Trending Topics

De rechtmatigheid van datamining door de politie

Mr. dr. E. Gritter*

In de literatuur – ten dele terug te vinden in de archieven van dit tijdschrift – is diverse malen aandacht gevraagd voor de grondslag van *datamining* door de politie.[1] Deze onderzoeksactiviteit lijkt met name op bezwaren te stuiten als die wordt uitgevoerd als vorm van geautomatiseerde surveillance of 'monitoring'.[2] In die situatie kan bijvoorbeeld door middel van *webcrawlers* een zoekslag worden gemaakt in openbare bronnen op het internet ten behoeve van het verbeteren van de informatiepositie van de politie. De binnengehaalde data kunnen vervolgens verder worden geanalyseerd, met als mogelijk gevolg dat tussen de 'geminede' gegevens informatie te vinden is die als voldoende startinformatie kan dienen voor vervolgonderzoek, waarbij mogelijk dwangmiddelen kunnen worden ingezet. Op deze wijze kunnen bijvoorbeeld op automatische wijze twitterberichten worden 'gemonitord', om uiteindelijk zicht te krijgen op mogelijke 'dreigtweets'.[3]

Als grondslag voor big data datamining als surveillancemethode wordt veelal artikel 3 Politiewet 2012 aangewezen. Maar of dit een *rechtmatige* grondslag is, wordt sterk betwijfeld.[4] Door middel van *webcrawlers* kunnen namelijk grote hoeveelheden gegevens worden binnengehaald, waartussen zich ook gegevens van onschuldige burgers kunnen bevinden. Deze aspecten zouden dan maken dat deze vorm van onderzoek een meer dan beperkte inbreuk op de privacy van betrokkenen oplevert.[5] Artikel 3 Politiewet 2012 kan echter alleen als rechtmatige grondslag voor politiehandelen dienen als de activiteit een *niet* meer dan beperkte inbreuk op de privacy maakt.[6]

Voor wat betreft de grondslag meen ik, dat het bij het op automatische wijze vergaren van gegevens uit openbare bronnen op het internet wezenlijk gaat om een zeker type *opsporingsonderzoek*, zodat eerder artikel 141 Sv in beeld komt. Het automatisch scannen van social media met het oog op de vraag of tussen de geplaatste berichten *mogelijk* een bedreiging zit, heeft in ieder geval veel trekken van een zogenaamde 'repressieve controle', een type onderzoek (vergelijkbaar met een alcoholverkeerscontrole) dat in ieder geval volgens Keulen/Knigge als vorm van opsporing moet worden gezien, alhoewel op het moment van het uitvoeren van de opsporingsmethode er nog geen concrete verdenking bestaat (laat staan 'aanwijzingen') dát er een bedreiging is geuit.[7] Wezen-

* Mr. dr. E. (Erik) Gritter is als universitair docent straf(proces)recht verbonden aan de Rijkuniversiteit Groningen, en tevens redacteur van dit tijdschrift.

1. Zie bijvoorbeeld B.W. Schermer, 'Het gebruik van *Big Data* voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *TBS&H* 3(4) 2017, p. 207 e.v.; S. Brinkhoff, 'Datamining in een veranderende wereld van opsporing en vervolging', *TBS&H* 3(4) 2017, p. 224 e.v.; S. Brinkhoff, 'Big Data datamining door de politie. IJkpunten voor een toekomstige opsporingsmethode', *NJB* 2016, afl. 20, p. 1400 e.v.; J.J. Oerlemans en B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *JV* 38(5), p. 35 e.v. (m.n. p. 40 e.v.) en Bert-Jaap Koops e.a., *Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools*, Tilburg: TILT 2012, m.n. p. 37 e.v.
2. Brinkhoff 2016, p. 1402 e.v.
3. Zie hieromtrent het nieuwsbericht 'Politie onderzoekt 200 ernstige twitterbedreigingen per dag' (maart 2013, https://tweakers.net/nieuws/92299/politie-onderzoekt-200-ernstige-twitter-bedreigingen-per-dag.html, voor het laatst geraadpleegd op 26 april 2018), alsmede het item 'Social media surveillance in Nederland' (oktober 2017, https://www.burojansen.nl/observant/social-media-surveillance-in-nederland/, eveneens voor het laatst geraadpleegd op 26 april 2018).
4. Brinkhoff 2016, p. 1405; Oerlemans en Koops 2012, p. 41 (m.b.t. de voorganger van art. 3 Politiewet 2012, art. 2 van de Politiewet 1993).
5. Brinkhoff 2016, p. 1402 en Koops 2012, p. 37.
6. Zie bijvoorbeeld Brinkhoff 2017, p. 226. De oorsprong van deze zienswijze ligt in het Zwolsmanarrest, HR 19 december 1995, *NJ* 1996/249.
7. B.F. Keulen en G. Knigge, *Strafprocesrecht*, Ons Strafrecht deel 2, dertiende druk, Deventer: Wolters Kluwer 2016, p. 276 en 277.

doi: 10.5553/TBSenH/229567002018004002009

lijk is er in dergelijke gevallen sprake van een dubbele grondslag, nu de uitvoering van de politietaak in de zin van artikel 3 Politiewet 2012 mede de strafrechtelijke handhaving van de rechtsorde omvat (zie art. 12 van de Politiewet 2012). Ook ten aanzien van opsporingshandelingen op grond van artikel 141 Sv geldt dat dit alleen mogelijk is, mits en voor zover niet een meer dan beperkte inbreuk op de privacy wordt gemaakt. Opmerking verdient dat de politie zowel bij het handelen op grond van artikel 141 Sv als bij het optreden op grond van artikel 3 Politiewet 2012 in het kader van de strafrechtelijke handhaving van de rechtsorde onder gezag van de officier van justitie handelt.[8]

Bieden de artikelen 3 Politiewet 2012 en/of 141 Sv voldoende grondslag voor het geautomatiseerd vergaren van gegevens uit openbare bronnen op het internet? Betekent het binnenhalen van *veel gegevens* over mogelijk ook *onschuldige* burgers een meer dan beperkte inbreuk op de privacy, zodat er een specifieke wettelijke grondslag dient te bestaan voor deze methode van repressieve controle? Wat mij betreft niet, mits de methode van gegevensverzameling maar niet neerkomt op stelselmatige observatie van een specifieke persoon.[9] Het door de politie ongericht binnenhalen van grote hoeveelheden data in het kader van repressieve controle raakt ontegenzeggelijk indringende aspecten van de privacy, maar dat betekent niet per se dat buiten de begrenzing van artikel 3 Politiewet 2012 en/of artikel 141 Sv wordt gehandeld. Daarbij is het van belang een onderscheid te maken tussen twee kanten van datamining: enerzijds het *vergaren* van gegevens, en anderzijds het *verwerken* daarvan in de zin van analyseren en bewaren.

Met Mac Gillavry kan worden gesteld dat een niet-verdachte het recht om niet betrokken te worden in een strafvorderlijk onderzoek moet worden ontzegd.[10] Hij schrijft: 'Het is vrijwel onvermijdelijk dat opsporingsonderzoek tevens inbreuk maakt op de privacy van burgers waarvan, mogelijk achteraf, blijkt dat zij zich niet schuldig hebben gemaakt aan het plegen van strafbare feiten. Bij bepaalde onderzoeksmethoden zoals datamining of verkennend onderzoek staat zelfs op voorhand vast dat opsporingsambtenaren gegevens verzamelen en verwerken van (grote groepen van) personen die geen andere relatie hebben met het onderzochte strafbare feit dan dat zij passen in het daderprofiel.'[11] De achtergrond schuilt in het uitgangspunt dat het verzamelen, opslaan en gebruiken van gegevens de kernactiviteit is van opsporing. 'Opsporingsonderzoek staat of valt met de verzameling van informatie,' zo schrijft Mac Gillavry.[12] Hij vervolgt: 'Doel van het opsporingsonderzoek is te komen tot op personen herleidbare informatie.'[13] Keulen/Knigge stellen in dezelfde lijn dat opsporing 'welhaast per definitie een stelselmatig en gericht onderzoek met zich brengt naar de handel en wandel van personen die mogelijk bij het delict betrokken zijn.'[14]

Deze uitgangspositie kleurt het antwoord op de vraag welk politiehandelen een specifieke wettelijke grondslag eist. Keulen/Knigge stellen dat er geen specifieke wettelijke voorziening vereist is voor de politiële 'informatie-inwinning' als zodanig.[15] Geredeneerd vanuit het doel van de opsporing – de waarheidsvinding – is het verzamelen van gegevens onlosmakelijk verbonden aan 'de opsporing', en daarmee dus inherent aan de uitoefening van de opsporingstaak. '[D]e opsporing als vorm van informatiewinning zelf'[16] – het verzamelen en opslaan van persoonsgegevens – kent voor wat betreft de opsporing vervolgens een toereikende grondslag in de artikelen 141 en 142 Sv, die in algemene zin aangeven wie met de opsporing zijn belast. Om de opsporing naar behoren te kunnen uitvoeren, mag de politie op grond van deze bepaling gegevens verzamelen met het oog op verdere verwerking. Dit verklaart bijvoorbeeld dat het horen van getuigen door de politie – dat gepaard kan gaan met het verzamelen van privacygevoelige gegevens – momenteel geen afzonderlijke, uitgewerkte regeling kent in het Wetboek van Strafvordering.[17] Een specifieke wettelijke grondslag komt pas in beeld, als de informatieverzameling gepaard gaat met *directe inbreuken* op *klassieke kernwaarden* van de privacy, zoals het huisrecht en de lichamelijke integriteit.[18] Bij het ongericht binnenhalen van veel gegevens uit openbare bronnen op het internet lijkt daarvan geen sprake te zijn, wederom voor zover niet gesproken kan worden van stelselmatige observatie.

Dat bij politieonderzoek gegevens van niet-verdachten in het vizier kunnen komen, wordt uitdrukkelijk erkend in de toelichting op de Wet politiegegevens. Daaruit volgt, in relatie tot de voorganger van artikel 3 Politiewet 2012 (art. 2 Politiewet 1993):

> 'Bij de uitvoering van de dagelijkse politietaak komt de politie in contact met veel burgers ter zake van zeer diverse gebeurtenissen. Het gaat bijvoorbeeld om burgers die zich om hulp tot de politie wenden,

8. Politiehandelen op grond van art. 3 Politiewet 2012 en/of art. 141 Sv kent een tweede begrenzing: de ingezette methode mag niet zeer risicovol zijn voor de beheersbaarheid en integriteit van 'de opsporing'. Dit aspect lijkt veelal gedekt geacht, als in een concrete zaak blijkt van *toestemming* van de officier van justitie. Mogelijk kan uit de tweede begrenzing zelfs een 'positief aspect' worden afgeleid, *ter legitimatie* van de inzet van automatische zoekslagen: teneinde de opsporing van kinderpornografie beheersbaar te houden, mogen webcrawlers worden ingezet die aan de hand van hash-lijsten van bij justitie bekend materiaal een eerste selectie maken. Een directe confrontatie van politieambtenaren met schokkend materiaal kan daarmee deels voorkomen worden. Zie hieromtrent Edward Siddons, 'Meet Arachnid, the crawler hunting child abuse photos across the web. Automation is revolutionising the fight against child abuse online', (december 2017, https://apolitical.co/solution_article/meet-arachnid-crawler-hunting-child-abuse-photos-across-web/, voor het laatst geraadpleegd op 26 april 2018).
9. Dat is op grond van art. 126g Sv alleen mogelijk, als in het onderzoek een redelijk vermoeden van een misdrijf is ontstaan.
10. E.C. Mac Gillavry, *Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven* (diss. Groningen), z.p.: WLP 2004, p. 509.
11. Mac Gillavry 2004, p. 509.
12. Mac Gillavry 2004, p. 472.
13. Mac Gillavry 2004, p. 472.
14. Keulen/Knigge 2016, p. 291.
15. Keulen/Knigge 2016, p. 291.
16. Keulen/Knigge 2016, p. 291.
17. Mac Gillavry 2004, p. 474.
18. Keulen/Knigge 2016, p. 291; Mac Gillavry 2004, p. 472.

doi: 10.5553/TBSenH/229567002018004002009

> betrokken zijn bij verstoringen van de openbare orde, meldingen van overlast doen, aangifte doen of slachtoffer, getuige of verdachte zijn van een strafbaar feit. Van de politie wordt verwacht dat zij ogen en oren goed de kost geeft en dat zij de gegevens die ze daarbij verzamelt, verwerkt en waar nodig met elkaar in verband brengt. Het zal hierbij vaak gaan om gegevens over personen jegens wie (nog) geen verdenking bestaat en om gegevens die niet zijn voortgekomen uit diepgaand onderzoek. Gelegde verbanden en opvallende feiten die uit die gegevens naar voren komen, kunnen eventueel aanleiding geven tot verdieping en gerichte verwerking voor een bepaald doel. Op die manier vormt de uitvoering van de dagelijkse politietaak de uiterst belangrijke basis voor de algehele uitvoering van de politietaak op grond van artikel 2 Politiewet 1993.'[19]

Als enkel de informationele privacy in het geding is, volstaan voor wat betreft de grondslag van het handelen algemene bepalingen zoals artikel 3 Politiewet 2012 of de artikelen 141 en 142 Sv, omdat het inbreuk maken op dát aspect van de privacy nu eenmaal 'ingebakken' zit in de toekenning van de politie- of opsporingstaak, samenhangend met het belang van het kunnen opbouwen van een goede informatiepositie. Volgens Keulen/Knigge is dit een bewuste keuze geweest van de wetgever. De auteurs schrijven: 'Met de grondwettelijke eis van een specifieke voorziening is dat niet in strijd. De inbreuk op de informationele privacy die in de opsporing is ingebakken, berust (…) onmiskenbaar op een belangenafweging die de wetgever geacht kan worden voor zijn rekening te hebben genomen.'[20] Opmerking verdient daarbij dat het vergaren van gegevens op grond van artikel 3 Politiewet 2012 of de artikelen 141 en 142 Sv niet zonder normering in. Zoals ieder ander politiehandelen wordt dat verzamelen beheerst door de beginselen van een behoorlijke procesorde. Daarbij kan in het bijzonder worden gewezen op de beginselen van proportionaliteit en subsidiariteit.[21]

Op basis van het voorgaande kan worden gesteld dat het op automatische wijze ongericht vergaren van gegevens, bijvoorbeeld in het kader van het monitoren van social media op eventuele bedreigingen, een afdoende grondslag kent in artikel 3 Politiewet 2012 en/of artikel 141 Sv. De werkelijke *privacy concerns* dienen zich aan op een ander vlak, namelijk op het terrein van de *gegevensbescherming*. De bescherming van dit informationele privacy-aspect kent een uitgebreide regeling in de Wet politiegegevens. Deze wet verschaft onder meer regels omtrent opslag, bewaartermijnen, verstrekking aan derden en inzage van betrokkenen. De leden 1 en 2 van artikel 3 van de Wet politiegegevens kunnen worden gezien als scharnier tussen vergaring (op grond van art. 3 Politiewet 2012 en/of art. 141 Sv) en verdere verwerking (binnen de kaders van de Wet politiegegevens). Artikel 3 lid 1 van de Wet politiegegevens stelt: 'Politiegegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens deze wet geformuleerde doeleinden.' Het tweede lid voegt daaraan toe: 'Politiegegevens worden slechts verwerkt voor zover zij rechtmatig zijn verkregen en, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn.' Voor wat betreft de doelbinding wijst de wet onder meer op de uitvoering van de dagelijkse politietaak (art. 8), onderzoek met het oog op de handhaving van de openbare orde in een bepaald geval (art. 9) en controle op en beheer van informanten (art. 12).

De kern van eventuele privacyproblemen rondom datamining door de politie schuilt dus niet zozeer in het *vergaren* van de gegevens, maar in het verder verwerken en bewaren daarvan. Het is dus niet zozeer Orwell die we erop moeten naslaan, maar Kafka.[22] Of datamining door de politie afdoende privacybescherming biedt, vergt dus vooral een kritische analyse van de Wet politiegegevens.[23] Maar dat het ongericht automatisch vergaren van gegevens (niet neerkomend op een stelselmatige observatie) op grond van artikel 3 Politiewet 2012 en/of artikel 141 Sv rechtmatig is, staat wat mij betreft buiten kijf.

19. *Kamerstukken II*, 2005/06, 30327, 3, par. 6.2.
20. Keulen/Knigge 2016, p. 291, voetnoot 51.
21. Mac Gillavry 2004, p. 475.
22. Ontleend aan Daniel J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', *Stanford Law Review* 2001 vol. 53, p. 1393 e.v. Op p. 1429 en 1430 komt de auteur met een illustratie van de metaforen: 'Viewing the database problem in terms of the Kafka metaphor as opposed to the Big Brother metaphor has important ramifications for the way we apply legal concepts and craft policies. For example, Amazon.com—one of the largest retailers of books on the Internet—collects information about a customer's taste in books (based on its sales to the user) and then provides book recommendations tailored to the customer. If the problem is surveillance, then the most obvious solution would be to provide strict limits on Amazon.com's collection of information. This solution, however, would curtail much information collection that is necessary for business in today's society and that is put to beneficial uses. Indeed, many Amazon.com customers, myself included, find Amazon.com's book recommendation service to be very helpful. In contrast, if the problem is understood as I have depicted it, then the problem is not that Amazon is spying on its users or that it can use personal data to induce its customers to buy more books. What is troubling is the unfettered ability of Amazon.com to do whatever it wants with this information.'
23. Die analyse vergt ook onderzoek naar de praktische omgang door de politie met de Wet politiegegevens. Dat het belang van gegevensbescherming nog de nodige internalisatie behoeft bij de politie, blijkt bijvoorbeeld uit het bericht 'Nieuws: de politie blijkt op grote schaal de wet te overtreden' (december 2015, https://decorrespondent.nl/3734/nieuws-de-politie-blijkt-op-grote-schaal-de-wet-te-overtreden/510916939412-7be7c192, voor het laatst geraadpleegd op 26 april 2018): 'In werkelijkheid interesseert het de meeste politiemensen nauwelijks. Privacy is iets voor speciale privacyfunctionarissen, niet voor gewone agenten en rechercheurs. De privacy-audit bevestigt dat gebrek aan belangstelling in de conclusies: "De grootste oorzaak hiervan lijkt te zijn dat de Wpg binnen de politie wordt gezien als een 'losstaand project'".'

doi: 10.5553/TBSenH/229567002018004002009