

Internetonderzoek door bestuursorganen

Jan-Jaap Oerlemans & Ymre Schuurmans¹

In besluitvormingstrajecten waarin de overheid zéér afhankelijk is van privéinformatie van burgers, zoals in de sociale zekerheid, het vreemdelingenrecht en het belastingrecht, biedt internet ongekende en verruimde mogelijkheden om die privéomstandigheden met een paar muisklikken te achterhalen. In hoeverre is openbronnenonderzoek op internet binnen het bestuursrechtelijk kader toelaatbaar? Binnen het strafrecht en het inlichtingendomein worden nieuwe bevoegdheden geïntroduceerd voor ‘stelselmatig openbronnenonderzoek’, terwijl binnen het bestuursrecht dergelijke plannen ontbreken. In dit artikel wordt de achtergrond van dit verschil in regulering geanalyseerd en bezien of normen en waarborgen uit het strafvorderlijk domein toepasbaar zijn in het bestuursrecht teneinde de grondrechten van betrokkenen (beter) te beschermen.

1. Inleiding

Stel, u bent advocaat te Amsterdam en kan één kamer in uw appartement verhuren voor € 100 per nacht. Daarvoor plaatst u een advertentie op de website Airbnb.² Airbnb is een dienstverlener die een platform aanbiedt waarop mensen hun kamer of woning voor verhuur kunnen aanbieden. De verhuur van uw kamer blijkt een groot succes.

Dat leidt niet alleen tot mogelijk ongenoegen bij omwonenden, maar ook bij de gemeente Amsterdam. De gemeente heeft namelijk in de Huisvestingsverordening het voorschrift opgenomen dat woonruimte niet meer dan 30 dagen per jaar mag worden verhuurd. Zij kunnen eenvoudig vaststellen of u de regels overtreedt door op internet met u mee te kijken. De webpagina op Airbnb met het aanbod van de kamer in Amsterdam en de reviews van gasten zijn immers voor een ieder beschikbaar. Met behulp van zogenoemde ‘scraping’-technieken legt een ICT-systeem van de gemeente Amsterdam elke dag de advertenties en reviews op de advertenties op Airbnb vast ten behoeve van handavingsdoeleinden. Deze informatie uit ‘open bron’ vormt mogelijk bewijsmateriaal in handavingsacties. Uit jurisprudentie blijkt dat bewoners van het college van burgemeester en wethouders een last onder dwangsom opgelegd kunnen krijgen als zij – blijkend uit de advertentie en de reviews op de website Airbnb – de regels uit de Huisvestingsverordening overtreden.³

In dit artikel staat de vraag centraal in hoeverre openbronnenonderzoek op internet binnen het bestuursrechtelijk kader toelaatbaar is. Binnen het strafrecht en het inlichtingendomein worden nieuwe bevoegdheden geïntroduceerd voor ‘stelselmatig openbronnenonderzoek’, terwijl binnen het bestuursrecht dergelijke plannen ont-

breken. Wij analyseren de achtergrond van dit verschil in regulering en bezien of normen en waarborgen uit het strafvorderlijk domein toepasbaar zijn in het bestuursrecht teneinde de grondrechten van betrokkenen (beter) te beschermen. Het onderzoek naar de noodzaak van regulering is primair gebaseerd op een analyse van rechtspraak met betrekking tot artikel 8 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Bij een openbronnenonderzoek zullen al snel persoonsgegevens van burgers worden verwerkt. Daarop zijn ook gegevensbeschermingsrechtelijke normen van toepassing, in het bijzonder de eisen die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG).⁴ De AVG geeft echter minder richting aan de wettelijke *grondslag* voor gegevensverwerking in het publieke domein, nu de wettelijke plicht dan wel publieke taak in beginsel voldoende basis biedt voor gegevensverwerking.⁵ De AVG eist met name dat de gegevens voor een bepaald doel worden verzameld en niet meer dan noodzakelijk zijn om dat doel te bereiken. In principe mogen geen gevoelige persoonsgegevens worden verwerkt, tenzij dat onvermijdelijk is voor het doel. Bovendien mogen de persoonsgegevens niet langer dan noodzakelijk worden bewaard en hebben personen een recht op inzage en correctie.⁶ Voor een deel liggen de eisen in het verlengde van die van artikel 8 EVRM, zoals de (nog te behandelen) noodzakelijkheids- en proportionaliteitseis; voor een deel stelt de AVG meer precieze eisen aan de gegevensverwerking in het concrete geval. Nu onze bijdrage primair gaat over de bevoegdheid tot het doen van openbronnenonderzoek, richt onze analyse zich op artikel 8 EVRM; welke nadere eisen de AVG precies stelt, vergt een op zichzelf staande analyse.

Het artikel houdt voor het beantwoorden van de bovenstaande onderzoeksvraag de volgende structuur aan. In par. 2 wordt de praktijk van openbronnenonderzoek op internet door bestuursorganen onderzocht. Par. 3 onderzoekt de ernst van de privacy-inmenging en de noodzaak tot nadere regulering. In dat kader wordt kort stil gestaan bij de wijze waarop in het strafrecht en het inlichtingendomein een wettelijke grondslag voor openbronnenonderzoek is gecreëerd en welke waarborgen die bevatten tegen te verstrekende privacy-inmengingen. Par. 4 beziet of de waarborgen uit met name de strafrechtelijke regulering ook in een bestuursrechtelijke context kunnen worden toegepast. Het artikel sluit af met een conclusie over de mate waarin openbronnenonderzoek op internet binnen het bestuursrecht toelaatbaar is.

2. Openbronnenonderzoek in het bestuursrecht

2.1. Toepassingen openbronnenonderzoek

Hoewel het college van burgemeester en wethouders van Amsterdam behoorlijk transparant is in het internetonderzoek dat het verricht,⁷ is het zeker niet het enige bestuursorgaan dat informatie op internet verzamelt ten behoeve van de uitvoering. Zo wordt in het kader van de sociale zekerheid veelvuldig op *social media* en online handelsplatformen als 'Marktplaats' gezocht naar informatie die op mogelijke fraude wijst. In het creëren van het ideale beeld van het persoonlijk leven op sociale media, verschijnen *posts* die op mogelijke samenleving tussen personen kunnen wijzen, zoals 'bij de liefde van mijn leven ingetrokken' of 'het is en blijft toch mijn lieve moedertje dus als het even kan ben ik bij haar'.⁸ Een groot aantal advertenties voor goederen of diensten doet het vermoeden rijzen dat er verzwegen inkomsten zijn.⁹ Moest het bestuursorgaan vroeger vooral volstaan met het checken

In het kader van de sociale zekerheid wordt veelvuldig op *social media* en online handelsplatformen als 'Marktplaats' gezocht naar informatie die op mogelijke fraude wijst

van inlichtingenformulieren, tegenwoordig kan het laagdrempelig op het internet surfen en op zoek gaan naar relevante informatie voor zijn handhavingstaak.

Ook in het vreemdelingenrecht duikt het gebruik van *social media* steeds vaker op. Waar asielzoekers doorgaans over vrijwel geen bewijsmateriaal beschikken om hun vluchtrelaas aannemelijk te maken, blijken *posts* op de tijdlijn van Facebook of de activiteiten op LinkedIn inzicht te verschaffen in de politieke of religieuze activiteiten,¹⁰ de seksuele oriëntatie¹¹ of in de mogelijkheden om vakanties in het buitenland door te brengen, zonder problemen met de autoriteiten te ondervinden.¹² Andere opvallende zaken die soms de publiciteit haalden, vormen de in de inleiding genoemde handhaving in de *Airbnb*-zaak, de sluiting van de Amsterdamse sexclub Bianca mede vanwege anonieme recensies op hookers.nl¹³ en de grootschalige Facebookanalyse die dezelfde gemeente uitvoerde om meer grip te krijgen op overlastgevende hangjongeren.¹⁴ Wij vermoeden dat dit slechts het topje van de ijsberg is, gezien de diensten die verschillende *data-science* bedrijven aan de publieke sector aanbieden.¹⁵

Juist in besluitvormingstrajecten waarin de overheid zéér afhankelijk is van privéinformatie van burgers, zoals ook in het belastingrecht,¹⁶ biedt internet ongekende en

Auteurs

1. Beide auteurs zijn verbonden aan de Faculteit der Rechtsgeleerdheid van de Universiteit Leiden. Mr. dr. J.J. Oerlemans is onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten en eLaw, het Centrum voor Recht en digitale technologie. Prof. mr. Y.E. Schuurmans is hoogleraar Staats- en bestuursrecht.

Noten

2. Zie www.airbnb.nl/s/Amsterdam/homes met een gemiddelde huurprijs van € 123 per nacht.
3. Rb. Amsterdam 5 april 2017, ECLI:NL:RBAMS:2017:2123; Rb. Amsterdam 15 februari 2018, ECLI:NL:RBAMS:2018:780; en Rb. Amsterdam 27 juni 2018, ECLI:NL:RBAMS:2018:4442.
4. Zie voor de doorwerking van de AVG in het bestuursrecht o.a. L.H. von Meijenfeldt, 'De AVG en Awb: vragen om Baby-lonische spraakverwarring', *P&I* 2017,

p. 124-129; N. Jak & S. Bastiaans, 'De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid. Een black box voor een black box?', *NJB* 2018/2102, afl. 40.
5. Zie art. 6 lid 1 onder c en e AVG. Over de reikwijdte van deze grondslagen is, net als onder de Wet bescherming persoonsgegevens, (nog) vrijwel geen rechtspraak geweest. Zie voor enige analyse van de invloed van de AVG op toezicht o.a. G.J. Zwenne, W. Steenbruggen & M. Reker, 'Rechtsbescherming bij het gebruik van big data door toezichthouders: een verkenning', *TvT* 2016 (7), p. 29-44; M. Venderbos, 'Normering van bestuurlijk toezichts- en controleonderzoek en recente jurisprudentiële ontwikkelingen', *JBplus* 2019/1.
6. Zie bijv. B.W. Schermer, D. Hagenauw & N. Falot, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', Ministerie van Justitie en Veiligheid 2018.

7. Zie Rb. Amsterdam 5 april 2017, ECLI:NL:RBAMS:2017:2123; Rb. Amsterdam 15 februari 2018, ECLI:NL:RBAMS:2018:780 en Rb. Amsterdam 27 juni 2018, ECLI:NL:RBAMS:2018:4442.
8. Bloemlezing uit Rb. Den Haag 19 juli 2016, ECLI:NL:RBDHA:2016:8215; CRvB 6 oktober 2015, ECLI:NL:CRVB:2015:3400.
9. Zie o.a. CRvB 31 maart 2015, ECLI:NL:CRVB:2015:979; Rb. Limburg 10 november 2016, ECLI:NL:RBLIM:2016:9698; CRvB 12 december 2017, ECLI:NL:CRVB:2017:4301; en CRvB 10 juli 2018, ECLI:NL:CRVB:2018:2090.
10. Rb. Den Haag 8 juni 2017, ECLI:NL:RBDHA:2017:6180.
11. Rb. Den Haag 12 augustus 2014, ECLI:NL:RBDHA:2014:10266.
12. Rb. Den Haag 27 juni 2017, ECLI:NL:RBDHA:2017:7852. Die zaak laat ook zien dat vreemdelingen zelf berichten op Facebook plaatsen ten einde vrees voor

vervolgning (bijvoorbeeld door politieke uitlatingen) bij terugkomst aannemelijk te maken.
13. ABRvS 21 augustus 2013, ECLI:NL:RVS:2013:792, AB 2014/82, m.nt. Vermeer.
14. Zie o.a. 'Gemeente Amsterdam spitte Facebook van hangjongeren door', *NRC Handelsblad* 17 augustus 2018, waaruit blijkt dat om vat te krijgen op het netwerk van 126 hangjongeren 64.540 Facebook-profielen zijn geanalyseerd.
15. Zie bijvoorbeeld www.ynformed.nl/, dat het Amsterdamse Facebookonderzoek uitvoerde of Totta data lab, www.tottadata-lab.nl/totta/klantcases/ dat diverse bestuursorganen als klanten heeft.
16. Veel publieke aandacht kreeg 'De Broedkamer' waarin data-analytics leidt tot informatiegestuurde subjectgerichte handhaving, zie o.a. M. Martijn, 'De fiscus experimenteert volop met onze persoonsgegevens (en dat ging goed mis)', *De Correspondent* 1 februari 2017.



verruimde mogelijkheden om die privéomstandigheden met een paar muisklikken te achterhalen. Soms leiden een paar muisklikken tot uren surfen, maar soms komt er geen ambtenaar meer aan te pas. In dat geval downloadt software structureel bepaalde data op basis van bepaalde criteria en instellingen en slaat deze op in eigen systemen (deze techniek wordt *scraping* genoemd). De vraag rijst in welke mate bestuursorganen internetonderzoek mogen uitvoeren ter verificatie van aanvragen en ter controle van de rechtmatigheid van reeds verstrekte voorzieningen.

2.2. Verificatie, toezicht & opsporing

Over de mogelijkheden tot het doen van internetonderzoek en de voorwaarden waaraan dat onderzoek moet voldoen, is weinig informatie voorhanden. De Awb, noch bijzondere bestuursrechtelijke wetten bevatten een specifieke grondslag voor het doen van openbronnenonderzoek. Dat is op zich weinig opzienbarend. Het bestuursorgaan komt een algemene onderzoeksplicht toe en vergaart op basis van het zorgvuldigheidsbeginsel de nodige kennis (artikel 3:2 Awb), maar de wet geeft geen

specifieke onderzoeksbevoegdheden.¹⁷ Zo zijn ook veel toegepaste methoden als het buurtonderzoek en de heimelijke observatie zonder wettelijke regeling gebleven.

In de klassieke verzorgingsstaat draagt de overheid er zorg voor dat bepaalde voorzieningen terecht komen bij de vaak zwakkeren in de samenleving. Zij oefent eenzijdig gezag uit in een ongelijkwaardige rechtsverhouding. Vanuit die notie is veel aandacht besteed aan de onderzoeksplicht van het bestuur, maar vooral in de zin dat niet teveel van de burger mag worden verwacht en het bestuursorgaan als hoofdregel de bewijslast draagt. Controle en handhaving werden bovendien lang niet altijd erkend als integraal onderdeel van de uitvoering, waarbij speelde dat enig politiek taboe lag op het agenderen van fraudegedrag binnen de maakbare verzorgingsstaat.¹⁸ In de jaren vijftig en zestig zal ongetwijfeld ook hebben meegespeeld dat veel lokale bestuursorganen hun inwoners kenden en een verificatieonderzoek onnodig was.¹⁹

Pas vanaf de jaren tachtig en negentig van de vorige eeuw staat het handhavingstekort prominent op de politieke agenda en komt een algemene regeling van bestuursrechtelijke handhaving tot stand. De wetgever introduceert

toezicht en reparatoire sancties in de derde tranche van de Awb, maar ziet af van de creatie van opsporingsbevoegdheden. (Preventief) toezicht en opsporing (naar aanleiding van een verdenking) dienen van elkaar te worden onderscheiden, waarbij het strafrecht het kader voor de opsporing geeft.²⁰ De in de Awb opgenomen toezichtsbevoegdheden zouden in vele handhavingskaders toereikend moeten zijn. Voor sommige terreinen zal een meer specifieke toezichtsbevoegdheid nodig zijn en dan lijkt de Awb-wetgever ervan uit te gaan dat die steeds in de bijzondere wet zal worden gecreëerd.²¹ We weten inmiddels dat dat niet het geval is, althans dat de bevoegdheid om inlichtingen te vorderen en om zakelijke gegevens in te zien (artikel 5:16 en 5:17 Awb), zo ruim wordt uitgelegd dat in de praktijk toezichthouders ook gegevensbestanden van servers downloaden,²² heimelijke observaties uitvoeren of openbronnenonderzoek verrichten, zonder dat daar een meer specifieke wettelijke grondslag voor is.

Op basis van fraudeprofielen kan een algoritme verdachte zaken selecteren, waarna het bestuursorgaan klassieke onderzoeksbevoegdheden aanwendt

De bestuursrechtspraak heeft tot nu toe weinig paal en perk gesteld aan openbronnenonderzoek op internet. Mogelijk vindt bij fraudeonderzoek veelvuldig internetrecherche plaats, maar blijft dit buiten het gezichtsveld van belanghebbenden – en daarmee van de rechter.²³ Zo kan op basis van fraudeprofielen een algoritme verdachte zaken selecteren,²⁴ waarna het bestuursorgaan klassieke onderzoeksbevoegdheden aanwendt, zoals het vragen van inlichtingen en het afleggen van een huisbezoek. Het dossier zal wellicht alleen van dat klassieke onderzoek verslag doen. In de zaken waarin belanghebbenden wél met het internetonderzoek bekend zijn, zal de rechter alleen de rechtmatigheid van dat onderzoek beoordelen als daar-

over beroepsgronden zijn opgenomen.²⁵ Maar ook in die gevallen komt de juridische normering weinig uit de verf.

In een zaak uit 2017 voerde een bijstandontvanger de principiële grond aan dat het naar hem en zijn vrouw verrichte onderzoek op Facebook een ongerechtvaardigde inbreuk op het recht op respect voor het privéleven maakte en dat de onderzoeksbevindingen buiten beschouwing hadden moeten blijven. In deze zaak was naar aanleiding van de informatie op beider Facebookprofielen het vermoeden ontstaan dat de partners in werkelijkheid samenwoonden, waarna een klassiek rechtmatigheidsonderzoek is verricht. Volgens de Centrale Raad van Beroep kon deze beroepsgrond niet slagen.²⁶ Op grond van art. 53a lid 6 Participatiewet is het college bevoegd onderzoek in te stellen naar de juistheid en volledigheid van de verstrekte gegevens en zo nodig naar andere gegevens die noodzakelijk zijn voor de verlening dan wel de voortzetting van de bijstand. Deze controlebevoegdheid mag steeds en spontaan worden uitgeoefend, dus ook als het Facebookaccount tot geen enkele twijfel had geleid. Als al een onrechtmatige onderzoeksmethode is toegepast, dan wordt onrechtmatig verkregen bewijsmateriaal in het bestuursrecht pas uitgesloten bij zeer ernstige rechtsschendingen, zoals een grove inbreuk op een fundamenteel recht.²⁷ Openbronnenonderzoek is tot nu toe niet als een onrechtmatige onderzoeksmethode aangemerkt en uitsluiting van het vergaarde bewijsmateriaal heeft nog niet plaatsgevonden.

De taak tot controle van verstrekte gegevens bij aanvragen en algemeen handhavingstoezicht maakt het voor bestuursorganen vrij logisch om even op internet te kijken. De ene keer zal de bevoegdheid worden afgeleid uit een controlebevoegdheid in de Participatiewet,²⁸ dan uit de toezichtsbevoegdheden van artikel 5:16 en 5:17 Awb en dan weer uit de algemene onderzoeksplicht van artikel 3:2 Awb. Zo mocht het college van B&W van Amsterdam *scraping* software inzetten op basis van deze algemene onderzoeksplicht, mede omdat de rechter de mate van aantasting van de persoonlijke levenssfeer zeer gering achtte.²⁹

2.3. Protocol internetonderzoek

Dat internetonderzoek meer dan incidenteel wordt toegepast in de bestuurlijke praktijk, blijkt ook uit het 'Protocol internetonderzoek door gemeenten'.³⁰ In 2014 heeft het Kenniscentrum Handhaving en Naleving het protocol voor gemeenten opgesteld. Het protocol biedt richtlijnen voor openbronnenonderzoek naar de rechtmatigheid van diverse gemeentelijke inkomensvoorzieningen, waaronder de bijstand. Dat protocol is door de Autoriteit Per-

17. Los van de toezichttitel in art. 5.2 Awb.

18. Zie Nota 'Aspecten van rechtshandhaving op het gebied van de sociale zekerheid', Kamerstukken II 1991/92, 22457, 2, p. 12.

19. Zie ook het interview met Blokpoel, voormalig algemeen directeur van de belastingdienst, *De Correspondent* 1 februari 2017.

20. Kamerstukken II 1993/94, 23700, 3, p. 134-136.

21. Kamerstukken II 1993/94, 23700, 3, p. 137.

22. Zie bijv. 'ACM Werkwijze voor onderzoek in digitale gegevens 2014', www.acm.nl/sites/default/files/old_publication/publicaties/12594_acm-werkwijze-digitaal-onderzoek-2014-02-06.pdf (laatst geraadpleegd op 13 mei 2019).

23. Vergelijk G.J. Zwenne, W. Steenbruggen & M. Reker, 'Rechtsbescherming bij het gebruik van big data door toezichthouders: een verkenning', *TvT* 2016 (7), p. 38.

24. Zoals geschiedt in het Systeem Risico Indicatie (SyRI) dat onder verantwoordelijk-

heid van de Minister van Sociale Zaken en Werkgelegenheid functioneert. Zie voor meer info <https://bijvoorbautverdacht.nl/wat-is-syri/> (laatst geraadpleegd op 13 mei 2019).

25. Art. 8:69 lid 1 Awb.

26. CRvB 4 juli 2017, ECLI:NL:CRVB:2017:2284, r.o. 4.6.3, *Gst.* 2017/180, m.nt. Stolze & De Wit.

27. Y.E. Schuurmans, 'Onrechtmatig verkregen bewijsmateriaal in het bestuursrecht', AA 2017, p. 388-399.

28. Zie nader W.L. Roozendaal, 'Bestuurlijke opsporing en privacy van bijstandsgerechtigden', *Gst.* 2017/134.

29. Rb. Amsterdam 27 juni 2018, ECLI:NL:RBAMS:2018:4442, r.o. 21.

30. RCF KNHV, dat (inmiddels) onderdeel van de VNG (Vereniging Nederlandse Gemeenten) is, zie <https://www.naleving.net/over-vng-kchn/> (laatst geraadpleegd op 13 mei 2019).

soonsgegevens (onder de oude Wbp) op rechtmatigheid getoetst en goedgekeurd.³¹ Interessant is om te bezien op welke elementen het protocol de nadruk legt om de toets aan het gegevensbeschermingsrecht te kunnen doorstaan én om te constateren dat de in de vorige paragraaf beschreven praktijk verder gaat dan het officiële protocol voorstaat.

Het 'Protocol internetonderzoek door gemeenten' merkt openbronnenonderzoek aan als een vorm van heimelijk waarnemen. Het vindt de bevoegdheidsgrondslag daarvoor in de bevoegdheid tot het doen van rechtmatigheidsonderzoek in bijstandswetgeving (destijds de Wet werk en bijstand, Wwb)³² en ontleent de normering aan de Wwb en (impliciet) artikel 8 EVRM. Zo komt de nadruk te liggen op de noodzakelijkheid en proportionaliteit van het internetonderzoek. De gemeentes zijn zich ervan bewust dat het verzamelen van informatie 'een grote inbreuk vormt op de persoonlijke levenssfeer van de belanghebbende'.³³ Eerst dienen de specifiek wettelijk geregelde verificatiemogelijkheden te worden benut, zoals raadpleging van gegevens van energiebedrijven en de verhuurder,³⁴ voordat een ambtenaar zich op internet kan begeven.³⁵ In het kader van de proportionaliteit verlangt het protocol dat er een 'gegrond vermoeden' van fraude bestaat. Gemeenteambtenaren mogen ook inloggen op een afgeschermd omgeving en onder eigen naam en functie rondkijken om publiekelijk toegankelijke informatie te verzamelen.³⁶ Het preventief raadplegen van openbronnen bij het in behandeling nemen van een aanvraag of om een eerste indicatie van fraude op het spoor te komen, wordt door het protocol afgewezen.³⁷

De wijze waarop het internetonderzoek wordt uitgevoerd is ook geprotocolleerd. De ambtenaar legt een dossier aan op basis van een stappenplan en noteert waarop het gegronde vermoeden van fraude is gebaseerd. Hij vraagt toestemming van de leidinggevende en doet verslag van zijn zoekstrategie. Zo noteert hij welke zoekwoorden hij invoert, welke zoekmachines hij gebruikt en in welke bron hij de informatie vindt.³⁸ Eerst vindt een kortstondig en incidenteel onderzoek binnen een vooraf afgebakende periode plaats, waarna het onderzoek kan worden herhaald, afhankelijk van de feiten gedurende drie tot maximaal zes weken. Informatie waarop de ambtenaar stuit en die niet relevant is voor het rechtmatigheidsonderzoek blijft buiten het dossier en wordt vernietigd. Binnen drie maanden na afronding van het onderzoek wordt de betrokkene daarover geïnformeerd, ook als geen fraude is geconstateerd. In dat laatste geval wordt de vergaarde informatie vernietigd. In het geval van fraude blijven de onderzoeksgegevens maximaal drie jaar bewaard.

Hoewel er geen specifieke wettelijke bepaling is voor openbronnenonderzoek met bijbehorende waarborgen, kan beleid, zoals verwoord in het protocol, de voorzienbaarheid van privacy-inmengingen op internet versterken. Immers, het vereiste van voorzienbaarheid ('prescribed by law') uit artikel 8 EVRM kan ook worden ingevuld door normen die in de rechtspraak worden ontwikkeld, mogelijk aan de hand van door bestuursorganen ontwikkeld beleid.³⁹ Lastig is wel dat het protocol een geground vermoeden van fraude nodig acht, welke eis Awb noch rechtspraak stelt bij uitoefenen van toezichtsbevoegdheden.

Dat doet de vraag rijzen in welke mate het protocol daadwerkelijk leidend is voor de praktijk en de facto die voorzienbaarheid brengt.

3. Een wettelijke grondslag voor de privacy-inmenging bij openbronnenonderzoek

3.1. Ernst van de privacy-inmenging

Om te beoordelen onder welke omstandigheden en met welke randvoorwaarden openbronnenonderzoek rechtmatig is, moet worden geduid hoe groot de inbreuk is die wordt gemaakt op het persoonlijke leven. De term 'open bron' kan de indruk geven dat het vergaren van gegevens 'vrij' of 'onbeperkt' is. Dat is echter niet het geval.

Het Europees Hof voor de Rechten van de Mens (hierna: EHRM) maakt in jurisprudentie duidelijk dat 'ook publieke informatie binnen de reikwijdte van het recht op een privéleven valt, voor zover de informatie systematisch wordt vergaard en wordt opgeslagen door overheidsinstanties'.⁴⁰ Als publiekelijk beschikbare informatie van internet wordt verzameld en wordt gebruikt in handhavingsacties of de besluitvorming van een bestuursorgaan, dan brengt dat een inmenging in het recht op privacy als bedoeld in artikel 8 EVRM met zich mee. De persoonsgegevens mogen dan slechts worden verwerkt voor een bepaald doel, voor zover dat bij de wet is voorzien en voor zover dat noodzakelijk is voor het verwezenlijken van dat doel.⁴¹ De eisen die het Hof stelt aan de wettelijke grondslag voor de onderzoeksbevoegdheid hangen af van de ernst van de privacy-inmenging.

Mensen mogen een minder grote verwachting van privacy hebben als hun informatie in een open bron voor een ieder beschikbaar is

Hoewel het EHRM zich nog nooit specifiek heeft uitgelaten over het verzamelen van persoonsgegevens op internet voor handhavingsdoeleinden, verwachten wij dat het Hof de privacy-inmenging in beginsel niet als bijzonder ernstig zal aanmerken. Mensen mogen een minder grote verwachting van privacy hebben als hun informatie in een open bron voor een ieder beschikbaar is. Het EHRM neemt deze redelijke verwachting van privacy in aanmerking bij de beoordeling van de zwaarte van de inmenging in zaken met betrekking tot cameratoezicht en GPS-tracking in de publieke ruimte.⁴² Dat heeft tot gevolg dat de kwalitatieve vereisten aan nationale wetgeving minder groot hoeven te zijn. Het onderzoek op internet kan dan veelal worden gebaseerd op een algemene grondslag in wetgeving, waarin staat dat voor de taakuitoefening informatie mag worden verzameld en verwerkt.⁴³ Bij meer ernstige privacy-inmengingen, zoals bij het aftappen van

telecommunicatie, vereist het EHRM onder andere een meer gedetailleerde wettelijke regeling en een voorafgaande rechterlijke toets.⁴⁴

Het EHRM heeft met betrekking tot het vergaren van publieke informatie in de zaak *Rotaru* overwogen dat het voor de betrokkene voorzienbaar moet zijn onder welke voorwaarden de overheid op systematische wijze persoonsgegevens mag verwerken.⁴⁵ Ook in de GPS-tracking zaken *Uzun* en *Ben Faiza* overweegt het Hof dat een algemene rechtsbasis voor de toepassing van de opsporingsmethode voldoende kan zijn, voor zover in jurisprudentie of beleid de gronden en voorwaarden voor de toepassing van de maatregel voorzienbaar zijn en het nationale recht voldoende bescherming voor de betrokkenen biedt. De beoordeling of sprake is van adequate en effectieve waarborgen hangt af van de omstandigheden van het geval, zoals de aard, de reikwijdte en de duur van de maatregelen, de vereiste gronden voor toepassing ervan, de autoriteiten die bevoegd zijn de maatregelen te autoriseren, uit te voeren en te controleren en de geboden rechtsmiddelen.⁴⁶

Bij openbronnenonderzoek op internet kan de ernst van privacy-inmenging van geval tot geval verschillen, vanwege de variërende intensiteit van het onderzoek. De hoeveelheid gegevens die over een persoon wordt vergaard kan aanzienlijk verschillen, maar ook de aard van de gegevens en de wijze waarop deze worden vergaard verschilt van geval tot geval. Het eenmaal downloaden van profielinformatie op *LinkedIn* verschilt bijvoorbeeld in intensiteit van het downloaden van alle beschikbare posts en connecties van mensen op Facebook. Ook het gebruik van scraping-technieken, waarbij vooraf grote hoeveelheden persoonsgegevens worden opgeslagen, levert een grotere spanning op met het recht op privacy dan het eenmalig bekijken van recente Twitterberichten van een persoon. Dat komt omdat een grotere hoeveelheid persoonsgegevens wordt vergaard, waaronder ook

voor het doel irrelevante en mogelijk tevens van individuen die niet direct vallen onder het onderzoek van de overheidsinstantie.⁴⁷

De Commissie-Koops, die onderzoek heeft gedaan naar 'de regulering van opsporingsbevoegdheden in het digitale tijdperk' identificeert in totaal 17 factoren die de ernst van de inbreuk op de persoonlijke levenssfeer beïnvloeden bij openbronnenonderzoek. Deze factoren kunnen worden gegroepeerd in de volgende vier factoren: 1. omvang en type van de (over te nemen) gegevens, 2. aard van de bron, 3. wijze van zoeken (zoals het gebruik van scrapers) en 4. het gebruik van de gegevens en de mogelijke impact op de persoon.⁴⁸ Deze vier factoren kunnen behulpzaam zijn om de ernst van de privacy-inmenging te bepalen.

Kortom, de aard en intensiteit van het openbronnenonderzoek bepalen de eisen die worden gesteld aan de wettelijke grondslag van deze onderzoeksbevoegdheid. In de volgende paragraaf bezien we hoe binnen het strafrecht en inlichtingendomein openbronnenonderzoek wordt gereguleerd als mogelijke inspiratie voor nadere normering in het bestuursrecht.

3.2. Openbronnenonderzoek in het strafrecht en inlichtingendomein

In het strafrecht en in regelgeving voor inlichtingen- en veiligheidsdiensten worden meer gedetailleerde regelingen in de wet neergelegd als 'bijzondere opsporingsbevoegdheden' (BOB-bevoegdheden) en 'bijzondere bevoegdheden' als de inbreuk op de persoonlijke levenssfeer van de betrokkene 'meer dan gering' is. Om het risico van willekeur en misbruik tegen te gaan, dient de wet voldoende helder te zijn over de gevallen waarin en de voorwaarden waaronder de autoriteiten de bevoegdheid hebben een meer dan geringe inbreuk te maken op het recht op de persoonlijke levenssfeer.⁴⁹ Dat betekent dat in het strafrecht de wetgeving moet voorzien in meer gedetailleerde

31. *Stcrt.* 2015, 10540. Het gehele protocol is beschikbaar op: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/protocol_internetonderzoek_door_gemeenten.pdf (laatst geraadpleegd op 13 mei 2019).

32. Art. 63 en 64 Wvb, thans art. 53a Participatiewet.

33. Zie p. 1 van het Protocol internetonderzoek door gemeenten.

34. Art. 63 en 64 Wvb, thans art. 53a Participatiewet.

35. Zie p. 7 en 8 Protocol internetonderzoek door gemeenten.

36. Zie stap 6, sub d Stappenplan. Zie over de reikwijdte van het begrip open bron ook het rapport van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 152 (hierna: Commissie-Koops).

37. P. 8 en 9 Protocol internetonderzoek door gemeenten.

38. Zie stap 6 van het 'Stappenplan toepas-

sing internet onderzoek', bijlage 1 van Protocol internetonderzoek door gemeenten.

39. Zie o.a. EHRM 26 april 1979, 6538/74, par. 49 (*Sunday Times/Het Verenigd Koninkrijk*); EHRM 14 april 1990, 11801/85, par. 28 (*Kruslin/Frankrijk*); en EHRM 2 augustus 1984, 8691/79, par. 66 (*Malone/Het Verenigd Koninkrijk*).

40. EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, par. 43 (*Rotaru/Roemenië*);

EHRM 6 juni 2006, 62332/00, ECLI:CE:ECHR:2006:0606JUD006233200, par. 72 (*Segerstedt-Wiberg e.a./Zweden*) en EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 44, (*Uzun/Duitsland*), EHRC 2010/123, m.nt. De Hert en Van Caeneghem; en *NJB* 2010/1935 en EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, par. 53 (*Ben Faiza/Frankrijk*), EHRC 2018/85, m.nt. Hagens.

41. Ook art. 5:13 Awb verlangt dat toezichthouders slechts gebruik maken van hun bevoegdheden voor zover dat redelijkerwijs nodig is voor de vervulling van hun taak en voor die evenredigheidsdoets is de grootte van de privacy-inbreuk van belang.

42. Zie met betrekking tot cameratoezicht EHRM 21 september 2001, 44787/98, ECLI:CE:ECHR:2001:0925JUD004478798, par. 57 (*P.G. en J.H./Het Verenigd Koninkrijk*); EHRC 2001/76, m.nt. Spronken en GPS-tracking EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 44, (*Uzun/Duitsland*), EHRC 2010/123, m.nt. De Hert en Van Caeneghem en *NJB* 2010/1935.

43. Zie uitgebreid over het recht op privacy (art. 8 EVRM) en openbronnenonderzoek: J.J. Oerlemans, *Investigating Cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017, p. 86-104.

44. Zie in het bijzonder EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, par. 257-267 (*Zakharov/Rusland*), EHRC 2016/87, m.nt. Hagens.

45. EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, par. 43 (*Rotaru/Roemenië*), EHRC 2000/53, m.nt. Brems.

46. EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 63 (*Uzun/Duitsland*), EHRC 2010/123, m.nt. De Hert en Van Caeneghem en *NJB* 2010/1935 en EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, par. 63 (*Ben Faiza/Frankrijk*), EHRC 2018/85, m.nt. Hagens.

47. Zie ook Oerlemans 2017, p. 97-98.

48. Commissie-Koops 2018, p. 163-164.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

ECLI:CE:ECHR:2015:1204JUD004714306, par. 257-267 (*Zakharov/Rusland*), EHRC 2016/87, m.nt. Hagens.

45. EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, par. 43 (*Rotaru/Roemenië*), EHRC 2000/53, m.nt. Brems.

46. EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 63 (*Uzun/Duitsland*), EHRC 2010/123, m.nt. De Hert en Van Caeneghem en *NJB* 2010/1935 en EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, par. 63 (*Ben Faiza/Frankrijk*), EHRC 2018/85, m.nt. Hagens.

47. Zie ook Oerlemans 2017, p. 97-98.

48. Commissie-Koops 2018, p. 163-164.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

49. Deze uitwerking van het legaliteitsvereiste betreft een belangrijk kenmerk van een rechtsstaat.

regels voor de inzet van bevoegdheden die een meer dan geringe inbreuk vormen op de persoonlijke levenssfeer van betrokkenen.⁵⁰ Een belangrijke waarborg is gelegen in de voorafgaande toestemming die van een hogere autoriteit moet worden verkregen bij de inzet van ingrijpende onderzoeksbevoegdheden, zoals een officier van justitie en rechter-commissaris in het strafrecht.

De grote hoeveelheden persoonsgegevens die tegenwoordig over mensen publiekelijk beschikbaar zijn en de toegenomen mogelijkheden deze gegevens te verzamelen en te verwerken hebben binnen het strafrecht en inlichtingendomein geleid tot de introductie van een bijzondere bevoegdheid tot het 'stelselmatig vergaren van persoonsgegevens uit open bron'.⁵¹ Voor de invulling van

Zet men het openbronnenonderzoek af tegen het opvragen van gegevens bij derden, het huisbezoek of het buurtonderzoek, dan vormt het openbronnenonderzoek niet een bijzonder ingrijpende manier van informatiegaring

het criterium van 'stelselmatigheid' kunnen de eerder genoemde factoren van de Commissie-Koops geschikt zijn. Volgens de Commissie zou de inzet van de bevoegdheid op zijn plaats zijn als 'op voorhand redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan'. In dat geval is sprake van stelselmatigheid en is de toepassing van de voorgestelde bijzondere opsporingsbevoegdheid tot het stelselmatig verzamelen van persoonsgegevens uit open bron op zijn plaats. De inschatting van de zwaarte van de privacy-inmenging moet volgens de Commissie-Koops vooraf worden gemaakt, voor zover deze 'redelijkerwijs voorzienbaar' is 'aan de hand van algemene en contextspecifieke ervaringsregels en van een redelijke inschatting van de omstandigheden van het geval'.⁵² De bijzondere bevoegdheid in het inlichtingendomein en in het strafrecht voorgestelde bijzonder opsporingsbevoegdheid creëert dus een wettelijke grondslag voor het stelselmatig vastleggen van persoonsgegevens uit open bronnen. Waarborgen tegen misbruik zijn gelegen in het autorisatievereiste, in de maximale duur van het onderzoek (drie maanden, die kunnen worden verlengd) en de wijze waarop de persoonsgegevens geautomatiseerd worden vastgelegd.⁵³

Het voorgaande laat veel ruimte voor invulling voor de internetrechercheurs om te bepalen of er sprake is van stelselmatigheid. Die flexibiliteit is op zich ook gewenst, omdat de aard van de informatie die over personen op internet is te vinden zeer verschillend is. Verschillende

auteurs hebben er echter ook op gewezen dat de regeling niet tot de nodige duidelijkheid leidt met betrekking tot de vraag wanneer de bijzondere (opsporings)bevoegdheid moet worden toegepast.⁵⁴

4. Normering van openbronnenonderzoek in het bestuursrecht

Uiteraard kunnen de bijzondere opsporingsbevoegdheden uit het strafrecht en de inlichtingsfeer niet zomaar naar het bestuursrecht worden overgezet. Het bestuursrecht kent geen bijzondere opsporingsbevoegdheden en dat is tot nu toe een bewuste keuze geweest. Dusdanig ingrijpende opsporingshandelingen horen primair binnen het kader van het strafrecht thuis, waar de inzet van de opsporingsbevoegdheid *vooraf* met meer waarborgen is omgeven, zoals een bevel van een officier van justitie of een machtiging door een rechter-commissaris. Hoewel de wetgever ook in het bestuursrecht een vorm van 'toestemming vooraf' zou kunnen creëren,⁵⁵ zal hij dat niet snel voor één specifieke opsporingsbevoegdheid doen. Voor het bestuursrecht is de waarde van de analyse van de regulering van het openbronnenonderzoek als bijzondere opsporingsbevoegdheid met name gelegen in de factoren die bepalen of iets een open bron is en hoe ingrijpend het onderzoek is.

4.1. Definitie open bron

Een open bron kan worden gedefinieerd als informatie die voor een ieder toegankelijk is. Voor zover toegang tot informatie op internet gebonden is aan een account en het verkrijgen van een account een (semi)geautomatiseerd proces is (waarbij niet bepaalde groepen worden uitgesloten van registratie), kan die informatie als voor een ieder toegankelijk worden gekwalificeerd.⁵⁶ Hierbij kan worden gedacht aan de sociale mediadienst Facebook, waarbij een ieder in principe een account kan aanmaken. Na registratie is dan meer informatie beschikbaar dan informatie die slechts door zoekmachines zoals Google beschikbaar wordt gemaakt. Ook betaaldiensten zonder nadere toegangscontrole, zoals toegang tot LexisNexis en de Kamer van Koophandel, worden gezien als een open bron.⁵⁷ Open bronnen staan dus tegenover *afgeschermd* bronnen, die zich kenmerken doordat een internetgebruiker er uitdrukkelijk voor kiest andere internetgebruikers al dan niet toe te laten tot de bron.⁵⁸ Daarbij kan gedacht worden aan profielgegevens van een gebruiker van Facebook, waarbij de gebruiker slechts toegang geeft tot de informatie op zijn profiel na het accepteren van een vriendschapsverzoek.

4.2. Ernst van de privacy-inmenging

De ernst van de privacy-inmenging kan worden bepaald aan de hand van factoren als: 1. de omvang en type van de (over te nemen) gegevens, 2. de aard van de bron, 3. de wijze van zoeken en 4. het gebruik van de gegevens en de mogelijke impact op de persoon. De inmenging wordt bijvoorbeeld groter naarmate een ambtenaar vaker een bepaalde burger googlet, langer surft en de uitlatingen op internet aan een inhoudelijke analyse onderwerpt. Bij een meer dan geringe privacy-inbreuk verlangt het EHRM een wettelijke grondslag voor de inzet van de onderzoeksbevoegdheid, die waarborgen tegen misbruik biedt. Verslag-



legging van het internetonderzoek, zoals in het 'Protocol internetonderzoek door gemeenten', biedt een belangrijke waarborg, omdat gelogd moet worden hoe lang, met welke zoekmachines, met welke trefwoorden is gezocht. Uit de analyse blijkt dat ook transparantie over de doelen waarvoor en de wijze waarop openbronnenonderzoek plaatsvindt zeer relevant is.

4.3. Waarborgen bij openbronnenonderzoek in het bestuursrecht

Openbronnenonderzoek lijkt in het bestuursrecht een veel gebruikte methode om laagdrempelig gegevens uit aanvragen te controleren of om eerste signalen van fraude op te pikken, zodat handhavingscapaciteit efficiënt kan worden ingezet. Onderzoek, toezicht en verificatie worden in het algemeen noodzakelijk geacht, vaak vanwege het economisch welzijn of ter bescherming van de openbare veiligheid. Hoewel de digitale dimensie nieuwe vragen oproept en ons vaak waakzaam maakt voor privacy-inmengingen, is het niet bij voorbaat zo dat de inmenging ingrijpender is dan met middelen in de analoge wereld. Zet men het openbronnenonderzoek af tegen het opvragen van gegevens bij derden, het huisbezoek of het buurtonderzoek, dan vormt het openbronnenonderzoek niet een bijzonder ingrijpende manier van informatiegaring. De privacy-inbreuk bij het doorzoeken van bijvoorbeeld de advertenties op verkoopsites, zal doorgaans minder ingrijpend zijn dan het opvragen van allerhande rekening-afschriften. Gegevens die op internet voor een ieder beschikbaar zijn, mogen naar ons oordeel in beginsel door bestuursorganen worden verzameld, als onderdeel van hun algemene bevoegdheid om informatie te verzamelen (artikel 3:2 Awb) en toezicht uit te oefenen.⁵⁹

Openbronnenonderzoek is echter niet vrij en onbeperkt; het brengt enkele verantwoordelijkheden voor bestuursorganen met zich. In de kern is dat volgens ons zoveel mogelijk transparantie over de wijze waarop en de voorwaarden waaronder openbronnenonderzoek wordt toegepast, zodat de proportionaliteit van het uitgevoerde onderzoek en de mogelijke stelselmatigheid kan worden beoordeeld. Bij de inzet van andere 'opsporingsmethoden' waarmee een min of meer compleet beeld van een bepaald aspect van het persoonlijk leven in kaart kan worden gebracht, zoals locatietracking met behulp van GPS of cameratoezicht, is de bestuursrechter al een strengere koers gaan varen.⁶⁰ Het zou in die lijn passen als de bestuursrechter meer kritisch beziet hoe het internet-

onderzoek is uitgevoerd en verder gaat dan de enkele overweging dat een bestuursorgaan steeds spontaan en zonder aanleiding onderzoek mag doen. Bij een grotere privacy-inbreuk is het onzes inziens wenselijk dat bepaalde waarborgen een nadere bestuursrechtelijke invulling krijgen, bijvoorbeeld in beleid van bestuursorganen. Zo verdient het aanbeveling de proportionaliteitstoets in de toezichtfase (artikel 5:13 Awb) meer inhoud te geven, grenzen te stellen aan de duur van het onderzoek en in een regeling vast te leggen wie een meer omvattend internetonderzoek moet autoriseren.

5. Conclusie

In dit artikel stond de vraag centraal in hoeverre openbronnenonderzoek op internet binnen het bestuursrechtelijk kader toelaatbaar is. Bestuursorganen hebben ruime bevoegdheden om in het kader van toezicht gegevens te verzamelen en spontaan onderzoek te doen. In de praktijk worden diverse onderzoeksbevoegdheden aangewend zonder dat daarvoor een specifieke wettelijke grondslag is, zoals heimelijke observatie. Een onderzoek in openbronnen op internet vertoont daarmee sterke parallellen.

Uit Europese jurisprudentie over de verwerking van gegevens uit open bron en observatie leiden wij af dat incidenteel internetonderzoek kwalificeert als een beperkte inmenging in het privéleven. Binnen het bestuursrecht zou deze vorm van openbronnenonderzoek mogelijk moeten zijn op grond van de algemene onderzoeksplicht op grond van artikel 3:2 Awb.⁶¹ De ernst van de privacy-inmenging bij openbronnenonderzoek verschilt echter van geval tot geval. De factoren die zijn geformuleerd door de Commissie-Koops kunnen behulpzaam zijn bij het bepalen van de ernst van de privacy-inmenging. Hoe groter de privacy-inmenging die plaatsvindt, hoe meer waarborgen nodig zijn. Deze factoren betreffen 1. de omvang en type van de (over te nemen) gegevens, 2. de aard van de bron, 3. de wijze van zoeken en 4. het gebruik van de gegevens en de mogelijke impact op de persoon. Binnen het inlichtingendomein en in de toekomst mogelijk binnen het strafrecht kunnen deze factoren worden gebruikt om openbronnenonderzoek op een bepaald moment als 'stelselmatig' aan te merken, waarvoor een algemene onderzoeksbevoegdheid niet langer als grondslag kan dienen.

De bijzondere bevoegdheden zoals aanwezig in de Wiv 2017 en voorgesteld in het strafrecht passen niet goed in het bestuursrecht; rechterlijke controle voorafgaand aan de inzet van opsporingsbevoegdheden kent het

50. Zie bijv. ook *Kamerstukken II 1996/97*, 25403, 3, p. 110 en 115 (memorie van toelichting Wet bijzondere opsporingsbevoegdheden) en *Kamerstukken II 2016/17*, 34588, 3, p. 193 (memorie van toelichting Wiv 2017).

51. Zie art. 2.8.2.4.1 uit het conceptwetsvoorstel tot wijziging van boek 2 van het nieuwe Wetboek van Strafvordering ('het opsporingsonderzoek') en art. 38 Wiv 2017. Zie over het gebruik van sociale media bij de strafrechtelijke opsporing ook E.M. Moerman, 'Burgers in het digitale

opsporingstijdperk', *NJB* 2019/94, afl. 2 in het bijzonder p. 113-115.

52. Zie Commissie-Koops 2018, p. 38.

53. Zie art. 2.8.2.4.1 uit het conceptwetsvoorstel. Zie ook art. 38 jo art. 29 Wiv 2017.

54. Zie ook W. Stol & L. Strikwerda, 'Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving', *Tijdschrift voor Handhaving* 2018, nr. 1-2, p. 17; M. Feenstra, 'Opsporingsmiddelen in ontwikkeling. Open-bronnenonderzoek als de nieuwe

"tap", *PROCES*, afl. 97, nr. 6, p. 374; en J.J. Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', Platform Modernisering Strafvordering 2018.

55. Zie nader T. Barkhuysen e.a., *Adequate rechtsbescherming bij grondrechtenbeperking overheidsingrijpen*, Deventer: Kluwer 2014, met name par. 4.2.9 en p. 182.

56. Zie Commissie-Koops 2018, p. 152.

57. Zie Commissie-Koops 2018, p. 154.

58. Commissie-Koops 2018, p. 152.

59. Vgl. Rb. Amsterdam 27 juni 2018,

ECLI:NL:RBAMS:2018:4442, r.o. 21.

60. Zie o.a. CRvB 15 maart 2016, ECLI:NL:CRVB:2016:947, AB 2016/329, m.nt. T. Barkhuysen en M.L. van Emmerik en CRvB 13 september 2016,

ECLI:NL:CRVB:2016:3479, *USZ* 2016/377, m.nt. M.W. Venderbos en M. Venderbos, 'Normering van bestuurlijk toezichts- en controleonderzoek en recente jurisprudentiële ontwikkelingen', *JBplus* 2019/1.

61. En op grond van art. 6 lid 1 onder e AVG.

Onze aanbeveling is in beleid en rechtspraak (en mogelijk in een bijzondere wet, zoals de Participatiewet) een nadere invulling te geven voor stelselmatig openbronnenonderzoek binnen het bestuursrecht

stelsel niet. Dat laat onverlet dat bepaalde waarborgen wel een bestuursrechtelijke invulling moeten krijgen, in wet, rechtspraak en beleid. Openbronnenonderzoek brengt enkele verantwoordelijkheden voor bestuursorganen met zich. In de kern is dat volgens ons zoveel mogelijk transparantie over de wijze waarop en de voorwaarden waaronder openbronnenonderzoek wordt toegepast, zodat de proportionaliteit van het uitgevoerde onderzoek en de mogelijke stelselmatigheid kan worden beoordeeld.

Onze aanbeveling is aldus in beleid en rechtspraak (en mogelijk in een bijzondere wet, zoals de Participatiewet) een nadere invulling te geven voor stelselmatig openbronnenonderzoek binnen het bestuursrecht. Dat moet duidelijk maken voor welke doelen en onder welke voorwaarden openbronnenonderzoek door bestuursorganen plaatsvindt. Het vergroot de voorzienbaarheid van de toepassing van het instrument voor de burger en dwingt bepaalde waarborgen af. Daarbij valt te denken aan een nadere invulling van de proportionaliteitstoets in de toezichtfase (artikel 5:13 Awb), het stellen van eisen aan de verslaglegging, het stellen van grenzen aan de duur van het onderzoek, het bepalen van een bewaartermijn van gegevens en de wijze waarop wordt omgegaan met de informatieplicht uit de AVG. Het protocol internetrecheren voor gemeenten biedt een eerste invulling van deze waarborgen.

Met het voorbeeld uit de inleiding van *scraping* op de website van Airbnb in ons achterhoofd, is de Rechtbank Amsterdam ons inziens te weinig gemotiveerd

akkoord gegaan met de inzet van scrapers ter handhaving van het woonbeleid van de gemeente Amsterdam. Nu hechtte zij vooral belang aan de open bron van de informatie en aan het feit dat de 'listing ID' niet direct tot betrokkene herleidbaar is.⁶² Dat vormt echter maar een van de relevante factoren van de Commissie-Koops (met name factor 2). Hoewel artikel 3:2 Awb een wettelijke grondslag kan bieden voor openbronnenonderzoek, had de rechtbank meer inzichtelijk moeten maken hoe groot de privacy-inbreuk is en hoe verstrekkend de omvang van persoonsgegevensverzameling is geweest. Met een *scraper* wordt immers een zeer grote hoeveelheid gegevens verwerkt en het hangt zeer van de instellingen van de software af hoeveel wordt geogst (de factoren 1 en 3 van de Commissie-Koops). Dat had de rechtbank in ogenschouw moeten nemen.

Eén ding is in ieder geval zeker: openbronnenonderzoek op internet is '*here to stay*'. In de huidige datasamenleving vormt het een eenvoudig toe te passen onderzoeksbevoegdheid die met een zorgvuldige inzet ervoor zorgt dat handhavingscapaciteit meer efficiënt wordt ingezet. Uiteraard moeten de kwaliteit en betrouwbaarheid van de vergaarde gegevens kritisch worden bezien; in de praktijk zal het openbronnenonderzoek vaak de eerste zet zijn om aanwijzingen voor fraude op het spoor te komen. •

⁶². Zie r.o. 21 van Rb. Amsterdam 27 juni 2018, ECLI:NL:RBAMS:2018:4442.