgenomen.
Ook bij de opsporing op social media bestaat de kans dat het onderzoek in de vrij (in de zin van: zonder technische beperkingen) beschikbare informatie op internet een dusdanig grote inbreuk maakt op de privacy van de onderzochte persoon, dat er sprake is van stelselmatig onderzoek, in de zin van 'een min of meer compleet beeld krijgen van een of meer aspecten van iemands leven'.
Hoewel bij de opstelling van de Wet BOB nog geen rekening gehouden kon worden met de stormachtige ontwikkelingen van social media, is de opsporing toch gebonden aan de bestaande bevoegdheden in het Wetboek van Strafvordering.
Voor het bepalen wanneer er sprake is van een meer dan geringe inbreuk op de privacy moeten diverse factoren meegewogen worden, zoals de duur van de onderzoekshandeling, de plaats waar de gegevens vandaan gehaald worden, de intensiteit van de onderzoekshandeling, de mate van gevoeligheid van de gegevens, het doel van het onderzoek, het al dan niet toepassen van een technisch hulpmiddel, of de gevonden gegevens worden opgeslagen en de proportionaliteit. De weging van deze factoren kan verschillen tussen handmatig onderzoek in de fysieke wereld en geautomatiseerd zoeken in een online omgeving, maar beiden kunnen leiden tot een "min of meer compleet beeld".

Van de bestaande bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering komen stelselmatige observatie (art. 126g) en stelselmatige informatie-inwinning (art. 126j) in aanmerking om als grondslag voor opsporing op social media te gebruiken. Stelselmatige observatie valt echter af omdat dit artikel ziet op het waarnemen van gedrag, terwijl het bij opsporing op social media gaat over het verzamelen van informatie. Stelselmatige informatie-inwinning biedt wel voldoende aanknopingspunten om als grondslag gebruikt te worden. Met name het karakter van de opsporing op social media (het verzamelen of inwinnen van informatie) en het feit dat deze opsporing over het algemeen zo plaatsvindt dat de opsporingsambtenaar niet in die hoedanigheid bekend is, leiden tot de conclusie dat bij ontbreken van een specifieke bevoegdheid voor opsporing in de virtuele wereld art. 126j Sv het beste als grondslag voor de opsporing op social media gebruikt kan worden.
Met alleen het vaststellen van de van toepassing zijnde bevoegdheid wordt echter nog niet voldaan aan de eis van rechtmatigheid. Om de rechtmatigheid van het onderzoek op social media te kunnen beoordelen is het van groot belang dat in de verantwoording in het procesdossier meer inzicht wordt gegeven in de wijze van opsporing en de gebruikte hulpmiddelen. Alleen zo wordt het voor de rechter mogelijk om de rechtmatigheid van het uitgevoerde opsporingsonderzoek objectief te toetsen.

Voor wat betreft de eisen die art. 8 EVRM stelt aan inbreuken op de privacy is met name de voorzienbaarheid een heikel punt. Omdat stelselmatige informatie-inwinning een heimelijke bevoegdheid is en het opsporingsbelang gediend is met het feit dat niet bekend is over welke methoden, technieken en hulpmiddelen de politie beschikt, zal er weinig naar buiten gebracht worden over de inhoud van de opsporingsmethoden die de politie in dit kader toepast. Om toch invulling te geven aan de eis van voorzienbaarheid, geldt ook hier dat de politie serieus werk moet maken van de verantwoording in het dossier.

Gelet op het eigen karakter van online informatie-inwinning, verdient het aanbeveling om bij de herziening van het Wetboek van Strafvordering een aparte bevoegdheid te creëren voor online inwinning. Omdat de uiteindelijke invoering van het herziene wetboek naar verwachting nog enige jaren zal duren, zou het goed zijn als de wetgever met concrete ijkpunten komt aan de hand waarvan door de opsporing vastgesteld kan worden wanneer er sprake is van stelselmatigheid bij de opsporing op social media. Wel is het van groot belang dat een dergelijke nieuwe bevoegdheid zoveel mogelijk technologie-neutraal wordt geformuleerd om te voorkomen dat de opsporing over twintig jaar opnieuw moet werken met wetgeving die achterloopt bij de stand van de techniek.

5 Conclusie en discussie

5.1 Inleiding

De doelstelling van dit onderzoek is om een bijdrage te leveren aan een rechtmatige, effectieve en verantwoorde wijze van opsporing op social media waarbij een goede balans bestaat tussen de belangen van de opsporing en de grondrechten van de burgers. Daartoe is eerst op empirische wijze nagegaan op welke wijze de politie informatievergaring op social media uitvoert en welke rol het vraagstuk rondom de bevoegdheden daarbij speelt. Vervolgens is nagegaan op welke wijze het in het geding zijnde grondrecht, namelijk het recht op privacy, gedefinieerd kan worden en hoe dit grondrecht juridisch verankerd is. Daarna is vastgesteld op welke wijze de informatievergaring genormeerd kan worden met de bestaande bevoegdheden uit de Politiewet en het Wetboek van Strafvordering zodanig dat er sprake is van een goede balans tussen het opsporingsbelang en de grondrechtenbescherming.

In dit hoofdstuk worden in 5.2 eerst de onderzoeksvragen beantwoord. Vervolgens wordt in 5.3 dieper ingegaan op de conclusies van het onderzoek en worden enkele suggesties voor mogelijk vervolgonderzoek gedaan.

5.2 Antwoorden op de onderzoeksvragen en conclusies

De eerste deelvraag in dit onderzoek was

> *Op welke wijze is de politie actief op social media en hoe worden op dit moment informatievergarende werkzaamheden van de politie verantwoord?*

In hoofdstuk 2 zijn de resultaten van het onderzoek binnen de politie beschreven. Geconstateerd is dat de politie als ambitie heeft geformuleerd om binnen alle politieprocessen een inhaalslag te plegen waar het gaat om het gebruik van social media. Deze ambitie is echter nogal algemeen geformuleerd en zal door middel van concrete maatregelen nader uitgewerkt moeten worden. Voor het gebruik van social media binnen de opsporing is door middel van veldwerk vastgesteld dat de politie zowel in de proactieve als de reguliere opsporing op diverse manieren gebruik maakt van de informatie die op social media te vinden is. Dit kunnen gegevens zijn die op een persoon gericht zijn, maar ook gegevens die betrekking hebben op een bepaald incident. Met name in die tweede categorie kan het gemakkelijk voorkomen dat er ook gegevens van of over niet-verdachten worden verzameld.

Met name in de reguliere opsporing wordt veel van dit onderzoek, vaak op aangeven van de officier van justitie, uitgevoerd op basis van art. 3 PolW. Dit onderzoek vindt vaak plaats op verzoek van politiemensen van een tactisch onderzoek. Binnen het aanvragende team wordt dan met de officier afgestemd over de uit te voeren onderzoekshandelingen, de social media rechercheur is daar vaak

niet bij betrokken. De proactieve onderzoeken zijn vaker zelfstandige onderzoeken, waarbinnen rechtstreeks met de officier wordt overlegd. Binnen die onderzoeken wordt ook vaker gebruik gemaakt van bijzondere opsporingsbevoegdheden als grondslag voor het onderzoek op social media. De verantwoording van de uitgevoerde onderzoekshandelingen op social media vindt bij de reguliere opsporing over het algemeen plaats in algemene termen: “Uit onderzoek op social media is gebleken dat …”. Hierdoor is het op basis van het dossier niet goed mogelijk om vast te stellen in hoeverre de uitgevoerde onderzoekshandelingen rechtmatig zijn uitgevoerd. Bij de onderzochte teams waren geen voorbeelden bekend van een zaak waarbij dit tijdens de terechtzitting expliciet aan de orde is geweest.

Omdat het recht op privacy het belangrijkste grondrecht is dat in het geding is bij informatievergaring op social media, is vervolgens nagegaan hoe het begrip privacy geduid moet worden in de online wereld om een antwoord te formuleren op de tweede deelvraag:

Welke definitie van het recht op privacy is het meest geschikt in online omgevingen?

Zowel de doctrine van de *reasonable expectation of privacy* als de door Nissenbaum geïntroduceerde *contextual integrity* definiëren het recht op privacy met een sterke subjectieve maar ook normatieve component. De passendheid van het kennis nemen van informatie op social media door opsporingsinstanties moet in een voortdurende maatschappelijke discussie door de samenleving worden vastgesteld en bijgesteld. De objectieve en subjectieve elementen van privacy zijn verwoord in de volgende definitie van dit begrip:

> *Privacy is het recht om onbevangen zichzelf te zijn, binnen de grenzen die door het betrokken individu en door de maatschappij als passend worden ervaren. De precieze ligging van deze grenzen wordt mede beïnvloed door de mate waarin het individu door zijn gedrag laat merken dit recht op te geven.*

De derde deelvraag van het onderzoek was

> *Hoe heeft het recht op privacy zich in de geschiedenis ontwikkeld en hoe is dit recht in de wet verankerd?*

Uit bestudering van de historische ontwikkeling van het recht op privacy is gebleken dat dit recht tot de grondrechten gerekend mag worden. Sinds het begin van de jaren 90 is de invloed van het Europese recht op de Nederlandse rechtsorde steeds sterker geworden. Op grond van de rechtstreekse werking van het EVRM en het feit dat het Handvest van de grondrechten van de Europese Unie onderdeel uitmaakt van de Nederlandse rechtsorde, valt de bescherming van het recht op privacy inmiddels volledig onder het beslag van de rechtspraak van het EHRM en het Hof van Justitie. De wijze waarop in art. 8 EVRM het recht op privacy is gedefinieerd laat volop ruimte

voor de gewenste balans tussen individu en omgeving omdat ook gedefinieerd is op welke wijze vastgesteld kan worden of inbreuken op de privacy toelaatbaar geacht worden in een democratische samenleving.

De vierde deelvraag van dit onderzoek heeft betrekking op de benodigde bevoegdheid voor opsporing op social media:

> *Welke informatievergarende werkzaamheden kan de politie uitvoeren op basis van art. 3 Politiewet en wanneer is de inbreuk op de privacy dusdanig groot dat hiervoor een eigenstandige bevoegdheid noodzakelijk is?*

Op basis van art. 8 EVRM is een inbreuk op de privacy op basis van art. 3 PolW toegestaan als deze inbreuk gering is. Er zijn diverse factoren geïdentificeerd die van invloed zijn op de mate van inbreuk, zoals de duur van de onderzoekshandeling, de plaats waar de gegevens vandaan gehaald worden, de intensiteit van de onderzoekshandeling, de mate van gevoeligheid van de gegevens, het doel van het onderzoek, het al dan niet toepassen van een technisch hulpmiddel, of de gevonden gegevens worden opgeslagen en de proportionaliteit.

Als de inbreuk op de privacy meer dan gering is, is een eigenstandige bevoegdheid nodig. De vijfde deelvraag gaat over de bestaande bijzondere opsporingsbevoegdheden in de wet:

> *In hoeverre zijn de bevoegdheden stelselmatige observatie (126g) en stelselmatige informatie-inwinning (126j) van toepassing op informatievergarende werkzaamheden op social media en voldoen ze?*

Van stelselmatige observatie is vastgesteld dat deze afvalt omdat dit artikel ziet op het waarnemen van gedrag, terwijl het bij opsporing op social media gaat over het verzamelen van informatie. Stelselmatige informatie-inwinning biedt wel voldoende aanknopingspunten om als grondslag gebruikt te worden. Met name het karakter van de opsporing op social media (het verzamelen of inwinnen van informatie) en het feit dat deze opsporing over het algemeen zo plaatsvindt dat de opsporingsambtenaar niet in die hoedanigheid bekend is, leiden tot de conclusie dat bij ontbreken van een specifieke bevoegdheid voor opsporing in de virtuele wereld art. 126j Sv het beste als grondslag voor de opsporing op social media gebruikt kan worden.
Met alleen het vaststellen van de van toepassing zijnde bevoegdheid wordt echter nog niet voldaan aan de eis van rechtmatigheid. Om de rechtmatigheid van het onderzoek op social media te kunnen beoordelen is het van groot belang dat in de verantwoording in het procesdossier meer inzicht wordt gegeven in de wijze van opsporing en de gebruikte hulpmiddelen. Alleen zo wordt het voor de rechter mogelijk om de rechtmatigheid van het uitgevoerde opsporingsonderzoek objectief te toetsen.

De hoofdvraag die deze scriptie wil beantwoorden is:

> *Bieden de bijzondere opsporingsbevoegdheden stelselmatige observatie (126g) en stelselmatige informatie-inwinning (126j) in het Wetboek van Strafvordering voldoende mogelijkheden om binnen de grenzen van het strafvorderlijk legaliteitsbeginsel op rechtmatige en verantwoorde wijze opsporingswerkzaamheden op social media uit te voeren in die situaties waarin art. 3 Politiewet onvoldoende grondslag vormt?*

Op basis van het bovenstaande kan geconstateerd worden dat de politie ernaar streeft om ook op social media op rechtmatige en verantwoorde wijze informatie te vergaren binnen de grenzen die vanuit art. 1 Sv en art. 8 EVRM daaraan gesteld worden. Bij deze opsporingswerkzaamheden is het grondrecht op privacy in het geding, een recht dat in een online omgeving vooral bepaald wordt aan de hand van de "passendheid" van de kennisname van de informatie op social media. Alleen door middel van een voortdurende maatschappelijke discussie kan geborgd worden dat deze passendheid op de juiste wijze wordt ingevuld. Wanneer de inbreuk op het recht op privacy gering is, kan de opsporing op social media plaatsvinden op basis van art. 3 Politiewet. Bij een meer dan geringe inbreuk is een aanvullende bevoegdheid noodzakelijk. Deze bevoegdheid kan gevonden worden in de stelselmatige informatie-inwinning van art. 126j Sv. Voor een rechtmatige en verantwoorde opsporing is het echter wel noodzakelijk dat op eenduidige wijze wordt vastgelegd hoe bepaald kan worden of de inbreuk op de privacy meer dan gering is. Hiertoe is in het onderzoek vastgesteld welke factoren van invloed zijn op de mate van inbreuk.

5.3 Discussie

Uit het veldwerk binnen de politie is gebleken dat de politie bezig is om social media te integreren in alle aspecten van het politiewerk. De korpsleiding heeft dit uitgesproken in een visiedocument en verder geconcretiseerd in de zogenaamde negen-domeinen strategie. Voor elk van deze domeinen is vastgesteld op welke wijze de politieorganisatie ingericht moet worden om social media optimaal binnen deze domeinen te integreren in het politiewerk om zo de politieprestaties te verbeteren. Specifiek voor de opsporing is met een aantal politiemedewerkers gesproken over de wijze waarop de politie omgaat met social media, hoe de opsporingswerkzaamheden worden verantwoord en op welke wijze wordt omgegaan met de opsporingsbevoegdheden. Het aantal interviews is beperkt gebleven. Wel is bij de planning van de interviews over de eenheden en de soorten rechercheurs gestreefd naar een zo breed mogelijke spreiding. Vanuit het landelijke social media programma is aangegeven dat het geschetste beeld representatief is voor de stand van zaken binnen de politie in Nederland. Mogelijk dat in een vervolgonderzoek een bredere steekproef genomen kan worden, waardoor een nauwkeuriger beeld van de politie verkregen wordt.

Uit de gesprekken is gebleken dat de opsporing zowel in de pro-actieve fase als tijdens de reguliere opsporing waar mogelijk gebruik maakt van de informatie die op social media gevonden kan worden. Dit kunnen zowel gegevens zijn die op een persoon gericht zijn, maar ook gegevens die betrekking hebben op een bepaald incident. Met name in die tweede categorie kan het gemakkelijk voorkomen dat er gegevens van of over niet-verdachte personen worden verzameld. Er zijn geen kwantitatieve gegevens verzameld over de resultaten die met deze onderzoeken zijn verkregen en in welke mate de gevonden gegevens relevant waren voor het desbetreffende opsporingsonderzoek.

Het antwoord op de vraag in welke mate dergelijke opsporingshandelingen inbreuk maken op het recht op privacy wordt mede bepaald door de definitie van privacy die gehanteerd wordt. In het denken over privacy is een ontwikkeling zichtbaar van een meer algemeen geformuleerd recht (zoals het recht om het rust gelaten te worden) naar een definitie die meer rekening houdt met de opvattingen en emoties van de persoon op wie de informatie betrekking heeft. Privacy wordt daarmee in toenemende mate contextafhankelijk. Nissenbaum introduceert het begrip *contextual integrity* waarbij er sprake is van een schending van de privacy als een informatiestroom niet gebruikt wordt voor het doel waarmee de zender de informatie heeft verzonden en de informatiestroom daarmee door de zender als niet gepast wordt ervaren. Dit hangt nauw samen met de doctrine van de *reasonable expectation of privacy*, zoals die door het EHRM wordt gehanteerd. Ook hierin wordt de beoordeling van de vraag of er sprake is van een schending van de privacy voor een groot deel overgelaten aan de subjectieve mening van de betrokken persoon.
Een dergelijk subjectief privacybegrip maakt het moeilijker om te bepalen wanneer er sprake is van een inbreuk op het recht op privacy. Immers, als de beoordeling van de inbreuk wordt overgelaten aan het subjectieve oordeel van de betrokken persoon, kan bij overigens gelijkblijvende omstandigheden een bepaalde handeling door de ene persoon wel en door een andere persoon niet als inbreuk op de privacy worden beschouwd. Toegepast op social media: de ene persoon zal er geen moeite mee hebben dat de politie zijn openbare berichten op Facebook leest, terwijl een andere persoon dat als ongepast zal beschouwen omdat hij het niet met dat doel op Facebook heeft geplaatst. De overheid zal in dat geval niet anders kunnen dan een voorzichtige houding aannemen en dan al snel het in het kader van de opsporing verzamelen van informatie op social media als inbreuk op het recht op privacy moeten beschouwen. Door middel van een voortdurende maatschappelijke discussie en eventuele proefprocessen zal moeten worden vastgesteld wat passend is en wat niet.

Gelet op de prominente rol die art. 8 EVRM speelt in de juridische bescherming van het recht op privacy, is een inbreuk op de privacy alleen toegelaten als voldaan wordt aan de eisen die in dat

artikel zijn geformuleerd. Er moet sprake zijn van een beperking die *in accordance with the law* is, de beperking moet *necessary (zijn) in a democratic society* en moet een *legitimate aim* dienen.
Ten aanzien van de eis dat een inbreuk *in accordance with the law* moet zijn, geldt dat In Nederland de algemene taakstelling van de politie is beschreven in art. 3 PolW. Op basis van deze algemene bevoegdheid mag de politie inbreuk maken op de rechten van burgers, dus ook op het recht op privacy. Echter, als die inbreuk meer dan gering is, vormt art. 3 PolW onvoldoende basis, en zijn aanvullende bevoegdheden noodzakelijk. De bevoegdheid kan gevonden worden in de BOB-wetgeving, maar dan moet wel aan de daarin opgenomen voorwaarden zijn voldaan.
Onderdeel van de eisen die art. 8 EVRM stelt aan een inbreuk is dat deze voorzienbaar moet zijn. Ten aanzien van de opsporing op social media betekent dat, dat de burger op de hoogte moet zijn van het feit dat de politie ook op social media opsporingshandelingen uitvoert. Alleen dan kan de burger op een adequate manier afwegen of hij informatie op social media wil publiceren, welke informatie en op welke wijze. Dit gaat echter niet zo ver dat de politie moet aangeven *op welke wijze* die opsporing plaatsvindt. Dat zou een te grote beperking betekenen voor de uitvoering van de opsporingstaak.
De overige eisen die art. 8 EVRM stelt aan een inbreuk op de privacy (*necessary in a democratic society* en *legitimate aim*) worden volgens de memorie van toelichting bij de Wet BOB ingevuld door middel van het opsporingsbelang: het betreffen opsporingshandelingen die bij de bestrijding van de criminaliteit niet gemist zouden kunnen worden. Bij nieuwe opsporingsmethoden wordt deze beoordeling aan de rechter overgelaten. Terecht zijn verschillende schrijvers kritisch op deze beperkte invulling door de wetgever van het begrip “beperkte inbreuk”.

De vraag wanneer de inbreuk op de privacy door bepaalde opsporingshandelingen meer dan gering is is niet exact te beantwoorden. In dit onderzoek zijn wel factoren geïdentificeerd die de mate van inbreuk beïnvloeden. Dat zijn: de duur van de onderzoekshandeling, de plaats waar de informatie verzameld wordt, de intensiteit waarmee de informatieverzameling plaatsvindt, de gevoelige aard van de gegevens, het doel van de onderzoekshandeling, het al dan niet toepassen van een technisch hulpmiddel, het al of niet opslaan van de gevonden gegevens en de proportionaliteit. De uiteindelijke weging van deze factoren is geen exacte wetenschap: de professionele inschatting van de politieambtenaar en de uiteindelijke rechterlijke toetsing daarvan, blijfven, net als bij de toepassing van “gewone” bevoegdheden, belangrijk gegevens.

Van de bijzondere opsporingsbevoegdheden stelselmatige observatie (art. 126g Sv) en stelselmatige informatie-inwinning (art. 126j Sv) is vastgesteld of deze kunnen dienen als bevoegdheid voor opsporingshandelingen die een meer dan geringe inbreuk maken op de privacy. Geconstateerd is dat

stelselmatige observatie daarvoor niet in aanmerking komt, vooral vanwege het feit dat observatie betrekking heeft op waarneming van gedrag, terwijl het bij informatievergaring op social media niet om waarneming van gedrag gaat maar om de resultaten daarvan. Aangegeven is dat een ander standpunt hierover ook verdedigbaar is, al lijkt de wetgever uit te gaan van een smalle definitie van observatie. Stelselmatige informatie-inwinning komt in beginsel wel in aanmerking. De actieve interferentie in het leven van de verdachte is in een online omgeving van een andere aard dan in de fysieke wereld omdat in een online wereld informatie zonder vragen beschikbaar is. Stelselmatige informatie-inwinning is daarom bruikbaar als grondslag voor opsporing op social media.
Gelet op de door verschillende auteurs gesignaleerde knelpunten rondom de toepassing van dit artikel en het feit dat niet volledig helder is op welke wijze dit artikel moet worden toegepast bij informatie-inwinning in een niet-fysieke omgeving verdient het aanbeveling om een aparte bevoegdheid voor online informatievergaring in het leven te beroepen, bijvoorbeeld als onderdeel van het lopende traject van herziening van het wetboek van strafvordering. Deze bevoegdheid zal dan wel technologie-onafhankelijk geformuleerd moeten worden.

Om de rechtmatigheid van de opsporingshandelingen op social media te kunnen beoordelen, is het noodzakelijk dat in het procesdossier wordt verantwoord op welke wijze dit onderzoek heeft plaatsgevonden. Uit het veldwerk is gebleken dat in de reguliere opsporing deze verantwoording vaak beperkt is tot zinnen als “Uit onderzoek op social media is gebleken dat ….”. Het is zeer de vraag of de rechter en de verdediging hierdoor in staat zijn te beoordelen of dit onderzoek op rechtmatige wijze heeft plaatsgevonden. Het zou daarom goed zijn als politie en Openbaar Ministerie hier meer aandacht voor zouden hebben en de uitgevoerde onderzoekshandelingen uitgebreider zouden verantwoorden. Daar staat tegenover dat uit de interviews bleek dat dit vraagstuk tijdens terechtzittingen ook nauwelijks aan de orde komt. Vooral van de verdediging zou in dezen een actievere proceshouding verwacht mogen worden. De vraag naar de reden van het niet aan de orde komen van dit vraagstuk op terechtzittingen zou in een vervolgonderzoek onderzocht kunnen worden.

Verwijzingen

Geraadpleegde literatuur

Azouz e.a. 2007

A. Azouz e.a., *De toekomst van persoonsinformatiebeleid. Een dynamische kijk op privacy*, Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2007

Barkhuysen & Bos 2011

T. Barkhuysen & A.W. Bos, 'De betekenis van het Handvest van de Grondrechten van de Europese Unie voor het bestuursrecht', *JBPlus*, 2011

Belinfante & de Reede 2009

A.D. Belinfante & J.L. de Reede, *Beginselen van het Nederlandse staatsrecht*, Deventer: Kluwer 2009

Blom 2001

T. Blom, 'Privacy, EVRM en (straf)rechtshandhaving', in: C.H. Brants, P.A.M. Mevis & E. Prakken (red.), *Legitieme strafvordering, Rechten van de mens als inspiratie in de 21e eeuw*, Groningen- Antwerpen: Intersentia 2001, p. 126-134

Brunst & Sieber 2010

P.W. Brunst en U. Sieber, 'Cybercrime legislation in Germany', in: Basedow, Kischl & Sieber (red.), *German national reports to the XVIII. International Congress of Comparative Law*, Tübingen: Morh Siebeck 2010

Buruma 2001

Y. Buruma, *Buitengewone opsporingsmethoden*, Deventer: Tjeenk W.E.J. Willink 2001

Cleiren, Crijns & Verpalen 2013

C.P.M. Cleiren, J.H. Crijns en R. Verpalen, *Tekst & Commentaar: Strafvordering*, Deventer: Kluwer 2013

Corstens 1995

G.J.M. Corstens, 'Vroegsporing', *Delikt en Delinkwent*, 1995, p.1 e.v.

Corstens 2014

G.J.M. Corstens, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2014

***Eindrapport van de Staatscommissie van advies inzake de Grondwet en de Kieswet* 1971**

Eindrapport van de Staatscommissie van advies inzake de Grondwet en de Kieswet, 's-Gravenhage: Staatsuitgeverij 1971

***Eindrapport van de Staatscommissie Koopmans* 1976**

Privacy en persoonsregistratie. Eindrapport van de Staatscommissie, 's-Gravenhage: Staatsuitgeverij 1976

Eskens 2015

S.J. Eskens, 'Ongerichte interceptie, of het verwerven van bulk-communicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden', *Computerrecht* 2015/85

Fried 1986

C. Fried, 'Privacy', *The Yale Law Review* 1986, Vol. 77, no. 3, p. 475-493

Gavison 1980

R. Gavison, 'Privacy and the Limits of the Law', *The Yale Law Review* 1980, Vol. 89, no. 3, p. 421-471

Gerards 2014

J.H. Gerards (red.), *Sdu Commentaar EVRM, Deel 2, procedurele rechten*, 's-Gravenhage: SDU 2014

De Hert & Gutwirth 2009

P. de Hert & S. Gutwirth, 'Data protection in the case law of Strasbourg and Luxembourg: Constitutionalization in action', in: S. Gutwirth e.a. (eds.), *Reinventing data protection*, Berlin: Springer 2009, p. 57-71

Inzake opsporing 1996

Inzake opsporing. Eindrapport enquêtecommissie Opsporingsmethoden, 's-Gravenhage: Sdu Uitgevers 1996

Johnson 1989

J.L. Johnson, 'Privacy and the Judgments of others', *The Journal of Value Inquiry* 1989, p. 157

Keulen & Knigge 2010

B.F. Keulen en G. Knigge, *Strafprocesrecht*, Deventer: Kluwer 2010

Knigge & Kwakman 2001

G. Knigge en N.J.M. Kwakman, 'Het opsporingsbegrip en de normering van de opsporingstaak', in: *Strafvordering 2001*, II, p. 243-347

Koops 2012

B.J. Koops, 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *Tijdschrift voor veiligheid* 2012(11), p. 30-46

Meij 2010

P.P.J. Meij, *De driehoeksverhouding in het strafrechtelijk vooronderzoek* (diss. Leiden), Deventer: Kluwer, 2010

Van der Meijde (*Handboek strafzaken)*

K. van der Meijde, 'Hoofdstuk 16: Bijzondere opsporingsbevoegdheden', in: P.A.M. Mevis e.a. (red.), *Handboek strafzaken*, Deventer: Kluwer (losbl.)

Melai, Groenhuijsen e.a. 2013

A.L. Melai, M.S. Groenhuijsen e.a., *Wetboek van Strafvordering*, 2013

De Mul & Van der Ploeg 2001

J. de Mul & Y.H. van der Ploeg, *Internet & Privacy. Een inventarisatie van normatieve aspecten van toezicht op internetgebruik in de organisatie* (onderzoeksprogramma Internet & Openbaar bestuur), 2001

Nissenbaum 2010

H. Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford: Stanford University Press 2010

Oerlemans & Koops 2012

J.J. Oerlemans en B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen* 2012, jrg, 38, nr. 5.

Orwell 1949

G. Orwell, *Nineteen eighty-four*, London: Secker & Warburg, 1949

Overkleeft-Verburg 2014

G. Overkleeft-Verburg, 'Commentaar op artikel 10 van de grondwet', in: E.M.H. Hirsch Ballin en G. Leenknegt (red.), *Artikelsgewijs commentaar op de Grondwet*, webeditie 2014 (www.Nederlandrechtsstaat.nl)

Rainey, Wicks & Ovey 2014

B. Rainey, E. Wicks & C. Ovey, *Jacobs, White & Ovey: The European Convention on Human Rights*, Oxford: Oxford University Press 2014

Schermer 2012

B.W. Schermer, 'Digitale IRT-affaire of nieuwe opsporing?', *Webwereld* 14 maart 2012, http://webwereld.nl/opinie/109837/digitale-irt-affaire-of-nieuwe-opsporing---opinie-.html

Siemerink 2000

L.A.R. Siemerink, 'Bob logt in: infiltratie en pseudokoop op het internet', *Computerrecht 2000* p. 141

Smink, Hamstra & Van Dijk 1999

G. Smink, A. Hamstra & H. van Dijk, *Privacybeleving van burgers in de informatiemaatschappij*, Den Haag: Rathenau Instituut 1999

Solove 2008

D. Solove, *Understanding privacy*, Washington DC: Harvard University Press 2008

Steenbruggen 2009

W.A.M. Steenbruggen, *Publieke dimensies van prive-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk* (diss. UvA), Amsterdam: Otto Cramwinckel 2009

Stol 2014

W.Ph. Stol, 'Informatie voor politiewerk: basisprincipes', in: E.R. Muller e.a. (red.), *Politie. Studies over haar werking en organisatie* (serie Handboeken Veiligheid), Deventer: Kluwer 2014

Stol, Leukfeldt & Klap 2012

W.Ph. Stol, E.R. Leukfeldt & H. Klap, 'Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012', *Justitiële verkenningen* 2012, jrg. 38, nr. 1, p. 25-39

Stol, Leukfeldt & Klap 2013

W.Ph. Stol, E.R. Leukfeldt & H. Klap, 'Politie in een digitale samenleving', in: W.Ph. Stol en J. Jansen, *Cybercrime en de politie*, Den Haag: Boom|Lemma 2013

Stol & Van Treeck 1997

W.Ph. Stol & R. van Treeck, 'Cameratoezicht op de snelweg - over het maatschappelijk draagvlak van een nieuwe opsporingsmethode', *Tijdschrift voor de politie* 1997, 59, 5, 10 14

Strikwerda 2014

L. Strikwerda, *Virtual acts, real crimes? A Legal-Philosophical Analysis of Virtual Cybercrime* (diss. University of Twente), Zutphen 2014

***Tweede rapport van de Staatscommissie van advies inzake de Grondwet en de Kieswet* 1969**

Tweede rapport van de Staatscommissie van advies inzake de Grondwet en de Kieswet, 's-Gravenhage: Staatsuitgeverij 1969

Veenstra, Leukfeldt & Boes 2013

S. Veenstra, E.R. Leukfeldt & S. Boes, 'Criminaliteitsbestrijding in een gedigitaliseerde samenleving', in: W.Ph. Stol en J. Jansen, *Cybercrime en de politie*, Den Haag: Boom|Lemma 2013

De Vries & Smilda 2014

A. de Vries & F. Smilda, *Social media: het nieuwe DNA. Een revolutie in opsporing*, Amsterdam: Reed Business 2014

Walden 2007

I. Walden, *Computer crimes and digital investigation*, Oxford: Oxford University Press 2007

Warren & Brandeis 1890

S. Warren & L. Brandeis, 'The right to privacy', *Harvard Law Review* 1890, nr. 5, p. 192

Westin 1967

A. Westin, *Privacy and Freedom*, New York: Atheneum 1967

Jurisprudentie

EHRM

EHRM 26 april 1979, NJ 1980, m.nt. E.A. Alkema (Sunday Times/Verenigd Koninkrijk)

EHRM 2 augustus 1984, NJ 1988, 534 m.nt. P. van Dijk (Malone)

EHRM 24 april 1990, NJ 1981, 523 m.nt. EJD (Huvig-Kruslin)

EHRM 19 februari 1991 (Lüdi v. Zwitserland)

EHRM 23 november 1992 (Niemitz v. Germany)

EHRM 28 oktober 1994, NL 1995, 509 m.nt. Kn. (Murray v. Verenigd Koninkrijk)

EHRM 27 maart 1997 (Halford v. the UK)

EHRM 29 augustus 1997, NJ 1999, 710 m.nt. EJD (Worm)

EHRM 24 augustus 1998 (Lambert v. Frankrijk)

EHRM 16 februari 2000 (Amann v. Zwitserland)

EHRM 5 november 2002, NJ 2004/262 m.nt. Kn (Allen)

EHRM 8 april 2003, nr. 39339/98 (M.M. v. Nederland)

EHRM 24 juni 2004, nr. 59320/00 (Hannover v. Duitsland)

EHRM 3 april 2007 (Copland v. the UK)

EHRM 25 oktober 2007, nr. 38258/03 (Van Vondel v. Nederland)

EHRM 4 december 2008, nr. 30562/04 en 30566/04 (S. en Marper v. Verenigd Koninkrijk)

EHRM 12 januari 2010 (Gillan and Quinton v. the UK)

Europees Hof van Justitie

EU Hof van Justitie van 26 februari 2013, Melloni v. Mnisterio Fiscal, zaaknr. C-399/11

EU Hof van Justitie van 26 februari 2013, Aklagaren v. Hans Akerberg Fransson, zaaknr. C-617/10

EU Hof van Justitie van 7 november 2013, Romeo v. Regione Siciliana, zaaknr. C-313/12

Hoge Raad

HR 4 december 1979, *NJ* 1980, 356 (Tallon) m.nt. ThWvV

HR 14 oktober 1986, *NJ* 1988, 511

HR 14 oktober 1986, *NJ* 1987, 564

HR 19 december 1995, *NJ* 1996, 249

HR 19 maart 1996, *NJ* 1997, 85 (Beslagen Autoruiten) m.nt. Kn

HR 13 oktober 1998, *NJB* 1998, nr. 129

HR 25 januari 2000, *NJ* 2000, 279

HR 21 maart 2000, ECLI:NL:HR:2000:AA5254

HR 12 februari 2002, *LJN* AD7804

HR 20 april 2004, *NJ* 2004, 525

HR 29 maart 2005, *LJN* AS2752

HR 13 november 2012, ECLI:NL:HR:2012:BW9338

HR 1 juli 2014, ECLI:NL:HR:2014:1562

Rechtbank

Rb. Rotterdam, 11 april 2012, LJN BW3105

Rb. Den Haag, 10 december 2015, ECLI:NL:RBDHA:2015:14365

Bijlage 1 – Interviewvragen

Introductie

Voorstellen, positionering van het onderwerp, doel van het interview, procesafspraken (geheimhouding, terugkoppeling e.d.)

1 – Wanneer en hoe vindt opsporing op social media plaats?

Welke opsporingshandelingen verricht de politie op social media?

Welke hulpmiddelen gebruiken ze daarbij?

Op basis van welke criteria besluit de politie om op social media te gaan zoeken?

Wie voeren de opsporingshandelingen uit: elke rechercheur of de specialist?

2 - Hoe gaat de opsporing om met het vraagstuk rondom opsporingsbevoegdheden op social media?

Op basis van welke bevoegdheid wordt het onderzoek gedaan?

Wanneer wordt er vooraf toestemming gevraagd aan c.q. overleg gevoerd met de OvJ?

3 - Op welke wijze wordt het uitgevoerde politieonderzoek verantwoord en welke rol speelt dit deel van het politieonderzoek op de terechtzitting?

Hoe wordt het uitgevoerde onderzoek verantwoord in het PV/dossier?

In hoeverre is de manier van onderzoek een onderwerp tijdens de zitting?

Heeft de rechter of de advocaat (kritische) vragen gesteld naar aanleiding van het onderzoek op social media?

Afsluiting

Vervolgafspraken

Bijlage 2 - Gespreksverslag prof. Fijnaut

De IRT-affaire is ontstaan niet uit brede onvrede over de bestaande bevoegdheden maar uit een ontploffing. Een en ander escaleerde verder tot een gevecht tussen politie en OM over de toelaatbaarheid van bepaalde opsporingsmethoden en werd verder verergerd door de beschuldiging van corruptie binnen het Amsterdamse korps (Jan Wiarda). Het geheel is te karakteriseren als een oorlog tussen politie en OM.

De rol van Fijnaut bij de commissie Van Traa ontstond vanuit de vraag naar de omvang van de georganiseerde criminaliteit. Van Traa wilde die omvang weten, om de proportionaliteit van de opsporingsbevoegdheden te kunnen inschatten. Fijnaut c.s. hebben dat toen in een vooronderzoek onderzocht. Op voorhand was niet iedereen ervan overtuigd dat er een parlementaire enquête moest komen, al was het maar vanwege het vertrouwelijke karakter van de opsporingsmethoden. De uiteindelijke aanbevelingen van de commissie waren ook mede gebaseerd op de uitkomsten van dat vooronderzoek.

De BOB-middelen zijn fysiek gericht en de aanleiding was de bestrijding van de georganiseerde criminaliteit. Het is de ironie van de geschiedenis dat het toepassingsbereik in de loop van de tijd steeds verder is gegroeid.

BOB-middelen waren nodig omdat de bestaande middelen niet altijd voldeden

De Oosterbeek-zaak: opsporing vond plaats door een groot team mensen die in eerste instantie een heel groot net spanden en daarmee een groot aantal niet verdachte personen intensief onderzocht. Door stevig speurwerk werd de juiste persoon gevonden

De term “Verdacht, maar nog geen verdachte” geeft het spanningsveld goed aan: ook als iemand nog niet voldoet aan het wettelijke verdachte-begrip (27 Sv) wil je soms vergaande middelen inzetten om uit te zoeken of iemand toch als verdachte is aan te merken

126gg is een van de middelen om de brug te slaan tussen 3 Polw en BOB/Sv

Vwb opsporing in het kader van de openbare orde kom je eigenlijk terecht bij de AIVD

De sterke nadruk in Nederland op de noodzakelijke bevoegdheden voor de politie valt terug te voeren op de ontstaansgeschiedenis van de gemeentewet rond 1850 en op Thorbecke. Er bestond een enorme angst voor een politieapparaat zoals dat op dat moment georganiseerd was in Frankrijk en Duitsland. Men ervoer dat als echte politiestaten. In Nederland wilde men voor alles ruimte geven aan de vrijheid van de burger, en daarbij paste een model waarin de politie alleen bij een concrete verdenking mocht optreden en daarom buiten strafvordering geen bevoegdheden mocht krijgen. De gevolgen daarvan zijn nog steeds te merken in het algemeen geformuleerde artikel 3 van de politiewet en het verder ontbreken van bevoegdheden voor de politie in de politiewet.
Waar het gaat om de grote nadruk op de privacy in Nederland (bijvoorbeeld in vergelijking met de Verenigde Staten) valt ook die beweging terug te voeren op Thorbecke: overheid op afstand!

Een echte parallel tussen de IRT-affaire en het bestaande bevoegdhedenvacuüm rondom opsporing op social media is er niet. De IRT-affaire was een negatieve aanleiding die uiteindelijk tot iets moois (de BOB-wetgeving) heeft geleid. Beter is het om een parallel te zoeken met technische ontwikkelingen binnen andere vakgebieden van de politie (denk met name aan DNA). Daarmee wordt het bestaande arsenaal aan onderzoeksmethoden en -technieken enorm vergroot, met de bijbehorende toename aan kansen voor de opsporing. Ook dan is regulering en begrenzing noodzakelijk, maar dan met behoud van het goede van de ontwikkeling. Door teveel te redeneren vanuit de gedachte dat die nieuwe mogelijkheden een bedreiging vormen voor een of meer grondrechten, ontstaat een reactie vanuit het negatieve met bijbehorende kans op gemiste kansen.

Waar het gaat om momentum valt nog te wijzen op het feit dat de publieke opinie ten aanzien van de proportionaliteit van een middel vaak ook beïnvloed wordt de actualiteit. Zodra zich een calamiteit voordoet (denk aan de aanslagen in Parijs rondom Charlie Hebdo, maar ook op kleinere schaal rondom Project X in Haren) wordt het gebruik van een opsporingsmiddel veel sneller ervaren als proportioneel dan wanneer er niets aan de hand is.