Surveilleren en opsporen in een internetomgeving

J.J. Oerlemans en B.J. Koops[*]

Surveilleren en opsporen op internet lijkt voor sommige mensen misschien nog sciencefiction, maar wordt in de praktijk al op grote schaal gedaan. Het iColumbo-systeem, de beoogde opvolger van het Internet Recherche (& Onderzoek) Netwerk (iRN), heeft bijvoorbeeld als doel een:

> 'intelligente, geautomatiseerde, "near" real time Internet monitoring service te bieden aan gebruikers van alle overheidsdiensten, die van het iRN gebruik maken. (…) iColumbo wordt ontwikkeld als breed inzetbare toepassing voor opsporing en onderzoek op internet, voor fenomenen of thematisch Internet onderzoek maar ook voor bv. Internet monitoring en alertering in crisissituaties'.[1]

De vraag is in hoeverre een dergelijke 'near real time Internet monitoring service' voor toezicht en opsporing legitiem kan worden toegepast. In principe kunnen opsporingambtenaren net als in de fysieke wereld al dan niet in burger in een internetomgeving rondkijken op basis van de toezichthoudende taak van de politie ter handhaving van de openbare orde, zoals bedoeld in artikel 2 Politiewet 1993 (Polw 1993). Tevens kunnen op grond van artikel 2 Polw 1993 in combinatie met artikel 141 Wetboek van Strafvordering (Sv) tot op zekere hoogte opsporingshandelingen in een internetomgeving worden verricht; bij een meer dan geringe privacyinbreuk moet echter een bijzondere opsporingsbevoegdheid worden ingezet. De factoren die door de wetgever en in jurisprudentie zijn ontwikkeld om de grenzen van deze

* Mr. Jan-Jaap Oerlemans is promovendus bij eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij van de Universiteit Leiden. Daarnaast is hij juridisch adviseur bij Fox-IT. Prof. dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT – Tilburg Institute for Law, Technology and Society van de Universiteit van Tilburg.

1 Citaat afkomstig uit het document 'Deelprojectvoorstel, Ontwikkeling Real Time Analyse Framework voor het iRN Open Internet Monitor Network', 'iColumbo', beschikbaar via www.nctb.nl/Images/deel-projectvoorstel-ontwikkeling-icolumbo-alternatief_tcm91-405727.pdf (laatst geraadpleegd op 25 juni 2012).

bevoegdheden aan te geven, zijn echter geënt op voorbeelden uit de fysieke ruimte. Ze zijn niet direct goed toepasbaar op een internetomgeving. Daardoor is het onduidelijk waar concreet de grenzen liggen bij surveilleren en opsporen in een internetomgeving. Het gebrek aan helderheid is onwenselijk voor opsporingsambtenaren die niet weten hoe ver ze precies mogen gaan, maar ook voor burgers die niet weten waar ze aan toe zijn.
In dit artikel wordt onderzocht welke normen gelden voor het verwerken van gegevens op internet door politie en justitie in het kader van – ten eerste – toezicht, en – ten tweede – in het kader van een opsporingsonderzoek. Daarbij wordt ook ingegaan op het gebruik van geautomatiseerde toepassingen voor politiedoeleinden.

Surveilleren op internet

Allereerst is belangrijk vast te stellen dat de politie *niet* hetzelfde mag als iedere burger op internet, dit in tegenstelling tot wat bijvoorbeeld Stol, Leukfeldt e.a. (2012, p. 29) suggereren. Opsporingsambtenaren mogen namelijk niet altijd hetzelfde als burgers: soms mag de politie meer, soms mag de politie minder (Groenhuijsen en Knigge, 2001, p. 265-268). De bevoegdheden van opsporingsambtenaren staan omschreven in de Politiewet 1993 en het Wetboek van Strafvordering. Surveilleren door de politie is een vorm van toezicht of controle die besloten ligt in de algemene politietaak van artikel 2 Polw 1993 (Melai, Groenhuijsen e.a. 2008, aant. 4.3 op art. 27 Sv). Op grond van artikel 2 Polw 1993 mogen mensen ook worden gevolgd of geobserveerd, voor zover slechts beperkte inbreuken op de persoonlijke levenssfeer worden gemaakt.[2] De vraag is of bij surveilleren op internet slechts een beperkte inbreuk op het privacyrecht van mensen wordt gemaakt of een verdergaande inbreuk waardoor het handelen van de politie niet meer op artikel 2 Polw 1993 kan worden gebaseerd.
In ieder geval is bekend dat ook bij het vergaren van gegevens op internet een inbreuk wordt gemaakt op het recht op privacy, zoals vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM). In de zaak *Uzun* wordt bijvoorbeeld beschreven dat het Europese recht op privacy uit artikel 8 EVRM een ruimte creëert

2 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 98.

voor interactie met andere mensen, zelfs wanneer dat in een publieke ruimte plaatsvindt.[3] In een online context kan als publieke ruimte gedacht worden aan de gedragingen van mensen die voor een ieder zichtbaar zijn, zoals *tweets*, *wall posts*, krabbels, *geo tags* of reacties van mensen op een webforum.[4] Uit deze gegevens kan informatie worden afgeleid over het gedrag, de meningen en gevoelens van personen en daarmee zal een inbreuk op het recht op privacy sneller aan de orde zijn.[5] Deze schending op het recht van privacy moet bij wet voorzienbaar zijn, omdat burgers moeten weten wat ze kunnen verwachten van de overheid.[6] Duidelijk is dat deze wettelijke grondslag gebaseerd kan worden op grond van artikel 2 Polw 1993, voor zover het surveilleren op internet een beperkte inbreuk op de persoonlijke levenssfeer maakt. De mogelijkheid van surveilleren op internet wordt in de memorie van toelichting van de Wet computercriminaliteit II bevestigd:

> 'Zoals de politie, al dan niet in burger, op straat mag surveilleren en rondkijken, zo mag een rechercheur vanachter zijn computer hetzelfde doen op internet. Een uitdrukkelijke wettelijke grondslag is daarvoor niet nodig, mits dat optreden gerekend kan worden tot de uitvoering van de politietaak (zie artikel 2 Politiewet 1993).'[7]

Het is naar onze mening bijvoorbeeld voorstelbaar dat een opsporingsambtenaar handmatig via de zoekmachine Google het doorzoekbare gedeelte van het web en andere delen van internet bekijkt en controleert op strafbare feiten. Tevens is het mogelijk dat een profiel op een sociale netwerkdienst of de Twitterberichten van een bekende door de politie af en toe worden gecontroleerd, net zoals opsporingsambtenaren bij het surveilleren in een openbare ruimte een bepaalde

3 EHRM 2 september 2010, *DD* 2010, m.nt. J.M.W. Lindeman, r.o. 43 (*Uzun t. Duitsland*).

4 *Tweets* zijn berichten van 140 karakters die via de communicatiedienst Twitter op internet worden gepubliceerd. *Wall posts* zijn berichten die op de communicatiedienst Facebook op een profiel worden gezet. Krabbels zijn hetzelfde, maar dan op de Nederlandse communicatiedienst Hyves. Een *geo tag* is ten slotte een kenmerk omtrent de geografische positie waar een persoon zich op enig moment begeeft.

5 Zie ook EHRM 2 september 2010, *DD* 2010, m.nt. J.M.W. Lindeman, r.o. 52 (*Uzun t. Duitsland*).

6 Zie EHRM 25 september 2001, *NJ* 2003, m.nt. E.J. Dommering (*P.G. en J.H. t. Verenigd Koninkrijk*), EHRM 28 januari 2003, *EHRC* 2003, 24 (*Peck t. Verenigd Koninkrijk*), EHRM 17 juli 2003, *EHRC* 2003, 79 (*Perry t. Verenigd Koninkrijk*).

7 *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 35.

groep jongeren oppervlakkig mag controleren.[8] Daarbij moet echter wel worden bedacht dat het in de gaten houden van internetgegevens iets anders is dan het observeren van fysiek gedrag (zonder communicatie). De drempel waarbij sprake is van een beperkte inbreuk op de persoonlijke levenssfeer van mensen wordt bij internetsurveilleren wellicht sneller overschreden. Op internet kunnen gegevens uit verschillende bronnen gecombineerd worden die een breder beeld geven van iemands leven dan wat op straat zichtbaar is. Het is onduidelijk hoe ver de politie mag gaan bij het 'handmatig' vergaren van gegevens in het kader van surveilleren op internet. Bovendien is nog onduidelijk of de aard van de bron waaruit de gegevens worden geput, een factor is die meetelt bij de beoordeling of er slechts sprake is van een beperkte inbreuk op de persoonlijke levenssfeer van de betrokkene.

Open bronnen versus publiekelijk toegankelijke bronnen

Onderscheid kan worden gemaakt tussen open bronnen die zonder enige drempel toegankelijk zijn, en bronnen waarvoor een registratie noodzakelijk is, maar die wel voor het publiek – na registratie – toegankelijk zijn. Is het verzamelen van gegevens uit open bronnen minder privacyschendend dan het verzamelen van gegevens uit bronnen waarvoor registratie noodzakelijk is? Zowel de wetgever als rechters hebben zich hier (nog) niet over uitgelaten, waardoor vooralsnog de interpretatie van de desbetreffende opsporingsambtenaar en officier van justitie bepaalt hoe hiermee wordt omgegaan.
De auteurs van deze bijdrage verschillen van mening op dit vlak. Koops is geneigd sneller een meer dan geringe inbreuk op de persoonlijke levenssfeer aan te nemen wanneer deze informatie op bijvoorbeeld socialenetwerkdiensten pas na registratie raadpleegbaar is. Burgers zullen minder snel verwachten dat informatie uit deze bronnen wordt verzameld door de politie, en er is misschien ook sprake van een vorm van misleiding als de politie een 'burgerprofiel' aanmaakt om op socialenetwerkdiensten of webfora mee te doen. Burgers hanteren contextgebonden normen (Nissenbaum, 2010) en verwachten niet dat informatie die zij in hun eigen sociale context prijsgeven, wordt gebruikt binnen een heel andere context, zoals politie, belasting-

8 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 27. Zie ook *Kamerstukken I* 1998/99, 25 403 en 23 251, nr. 119b (MvA Wet BOB), p. 2.

aangifte of sollicitatieprocedures. Het feit dat mensen informatie op internet zetten met een bepaald doel binnen een bepaalde context, wil nog niet zeggen dat zij daarmee politieel gebruik van deze informatie voorzien. Artikel 2 Polw 1993 levert aldus in de huidige maatschappelijke verhoudingen niet direct 'voorzienbaarheid bij wet' (zie voor een uitgebreidere behandeling Koops, 2012).

Oerlemans is daarentegen van mening dat (na registratie) publiekelijk toegankelijke informatie zich niet onderscheidt van informatie uit open bronnen op internet. Hoewel de subjectieve privacyverwachting van burgers ten aanzien van het soort bron wellicht anders is, hebben burgers bij publiekelijk toegankelijke informatie geen enkele maatregel genomen informatie af te schermen. Burgers kunnen namelijk welbewust profielen op socialenetwerkdiensten afschermen of in een openbaar chatkanaal een privégesprek aangaan en daarmee in vertrouwen de gegevens of informatie slechts binnen een beperkte kring delen.

Het voorgaande betekent echter niet dat publiekelijk toegankelijke informatie door politie en justitie ongelimiteerd kan worden vergaard ten behoeve van surveilleren of in het kader van een opsporingsonderzoek, omdat burgers geen beroep zouden kunnen doen op hun privacyrecht. De benadering heeft slechts tot gevolg dat publiekelijk toegankelijke informatie ten opzichte van informatie uit open bronnen geen *extra* privacybescherming krijgt. Deze zienswijze werkt niet onnodig complicerend en sluit beter aan bij artikel 32 sub a van het Cybercrimeverdrag, op grond waarvan informatie uit publiekelijk toegankelijke bronnen zonder beperkende voorwaarden grensoverschrijdend kan worden verzameld.[9] Zoals de wetgever in de memorie van toelichting bij de Wet computercriminaliteit II heeft opgemerkt, hoeft een opsporingsambtenaar zich niet te identificeren bij het raadplegen van websites op internet en mag de ambtenaar onder pseudoniem te werk gaan.[10] Anders dan Koops suggereert, is volgens Oerlemans van misleiding duidelijk geen sprake, omdat bij surveilleren en observatie geen interactie met de burger plaatsvindt.[11]

Onze verschillende interpretaties over de toelaatbaarheid van zoeken in publiekelijk toegankelijke bronnen waarvoor registratie nodig is,

9 Verdrag inzake de bestrijding van strafbare feiten verboden met elektronische netwerken, *Trb.* 2002, 18.

10 *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet Computercriminaliteit II), p. 35.

11 Zie ook *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 30.

illustreert de onduidelijkheid over de grenzen bij het surveilleren in de (openbare) digitale ruimte en daarmee het diffuse wettelijk kader voor online surveilleren. Dit gaat ten koste van de rechtszekerheid en mogelijk de rechtsbescherming van burgers. Het is bovendien onwenselijk voor opsporingsambtenaren zelf, omdat zij onvoldoende houvast hebben bij het benutten van de nieuwe mogelijkheden van internet.
In de loop der jaren heeft zich echter een praktijk ontwikkeld waarbij toezicht niet meer wordt uitgeoefend door handmatig te zoeken naar strafbare feiten via Google, maar politiesystemen constant internet afstruinen op zoek naar strafbare feiten en bewijsmateriaal. De ongekende hoeveelheid informatie die in relatief korte tijd door internet toegankelijk is geworden, kan niet meer handmatig in de gaten worden gehouden. Dat verklaart de opkomst van software die het efficiënt navigeren in de zee van informatie op internet mogelijk maakt. Echter, door het gebruik van geautomatiseerde politiesystemen wordt een ingrijpender privacyinbreuk gepleegd en treedt mogelijkerwijs een onwenselijke vorm van 'sfeercumulatie' op tussen toezicht en opsporing. We gaan hier in de volgende paragraaf nader op in.

Geautomatiseerd surveilleren op internet

Documentatie die beschikbaar is gekomen na een verzoek op grond van de Wet openbaarheid van bestuur (Wob) licht een tipje van de sluier op van de wijze waarop geautomatiseerde toepassingen worden ingezet in de politiepraktijk ten behoeve van toezicht en opsporing op internet.[12] Sinds 2004 maken de politie en tal van andere overheidsinstanties gebruik van het zogenoemde Internet Recherche (& Onderzoek) Netwerk (iRN).[13] In de documentatie wordt iRN beschreven als 'een overheid brede netwerkinfrastructuur voor onderzoek en opsporing op Internet'. Het iRN-systeem heeft als hoofdfunctionaliteit een zoekfunctie, waarbij 'crawlers' of 'spiders' het zichtbare deel van internet afstruinen op basis van bepaalde parameters teneinde mogelijke strafbare feiten te identificeren en gegevens te analyseren (vgl.

12 Een overzicht van de vrijgegeven documenten n.a.v. het WOB-verzoek is te vinden op: www.nctb.nl/Actueel/WOB-verzoeken/onderzoeksprogramma-herkenning-digitale-informatie-en-fingerprinting.aspx (laatst geraadpleegd op 25 juni 2012).
13 Zie 'Productsheet iRN', beschikbaar via: www.nctb.nl/Images/irn-product-sheet_tcm91-405729.pdf (laatst geraadpleegd op 25 juni 2012).

Schermer, 2007, p. 58). Dat gebeurt met afscherming van de bron, zodat niet zichtbaar is dat de 'crawler' van een met de politie geassocieerd IP-adres afkomstig is.
iRN wordt momenteel opgeschaald en uitgebreid tot een systeem, iColumbo genaamd, dat niet alleen gegevens uit internetbronnen zoekt, maar ook analyseert (bijvoorbeeld met objectherkenning en datamining), selecteert, ordent en overzichtelijk presenteert. Daarmee komt gemakkelijk informatie in beeld die niet zou zijn gevonden tijdens een 'handmatige' surveillance op internet (zonder gebruik van de software). Verder is de tijdsbesparing ten opzichte van het handmatig zoeken naar de informatie op internet enorm.
Dat er grote behoefte bestaat aan 'blauw op internet' en het gebruik van software als hulpmiddel voor toezichtdoeleinden, moge duidelijk zijn. Maar wij betwijfelen of artikel 2 Polw 1993 hiervoor een voldoende grondslag biedt, omdat de software op een systematische manier persoonsgegevens verwerkt die veel verder gaat dan de handmatige zoekactie die de wetgever rond 2000 als voorbeeld noemde van surveilleren op internet. Het gebruik van dergelijke software is naar onze mening onvoldoende voorzienbaar voor burgers en daarmee wordt, zonder een adequate wettelijke regeling, een ongerechtvaardigde inbreuk geleverd op het privacyrecht van betrokkenen (zie ook Koops, 2012). De wetgever zou wellicht een aparte regeling moeten treffen voor het gebruik van de software of op zijn minst meer duidelijkheid moeten geven over de voorwaarden waaronder deze kan worden gebruikt voor toezicht.
Wij vermoeden dat door het gebruik van dergelijke software de kans toeneemt dat de handhaving van de openbare orde (toezicht onder art. 2 Polw 1993) en het vergaren van bewijsmateriaal in een strafzaak, zoals het vergaren van gegevens ter identificatie van personen in een opsporingsonderzoek, door elkaar gaan lopen (dit wordt ook wel 'sfeercumulatie' genoemd). Alleen binnen een opsporingsonderzoek mogen onder bepaalde voorwaarden de gedragingen van personen stelselmatig gevolgd worden of grote hoeveelheden gegevens over personen worden vergaard. Denkbaar is bijvoorbeeld dat het met (politie)software mogelijk is met enkele muisklikken een heel netwerk van (socialemedia)contacten van een betrokkene op internet zichtbaar te maken of dat alle publiekelijk toegankelijke gegevens van een persoon op internet overzichtelijk en gesorteerd op vermoedelijke relevantie op het beeldscherm van de opsporingsambtenaar worden gepresen-

teerd. Door het gebruik van gegevens uit verschillende bronnen op internet en de verwerking van de gegevens door een politieel ICT-systeem door de politie is al snel sprake van een meer dan geringe inbreuk op de persoonlijke levenssfeer van de betrokkene. Dit houdt in dat een min of meer volledig beeld van bepaalde aspecten uit het privéleven van de betrokkene wordt gepresenteerd. Op dit moment kan een dergelijke verdergaande inbreuk op de persoonlijke levenssfeer slechts binnen het kader van een opsporingsonderzoek (dus niet voor toezicht) en onder bepaalde voorwaarden worden gemaakt.

Opsporen in een internetomgeving

Het is denkbaar dat naar aanleiding van (handmatig of beperkt) surveilleren via internet een redelijk vermoeden van schuld aan een strafbaar feit ontstaat, zodat surveilleren overgaat in een regulier opsporingsonderzoek. Het is uiteraard ook mogelijk dat anderszins een opsporingsonderzoek is gestart en een opsporingsambtenaar informatie op internet wil zoeken. (Een opsporingsonderzoek kan tevens plaatsvinden in het kader van onderzoek naar georganiseerde criminaliteit of bij aanwijzingen van terroristische misdrijven; het volgende kan dan mutatis mutandis op die context worden toegepast.) De opsporingsfase is de eerste fase van strafvordering waarbij het Wetboek van Strafvordering van toepassing is. In het Wetboek van Strafvordering zijn bijzondere opsporingsbevoegdheden vastgelegd die normen stellen aan methoden die een meer dan geringe inbreuk op de persoonlijke levenssfeer maken.[14] Het wettelijk vastleggen van verdergaande opsporingsmethoden en daaraan voorwaarden verbinden vloeit bovendien voort uit het strafvorderlijk legaliteitsbeginsel (art. 1 Sv), dat beoogt de overheid in haar optreden te binden aan bepaalde regels ter bescherming van willekeurige inbreuken op de rechten en vrijheden van burgers (Groenhuijsen en Knigge, 2001, p. 182). Ook in de memorie van toelichting van de Wet BOB wordt opgemerkt dat opsporingsmethoden zich in de loop der tijd ontwikkelen en dat de wetgever de taak heeft de wet bij de tijd te brengen indien nieuwe

14 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 98. De Hoge Raad bepaalde al eerder in het Zwolsman-arrest (HR 19 december 1995, *NJ* 1996, 249, overweging 6.3.5, m.nt. Sch) dat opsporingsmethoden die een ernstige inbreuk op de persoonlijke levenssfeer van betrokkenen maken, een specifieke wettelijke grondslag behoeven.

opsporingsmethoden een ingrijpende inbreuk maken op de persoonlijke levenssfeer van de betrokkene.[15]

Stelselmatige informatie-inwinning op internet

Op het eerste gezicht lijkt het bekijken en vastleggen van gegevens op internet wellicht op de bijzondere opsporingsbevoegdheid 'stelselmatig inwinnen van informatie', zoals vastgelegd in onder andere artikel 126j Sv (zie bijvoorbeeld Stol, Leukfeldt e.a., 2012, p. 29 en 30). Deze bevoegdheid is echter vooral geschreven voor de situatie waarin een opsporingsambtenaar actief gegevens ontlokt bij verdachten of personen uit diens directe omgeving. Stelselmatige informatie-inwinning is een undercover opsporingsmethode waarbij een vorm van directe interactie plaatsvindt met de verdachte; daarvan is bij observatie geen sprake. In een internetcontext kan bij toepassing van stelselmatige informatie-inwinning naar onze mening wel worden gedacht aan het vrienden worden met de verdachte op sociale netwerken, zoals Hyves en Facebook. Dit voorbeeld laat opnieuw zien dat in de literatuur en mogelijk in de opsporingspraktijk onduidelijkheid bestaat over de toepassing van het juridisch kader bij opsporing op internet.[16]

Stelselmatige observatie op internet

In de situatie waarbij passief gegevens over een verdachte via internet worden vergaard, ligt toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige observatie (art. 126g Sv) voor de hand. Voor zover de waarneming (of het vastleggen van gegevens) niet *stelselmatig* is, biedt artikel 2 Polw 1993 in combinatie met artikel 141 Sv daarvoor een voldoende grondslag. Het volgen of observeren door opsporingsambtenaren is namelijk inherent aan het uitvoeren van de opsporingstaak. Wanneer de observatie stelselmatig wordt is toepassing van de bijzondere opsporingsbevoegdheid vereist. Helaas is de grens tussen de algemene opsporingsbevoegdheid en stelselmatige

15 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 12.

16 Dit wordt bevestigd in *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 2: 'De belangrijkste conclusie van deze verkenning is dat er grote behoefte bestaat, aan uitleg over wetten en regelgeving en over de toepassing van (bijzondere) opsporingsbevoegdheden op internet.'

observatie – zelfs bij toepassing van de opsporingsmethode in de fysieke wereld – in de praktijk onduidelijk (zie Beijer e.a., 2004, p. 36 en 59). In de memorie van toelichting worden enkele factoren meegegeven die van invloed zijn op de vraag wanneer de opsporingshandeling stelselmatig wordt, namelijk de duur, plaats, intensiteit, frequentie en het al dan niet toepassen van een technisch hulpmiddel dat meer biedt dan alleen versterking van de zintuigen (zoals een camera die vastlegt in plaats van een verrekijker die alleen scherper helpt kijken).[17] Daarnaast heeft de Hoge Raad aangegeven dat de ernst van de ten laste gelegde feiten moet worden betrokken bij het oordeel of artikel 2 Polw 1993 in combinatie met artikel 141 Sv een voldoende grondslag biedt.[18] Deze factoren moeten allemaal in samenhang worden bekeken; zo kan het onder bepaalde omstandigheden zelfs mogelijk zijn een observatie van 60 maal in 27 maanden tijd op artikel 2 Polw 1993 in combinatie met artikel 141 Sv te baseren.[19] Problematisch is echter dat de factoren die in de rechtsontwikkeling tot nu toe worden genoemd, geïnterpreteerd worden vanuit een fysieke situatie, maar niet een-op-een toepasbaar zijn in een digitale context (zie ook Koops, 2012).

In essentie gaat het om de vraag of er sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer en of de opsporingsmethode om die reden een uitdrukkelijke grondslag met bijbehorende voorwaarden van de toepassing ervan behoeft. In onze visie is het mogelijk dat een opsporingsambtenaar via zoektermen in Google op zoek gaat naar informatie over betrokkenen in een opsporingsonderzoek en daarbij een paar websites of profielen op socialemediadiensten over de betrokkene bekijkt op basis van artikel 2 Polw 1993 in combinatie met artikel 141 Sv. Een uitspraak van 23 december 2011 van de Rechtbank Den Haag lijkt hiermee in lijn te zijn.[20] In deze zaak onderzocht de opsporingsambtenaar met een eenmalige zoekopdracht in Google Earth of de verdachte bepaalde stoelen in de tuin had staan, omdat dit relevant was voor een mogelijk frauduleuze belastingaangifte. De Rechtbank Den Haag oordeelde, naar onze mening terecht, dat deze opsporingshandeling viel onder artikel 2 Polw 1993, doordat niet meer dan een beperkte inbreuk werd gemaakt

17 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 27. Deze factoren worden tevens in HR 12 februari 2002, *NJ* 2002, 301, *LJN* AD7804 genoemd.
18 HR 29 maart 2005, *LJN* AS2752.
19 HR 18 mei 1999, *NJ* 2000, 104, m.nt. Sch (4M-zaak).
20 Rb. Den Haag, 23 december 2011, *LJN* BU9409.

op het recht op privacy van de verdachte. De rechtbank merkte daarbij op dat de bevoegdheid 'om rond te kijken in een openbaar netwerk niet de bevoegdheid impliceert om stelselmatig voor de uitoefening van de politietaak gegevens van internet te downloaden en in een politieregister op te slaan'.

Dat het 'stelselmatig downloaden van gegevens op internet' als een meer dan beperkte inbreuk op de persoonlijke levenssfeer kan worden aangemerkt, wordt enigszins bevestigd in jurisprudentie van het Europees Hof voor de Rechten van de Mens. Daaruit kan worden afgeleid dat het vastleggen van gegevens in dossiers of politiesystemen een factor vormt die de inbreuk op de persoonlijke levenssfeer verhoogt, in het bijzonder wanneer dit op systematische wijze gebeurt.[21] In situaties waarbij opsporingsambtenaren gebruikmaken van geautomatiseerde toepassingen, zoals het iRN- of het iColumbo-systeem, worden grote hoeveelheden gegevens van internet verwerkt en in politiesystemen opgeslagen. Naar onze mening wordt dan al snel een meer dan geringe inbreuk gemaakt op de persoonlijke levenssfeer van de betrokkenen en ligt toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige observatie voor de hand. Naast het gebruik van een technisch hulpmiddel bij het opsporen lijken in het bijzonder ook de duur (vaker dan eenmalig zoeken) en intensiteit (de hoeveelheid, gedetailleerdheid en het combineren van gegevens uit verschillende contexten) van belang voor de beoordeling of sprake is van stelselmatige observatie. Indien bijvoorbeeld een grootschalige zoekactie wordt gedaan waarbij (al dan niet geautomatiseerd) alle informatie over een persoon wordt geordend, zal naar onze mening al snel de bevoegdheid van stelselmatige observatie moeten worden toegepast, doordat een meer dan geringe inbreuk op het privacyrecht van betrokkene wordt gemaakt en een min of meer volledig beeld van een bepaald aspect uit het privéleven van een burger wordt verkregen.[22] Overigens zal het in de praktijk lastig te controleren zijn op welke manier gegevens over de verdachte via internet zijn vergaard. Slechts bij de toepassing van een bijzondere opsporingsbevoegdheid moet op grond van artikel 152 Sv een proces-verbaal worden opgemaakt en aan het procesdossier toe-

21 Zie EHRM 16 februari 2000, *EHRC* 2000, 31 m.nt. EB, r.o. 65-66 (*Amann t. Zwitserland*), EHRM 4 mei 2000, *EHRC* 2000, nr. 53, m.nt EB, r.o. 43-44 (*Rotaru t. Roemenië*), EHRM 28 januari 2003, *EHRC* 2003, 24 r.o. 59 (*Peck t. Verenigd Koninkrijk*) en EHRM 17 juli 2003, *EHRC* 2003, 79, r.o. 38 (*Perry t. Verenigd Koninkrijk*).

22 Dit laatste is tevens een criterium voor 'stelselmatigheid', zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 26-27.

gevoegd. Op welke grondslag dat wordt gebaseerd is op dit moment afhankelijk van de betreffende opsporingsambtenaar. Misschien is het een idee als waarborg standaard de logbestanden (die het iRN/iColumbo-systeem standaard genereert) aan het procesdossier toe te voegen wanneer gebruik is gemaakt van politiesoftware.

Nieuwe opsporingsbevoegdheid?

De genoemde voorbeelden laten een belangrijk verschil zien tussen online observatie en fysieke observatie. Bij online observatie kunnen namelijk gegevens uit het verleden over een persoon via internet worden verzameld. Bij observatie in de fysieke wereld gaat het doorgaans om het verwerken van toekomstige informatie die gegenereerd wordt door het volgen van personen of goederen gedurende een bepaalde tijd. Het is afhankelijk van de omstandigheden van het geval hoeveel informatie over een persoon op internet verschijnt gedurende de periode van observatie; in elk geval betreft dit meestal informatie over het huidige leven van de persoon. De informatie die door een betrokkene zelf of door anderen in een eerder stadium online is geplaatst, kan echter op een aanzienlijk langere periode in het verleden betrekking hebben. Daarbij komen niet alleen huidige activiteiten van de verdachte en personen in diens omgeving in beeld, maar ook gedrag en denkbeelden uit het verleden. Die kunnen zeer relevant zijn voor opsporingsonderzoeken, maar kunnen tegelijk ook het beeld vertroebelen doordat ze een verkeerd beeld scheppen, verouderd zijn of simpelweg onjuist zijn (vgl. over deze problematiek Mayer-Schönberger, 2009). Bij het verzamelen van gegevens uit verschillende bronnen zal de intensiteit van de opsporingsmethode hoog zijn door het gedetailleerde beeld dat kan worden verkregen van bepaalde aspecten uit het privéleven van een persoon. Toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige observatie ligt dan weliswaar voor de hand, maar het is de vraag of de wetgever ten tijde van de Wet BOB dit effect van de bijzondere opsporingsbevoegdheid, namelijk dat met terugwerkende kracht gedrag uit het verleden wordt geobserveerd, voor ogen had. Is het dan niet raadzaam opnieuw te analyseren wat observatie in een internetomgeving inhoudt en hoe dit moet worden geregeld?

Wij pleiten niet direct voor een algemene opsporingsbevoegdheid voor het verzamelen van informatie in een internetomgeving, hoewel dat zeker een interessant denkmodel is. Wel zou de wetgever deze problematiek bewust moeten analyseren en zich daarbij moeten baseren op de huidige internetomgeving, die veel verder is ontwikkeld en er anders uitziet dan in 2000 het geval was. Leidend daarbij kan nog steeds het criterium 'stelselmatigheid' zijn, dat inhoudt dat een min of meer volledig beeld van een bepaald aspect uit het leven van een persoon wordt verkregen.

Conclusie

In het kader van internetsurveilleren is het verzamelen van gegevens slechts toegestaan voor zover een beperkte inbreuk wordt gemaakt op de persoonlijke levenssfeer. Aangezien de wetsgeschiedenis niet verwijst naar het systematisch onderzoeken van informatie op open bronnen op internet, maar enkel iets zegt over 'rondkijken' op internet, is het momenteel afhankelijk van de interpretatie van opsporingsambtenaren of zij bij internetonderzoek een beperkte of ernstige inbreuk op de persoonlijke levenssfeer maken. Naar onze mening zijn de mogelijkheden van informatievergaring in het kader van surveilleren echter zeer beperkt, omdat bij een enigszins stelselmatige aanpak van het 'rondkijken' op internet al snel een gedetailleerd beeld van iemands leven te construeren valt. Dat geldt des te meer wanneer aangetroffen gegevens vervolgens ook worden opgeslagen. Surveilleren op internet zal daardoor al snel verder gaan dan wat is toegestaan op basis van artikel 2 Polw 1993. Dat levert een problematische situatie op voor de politie die meent, analoog aan het surveilleren in de openbare fysieke ruimte, te moeten of kunnen surveilleren 'in de openbare virtuele ruimte'. De analogie tussen fysieke en virtuele ruimte gaat al snel mank, vanwege hun verschillende karakteristieken.
De discussie moet echter niet alleen gaan over de grenzen van de 'googelende opsporingsambtenaar', maar ook over de geautomatiseerde gegevensverwerkingen van informatie op internet voor politiedoeleinden. Tegenwoordig kan een ongekende hoeveelheid beschikbare informatie op internet worden geïnventariseerd en geanalyseerd met behulp van speciale politiesoftware. Dit maakt het echter nog niet vanzelfsprekend dat publiekelijk toegankelijke informatie uit sociale-

mediadiensten of andere internetbronnen onbeperkt voor politiedoeleinden kan worden verzameld. Toch zijn in de laatste jaren politiesystemen in gebruik genomen die internet kunnen monitoren voor toezichts- en opsporingsdoeleinden. Naar onze mening is het gebruik van deze systemen voor geautomatiseerd surveilleren op internet op basis van artikel 2 Polw 1993 onvoldoende voorzienbaar voor burgers. De wetgever zou zich moeten uitspreken over deze gegevensverwerkingen en eventueel een nieuwe wettelijke grondslag met waarborgen voor het gebruik daarvan moeten creëren.

De wetgever heeft de nieuwe ontwikkelingen op internet en het gebruik van informatie op internet ten behoeve van de uitvoering van de politietaak en opsporing, ondanks enkele verwijzingen in de wetten Computercriminaliteit en BOB, niet goed (kunnen) overzien.

Op grond van de uitleg in de memorie van toelichting en één recente uitspraak kan worden afgeleid dat incidentele en kleinschalige raadplegingen van informatie op internet mogelijk zijn op grond van artikel 2 Polw 1993 en artikel 141 Sv. Het stelselmatig onderzoeken van informatie op internet is echter alleen mogelijk in het kader van een opsporingsonderzoek, met gebruikmaking van daartoe geëigende bevoegdheden als stelselmatige observatie. Als we willen dat de politie ook op internet systematisch uitgebreid moet kunnen surveilleren, is daartoe eerst de wetgever aan zet. In de tussentijd kunnen advocaten met een actieve proceshouding eventuele vormverzuimen bij internetsurveilleren of opsporen op internet door politie en justitie aan de kaak stellen. Rechters kunnen zich daar vervolgens over uitspreken, waardoor de normen voor digitaal surveilleren en opsporing op internet zich enigszins kunnen uitkristalliseren.

Literatuur

Beijer, A., R. J. Bokhorst e.a.
De Wet bijzondere opsporingsbevoegdheden: eindevaluatie
Den Haag, WODC/Boom Juridische uitgevers, 2004

Groenhuijsen, M.S., G. Knigge (red.)
Het vooronderzoek in strafzaken: tweede interimrapport van de onderzoeksproject Strafvordering 2001
Deventer, Gouda Quint, 2001

Koops, B.J.
Politieonderzoek in open bronnen op internet: strafvorderlijke aspecten
Tijdschrift voor Veiligheid, jrg. 11, nr. 2, 2012, p. 30-46

Mayer-Schönberger, V.
Delete: The virtue of forgetting in the digital age
Princeton, Princeton University Press, 2009

Melai, A.L., M.S. Groenhusijsen (red.)
Het Wetboek van Strafvordering
Deventer, Kluwer, 2008

Nissenbaum, H.
Privacy in context
Palo Alto CA, Stanford Law Books, 2010

Schermer, B.W.
Software agents, surveillance, and the right to privacy: A legislative framework for agent-enabled surveillance
Leiden, Leiden University Press, diss., 2007

Stol, Ph., E.R. Leukfeldt e.a.
Cybercrime en politie
Justitiële verkenningen, jrg. 39, nr. 1, 2012, p. 25-39