Dagelijkse en structurele monitoring

Social Media Surveillance door de Nederlandse politie

Over grootschalige surveillance door inlichtingendiensten op internet ontstond in 2013 veel discussie door de onthullingen van Edward Snowden. Bij die onthullingen ging het in eerste instantie om de activiteiten van de Amerikaanse inlichtingendienst NSA, National Security Agency. De NSA verzamelt zoveel mogelijk informatie van bronnen op het internet met het doel om mogelijke terroristen op te sporen.

Dat inlichtingendiensten over iedereen informatie verzamelen met het idee daar verdachten van staatsgevaarlijke activiteiten uit te distilleren is op zich niet nieuw. Tijdens de Koude Oorlog werden veel mensen met vermeende linkse sympathieën in de gaten gehouden. Zij zouden misschien wel communist zijn of voor de Sovjet-Unie werken. In Nederland werden om die reden niet alleen mensen van de Communistische Partij Nederland, maar tal van maatschappelijke organisaties zoals de Nederlandse Vrouwen Bond, in de gaten gehouden.

Massale surveillance door inlichtingendiensten zorgt voor ophef in de Verenigde Staten en grote delen van de wereld, maar wordt tegelijkertijd als een noodzakelijk kwaad gezien in de strijd tegen terrorisme. Het gaat dan meer om surveillance door inlichtingendiensten, die iedereen in de gaten houden, dan om afluisteren door opsporingsdiensten. In Nederland werd dit jaar een wijziging van de Wet op de inlichtingen- en veiligheidsdiensten, die de AIVD en MIVD grotere bevoegdheden geeft, soepel door de Kamer geloodst. Bij deze wijziging is er sprake van sleepnetwetgeving, vergelijkbaar met de uitgebreide bevoegdheden van de NSA.

Grootschalige surveillance door de politie roept meer weerstand op. Dit zou betekenen dat de overheid constant meekijkt, een politiestaat, waarbij burgers bang zijn zich openlijk te uiten. Vaak

wordt dan verwezen naar de praktijken van de Stasi in het voormalige Oost-Duitsland. Bijna dertig jaar na de val van de Muur in 1989, de digitale revolutie en verschillende aanslagen in de Westerse wereld, rukt echter de wens van overheden op om massaal hun burgers te bespioneren. Hiervoor worden niet alleen inlichtingendiensten ingezet, ook de politie begeeft zich op het terrein van online en social media surveillance.

Reputatiemanagement is eigenlijk risicomanagement

Voor die surveillance huurt de politie bedrijven in die zich bezig houden met social media monitoring en daarvoor online en bij de social media persoonsgegevens verzamelen. Deze bedrijven, Coosto en OBI4wan verzamelen al jaren dit soort gegevens en slaan die op. Buzzcapture wordt ingehuurd voor communicatiedoeleinden door de Nationale Politie. Er is echter geen bewijs dat Buzzcapture voor social media surveillance wordt ingezet. De reputatiemanagement bedrijven spreken in 2014 van 400.000 bronnen (Coosto) en 400.000 Nederlandstalige bronnen (OBI4wan). Onder bronnen verstaan de bedrijven social media platforms als Facebook en Twitter, websites zoals nu.nl en tweakers.net, maar ook Wordpress sites en internetfora.

De bedrijven presenteren zich als reputatiemanagement bedrijven. De informatie is primair bedoeld om de communicatie tussen producent en consument of overheid en burger te verbeteren. De social media monitoring bedrijven verzamelen data, indexeren die, maken die doorzoekbaar en voorzien ze van een sentiment analyse, een functionaliteit die bepaald of een bericht positief, negatief of neutraal is. De bedrijven beheren grote historische archieven die teruggaan tot 2009 (Coosto en Obi4wan) en 2007 (Buzzcapture). Vervolgens verkopen zij die data door, zodat merken als Shell of Unilever de risico´s die ze lopen bij een online mediastorm kunnen beperken. Reputatiemanagement is in feite risicomanagement. Niet alleen bedrijven gebruiken de monitoring tools, ook maatschappelijke organisaties en overheidsdiensten, waaronder de politie. De politie gebruikt de tools niet alleen voor communicatie, maar ook voor social media surveillance en opsporing. Buro Jansen

& Janssen heeft verschillend Wob-verzoeken ingediend om social media surveillance door de politie in beeld te brengen.

Real Time Crime Center RTCC

Het toenemende gebruik van social media surveillance door de politie hangt samen met de ontwikkeling van Real Time Intelligence Centers (RTIC). De RTIC is een uitgebreide meldkamer, een inlichtingenmeldkamer, maar geen vervanging van de klassieke meldkamer. In de Verenigde Staten zijn deze aan het begin van deze eeuw opgezet als crime centers om moord en doodslag aan te pakken, maar uiteindelijk doorontwikkeld als surveillance centra. In Nederland zijn de RTIC'S vanaf 2010 ontwikkeld. In zulke Intelligence Centers komen *harde* en *zachte* data, waaronder online en social media gegevens samen. Met behulp van een sentiment analyse worden die data geanalyseerd en kunnen daarmee het politiewerk sturen.

De RTIC is gemodelleerd naar de Amerikaanse RTCC, Real Time Crime Center. De eerste RTCC's werden rond 2005 opgezet. Bij deze centra ging het vooral om het samenbrengen van lokale en federale politie-informatie, zoals posities van politieagenten en auto´s, gegevens uit politieregisters over overtredingen, strafbare feiten en gevangenisstraffen; en publieke informatie als gegevens van het bevolkingsregister, kadaster, kamer van koophandel en andere overheidsdatabestanden; maar ook om cameratoezicht, kaarten en beelden van helikopters. Online media of social media gegevens speelden nog geen rol van betekenis in de beginfase van de RTCC's.

Bij de inlichtingenmeldkamers in de VS werd al snel duidelijk dat er sprake was van een verschuiving in de doelstellingen. Bij de start van de New Yorkse RTCC zou het centrum alleen moord, doodslag en schietincidenten behandelen. De risico´s van massale surveillance op basis van zowel politieregisters als openbare data werden door de politie onderkend. Van die aanvankelijke beperkte doelstelling is echter weinig over. De RTCC's zijn ingezet om demonstranten te bespioneren, zoals die van de Black Lives Matter beweging. Onderzoek van de American Civil Liberties Union (ACLU) in 2016 toonde aan dat de politie Facebook, Instagram, Twitter,

YouTube en andere sociale media rond de klok monitorde en leden van actiegroepen in de gaten hield.

De kop boven het artikel in De Leeuwarder Courant uit december 2012 over de opening van het RTIC (Real Time Intelligence Center) in Drachten is dan ook niet misplaatst. *Politiespionnen zoeken verdachten op internet* klinkt als een inlichtingendienst die mensen in de gaten houdt. De techniek heeft die surveillance mede mogelijk gemaakt. Mensen delen hun persoonlijk leven op internet. Soms met gebruikmaking van de privacy settings die berichten afschermen van het brede publiek, maar meestal niet. Berichten, foto´s, meningen en fantasieën worden gedeeld met iedereen. Daarnaast hebben de lage kosten van opslag van data en het voor handen zijn van allerlei simpele programma's die het verzamelen van data op het internet vergemakkelijken, bijgedragen aan de ontwikkeling.

Real Time Intelligence Center, RTIC in Nederland

De Nederlandse RTIC´s gingen in 2012 van start. Doel van de RTIC's is om de politie beter voorbereid op een melding te laten reageren. Bij de RTIC´s komen naast de gebruikelijke politieregisters en NAW (naam, adres en woonplaats) gegevens ook cameratoezicht en informatie vanuit internet en social media binnen. Daarnaast wordt ook informatie van burger apps zoals Burgernet, informatie van beveiligingsbedrijven en van sensoren voor bewegings- en geluidsdetectie aan de inlichtingen van de RTIC´s toegevoegd.

Inge Hoogstad van de politie-eenheid Rotterdam geeft in een presentatie uit februari 2016 over de Dienst Regionaal Operationeel Centrum (DROC) aan, wat voor informatie er bij het RTIC samenkomt. Bij de DROC zijn de meldkamer Rotterdam en de RTIC van de politie-eenheid Rotterdam samengebracht. Volgens de presentatie gaat het om gegevens uit Blueview (processen verbaal, verhoren, aangiftes, gegevens van verdachten en bijvoorbeeld openstaande boetes), Verona (wapenvergunningen), SKDB (strafrechtsketendatabank) en de Kamer van Koophandel. Deze

gegevens behoren tot de *hardere* informatie die de politie raadpleegt zowel bij meldingen als onderzoek.

Zachte informatie

Naast deze gegevens worden in de presentatie ook social media platforms zoals Google, Facebook en Twitter genoemd. Deze *zachte* informatie staat in de presentatie van Hoogstad in dezelfde lijst als de informatie uit politieregisters. De *harde* politie en overheidsdata komen samen met de *zachte* data die afkomstig is uit online en social media. Informatie die mensen zelf, al dan niet publiekelijk, delen op social media is ook *zachte* informatie die de inlichtingeneenheden van de Nederlandse politie, Teams Criminele Inlichtingen (TCI), de voormalig Criminele Inlichtingen Eenheden (CIE´s) en de Regionale Inlichtingen Diensten (RID), verzamelen. Het TCI richt zich voornamelijk op criminaliteit, de RID op de handhaving van de openbare orde en het in de gaten houden van politieke (buitenparlementaire) activiteiten.

Het TCI en de RID gebruiken voor hun informatie inwinning traditionele media, het internet en social media, maar ook gesprekken met verdachten die vastzitten om hen onder druk informatie te ontfutselen, en de inzet van informanten en infiltranten. Dit kan een bezoek zijn van een agent aan een café, een flat of moskee, maar ook het inzetten van infiltranten of informanten bij acties, demonstraties of vermeende criminele activiteiten. Het gaat onder meer om inlichtingen over mogelijke criminele activiteiten, relaties tussen verdachten, politieke activiteiten, actiegroepen en acties van voetbalsupporters. Informatie van het TCI en de RID wordt *zachte* informatie genoemd, omdat het vaak om informatie gaat die is gebaseerd op geruchten of roddels. Informanten kunnen bijvoorbeeld niet zomaar vertrouwd worden, maar kunnen ook door een criminele organisatie zijn ingehuurd om onjuiste informatie te verspreiden of concurrenten een hak te zetten. Ook anonieme tips zijn in principe zachte informatie.

Zachte informatie kan aanleiding zijn om nadere inlichtingen in te winnen, een huis binnen te treden en te doorzoeken, extra politie in te zetten bij een demonstratie of een manifestatie te verbieden.

Slechts een enkele keer rukt de politie naar aanleiding van zachte informatie groot uit. Dit heeft onder meer te maken met de omstandigheden, de betrouwbaarheid van de tip of de informant, en informatie uit de *harde* gegevens waar de politie over beschikt. Bij terrorismedreiging gebeurt het soms, zoals bij de melding over IKEA in maart 2009 (zie *Meer dan 200.000 professionals doen maar wat tegen terrorisme*, Buro Jansen & Janssen).

De RTIC's van de Nationale Politie maken geen gebruik van dezelfde zachte informatie als het TCI en de RID, zoals uit de presentatie van Inge Hoogstad van de politie eenheid Rotterdam blijkt. Dit kan informanten in gevaar brengen en bronnen van de diensten onthullen. De zachte informatie van de RTIC bestaat uit openbare bronnen van traditionele media, zowel fysiek als digitaal, en andere nieuwsorganen, fora, blogs en social media.

PID Social Media in operationele politieprocessen

De RTIC´s ontwikkelden zich in de periode dat de politieregio´s opgingen in de Nationale Politie. Allerlei regionale politiesystemen moesten bij de vorming van de Nationale Politie opgaan in een landelijk systeem. Het systeem Blueview bijvoorbeeld, een soort zoekmachine die in 2007 werd ingevoerd, maakt het mogelijk dat medewerkers van verschillende politieregio's in elkaars systemen kunnen kijken. De overgang naar de Nationale Politie ging gepaard met het opzetten van meldkamers en RTIC´s per eenheid, die echter wel een nationale verbinding hebben.

De Nationale Politie is op 1 januari 2013 gestart, maar veel ontwikkelingen waren daarvoor al in de afzonderlijke politieregio´s ingezet, zo ook het denken over RTIC´s en de inzet van risico- of reputatiemanagement tools. In 2013 werd een voorstel gedaan om te onderzoeken wat de mogelijkheden waren voor het gebruik van social media door de politie. Als startpunt gebruikt de Nationale Politie het document *Project Initiatie Document (PID) Social Media in operationele politie processen*. Volgens het PID document is één van de doelen voor fase 0 van het project Social Media in operationele Politie Processen (SMPP) "een ruwe inventarisatie van wat er in de eenheden reeds is gerealiseerd: de nulmeting (peildatum 1 maart

2013).” Voor deze ruwe inventarisatie is gebruik gemaakt van “de bevindingen uit praktijkervaringen m.b.t. social media in elke politie eenheid (2009-2013)”.

In het PID wordt opgesomd wanneer de politie social media bruikbaar acht. Het document noemt “actieve wederkerigheid (tweerichtingsverkeer), crisis watch, webcare, crowdcontrol, event watch, realtime intelligence tool, operationele opsporingstool en kennisdeler”. De terreinen waarbij de politie social media wil inzetten, lopen sterk uiteen. Het gaat om communicatie met burgers over aangiften, meldingen, maar ook om de eigen communicatie van de politie over haar werk. Daarnaast noemt het document de inzet van social media door de politie bij evenementen en crowd control. Dan is er de inzet als inlichtingenbron bij dezelfde meldingen en communicatie met politieagenten in de wijk of op locatie. Daarnaast formuleert het document als ambitie dat “de eenheden dagelijks online een structurele monitor draaien” en als laatste zou social media ook voor de opsporing een belangrijk middel kunnen zijn. De Nationale Politie wil hier kennelijk weinig ruchtbaarheid aan geven. De passages over opsporing zijn in de, naar aanleiding van de Wob-verzoeken van Buro Jansen & Janssen, openbaar gemaakte documenten namelijk zwart gemaakt.

Van communicatie naar permanente surveillance

De Nationale Politie huurt dus reputatiemanagement bedrijven als Coosto, Obi4wan/HowAboutYou en Buzzcapture in. De politie gebruikt de diensten van de bedrijven niet alleen voor haar eigen communicatiebeleid (Buzzcapture) en de contacten met burgers, maar ook voor meldingen, aangiften, handhaving, Real Time Intelligence Center en opsporing (Coosto, OBI4wan en HowAboutYou).

De politie verstrekt geen documenten over Coosto. Uit het document *Online media monitoring: tool en proces (2), Ervaringen en inzichten naar aanleiding van operationele ervaring bij de politie-eenheid Zeeland - West-Brabant* blijkt echter dat Coosto op dezelfde wijze wordt ingezet als OBI4wan. Zo staat in het document dat Coosto meer data van Facebook boven tafel krijgt dan OBI4wan. “De

gegenereerde resultaten van OBI4wan zijn niet zo volledig als bij de andere gebruikte online media monitor op het RTIC (Coosto). Vooral bij de bronnen Facebook, YouTube en Instagram zijn de resultaten bij het gebruik van dezelfde zoekopdrachten van Coosto volledigen." De reden voor het verschil wordt niet in het rapport vermeld. Het kan een aanwijzing zijn voor het gebruik van nep- of schaduwaccounts of andere manieren waarop in Facebook vriendengroepen wordt binnengedrongen.
Het PID document stelt in 2013 vast, dat de politie vaak geen strategie heeft op het gebied van social media surveillance. "Tijdens crisissituaties en evenementen hebben eenheden als zodanig geen vastgesteld beleid over de inzet van social media. In een aantal grote steden is dit wel het geval." Aan de andere kant spreekt het document over "een divers beeld" en over social media in "verschillende operationele processen en op verschillende organisatieniveaus".

Eigenlijk zijn de verschillende regiokorpsen al lang voor de aanvang van de Nationale Politie begonnen met online en social media surveillance. Het PID document concludeert: "In de huidige situatie wordt binnen de eenheden verschillend omgegaan met het monitoren van social media. Ook zijn er veel verschillende software tools en diverse soorten ICT-hardware in gebruik (groot/klein, freeware/licentie, etc). Voor de aanschaf van tools is er geen landelijke standaard."

In het PID document passeren mogelijke strategieën de revue: van online opschalen in geval van crisis en evenementen, tot aan twitterende agenten, monitoring en opsporing. In grote lijnen zijn er twee strategieën. De incidentele benadering waarbij social media pas worden geraadpleegd wanneer iemand een feestje op Facebook aankondigt en wanneer er camerabeelden van een mishandeling worden gedeeld, als een vorm van crisisbeheersing of opschaling vanuit de social media surveillance. En de surveillance zelf, waarbij social media data zijn opgenomen in de informatie organisatie van de politie. Van RTIC tot de inlichtingentak van de politie-organisatie met lokale onderdelen (Districtelijk Informatie Knooppunt), regionale RIK (Regionaal Informatie Knooppunt), het landelijke team OSINT (Open Source INTelligence), Opsporing en SGBO, wordt social media gebruikt. "Door de informatieorganisatie in de eenheden wordt er dagelijks online een structurele monitor

gedraaid", is het doel dat het PID document van 2013 voor social media surveillance formuleert.

Open Source Intelligence OSINT

OSINT (Open Source INTelligence) heeft altijd een belangrijke rol gespeeld bij de politie, maar vooral bij de inlichtingendiensten van de politie, het TCI en de RID. Naast de klassieke inlichtingen elementen HUMINT (de menselijke bronnen zoals informanten) en SIGINT (Signal Intelligence, het tappen van communicatie) is OSINT voor de politie de belangrijkste informatiebron. OSINT kan bestaan uit de verhalen die de wijkagent opvangt om zicht te houden op de wijk, of de rechercheur die geruchten hoort tijdens een onderzoek naar een overval. Naast die informatie verzamelen het TCI en de RID andere *zachte* informatie, zoals berichten, verhalen, geruchten en folders.

Met de ontwikkeling van online en social media is OSINT voor de gehele politie van groot belang geworden, Dit wordt onderstreept door de oprichting van het *landelijke Team OSINT* in 2011 dat open bronnen op internet monitort. In navolging zijn de Real Time Intelligence Centers per 1 januari 2014 met social media surveillance begonnen. Vanaf dat moment voeren de RTIC's de klok rond social media surveillance uit met het doel om de social media te monitoren, analyseren en vervolgens te interveniëren.

Twee jaar na het verschijnen van het PID document, in 2015, wordt het belang van OSINT veelvuldig benadrukt in het adviesrapport *IM Adviesrapport Tools Informatieorganisatie Evaluatie en advies*. De politie wil OSINT inzetten voor het "versterken van de (realtime- en righttime) informatiepositie van de politie, verbeteren van de interpretatie (duiding) van informatie, kansen bieden voor verhoging van de heterdaadkracht". De politie voert ondertussen rond de klok online en social media surveillance uit, blijkt uit het rapport.

Het adviesrapport van 2015 spreekt over de *mindset* van politiefunctionarissen, over de inrichting van de Nationale Politie en het opleiden van medewerkers in het gebruik van social media monitoring tools. Er wordt gesproken over de RTIC en de OSINT

taak van de politie en een evaluatie van de tools. "Juridische kaders voor de gebruikers van de tools" moeten nog worden opgesteld, staat in het document. Of alle politie eenheden dezelfde social media monitoring tools gebruiken voor communicatie, RTIC, opsporing, ofwel social media surveillance, zoals de wens was in het PID document van 2013 blijkt niet uit het rapport.

Project X

Het PID document van 2013 is nog enigszins terughoudend als het gaat om real time surveillance, hoewel het de wens uitspreekt om "dagelijks online een structurele monitor te draaien". In het advies rapport in 2015 wordt het belang van OSINT en social media surveillance onderstreept, al wordt de laatste term niet gebruikt. De omslag hangt samen met twee incidenten. De politie verwijst altijd naar *Project X* dat op 21 september 2012 in Haren plaatsvond en een mishandeling in Eindhoven op 4 januari 2013 waarbij de verdachten op social media werden omschreven als de Eindhovense kopschoppers. Bij het *Project X* feest werd een uitnodiging voor een verjaardagsfeest massaal rondgestuurd en kwamen er uiteindelijk heel veel mensen opdraven. Bij de mishandeling in Eindhoven ontstond naar aanleiding van camerabeelden op social media een klopjacht om de verdachten te vinden. Bij *Project X* werden uiteindelijk ook social media ingezet om verdachten van vernielingen en plundering op te sporen.

Het PID document van 2013 refereert aan beide incidenten: "Social media zijn niet meer weg te denken uit onze maatschappij. Mensen gebruiken social media om elkaar te betrekken, te informeren en te beïnvloeden met in hun kielzog de reguliere media. De gevolgen hiervan kunnen groot zijn: voor bestuurders, politie, het Openbaar Ministerie, maar ook voor de burger zelf. Recente voorbeelden zijn de publieke verontwaardiging over de verdachten van uitgaansgeweld in Eindhoven (camerabeelden) en een ogenschijnlijk onschuldige Facebook-uitnodiging die leidde tot grote ongeregeldheden in Haren (*Project X*)."

In het adviesrapport van 2015 wordt verder ingegaan op de redenen van het starten van het project Social Media in operationele Politie

Processen (SMPP). Daar wordt alleen verwezen naar *Project X*: "Het klein bedoelde feest groeide uit tot een ware hype", aldus het rapport. Social media worden afgeschilderd als een kanaal dat onbeheersbare gevolgen kan hebben. "Mensen gebruiken social media om elkaar te betrekken, te informeren en te beïnvloeden. De gevolgen hiervan kunnen voor bestuurders, politie, het Openbaar Ministerie … groot zijn."

De overheid gebruikt *Project X* als legitimatie om grootschalige surveillance op het internet te gaan organiseren. "De politie is toegerust om te acteren in de publieke ruimte. Surveilleren en handhaven op het internet en in de social media staan echter nog in de kinderschoenen", aldus het PID document. In het rapport wordt regelmatig verwezen naar de commissie *Project X* Haren (onder leiding van Job Cohen), die stelt dat "social media mogelijkheden bieden om verbinding te maken in de haarvaten van de maatschappij". Het rapport gebruikt die mogelijkheden om te stellen dat "in alle politieprocessen de social media een cruciale rol spelen. Denk daarbij onder andere aan handhaven, het verzamelen van informatie, het duiden ervan en het eventueel interveniëren".

Project X en de Eindhovense mishandeling zijn door de politie duidelijk gebruikt om het proces van de integratie van online en social media surveillance binnen de politie te versnellen en uit te breiden. Of social media bij die incidenten al dan niet daadwerkelijk een grote rol hebben gespeeld, is voor de politie van minder belang. Het uit de hand gelopen feest in Haren roept namelijk naast bestuurlijke en operationele vragen ook vragen op over de normale Open Source INTelligence en de toen gebruikte social media monitoring tools.

Project X werd misschien wel geïnitieerd op social media, maar het lijkt erop dat de aandacht van reguliere media, vooral radio 3FM, er uiteindelijk voor zorgde dat de uitnodiging voor het verjaardagfeest door veel jongeren werd opgepakt. Zelfs zonder social media monitoring tools had de politie kunnen voorspellen dat er op 21 september 2012 iets ging gebeuren in Haren. De hoeveelheid feestgangers was van tevoren niet te voorspellen, ook niet naar aanleiding van het aantal hypothetische bezoekers op Facebook. Monitoring tools hadden hooguit kunnen vaststellen dat *Project X* veel reacties opleverde op social media, maar het feit dat het de

reguliere media haalde was daar ook al een aanwijzing voor. Bij de Eindhovense *kopschoppers* speelde social media in eerste instantie geen rol van betekenis. Pas nadat de politie zelf de publiciteit had gezocht om de verdachten te vinden, werd op social media naar de verdachten gezocht.

Demonstraties, voetbal en feestjes als surveillancedoel

De ambities van de politie op het gebied van OSINT zijn uiteenlopend. Volgens het evaluatierapport van 2015 (IM Adviesrapport Tools Informatieorganisatie Evaluatie en advies) gaat het om het gebruiken ervan in het kader van de "opvolging van meldingen (MK) RTIC, een verzoek van de operatie (gepland en ad hoc, o.b.v. acties/instappen etc.), ter ondersteuning van probleemgerichte aanpak en creëren veiligheidsbeelden, bij het opsporingsproces (incl. veiligstellen bewijslast), internetmonitoring niet-thematisch, gerichte monitoring op thema's, gerichte monitoring in het kader van preparatie van evenementen en het onderbouwing van dreigingsmeldingen en inschattingen".

In het rapport wordt onderscheid gemaakt tussen "internetmonitoring niet-thematisch" en "gerichte monitoring op thema's (thematische informatie coördinatie)". Het gaat dus om respectievelijk monitoring rond de klok van het internet en om specifieke surveillance. Uit de via de Wob openbaar geworden documenten blijkt waar die gerichte monitoring op thema's op gericht is. Het gaat om evenementen zoals demonstraties (pro-Gaza demonstratie, protest tijdens de Nuclear Security Summit NSS), picket lines en andere manifestaties, maar ook voetbalwedstrijden, en gewone feesten, feesten van een motorclubs. Mensen die politiek actief zijn, supporter zijn van een voetbalvereniging of vermeend lid van een motorclub worden in de gaten gehouden op social media. De voorbeelden die de politie opsomt lopen uiteen van incidenten (ongeval, televisie uitzending, vermissing, terrorismemelding), mogelijke problemen met de openbare orde (*Project X* feest, motorclubfeest en voetbalwedstrijd) of demonstraties en manifestaties.

De vrijheid van meningsuiting, het recht op manifestatie en de vrijheid van vergadering komen hiermee evident in het geding. Social media surveillance staat op gespannen voet met de rechtstaat. Geen van de geopenbaarde documenten maken gewag van dit spanningsveld. Voor de politie bestaat er geen onderscheid meer tussen een demonstratie, een feest, een vermissing of een ongeval. In de documenten is er maar één juridisch kader: "Juridische kaders t.b.v. de operationele politieprocessen: actief wederkerige inzet, crisis en evenementen, big data, realtime intelligence, opsporen, veilig onderzoek doen en veiligstellen en gebruik politie+ (een soort politie Twitter)." Voor de politie is een "vermissing van een minderjarig meisje, een ongeval bij een treinstation, het uitzenden van een mogelijk maatschappelijke onrust veroorzakend televisieprogramma, een feest van een motorclub, een mogelijk *Project X*-achtig feest, terrorisme-gerelateerde melding, RKC – Feijenoord en een pro-Gaza demonstratie" eenzelfde crisissituatie.

Publiek-Private Samenwerking

Bij de ontwikkeling van de RTIC's en de ontsluiting van online en social media voor surveillance doeleinden wordt de samenwerking tussen opsporingsdiensten en private partijen zichtbaar. In de Verenigde Staten is die ontwikkeling door de Freedom of Information Requests van de American Civil Liberties Union (ACLU) duidelijk aan te wijzen. In Nederland is de Nationale politie weinig transparant over deze publiek-private samenwerking. De politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) hebben geen documenten openbaar gemaakt die aangeven hoe de diensten zijn uitgekomen bij private partijen als Coosto, Obi4wan, HowAboutYou en Buzzcapture. Het ministerie van Veiligheid en Justitie heeft bijvoorbeeld geen aanbesteding uitgeschreven voor een social media monitoring tool voor de NCTV.

Wat uit de openbaar gemaakte documenten wel duidelijk wordt is dat in tegenstelling tot de Amerikaanse tool Beware, van het bedrijft Intrado, de door de Nederlandse politie gebruikte reputatiemanagement tools van private bedrijven als Coosto tot op heden nog geen actief gebruik maken van politie-informatie. Zij

gebruiken alleen online en social media informatie. *Harde* informatie van de politie is nog gescheiden van online en sociale media inlichtingen.

Sentiment analyse, Positief - Negatief

De politie verzamelt niet zelf die data van het internet. Hiervoor huurt zij reputatiemanagement bedrijven in. Bedrijven zoals Coosto, OBI4wan en Buzzcapture bieden de politie een archief met historische data en real time monitoring van uiteenlopende social media platforms (zoals Facebook, Twitter), blogs en websites (zoals Nu.nl, Tweakers).

De bedrijven hebben een archief opgebouwd dat vele jaren teruggaat, Buzzcapture tot 2007 en Coosto en OBI4wan tot 2009. Van sommige platformen en websites worden nieuwe data elke 5 minuten verzameld. Om de data voor hun klanten inzichtelijk te maken wordt er op de berichten een sentiment analyse uitgevoerd. De politie krijgt ook de beschikking over deze sentiment analyse.

De sentiment analyse is een extra functionaliteit binnen de tool van de reputatiemanagement bedrijven, die bepaalt of een bericht goed/positief of slecht/negatief is. Er is meestal ook een derde optie toegevoegd: neutraal of sentiment onbekend. Met de gelabelde berichten van een persoon kan een profiel van een persoon worden samengesteld.

Voor producenten die een nieuw product op de markt brengen kan een sentiment analyse van belang zijn om de marketing op aan te passen. Een worst is lekker of vies, of de consument heeft geen mening. De meeste mensen zullen echter geen heel uitgesproken mening hebben over een product, dus blijft de vraag wat een sentiment analyse nu precies zegt. Is een opmerking van een klant dat de worst wel lekker is, maar dat de structuur van de worst niet bevalt, een positief of negatief sentiment? Voor de producent is het van belang dat de consument gewoon de worst gaat kopen.

Coosto, Buzzcapture en OBI4wan gebruiken een sentiment analyse met de labels positief, negatief en neutraal. Clipit, een ander

reputatiemanagement bedrijf, schrijft bij haar product dat "het sentiment wordt weergegeven niet alleen aan de hand van vijf niveaus met ook met verschillende kleuren". Donkergroen is dan heel positief en donkerrood heel negatief. Het verloop van groen via geel naar rood is de schaal van positief naar negatief.

Deze kleurschakering wordt ook gebruikt in het programma Beware van het Amerikaanse bedrijf Intrado Inc. bij het vaststellen van een gevarenscore, waarbij burgers en adressen een gevarenscore/risicoscore (Facebook Threat Score) krijgen op grond van een berekening door het programma. Beware geeft een score aan met groen (goed), geel (enigszins een gevaar) of rood (gevaarlijk).

Het systeem van de gevarenscores van Beware is nooit wetenschappelijk onderzocht. De Amerikaanse burgerrechtenorganisatie ACLU stelt dat effectiviteit en nauwkeurigheid van Beware niet gemeten is. Tevens ontbreekt het aan controle, transparantie en onafhankelijk onderzoek naar het gebruik van Beware. En tot slot wijst de burgerrechtenbeweging op het gevaar van profilering als gevolg van het gebruik van Beware. De technologie zou bijdragen aan etnisch profileren.

Sentiment analyse is analyse van de taal van een bericht. Hoofd ontwikkelaar van Buzzcapture Eike Dehling legt in 2014 in het artikel *How does sentiment analysis work?* uit hoe de analyse werkt. Hij stelt dat er verschillende mogelijkheden zijn voor het vaststellen van een sentiment. De aanwezigheid of afwezigheid van bepaalde woorden, groepen of samenstelling van woorden, type woorden zoals scheldwoorden, ontkenning of bevestiging en ten slotte emoticons, symbolen die een emotie zouden weergeven.

Als voorbeeld van een bericht met een positief sentiment schrijft de ontwikkelaar dat iemand een goed weekend heeft gehad. Een negatief sentiment is een bericht over de stomme reactie van een bank op een vraag over een hypotheek. De meeste risicomanagement bedrijven gebruiken een automatisch label mechanisme om een Facebook bericht, tweet, blogpost of iets anders van een stempel of score te voorzien. Dehling schrijft op de website van Buzzcapture dat die automatische stempelmachine

zelflerend is. Hij gaat er dus vanuit dat de nauwkeurigheid en de kwaliteit van de sentiment analyse in de loop der jaren beter wordt.

Koningssentiment

Natuurlijk zijn de reputatiemanagement bedrijven erg enthousiast over de sentiment analyse die zij aanbieden. OBI4wan schrijft dat zij "100% nauwkeurigheid nastreeft." Op de website staat echter dat "de nauwkeurigheid van het sentiment, maximaal 75% – 79% is". Wat deze waarden precies betekenen blijft onduidelijk, want er wordt niet ingegaan op de nulwaarde: 75% – 79% ten opzichte van wat? Daarnaast stelt het bedrijf dat "over het algemeen het sentiment 80% neutraal is."

OBI4wan garandeert haar klanten echter dat "de correctheid van het sentiment daadwerkelijk rond de 98% is". Of dit echt zo is, valt te betwijfelen. OBI4wan komt niet voor in de top vier bedrijven die volgens Emerce in 2016 het sentiment rond het Koningshuis goed hebben gemeten. Uit die test komt Buzzcapture als winnaar naar voren met 89% "correct beoordeeld sentiment". Daarna volgen SentiOne (75%), Clipit (74%) en Meltwater (36%).

De vraag is of het sentiment rond het Koningshuis wel eenduidig te meten valt. Sentiment analyse is geen exacte wetenschap en bevat tal van complexe elementen, zoals door bedrijven ook wordt onderkend. Zo schrijft OBI4wan in een artikel *meten is weten, maar weet ook wat je meet* dat "sarcasme en cynisme het lastig maken om hier écht een sluitend beeld te geven".

Natuurlijk zijn er uitgesproken meningen van Oranjegezinden en Republikeinen, maar het is de vraag of het merendeel van de Nederlanders ook zo´n scherpe mening heeft. Als 89% (64.629) van de geanalyseerde 72.617 berichten, wordt bestempeld als neutrale berichten over het Koningshuis, wat zegt dat dan? Zijn dat daadwerkelijk kleurloze meningen of zitten daar juist belangrijke

nuanceringen in? Volgens Emerce waren 89% van de geanalyseerde berichten nieuwsberichten en zijn deze daarom als neutraal beoordeeld.

Sentiment-industrie

Reputatiemanagement bedrijven proberen zich door middel van de sentiment analyse te onderscheiden. Een grote berg online en social media gegevens aanbieden is niet heel ingewikkeld, maar om die databerg inzichtelijk te maken voor de klant is lastiger. De sentiment analyse is voor bedrijven een mogelijkheid zich te onderscheiden en daarom benadrukken zij hoe succesvol hun methode zou zijn.

Zo stelt Amit Moran, data analist van het Amerikaanse bedrijf Crosswise, dat je met sentiment analyse de echte kracht van social media kan gebruiken. Door de hoeveelheid data kan volgens hem met behulp van sentiment analyse van individuele tweets de veranderende mening van gebruikers door de tijd worden vastgesteld. Anderzijds is Moran minder stellig over de toepasbaarheid van analyses voor alle onderwerpen. Hij stelt dat een sentiment analyse ten aanzien van bijvoorbeeld een worst niet automatisch kan worden gebruikt voor bijvoorbeeld het Koningshuis. "The phrases and patterns used to express sentiment varies across domains and need to be adapted when switching between domains."

Moran geeft aan dat sentimenten over een specifiek onderwerp niet noodzakelijkerwijs gebruikt kunnen worden op een ander terrein. Dit heeft natuurlijk alles te maken met taal en het taalbegrip. Hoe taal wordt gebruikt, en of online woordgebruik wel overeenkomt met offline taalgebruik, zijn vragen die sentiment analyse compliceren en bemoeilijken. Dominick Soar, content manager bij het bedrijf Brandwatch, schrijft in 2011 dat sentiment analyse is gebaseerd op taal, maar dat niet altijd kan worden vastgesteld welk sentiment de social media gebruikers uiten. Volgens de manager gebruiken mensen op sociale media geen normale of standaardtaal. Hij noemt het dialecten, slang of andere manieren om hun gevoelens te uiten. Brandwatch heeft hiervoor natuurlijk een oplossing, want volgens

Soar zou het bedrijf door machine learning de oplossing voor het taalprobleem hebben gevonden.

Naast de bovenstaande problemen is er ook nog het probleem van spelling en spelfouten. Frank Scheelen, ontwikkelaar bij Coosto zegt in een artikel op Recruitment Matters dat "15% van alle tweets spelfouten bevatten". Scheelen noemt naast de taalfouten ook andere aspecten die ervoor zorgen dat "sentiment analyse nooit perfect zal kunnen zijn". Zoals het feit dat cynisme en sarcasme niet kunnen worden vastgesteld door de systemen en dat gemengde gevoelens en de context waarin bepaalde opmerkingen worden gemaakt niet door analyses worden opgepikt.

Algoritmen

De reputatiemanagement bedrijven presenteren de sentiment analyse als een wetenschappelijke methode, maar de analyse is een verkooppraatje. Er wordt gesproken over analyse met behulp van machine learning, of slechts het automatisch en handmatig toepassen van een set regels. Hoe effectief het meten van sentimenten is blijft ongewis. Er is geen wetenschappelijke onderbouwing van de kwaliteit, nauwkeurigheid en totstandkoming van de analyses.

Sentiment analyse is gebaseerd op algoritmen: formele regels, vastgelegd door computertechnici, die een voorspelling maken over het sentiment van een bericht op basis van historische regels en patronen. Voor die voorspellingen, regels en patronen zijn wel historische data nodig. Daarom verzamelen de reputatiemanagement bedrijven veel data.

Coosto spreekt bijvoorbeeld over drie miljoen berichten die dagelijks worden verzameld en voorzien van een sentiment. Coosto en OBI4wan doen de sentiment analyse automatisch. Buzzcapture claimt dat het naast automatisch labelen ook nog aan het handmatig vaststellen van het sentiment, door medewerkers van het bedrijf doet. Het bedrijf stelt dat halverwege 2014 6,5 miljoen berichten in haar database zaten die handmatig waren gelabeld. Van een archief

dat sinds 2007 is aangelegd met miljoenen berichten die dagelijks worden verzameld is dat slechts een fractie.

Cathy O'Neil, Amerikaanse wiskundige en schrijfster van het boek Weapons of Math Destruction, trekt een parallel tussen het social media archief van de reputatiemanagement bedrijven en de historische data over algoritmen in het algemeen. Die historische data over algoritmen roepen vragen op over het succes van die algoritmen.

In het artikel *How can we stop algorithms telling lies?* In *The Guardian* van juli 2017 verwijst zij naar de financiële crisis van 2007/2008 en het enthousiasme over het gebruik van algoritmen in de financiële sector dat aan de crisis voorafging. "Financial risk models also use historical market changes to predict cataclysmic events in a more global sense, so not for an individual stock but rather for an entire market. The risk model for mortgage-backed securities was famously bad – intentionally so – and the trust in those models can be blamed for much of the scale and subsequent damage wrought by the 2008 financial crisis."

Politie-algoritmen

De vragen die O'Neil oproept zijn legitiem. Hoe werken de algoritmen en kunnen we ze vertrouwen? Begrijpen de bedrijven die sentiment analyse aanbieden de algoritmen zelf nog wel? Deze vraag is mede relevant omdat sommige bedrijven de technologie verhuren aan andere bedrijven. HowAboutYou huurt OBI4wan in. Buzzcapture huurt de technologie in van Coosto en TextKernel in. Vervolgens huurt de Nederlandse politie HowAboutYou en Buzzcapture weer in.

Het is duidelijk dat de politie samenwerkt met reputatiemanagement bedrijven. Uit de openbaar geworden documenten blijkt tevens dat de politie sentiment analyse gebruikt voor social media surveillance. In het rapport van de politie-eenheid Zeeland-West-Brabant van 18 februari 2015 over de ervaring met het gebruik van OBI4wan staan in "bijlage 1 eisen aan de online media monitor" bij "rapportages maken" dat de tool ingericht kan worden naar de wensen van de

politie. Volgens het rapport gaat het om allerlei aspecten waaronder "analyses van afzenders, locatie (kaartje), wanneer er over de zoekopdracht veel gesproken wordt, volumes, webcare status, gebruikers, bronsoorten, afhandelsnelheid, invloed van afzenders, sentiment".

Sentiment analyse is opgenomen in de tool en kan ook handmatig worden aangepast. Het rapport stelt tevens dat bij de social media monitoring de "metadata die beschikbaar zijn, worden opgeslagen bij het originele bericht". Het rapport vervolgt: "Daarnaast verrijken wij het bericht met metadata uit eigen analyses, zoals de belangrijkste woorden in een bericht, het sentiment, locatiegegevens en gegevens over de afzender."

De afdeling persvoorlichting van de politie eenheid Zeeland-West-Brabant ziet gescoord sentiment als een relevante functionaliteit. "Visualisaties van volumes, gerelateerde topics, sentiment, influencers en gesprekslocaties vertellen het online verhaal" staat in de paragraaf basisfuncties van de tool. Bij aanvullende werkafspraken wordt het belang van sentiment analyse opnieuw onderstreept: "Tijdens het monitoren blijft het relevant en noodzakelijk om toch alle berichten te scannen op inhoud, relevantie en sentiment." In het rapport blijkt dat naast de persvoorlichters, de politie-infodesk, het RTIC en de opsporing de sentiment analyse gebruiken.

"De Infodesk is servicepunt voor informatieverzoeken van verschillende afdelingen binnen de politie-eenheid Zeeland - West-Brabant", is de eerste zin van hoofdstuk 5 van het rapport van de politie eenheid Zeeland-West-Brabant. "De monitor gebruiken collega's vooral voor openbare orde, handhaving en strafrechtelijke onderzoeken (evenementen/demonstraties, opsporingsvragen, dreigingsinschatting, mensenhandel, enzovoort). Zaken waarbij online media voor de Infodesk van toegevoegde waarde is, zijn onder andere: Inzicht krijgen in netwerken van personen, kennisbron voor interesses, bewegingen en sentimenten rond personen voor omgevingsbeelden bij een incident; regie voeren op thema's (motorclubs, overvallen, inbraken, enzovoort)."

Hoeveel inzicht heeft de politie in de zoektechnologie en de sentiment analyse en daarmee de profilering van de bedrijven? Kan

de politie de zoekopdracht, de sentiment analyse van berichten en de profilering middels die gelabelde berichten nabootsen om te achterhalen waarom iemand als verdachte of potentieel gevaar wordt aangemerkt? In de openbaar gemaakte documenten naar aanleiding van de Wob verzoeken van Buro Jansen & Janssen staat niets over de aanwezigheid van deze kennis bij de politie of de Nationaal Coördinator Terrorisme en Veiligheid (NCTV).

Voor de sentiment analyse worden veel data door social media monitoring bedrijven verzameld. De bedrijven hebben daartoe grote databanken aangelegd met veel historisch materiaal. De politie gebruikt die historische gegevens, blijkt uit de openbaar gemaakte documenten. Dit staat op gespannen voet met wetgeving ten aanzien van de bescherming van persoonsgegevens.

Databanken vol Nederlanders en geen controle

Gebruikers van online media en social media weten niet dat hun berichten, meningen en opinies worden verzameld door deze social media surveillance bedrijven. Het gaat ook om persoonlijke informatie over woon- en verblijfplaats, werk, familieomstandigheden en allerlei andere tot de persoon herleidbare gegevens die gebruikers op het internet delen.

De gegevens die Coosto, OBI4wan, HowAboutYou en Buzzcapture verzamelen zijn persoonsgegevens. De bedrijven bevestigen dit in hun privacy verklaringen. Ook de Autoriteit Persoonsgegevens gaat er vanuit dat de online en social media gegevens die worden verzameld persoonsgegevens zijn. "De AP heeft geen onderzoek gedaan naar deze bedrijven, maar gaat er in algemene zin van uit dat gegevens die van sociale media worden verzameld in veel gevallen persoonsgegevens zijn als bedoeld in artikel 1, onder a, van de Wet bescherming persoonsgegevens (Wbp). Dit omdat de gegevens direct of indirect herleidbaar zijn naar natuurlijke personen, ofwel rechtstreeks via hun sociale media-account, of indirect, via de verantwoordelijken voor deze sociale netwerksites. Voorzover de door u genoemde bedrijven de inhoud van berichten verzamelen, al dan niet in combinatie met locaties, connecties en

persoonlijke interesses, hebben de gegevens betrekking op natuurlijke personen."

Aan het bewaren en het verwerken van persoonsgegevens worden wettelijke voorwaarden gesteld. De Autoriteit Persoonsgegevens verwijst naar *Beleidsregels publicatie van persoonsgegevens op internet uit 2007*. Hierin staan geen expliciete bewaartermijnen, maar wel staat vermeld dat "gegevens niet langer mogen verwijzen naar identificeerbare personen dan strikt noodzakelijk en de gegevens moeten juist zijn en ter zake dienend". In antwoord op vragen van Buro Jansen & Janssen over de archieven van de social media monitoring bedrijven antwoordt de Autoriteit Persoonsgegevens: "Het feit dat persoonsgegevens op internet staan, betekent niet dat ze zomaar opnieuw gebruikt mogen worden in een andere context, voor een ander doeleinde. … Zelfs als het nieuwe doel verenigbaar is met het oude doel, kan de verwerking onrechtmatig zijn."

Hoewel de Autoriteit Persoonsgegevens aangeeft geen zelfstandig onderzoek te hebben gedaan, stelt men wel dat: "bedrijven die de persoonsgegevens verzamelen van sociale media, een zelfstandige grondslag dienen te hebben voor de (verdere) verwerking, en er zorg voor moeten dragen dat de gegevens niet verouderd en niet onjuist zijn. Dat betekent ook dat deze bedrijven de gegevens niet langer mogen bewaren dan noodzakelijk voor het behalen van de gerechtvaardigde doeleinden die zij nastreven."

Geen van de reputatiemanagement bedrijven heeft het verwerken van persoonsgegevens gemeld bij de Autoriteit Persoonsgegevens (en haar voorganger het College Bescherming Persoonsgegevens). Tevens worden de bedrijven al tien jaar niet gecontroleerd door de bevoegde instantie, de Autoriteit Persoonsgegevens over bijvoorbeeld de verwerking van persoonsgegevens, de duur van het bewaren van de gegevens en de sentiment analyse.

OBI4wan stelt op vragen van Buro Jansen & Janssen dat zij recentelijk haar "privacy verklaring heeft aangepast op de nieuwe wetgeving" en dat "wij voldoen of gaan wij voldoen aan toekomstige wetgeving". Het bedrijf spreekt ook over "interne en externe audits" in haar privacyverklaring. Coosto spreekt in haar privacyverklaring over "toegangsbeveiliging, encryptie, monitoring en auditing,

periodieke penetratietests, scans op potentiële kwetsbaarheden en certificeringen". In de privacy verklaring van Buzzcapture staat hier niets over. De privacy verklaringen vermelden niet of de controles betrekking hebben op het verwerken van persoonsgegevens, de bewaarduur, de samenwerking met de overheid of de sentiment analyse.

De Autoriteit Persoonsgegevens ziet het niet als haar prioriteit om op te treden, geeft zij in haar antwoord aan Buro Jansen & Janssen aan. "De Autoriteit Persoonsgegevens beschouwt uw brief als een belangrijk signaal", schrijft het bestuursorgaan, maar "de Autoriteit Persoonsgegevens ontvangt jaarlijks duizenden tips en meldingen en moet daarom een selectie maken welke zij nader onderzoekt". De Autoriteit Persoonsgegevens maakt niet duidelijk of zij de genoemde bedrijven zal aanschrijven.

Dat controle op databanken noodzakelijk is blijkt uit een rapport van het College bescherming persoonsgegevens (de voorganger van Autoriteit Persoonsgegevens) van juni 2012. Het College deed onderzoek naar databanken van de Criminele Inlichtingen Eenheden (CIE's) van de politie. Die databanken zitten vol met gegevens, waaronder gegevens verkregen via informanten en infiltranten, geruchten en OSINT. Het is niet duidelijk of deze inlichtingen betrouwbaar zijn. Het gaat om informatie over vermeende criminele activiteiten, dus om burgers die nog niet verdacht zijn, maar dat op basis van de informatie wel kunnen worden. Onbetrouwbare informatie kan grote gevolgen hebben voor deze mensen.

Het CBP was van mening dat de CIE's van de regionale politiekorpsen Flevoland en Brabant Zuid-Oost "onvoldoende maatregelen hebben getroffen om de wettelijke eisen omtrent bewaartermijnen van politiegegevens na te leven. Daarmee handelen zij in strijd met de wet". De kritiek richtte zich op zowel het gebrek aan een jaarlijkse controle of de gegevens nog relevant zijn en bewaard dienen te blijven, als op het overschrijden van de maximale bewaartermijn van vijf jaar. De kritiek op de korpsen leidde eind 2013 tot het opleggen van een dwangsom door het CBP

omdat de politie de aanbevelingen van het College nog niet had opgevolgd.

ARBIT

De politie mag dus niet ongelimiteerd persoonsgegevens verzamelen, verwerken en bewaren. Haar beleid ten aanzien van opslag en verwerking van persoonsgegevens is wettelijk geregeld. Er vinden jaarlijkse audits plaats en er zijn maximum bewaartermijnen. Door gebruik te maken van de diensten van Coosto, OBI4wan, HowAboutYou en Buzzcapture omzeilt de politie deze wettelijke beperkingen. Zelfs door gebruikers verwijderde berichten op social media zijn gewoon terug te vinden in de databases van de social media monitoring bedrijven. Samenwerking met private IT-bedrijven is echter ook gebonden aan wet- en regelgeving, ook bij inhuur door de politie en de NCTV.

Van Coosto is bekend dat zij voor het werk voor de NCTV de standaard Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT) heeft ondertekend. De politie heeft deze ARBIT overeenkomsten die ze zou moeten sluiten met Coosto, OBI4wan, HowAboutYOU en Buzzcapture niet openbaar gemaakt. De verwerking van de persoonsgegevens en de veiligheid van de archieven wordt volgens de overheid geregeld door de ARBIT, Algemene Rijksvoorwaarden bij IT-overeenkomsten, die een kader scheppen voor de digitale veiligheid van de persoonsgegevens.

In artikel 18 komt de verwerking van persoonsgegevens aan bod. Deze moet op “behoorlijke en zorgvuldige wijze en in overeenstemming met de toepasselijke wet- en regelgeving” gebeuren. Tevens is in de ARBIT opgenomen dat er geen “onnodige verzameling en verdere verwerking van persoonsgegevens” plaatsvindt. Dit laatste artikel verwijst naar de *Beleidsregels publicatie van persoonsgegevens op internet uit 2007* van de Autoriteit Persoonsgegevens, die aangeeft dat gegevens niet “zomaar opnieuw mogen worden gebruikt”, dat er een “zelfstandige grondslag” moet zijn voor verwerking en gegevens “niet verouderd en onjuist” zijn. Uit de via de Wob openbaar gemaakte documenten

blijkt niet dat politie en de NCTV de bedrijven op deze aspecten hebben gecontroleerd.

Gebrek aan transparantie

Buro Jansen & Janssen heeft geprobeerd meer helderheid te krijgen over social media surveillance door politie en de NCTV. In 2016 vroeg Buro Jansen & Janssen via Wob-verzoeken documenten op over de bedrijven Coosto, Buzzcapture, OBI4wan en HowAboutYou, en over "nep account of schaduw accounts op sociale media of het internet in het algemeen", "het programma SMPP", het "Advies rapport ten aanzien van de evaluatie van het operationele gebruik van diverse social media monitoring tools op diverse afdelingen" en "de namen of bedrijven van diverse social media monitoring tools of online media monitoring tools (of vergelijkbare namen) waarmee de politie op diverse afdelingen de afgelopen jaren heeft geëxperimenteerd".

De politie maakte een rapport over het gebruik van OBI4wan door de politie-eenheid Zeeland-West- Brabant openbaar (*Online media monitoring: tool en proces (2)*). Ook werden enkele losse documenten over een proef met het gebruik van de tools van OBI4wan/ HowAboutYou bij de landelijke eenheid, de eenheid Zeeland-West- Brabant en de eenheid Den Haag verstrekt. HowAboutYou wordt in verschillende documenten als verantwoordelijke en contactpersoon voor de proef met OBI4wan genoemd. In 2017, ruim een half jaar na de verzoeken, maakte de politie documenten over Buzzcapture (een offerte aanvraag en offertes) en twee algemene documenten, het *Project Initiatie Document (PID)* en het *IM Adviesrapport* openbaar. De politie weigert documenten over Coosto openbaar te maken.

In 2017 diende Buro Jansen & Janssen vervolgens nieuwe verzoeken in over de relatie tussen de Nederlandse politie en de Amerikaanse social media monitoring bedrijven SnapTrends en Geofeedia, de Canadese bedrijven Media Sonar en Hootsuite en de Nederlandse bedrijven Meltwater, iMonitoring, Teezir en Tracebuzz. Tevens is Buro Jansen & Janssen bekend met het bestaan van andere documenten. Daar is in 2017 ook naar gevraagd. Het gaat om

Project Initiatie Document OSINT 2011 Open source intelligence mei 2011, Toepassingsdocument social media 2013-2015, Position paper OSINT in de Informatieorganisatie, Nationale Politie (PIO, SMPP), Nederland 2015, Open bronnen tools inwinning: Troonswisseling Nationale Politie Eenheid Amsterdam (CIO, DRI) Nederland 2013 / Referentiemodel Bedrijfsprocessen Politie (RBP2012), Verbeteren van Politie Processen (VVP), Online media monitoring: tool én proces, Nationale Politie Eenheid Zeeland West-Brabant, Nederland, 2014 / RTIC medewerkers (evaluaties), Nationale Politie, diverse eenheden, Nederland, 2014 en 2015, OSINT medewerkers (evaluaties), Nationale Politie, diverse eenheden, Nederland, 2014 en 2015 en Internetrechercheurs (evaluaties), Nationale Politie, diverse eenheden, Nederland, 2015. Deze documenten zijn nog niet openbaar gemaakt.

Verontrustend en opmerkelijk

Ondanks de weinig transparante houding van de overheid is aan de hand van allerlei bronnen en via de Wob openbaar gemaakte documenten, die via de Wob zijn verkregen, de social media surveillance in beeld gebracht. De politie werkt met verschillende reputatiemanagement bedrijven samen. De bedrijven Coosto, Obi4wan en HowAboutYou worden ingehuurd door de politie voor zowel communicatie als Real Time Intelligence Centers en opsporing. Buzzcapture is voor zover bekend alleen voor communicatie voor de Nationale Politie ingehuurd.

In het verleden werkte de politie aan een eigen tool die specifiek gericht was op de opsporing. Uit de openbaar gemaakte documenten blijkt dat de politie deze tool, iColumbo/IRN, wil ombouwen voor online en social media surveillance, dus niet meer exclusief voor de opsporing. Uit de openbaar gemaakte documenten blijkt niet of de ontwikkeling van die eigen tool wordt voortgezet. De commerciële tools kunnen dus worden ingehuurd in afwachting van de oplevering van de eigen tool, iColumbo/IRN, of vanwege de grote hoeveelheid historische data waarover de bedrijven beschikken en de toegevoegde waarde van de sentiment analyse.

In zowel het PID document project SMPP van 2013 als het evaluatiedocument van 2015 die via Wob-verzoeken van Buro Jansen & Janssen openbaar zijn geworden, wordt met geen woord gesproken over de consequenties van het inhuren van private bedrijven. Vragen met betrekking tot de grote historische archieven van de bedrijven, de kennis over de werking van de tools, de broncode, sentiment analyse en algoritmen komen in geen van de documenten aan bod. Ook in de stukken die openbaar zijn gemaakt door het ministerie van Veiligheid en Justitie over het gebruik van Coosto komen deze aspecten niet aan de orde.

De politie huurt private partijen in die informatie aanbieden voor surveillance, opsporing en het scoren van burgers, maar controle op de bewaartermijnen van de persoonsgegevens, de verwerking van die gegevens en audits van de kwaliteit en nauwkeurigheid van de databanken zijn niet beschikbaar. De bedrijven hebben de verwerking van de persoonsgegevens nooit aangemeld bij bevoegde instanties.

Het is opmerkelijk dat de politie en de NCTV geen informatie hebben over de consequenties van het inhuren van private partijen voor social media surveillance. Daarnaast is het verontrustend dat in de documenten met geen woord wordt gesproken over de mogelijke schendingen van grondrechten zoals de vrijheid van meningsuiting, het recht op manifestatie en de vrijheid van vergadering. De politie en de NCTV gaat rechtsstatelijke vragen uit de weg terwijl social media surveillance op gespannen voet staat met de rechtstaat.

Dagelijkse en structurele monitoring
De Nederlandse politie en social media surveillance (pdf)

Gehele Observant #70 social media surveillance in Nederland (pdf)

Andere artikelen

Social Media Surveillance in Nederland

Reputatie management bedrijven, de nieuwe private inlichtingendiensten

De burger als dreigingsscore; Social media surveillance in de Verenigde Staten

Overgeleverd aan de grillen van social media multinationals; Facebook en Twitter en de Nederlandse social media surveillance

Verder lezen

Meer dan 200.000 professionals doen maar wat tegen terrorisme

Bijlagen

Politie

presentatie Inge Hoogstad RTIC (pdf)

politie besluit OBI4wan HowAboutYou (pdf)

politie besluit OBI4wan online media monitoring tool en proces (pdf)

PID social media in de operationele politie processen (pdf)

politie besluit IM adviesrapport tools informatieorganisatie (pdf)

politie besluit Buzzcapture (pdf)

politie besluit nep accounts presentatie (pdf)

Ministerie van Veiligheid en Justitie

besluit ministerie van V en J Coosto Buzzcapture primair (pdf)

besluit ministerie van V en J Coosto Buzzcapture bij bezwaar (pdf)

Autoriteit Persoonsgegevens

persoonsgegevens_op_internet_2007 (pdf)

brief aan Autoriteit Persoonsgegevens (pdf)

aanvullende brief aan Autoriteit Persoonsgegevens (pdf)

Autoriteit Persoonsgegevens antwoord (pdf)