

Reputatiemanagement bedrijven, de nieuwe private inlichtingendiensten

De Nederlandse politie doet aan social media surveillance en werkt hierin samen met de social media monitoring bedrijven Coosto, OBI4wan en HowAboutYou. Dit blijkt uit onderzoek van Buro Jansen & Janssen.

De Nederlandse bedrijven Coosto, OBI4wan, HowAboutYou, Buzzcapture bieden monitoring tools aan op het terrein van reputatiemanagement of webcare. Deze worden afgenomen door bedrijven en overheidsorganen die negatieve publiciteit willen tegengaan. Essentieel onderdeel van het reputatiemanagement is de sentiment analyse. Bedrijven verzamelen data die worden voorzien van een label goed/positief, slecht/negatief en neutraal. De labels dienen om de publiciteit over een product of dienst te volgen. Daarbij gaat het natuurlijk vooral om negatieve berichtgeving, waar een producent snel op wil reageren.

Reputatiemanagement is dus risicomangement. Om risico's te vermijden worden zoveel mogelijk gegevens van online en social media verzameld. Coosto, OBI4wan, HowAboutYou, Buzzcapture verzamelen data met zoekmachines die het internet afspeuren. De gegevens komen in principe van open bronnen: informatie die door bedrijven en individuen op het internet wordt gedeeld. Zij bewaren die data in archieven in Nederland. Enkele van deze bedrijven hebben een archief van internet data dat terug gaat tot 2007 of 2009. In deze databanken wordt alle informatie die de bedrijven verzamelen bewaard, ook informatie die mensen later van hun social media account hebben verwijderd.

Coosto, OBI4wan, HowAboutYou en Buzzcapture borduren voort op de traditie van private inlichtingendiensten. Deze schimmige bedrijven werden eind vorige eeuw en begin deze eeuw vooral ingehuurd door multinationals om actiegroepen die campagnes tegen die bedrijven voerden in de gaten te houden. Gaandeweg werden de private inlichtingendiensten ook ingehuurd door politie,

inlichtingendiensten van de overheid en ministeries. Met de komst van social media en uitgebreide mogelijkheden internet data te verzamelen ontstonden social media monitoring of reputatiemanagement bedrijven. De Nederlandse politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) huren de diensten van bedrijven als Coosto, OBI4wan en HowAboutYou in. Niet alleen voor communicatiedoeleneinden, maar ook voor social media surveillance.

Inlichtingen verzamelen van AIVD naar politie

Op grote schaal inlichtingen verzamelen uit open bronnen is van oudsher één van de hoofdtaken van inlichtingendiensten. Zo verzamelt de Nederlandse Algemene Inlichtingen- en Veiligheidsdienst (AIVD) op grote schaal informatie over niet-verdachte burgers. Ten tijde van de Koude Oorlog werden allerlei organisaties en individuen in de gaten gehouden, waarvan men maar enigszins dacht dat ze communistische sympathieën hadden. Veel van hen stonden kritisch tegenover overheden of het bedrijfsleven. De meeste informatie die inlichtingendiensten verzamelen bestaat uit openbare informatie, zoals kranten, tijdschriften, flyers, posters. In het verleden ging het vooral om papieren materiaal, tegenwoordig merendeels digitaal.

Naast open bronnen verzamelen inlichtingendiensten ook informatie uit gesloten bronnen. Dit kunnen gegevens zijn die worden verkregen via een tap bij internetproviders of telefoonmaatschappijen, maar ook gegevens van energie- en waterleidingbedrijven, gemeentelijke diensten en woningbouwverenigingen, of informatie verkregen via informanten, infiltranten en afluisterapparatuur.

Ook de politie verzamelt inlichtingen, al was dat lange tijd op veel kleinere schaal dan inlichtingendiensten. Bij de politie stond inlichtingen verzamelen in het algemeen in het licht van opsporingsonderzoeken en de TCI, het Team Criminele Inlichtingen (de huidige naam voor de Criminele Inlichtingen Eenheden), die geruchten uit het criminele circuit al dan niet via informanten en

infiltranten in kaart brengt. Ook de RID's, de Regionale InlichtingenDiensten, verzamelen informatie over voetbalsupporters, demonstranten en kraakpanden in het kader van de handhaving van de openbare orde. De politie heeft zich de laatste jaren steeds meer gericht op het verzamelen van inlichtingen.

Algemene Beveiligings Consultancy

Lange tijd was inlichtingen verzamelen een staatsaangelegenheid. Voor private partijen was een eigen inlichtingendienst een te kostbaar middel. Multinationals hadden die mogelijkheden wel. In de jaren negentig kwamen de eerste verhalen bovendrijven van private inlichtingenbureaus die werden ingehuurd door multinationals. Buro Jansen & Janssen publiceerde in 1994 een onderzoek naar het bedrijf Algemene Beveiligings Consultancy (ABC) te Vinkeveen. ABC was van Peter Siebelt die zich vanaf eind jaren zeventig met zijn bedrijf Siebelt BV al presenteerde als veiligheidsadviseur.

Met ABC haalde Siebelt onder andere oud papier op bij verschillende organisaties, waaronder de waarnemersdelegatie van de Parlementariërs tegen Apartheid (Awepa) die de verkiezingen in Zuid-Afrika volgde, en de Werkgroep Medische Ontwikkelingssamenwerking (WEMOS). Van beide organisaties doken plotseling interne documenten op in de publiciteit. Siebelt verzamelde het oud papier en verkocht dit door aan de Telegraaf die zich fel keerde tegen de Awepa, en aan Nutricia (tegenwoordig Numico) dat de kritische houding van WEMOS wilde bestrijden. ABC zette ook informanten in die als vrijwilligers aan de slag gingen bij Ngo's om informatie te verzamelen. In 1994 ontmaskerde Buro Jansen & Janssen in dat kader Paul Oosterbeek, die als vrijwilliger werkte onder meer bij Osaci (Oecumenisch Studie- en Actiecentrum voor Investerings) en het Schone Kleren Overleg.

In 1998 was het opnieuw raak toen Adrian Franks voor het bedrijf Risk Crisis Analyses ASEED, een Nederlandse milieuorganisatie, bespioneerde. Het bleek dat Franks ook in andere Europese landen was geïnfiltrerd in actiegroepen om zo notulen en andere documenten te verzamelen. Adrian Franks probeerde die informatie

te verkopen aan bedrijven. Vijf jaar later bleek dat Franks opnieuw aan de slag was gegaan voor het Britse bedrijf Threat Response International en bij vredesgroepen infiltreerde.

Hij verkocht de informatie over de activiteiten van Campaign Against Arms Trade (CAAT) aan British Aerospace (BAE), een grote speler in de militaire industrie. The Sunday Times maakte openbaar dat Threat Response International vier jaar lang een dagelijks rapport aan BAE Systems stuurde voor een bedrag van 120.000 pond (in die tijd ongeveer 190.000 euro). De rapporten waren voor een groot deel gebaseerd op rapportages van Adrian Franks, die bij de Campaign Against Arms Trade was geïnfiltrerd. De rapporten bevatten daarnaast informatie uit tijdschriften, kranten en andere openbare bronnen.

Global Open Limited

In 2010 kwam een andere inlichtingenbedrijf in het nieuws. Het Britse Global Open Limited had voormalig politieagent Mark Kennedy ingehuurd om voor het Duitse energie bedrijf E.ON te infiltreren in milieuorganisaties om acties bij vervuilende energiecentrales te voorkomen. Kennedy infiltreerde eerder voor de Britse politie in de milieubeweging en had verschillende relaties met vrouwelijke activisten die niets van zijn undercover werk wisten. Die relaties zorgden voor een snelle carrière in de actiewereld. Na zijn vertrek bij de politie zette hij een eigen bedrijf op: Tokra. Het was op hetzelfde adres geregistreerd als de toenmalige directeur van Global Open Limited, Heather Mary Millgate.

Global Open Unlimited werd begin 2001 opgezet door een voormalig politieagent. Het bedrijf hield zich net als Algemene Beveiligings Consultancy, Risk Crisis Analyses en Threat Response International bezig met het verzamelen en doorverkopen van inlichtingen. Naast het verzamelen en ordenen van openbare informatie, zette het bedrijf ook infiltranten in.

ABC en Threat Response International hadden vooral bedrijven als klant, en hadden voor zover bekend geen contact met de politie en inlichtingendiensten. Global Open wist wel door te dringen tot

opsporings- en inlichtingendiensten. De reden hiervoor kan gelegen hebben in het feit dat Global Open geleid werd door Rod Leeming, een voormalig Special Branch agent. "Global Open Limited was founded in the United Kingdom and is run by former New Scotland Yard Special Branch officers," stond op de website van het bedrijf vermeld .

Ook de Nederlandse politie was klant van Global Open. Naar aanleiding van een Wob/WIV verzoek van Buro Jansen & Janssen zijn in 2017 200 pagina's door de AIVD openbaar gemaakt. De documenten maken duidelijk dat de politieregio Gelderland Midden tussen 2007 en 2009 de zogenaamde Weekly Digest van het bedrijf ontving. De Regionale Inlichtingendienst (RID) bestelde de weekberichten van Global Open in het kader van onderzoeken naar dierenrechtenactivisten. Een groot deel van de samengestelde knipselkranten gaat over acties gerelateerd aan dierenrechten.

Stratfor

Het bedrijf Stratfor wist nog grotere klanten binnen te slepen met een knipselkrant vergelijkbaar met de Weekly Digest van Global Open. Stratfor voegde aan de verzamelde berichten ook een 'intelligence analyse' toe. Stratfor had veel klanten bij grote bedrijven, ministeries, opsporingsdiensten, waaronder het Amerikaanse leger, politie en inlichtingendiensten en de Nederlandse ministeries van Binnenlandse Zaken (AIVD), Economische Zaken en Buitenlandse Zaken. Kennis over de klantenkring van Stratfor is in 2011 naar buiten gekomen door een hack die ervoor zorgde dat de gegevens van honderdduizenden abonnees en klanten openbaar werden. Stratfor werd gehackt door Jeremy Hammond die hiervoor in 2013 werd veroordeeld tot tien jaar gevangenisstraf.

Stratfor is op het eerste gezicht een gewoon bedrijf met Nederlandse en Amerikaanse bestuursorganen als klanten. Het bedrijf verzamelt data, die opnieuw worden geïndexeerd, van een analyse voorzien en doorverkocht. Stratfor presenteert zich echter iets chiquer dan Global Open. Het doet zich voor als een internationaal kennis instituut, een 'geopolitical intelligence platform'. Stratfor beweert

klanten inzicht geven in een complexe wereld: "To empower members to confidently understand and navigate a continuously changing and complex global environment."

Global Open richtte zich expliciet op toekomstige klanten die onder vuur zouden kunnen komen te liggen van kritische burgers. "Companies currently being targeted by activists require fast access to information in order to avoid the effects of economic sabotage and personal harassment," aldus de website van het bedrijf. De anti-globaliseringsbeweging, milieuorganisaties en dierenrechtengroepen werden door Global Open als mogelijk problematisch voor bedrijven omschreven.

Stratfor is minder expliciet als het gaat om het in de gaten houden van burgerrechtenbewegingen, actiegroepen en protestbewegingen, het bedrijf wil zich duidelijk niet afficheren met bedrijven als Global Open. Uit de hack van 2011 blijkt echter dat het bij hun diensten niet alleen gaat om het leveren van informatie over aanslagen, maar ook over actiegroepen en demonstranten. In 2001 omschrijft Barron 's Financial Investment News het bedrijf dan ook als 'the Shadow CIA', de Amerikaanse inlichtingendienst Central Intelligence Agency.

Evolutie van de private inlichtingendiensten

De ontwikkeling van de private inlichtingenbedrijven van de jaren tachtig tot ongeveer 2010 is er één van verdergaande acceptatie van deze bedrijven door overheden. Algemene Beveiligings Consultancy, Risk Crisis Analyses en Threat Response International waren private inlichtingendiensten, maar enigszins obscuur. Siebelt vond wel gehoor bij Nutricia. Threat Response International werd ingehuurd door een grote speler binnen de militaire industrie, BAE Systems. Global Open wist begin deze eeuw al een groot energie bedrijf (E.ON) en politiediensten als klant te werven, en Stratfor zelfs enkele Nederlandse ministeries. Rode draad bij de private inlichtingenbedrijven is dat hun slachtoffers altijd mensen zijn die een kritisch geluid laten horen over de bedrijven die hun klanten zijn.

De acceptatie van private inlichtingenbedrijven is met het reputatiemanagement een nieuwe fase in gegaan. Na de eeuwwisseling is het verzamelen van inlichtingen in een hoog tempo gedigitaliseerd. De reputatiemanagement bedrijven hebben van die online en social media data sinds ongeveer 2007 hun handelswaar gemaakt. Verzamelde data worden bewaard, geïndexeerd en doorzoekbaar gemaakt. De zogenaamde sentiment analyse van de verzamelde persoonsgegevens speelt een belangrijke rol in de dienstverlening van de reputatiemanagement bedrijven.

Sentiment analyse

Bij sentiment analyse worden online en social media berichten gelabeld als positief, negatief of neutraal. Ieder bericht krijgt zo een stempel en samen met het aantal volgers, vrienden, retweets, berichten die overgenomen zijn en andere aspecten met betrekking tot de invloed en het sentiment van de auteur kan een profiel van de burger worden gemaakt. Volgens een factsheet over Coosto staat in dat profiel onder andere de "auteur (profiel), invloed auteur, bronnen, invloed bron, bereik bron/site, sociaal netwerk, invloed, sentiment" (Coosto factsheet in de Social media monitoring en webcare tools 2014). Een dergelijk profiel is van groot belang om te beoordelen of de imagoschade mogelijk grote gevolgen kan hebben.

De social media monitoring bedrijven presenteren hun diensten als een service. Het gaat om het verbeteren van de communicatie met de klant of de burger, zoals het afhandelen van vragen, klachten, feedback en informatie. Snelle online communicatie beoogt assertieve burgers snel van dienst te zijn en slechte publiciteit niet lang te laten voortwoekeren.

Social media surveillance

Doelwit van de oude private inlichtingendiensten mensen en groepen die kritisch waren over bedrijven. Kranten en tijdschriften werden uitgedroogd over hun meningen en indien nodig werden papier- en

vuilnisbakken doorzocht of informanten ingezet. De bedrijven die de inlichtingen kochten wisten soms niet waar die vandaan kwamen, maar hadden daar in het algemeen geen interesse in. Net als de afnemers van de reputatietools geen inzicht hebben in de herkomst van de data en de broncode (de precieze werking/technische details) van de sentiment analyse of de zoekmachines.

Tegenwoordig wordt de kritische burger en iedereen die op het internet actief is uit online en sociale media gevist. De sentiment analyse is onderdeel van de screening die de social media monitoring bedrijven uitvoeren. De verzamelde informatie en bijbehorende diensten worden net als in het verleden aangeboden aan bedrijven en overheidsdiensten. Social media monitoring bedrijven hebben de activiteiten van de private inlichtingendiensten omgevormd tot social media surveillance. Daarom toont de overheid zoveel interesse in de tools.

De basis van de social media surveillance zijn, naast live meekijken, de archieven van de bedrijven die bestaan uit grote hoeveelheden data met informatie over woon- en verblijfplaats, werk en andere persoonsgegevens. De bedrijven hebben geen toegang tot overheidsdatabanken als de Gemeentelijke Basisadministratie (GBA), maar veel basisgegevens over burgers kunnen ook worden verzameld via Facebook, Instagram, Google Streetview en Earth, Twitter en andere online diensten. Naast deze basisgegevens verzamelen de bedrijven ook allerlei berichten, meningen, opmerkingen, likes en andere meningsuitingen van burgers op het internet.

Reputatiemanagement bedrijven zijn in tegenstelling tot hun voorgangers (de private inlichtingendiensten) geaccepteerd. Was het twintig jaar geleden ondenkbaar dat Greenpeace een bedrijf als ABC of Global Open zou inhuren, tegenwoordig gebruikt de milieuorganisatie de social media monitoring tool van Coosto. Ook de Consumentenbond maakt gebruik van Coosto. Oxfam Novib huurt OBI4waan. Vice media Buzzcapture. Ook de Nederlandse politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) huren Coosto, OBI4wan, HowAboutYou en Buzzcapture in.

Die acceptatie blijkt uit de ontwikkelingen van de social media monitoring bedrijven waarbij universiteiten ook een belangrijke rol hebben gespeeld zoals blijkt uit de profielen van die bedrijven. Buzzcapture werkt samen met de Universiteit Utrecht. SiteData BV staat aan de oorsprong van OBI4wan en is op de campus van de Technische Universiteit Eindhoven gevestigd. HowAboutYou werkt weer nauw samen met OBI4wan. En Coosto komt voort uit Wiseguys Internet BV dat nauwe banden heeft met de Technische Universiteit Eindhoven.

WiseGuys Internet BV

Het moeder bedrijf van Coosto is WiseGuys Internet BV (Wg Holding B.V.). De website van het bedrijf bevat alleen een contactformulier. De pagina's 'about wiseguys, products en read full story' zijn leeg. Op LinkedIn staat dat het bedrijf gespecialiseerd is in "spider/webcrawler and search technology as well as data mining", ofwel het verzamelen van internet data en die doorzoekbaar maken. Het bedrijf is niet groot, opgericht in 1999 en gevestigd op het terrein van de Technische Universiteit Eindhoven.

De mensen achter WiseGuys Internet BV zijn sinds de jaren negentig actief in het ontwikkelen van de zoekmachine Track. In 1996 ging Toine Verheul met zijn bedrijf Radar Internet samenwerken met enkele studenten van de Technische Universiteit Eindhoven en Universiteit van Tilburg. Vier studenten schreven de software en Verheul wist als zakelijk leider uitgever Wegener Arcade in 1997 te overtuigen om de zoekmachine Track.nl te kopen. Verheul stapte ook direct over naar Koninklijke Wegener NV, een uitgever van regionale dagbladen, huis-aan-huisbladen en tijdschriften, die 2015 werd overgenomen door het Belgische mediabedrijf De Persgroep.

In 1999 wordt WiseGuys Internet BV opgericht door onder andere Verheul. Al die tijd hebben de ontwikkelaars van Track verder aan de zoekmachine gesleuteld. Frank Scheelen, een student in de jaren negentig die meewerkte aan de ontwikkeling van Track, geeft dat tegen voelspriet.nl medewerker Henk van Es in 2001 aan: "Track verandert vooralsnog alleen de indexeer- en zoeksoftware. Het

spideren, gebeurt op dit moment nog met dezelfde spiders die WiseGuys al langer gebruikten voor het vullen van de Track database." Hoeveel data WiseGuys Internet BV al in 2002 verzamelde geeft Scheelen in een interview in het Reformatorisch Dagblad aan. "De laatste keer kregen we, nadat we alle dubbele pagina's eruit gegooid hadden, 200 gigabyte aan data binnen." In hetzelfde jaar, 2002, lanceert WiseGuys Internet BV een nieuwe zoekmachine Kobala.

Met spiders bedoelt Scheelen programma's die lijken op browsers als Firefox, Chrome of Internet Explorer, maar die webpagina's niet alleen opzoeken maar ook downloaden. Daarnaast gebruiken de bedrijven ook crawlers die op internetpagina's op zoek gaan naar de verschillende links en die vervolgens ook bezoeken. In de Tech industrie worden de woorden spider en crawler vaak door elkaar gebruikt. Daarnaast wordt ook het woord robot gebruikt. Meestal verwijst dit naar de automatisering van zowel het zoeken op het internet, het opslaan, het crawlen en het indexeren van de opgeslagen pagina's.

Wiseguys Internet BV leidt een betrekkelijk anoniem bestaan. In 2003 komt het bedrijf nog even in het nieuws omdat adverteerders voor geld een topositie in de zoekresultaten kopen. Verheul zegt op emerce.nl dat "het idee om de resultaten te verkopen uit nood is geboren. De markt dwingt ons om met dergelijke oplossingen te komen." Emerce schrijft in het artikel 'Zoekmachine Track verkoopt topositie' op 15 mei 2003: "adverteerders invloed laten uitoefenen op de rangschikking wordt traditiegetrouw afgekeurd door de meeste zoekmachines, de 'objectiviteit' van de zoekresultaten is voor de meesten nog heilig."

WiseGuys Internet BV blijft zich richten op zoektechnologie en ontwikkelt ook zoekmachines voor Freeler, Ben, Genie en RDnet (Reformatorisch Dagblad net). De basis van alle zoekmachines van WiseGuys Internet BV vormt het programma Kobala. Scheelen beschrijft het proces van de zoekmachine in het Reformatorisch Dagblad van 21 mei 2002: "We gebruiken daarvoor een spider, een complex computerprogramma dat de tekst uit al die internetpagina's op onze harde schijven zet. ... We beginnen met webdirectories, sites die veel verwijzingen naar andere pagina's bevatten."

WiseGuys Internet BV heeft de webcrawler Vagabondo (zwerfer) genoemd.

Het ontstaan van Coosto

Met de zoektechnologie van Kobala ontwikkelt WiseGuys Internet BV een nieuwe tool: Bluescope. Bluescope is de voorloper van de reputatiemanagement tool Coosto die in 2010 op de markt werd gezet door het bedrijf Coosto, een dochter firma van WiseGuys Internet BV. WiseGuys Internet BV omschrijft BlueScope als een "een nieuwe vorm van automatische webanalyse die u helpt om de internetpositie van uw bedrijf en uw concurrenten in kaart te brengen."

Eind 2002 koopt het internetbedrijf Ilse (Ilse Media) de broncode van de zoekspider van WiseGuys Internet BV. Ilse Media, begin deze eeuw één van de voornaamste zoekmachines in Nederland is in 2001 overgenomen door Sanoma Media, eigenaar van onder andere nu.nl. Voor WiseGuys Internet BV was de zoektechnologie voor zoekmachines als gevolg van de opkomst van Google een markt waar niet veel meer te verdienen was. Wiseguys Internet BV richtte zich daarom met BlueScope op dienstverlening door middel van reputatiemanagement voor het bedrijfsleven.

Op 30 augustus 2010 presenteren de voormalig ontwikkelaars van de zoekmachine Track Rob de Wit en Frank Scheelen en zakelijk leider van WiseGuys Internet BV Toine Verheul de social media monitoring tool en het bedrijf Coosto. "We spideren de hele dag door. Dan heb je ook de linkstructuur en kun je kijken wie naar wie linkt. Dat kan een virtual host zijn, of een eigen host waar het blog op draait," vertellen de oprichters aan emerge.nl. Coosto beweert ook meteen dat ze "de grootste aantallen van bijvoorbeeld de WordPress-blogs hebben." Daarbij zou het niet alleen om nl domeinen (websites die eindigen op .nl) gaan, maar ook om org domeinen (websites die eindigen op .org). Het bedrijf zoekt dus niet

exclusief in Nederlandse sites. Dit blijkt ook twee jaar later wanneer het bedrijf in het Verenigd Koninkrijk uitbreidt.

Inlichtingen databank Coosto, eens getweet altijd bewaard

In 2010 zeggen De Wit, Scheelen en Verheul, de mannen achter Coosto, dat zij al dagelijks spideren: het internet afzoeken naar data. Ze vertellen er echter in het interview met emerce.nl niet bij dit ze dat al vanaf de jaren negentig doen, en voor Coosto sinds 1 januari 2009. Retecool (redacteur Ome MC) publiceert in juni 2016 een Coosto Open Factsheet waarin staat dat het historisch archief terugloopt tot januari 2009. Dit komt overeen met de gegevens uit de 'Uitgebreide verkenning van de Nederlandse markt voor online monitoring- en webcaretools' van de bedrijven Upstream en Repmen van november 2012: "Volume aan data, historisch archief vanaf januari 2009 (onafhankelijk van zoekterm), flexibele snelle manier van zoeken, diepgaande data-analyse."

In 2012 geven de eigenaren van Coosto aan het Eindhovens Dagblad ook aan dat ze allerlei informatie verzamelen over mensen in Nederland, zoals data over hoe oud hun keuken of cv-ketel is, en dat ze de data ook doorverkopen aan de politie. "Het bedrijf slaat onder meer informatie op over woningen en vacatures. De data (ook over details als ouderdom van cv-ketels, keukens e.d.) worden doorverkocht. Een deel is ook bestemd voor opsporingsdiensten. Die kunnen een archief doorzoeken waarvan de opbouw begon in januari 2009," aldus De Wit, Scheelen en Verheul in het Eindhovens Dagblad van 4 oktober 2012.

Retecool publiceerde een factsheet van Coosto naar aanleiding van een artikel van RTLZ, 'Op bezoek bij @NS_online: de 'meest gehate mensen' van Nederland', over het social media team van de Nederlandse Spoorwegen. De NS gebruikt ook de social media monitoring tool Coosto. In het artikel van RTLZ stelt de auteur dat hij ooit eens "een vervelende tweet over NS" geschreven had." Het blijkt dat de tweet door de sociale media afdeling van de NS nog ingezien kan worden: "De webcare medewerker leest die tweet voor. Ondanks dat deze tweet al tijden geleden is verwijderd."

In een disclaimer van Coosto staat dat "het bedrijf niet aansprakelijk is voor onjuistheden of onvolledigheden in de aangeboden inhoud." En klanten van Coosto vrijwaren "het bedrijf ... van gerechtelijke en buitengerechtelijke maatregelen en de kosten daarvan." Het verwijderde Twitter bericht van RTLZ journalist Daniël Verlaan is onderdeel van de disclaimer.

Coosto is de afgelopen jaren een groter bedrijf geworden dan het moederbedrijf WiseGuys Internet BV. Bij het bedrijf werken nu meer dan honderd mensen, waaronder systeembeheerders, ontwikkelaars, data scientists en hitmen. Volgens de Vastgoedcourant van april 2016 zou Coosto werkzaam zijn voor "meer dan 600 bedrijven." Niet alleen de Nederlandse Spoorwegen, Greenpeace en de Consumentenbond maken gebruik van Coosto. Ook Natuurmonumenten, Ziggo, Microsoft, FNV, CBS, Belastingdienst, ANWB, KWF Kankerbestrijding, Achmea Zorg en andere bedrijven en instellingen.

Overheidsorganen waaronder de politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) behoren ook tot de klantenkring. Zij hebben ook toegang tot een grote database van persoonsgegevens van het bedrijf en gebruiken Coosto voor social media surveillance. De politie heeft geen documenten openbaar gemaakt over de samenwerking met Coosto, de NCTV wel en omschrijft de diensten van Coosto als "webmonitoring/webanalysefunctionaliteiten en webcarefunctionaliteiten."

Coosto en de overheid

Het imago van Coosto leidt in 2013 even onder de negatieve publiciteit over het moederbedrijf WiseGuys Internet BV. De Telegraaf kopt op 18 september 2013 met 'Overheid doet zaken met pornoboer.' Het dagblad schrijft: "Wie zoekt naar seks met dieren, met oma's of zelfs naar gewelddadige verkrachtingen, komt bij de website askjolene.com goed aan zijn trekken. Vele duizenden filmpjes, verhalen en pornowebcams worden er in de meest bizarre rubrieken gepresenteerd." Twee dagen later worden er Kamervragen gesteld over het belang van WiseGuys in AJ Beheer B.V., het bedrijf dat de exploitatie verzorgt van de website AskJolene.com.

Op 18 september 2013 reageert algemeen directeur Toine Verheul van Coosto en WiseGuys Internet BV op de beschuldigingen. Verheul stelt op het blog van Coosto dat het bedrijf "in het verleden een belang heeft gehad in de erotische zoekdienst AskJolene.com." Het bedrijf heeft een dag eerder op 17 september 2013 haar aandeel in AJ Beheer BV verkocht, volgens een persbericht van Coosto.

Over het gebruik van Coosto door de politie worden in 2013 geen verdere Kamervragen gesteld. In de beantwoording van de Kamervragen schrijft de minister voor Wonen en Rijksdienst Blok dat "de politie en de ministeries alleen gebruik maken van de zoektechnologie van Coosto om binnen sociale netwerken te zoeken in openbare bronnen. Voor de ministeries is dit een activiteit vergelijkbaar met het maken van een knipselkrant. De ministeries voeren echter zelf het onderzoek uit." Uit de antwoorden wordt niet duidelijk wat de minister onder openbare bronnen en openbare bronnen op sociale netwerken verstaat.

Minister Blok bagatelliseert het werk van Coosto door de databank te vergelijken met een knipselkrant. In een publicatie van Upstream / Repmen de 'Monitoring- & webcaretools 2012 gids voor het managen van de online dialoog,' stelt Coosto in 2013 dat zij gegevens van Twitter, Facebook, LinkedIn, Hyves en Google+ constant doorzoekt en opslaat. De knipselkrant van Blok bevat gedetailleerde informatie van Nederlandse burgers, met onder andere de naam van de auteur, locatie en andere persoonsgegevens die sinds 1 januari 2009 door het bedrijf worden bewaard. Ook door burgers verwijderde berichten worden bewaard door Coosto.

In antwoorden op vragen van Buro Jansen & Janssen verwijst Coosto naar haar privacyverklaring en wenst het bedrijf geen uitspraken te doen over haar klanten en haar betrokkenheid bij social media surveillance. "Gezien de onderwerpen in uw mail zal ik deze beantwoorden. We vinden het belangrijk om hier transparant over te zijn. Er zijn ook zaken, zoals aangeven wie er nu wel of niet klant is dan wel is geweest, welke we niet mogen delen omdat we

dit met onze opdrachtgevers hebben afgesproken," schrijft het bedrijf.

Buzzcapture

Buzzcapture is in 2006 opgezet door politicoloog Alex van Leeuwen. In een interview in NRC Handelsblad van 1 augustus 2007 zegt hij dat het bedrijf zich "niet alleen bezig houdt met het in kaart brengen van klachten." De politicoloog gaat verder door te stellen dat "bedrijven vaak ook willen weten hoe ze hun dienstverlening kunnen verbeteren." Dat het bedrijf geen gewoon PR-bedrijf is maar zich als inlichtingenbedrijf presenteert, blijkt uit de woordkeuze. "Wij houden 600.000 Nederlandstalige weblogs in de gaten," zegt van Leeuwen.

Buzzcapture houdt echter niet alleen sites in de gaten, maar leest ook mee. "Per merk of dienst lezen we ook relevante discussieforums." Buzzcapture lijkt verder te gaan dan Coosto door ook deel te nemen aan online discussies. "Op verzoek nemen medewerkers van Buzzcapture ook deel aan discussies op weblogs en forums," aldus van Leeuwen. Dit lijkt op het inzetten van informanten/infiltranten door de oude private inlichtingendiensten alleen in een nieuw jasje gegoten, de undercover accounts. Van Leeuwen geeft in antwoord op vragen van Buro Jansen & Janssen in augustus 2017 echter aan geen gebruik te maken van 'schaduw/nepaccounts.'

Buzzcapture houdt niet alleen weblogs in de gaten maar verzamelt en bewaart net als Cosoto ook data. Buzzcapture is hier echter twee jaar eerder mee begonnen dan Coosto. "Doordat Buzzcapture vanaf 2007 een archief heeft opgebouwd van alles wat online en op social media wordt gepost, kunnen we voor het eerst data vergelijken voorafgaand aan de gemeenteraadsverkiezingen. In 2010 was dit nog niet mogelijk," schrijft Jaap van Zessen, voormalig Social Media Analist van Buzzcapture, trots op 18 maart 2014 op de website van het bedrijf.

Van Zessen suggereert dus dat het bedrijf al sinds 2007 persoonsgegevens verzamelt en dat Buzzcapture misschien de gemeenteraadsverkiezingen van 2014 kan voorspellen. Volledig naar

analogie met de knipselkrant van minister Blok schrijft van Zessen dat "Buzzcapture het online archief afstofte en op zoek ging naar data in de eigen tool." Van Zessen bedoelt met afstoffen dat het bedrijf in 2014 alle data van de afgelopen jaren ging gebruiken voor het voorspellen van de gemeenteraadsverkiezingen van 2014.

Volgens van Leeuwen gebruikt Buzzcapture naast technologie ook medewerkers om de verzamelde data te analyseren en te interpreteren. Buzzcapture gebruikt de 'spider' van WiseGuys Internet BV en een andere technische tool, een semantische zoekmachine van Textkernel. In een artikel op emergc.nl van 18 april 2007 geeft van Leeuwen aan dat zijn bedrijf de twee technologieën van Wiseguys Internet BV en Textkernel aan elkaar koppelt.

In antwoord op vragen van Buro Jansen & Janssen in augustus 2017 stelt Buzzcapture dat zij "geen data beschikbaar aan Nederlandse opsporings- en inlichtingendiensten" stellen en tevens "geen oplossing voor opsporing of surveillance" bieden. De directeur van het bedrijf, Alex van Leeuwen, gaat verder door te stellen dat de "dienstverlening zich beperkt tot het faciliteren van corporate communicatie en webcare afdelingen." Uit openbaar gemaakte documenten naar aanleiding van Wob verzoeken van Buro Jansen & Janssen blijkt dat Buzzcapture de communicatie van de Nationale Politie verzorgt. De politie vraagt om "realtime social media analyseren, inzicht in sentimenten, geolocatie, stakeholders, en toegang tot historie/archief."

Universiteiten: Data van scholen

De technologie achter de software van Coosto is in de jaren negentig ontwikkeld door vier studenten van de Technische Universiteit Eindhoven en de Universiteit van Tilburg: Robert Brouwer, Pim van Pelt, Frank Scheelen en Rob de Wit. De laatste twee zijn anno 2017 nog werkzaam bij Coosto. Robert Brouwer is vertrokken naar Oracle en Pim van Pelt naar Google.

Het is opvallend dat meerdere universiteiten een relatie hebben met social media monitoring bedrijven. Coosto en Wiseguys Internet BV waren nauw verbonden met de Universiteit Tilburg en vooral de

Universiteit van Eindhoven, zowel wat betreft de ontwikkeling van de zoekmachine/spider/crawler als wat betreft het vestigingsadres. De Technische Universiteit Eindhoven noemt Coosto in haar campus folder: "Al ruim dertig jaar initieert en faciliteert de TU/e daarom startende bedrijven. Dat leidde tot het ontstaan van meer dan 150 technologiebedrijven, waaronder succesvolle namen zoals: Prodrive, Coosto, Xeltis en Flowid." Ook SiteData BV, het bedrijf waaruit OBI4wan uit voortkomt, is gevestigd op de campus van de Technische Universiteit Eindhoven.

Thomas Boeschoten van de Universiteit Utrecht werkt samen met Buzzcapture dat door de universiteit wordt gepresenteerd als technische partner. Boeschoten gebruikt bij zijn experiment rond de Nuclear Security Summit (NSS) data van Buzzcapture, die volgens het artikel 'Plaats delict: social media' van Vrij Nederland van 18 april 2014 door het bedrijf zijn verzameld. "Het bedrijf Buzzcapture heeft al wekenlang alle tweets en Facebook-updates verzameld en voor de deelnemers in een database gezet." Boeschoten zegt in het artikel niet dat Buzzcapture in 2014 al een database met gegevens van online en social media over Nederlandse burgers van zeven jaar heeft.

Boeschoten wordt door Vrij Nederland gepresenteerd als 'een deskundige op het gebied van social media en dataverwerking.' In 2014 leidt hij een experiment om met behulp van social media monitoring de ontwikkelingen rond de NSS in de gaten te houden. Bij het experiment schuiven politiemensen aan. Hierdoor ontstaat het idee dat het gaat om handhaving van de openbare orde. Dat blijkt ook uit het artikel in Vrij Nederland. Het gaat vooral over het in de gaten houden van burgers en actiegroepen die zich kritisch hebben uitgelaten over de NSS, met daardoor gevolgen voor zowel burgerrechten als bewegingsvrijheid van die burgers. Buro Jansen & Janssen heeft al eerder geschreven over het ontbreken van het demonstratierecht tijdens de NSS.

Dat social media surveillance ook wordt ingezet bij onder andere demonstraties blijkt ook uit de openbaar gemaakte documenten naar aanleiding van de Wob-verzoek van Buro Jansen & Janssen. Zo is de tool van OBI4wan door de politie eenheid Zeeland-West-Brabant ingezet tegen een pro-Gaza demonstratie. Bij de inzet van social media surveillance zijn duidelijk grondrechten als de vrijheid

van meningsuiting en de vrijheid van demonstratie in het geding. Opmerkelijk genoeg plaatst Boeschoten van de Universiteit Utrecht hier zelf ook vraagtekens bij. In het Vrij Nederland artikel merkt Boeschoten op: "Het gekke is: als ik het zelf doe, vind ik het helemaal niet eng, maar als ik bedenk dat anderen het ook kunnen doen, vind ik het wel verontrustend. Dergelijke netwerkanalyses worden pas echt boeiend als je de informatie koppelt aan metadata die niet openbaar toegankelijk is, als je bijvoorbeeld op hetzelfde moment kunt zien wie met wie belt. Of wie naar wie privéberichten stuurt, zoals de NSA en het Britse GCHQ dat kunnen." Boeschoten doelt met de verwijzing naar de NSA en GCHQ op de massale surveillance die door de onthullingen van Edward Snowden aan het licht kwam.

De social media monitoring tools kunnen echter ook al veel. Zo beschikt Buzzcapture over ongeveer dezelfde bronnen en mogelijkheden als Coosto. In het factsheet uit de 'Monitoring- en webcaretools' van november 2014 van Upstream geeft het bedrijf aan dat zij de volgende bronnen rond de klok monitort: "print, nieuws, fora, blogs, websites video (Youtube), radio/TV, twitter, Facebook, Instagram, Pinterest, LinkedIn, Google+ en Hyves." Het bedrijf geeft aan dat er historische analyses gemaakt kunnen worden "van data voorafgaand aan de datum waarop je de tool bent gaan gebruiken." Daarnaast staat bij analyse en selectiemogelijkheden onder andere: "de auteur (profiel), de invloed van auteur, de locatie (GPS/Geo), likes/RT's/Favorites, sociale netwerk, sentiment."

Naast Coosto en Buzzcapture, doet de politie in ieder geval zaken met twee andere social media monitoring bedrijven, OBI4wan en HowAboutYou. Deze bedrijven beschikken over vergelijkbare mogelijkheden en bronnen.

OBI4wan

Het Zaanse bedrijf OBI4wan is opgericht in 2011, maar is al sinds 2009 actief met het verzamelen van online en social media data, reputatiemanagement en webcare. OBI4wan komt voort uit het bedrijf SiteData B.V. dat in 2001 werd opgezet door Alex Slatman.

In dat jaar begon Slatman met de studie Information Retrieval aan de Radboud Universiteit Nijmegen die hij in 2006 afrondde. Slatman werkte tijdens zijn studietijd aan de ontwikkeling van een eigen spider. Vervolgens was hij in 2006 kort werkzaam voor Ilse Media, dat vier jaar eerder een samenwerking was aangegaan met WiseGuys Internet B.V.

Volgens de website van SiteData biedt het bedrijf vanaf 2007 "een breed scala aan producten aan die bijdragen aan een betere vindbaarheid voor uw website." Daarnaast is SiteData ook "actief op het gebied van datamining en information retrieval." SiteData biedt een imago management aan dat er vanuit gaat dat ranking in zoekmachines de strijd met de concurrentie beslechten. Vandaar ook dat het bedrijf diensten aanbiedt als "positiemeting (op basis van zoektermen bekijken wij hoe goed u te vinden bent in Google) en concurrentiecheck (op deze manier kunt u snel zien op welke termen u beter of slechter scoort ten opzichte van uw concurrentie!)."

SiteData is gevestigd op het terrein van de Technische Universiteit Eindhoven. In 2010 ontmoette Slatman Alexander de Ruijter, een consultant met een eigen bedrijf in voorlichting over gebruik van sociale media in het bedrijfsleven. Het klikte tussen Slatman en de Ruijter en in 2011 begonnen zij OBI4wan dat zich richt op reputatiemanagement en webcare.

Bij de lancering van Obi4wan in 2011 waren er drie klanten: ECI, EnergieDirect en Arriva. In 2012 komen daar verschillende nieuwe klanten bij, waaronder de eenheid Zeeland-West-Brabant van de Nationale Politie. Het LinkedIn bedrijfsprofiel van OBI4wan vermeldt: "Sinds 2009 worden alle relevante berichten verzameld van bekende social media platformen en miljoenen (inter)nationale blogs, fora en nieuwsbronnen. Aangevuld met innovatieve oplossingen voor radio-, tv- en printmonitoring mis je nooit meer een relevant bericht!" Het bedrijf verzuimt hier overigens te vermelden dat het ook data van LinkedIn verzamelt.

De data die OBI4wan verzamelt komen van ' 400.000 Nederlandstalige bronnen ' schrijft het bedrijf in een presentatie in 2014 (In 2012 waren dit er nog 350.000). OBI4wan gebruikt vergelijkbare bronnen als Coosto en Buzzcapture. Het gaat om radio en TV, nieuwspagina 's, fora, blogs, Youtube en andere video sites,

afbeeldingen platformen, Twitter, Facebook, en andere social media platformen.

HowAboutYou

HowAboutYou is een zelfstandig reputatiemanagement bedrijf, maar richt zich volledig op de inzet van de OBI4wan tool. OBI4wan geeft in de factsheet uit de 'Monitoring- en Webcaretools' van november 2014 van Upstream aan dat het samenwerkt met HowAboutYou, Engagement Media, Red Banana en Wisse Kommunikatie. Dat OBI4wan nauw samenwerkt met HowAboutYou blijkt ook uit documenten die door de politie openbaar zijn gemaakt over de twee bedrijven. Op haar website schrijft HowAboutYou over OBI4wan: "Een goede mediamonitor helpt enorm. Wij kiezen voor OBI4wan."

HowAboutYou werd in 2010 opgericht. Op de eerste website van het bedrijf in juni 2011 worden Ewoud de Voogd, Paul Suijkerbuijk en Frank Bruijninx vermeld als de drijvende krachten. Bij de nominatie van het bedrijf voor de 'Grote nieuwe organiseren prijs' ("De prijs is voor de persoon of organisatie die het beste het gedachtegoed van nieuw organiseren belichaamt en realiseert," aldus nieuworganiseren.nu) in 2014 staat dat Voogd en Bruijninx "merkten dat de overheidscommunicatie niet aansloot op de huidige tijd." HowAboutYou ging zich dan ook richten op de overheid.

Op haar LinkedIn pagina stelt het bedrijf uit het Gelderse Rossum dat het zich bezighoudt met de ondersteuning van "ruim 300 overheden bij de inzet van social media, webcare & monitoring met OBI4wan, omgevingsanalyses, issue- en reputatiemanagement en online campagnes." Op de website van het bedrijf staan de namen van 179 gemeenten, zes provincies en bijna alle veiligheidsregio's (brandweer, geneeskundige diensten gemeenten en politie) vermeld als klant van HowAboutYou.

In een memo van 17 september 2013 aan het Kernteam social media politie Zeeland-West-Brabant gebruikt het bedrijf de kop 'HowAboutYou heeft ervaring met het ondersteunen van (politie-)processen.' Volgens HowAboutYou moet "een online media monitor niet alleen aan technische functionele eisen voldoen

(zoektermen aanmaken, reageren) maar ook ondersteuning bieden bij de processen van de organisatie zoals opsporing, intelligence, participatie- en beleidsvormingstrajecten. De eerder opgenomen tabel biedt een overzicht van processen die de online media monitor ondersteunt." HowAboutYou gebruikt OBI4wan, maar op haar website en uit de openbaar gemaakte stukken wordt niet duidelijk of het bedrijf kennis heeft over de technische werking van de tool, de sentiment analyse, en het historisch archief.

In dezelfde memo 'Voorstel opzet proef online media monitoring en webcare' schrijft het bedrijf dat het allerlei ervaring heeft op het terrein van veiligheid. "HowAboutYou werkt op online media monitoring en vooral de aanpak en organisatie daarvan samen met de gemeenten Breda, Tilburg (oa ook de TaskForce Tilburg Veilig), ... en de veiligheidsregio Midden-West-Brabant." De memo vermeldt tevens: "HowAboutYou ondersteunde met media-analyses bij de brand in Oosterhout en het TGO na de rellen in Haren met rechercheonderzoeken op de online media."

Archieven zijn Big Business

De Nationale Politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) werken samen met Coosto, OBI4wan, HowAboutYou en Buzzcapture. De politie gebruikt de diensten van de bedrijven niet alleen voor haar eigen communicatiebeleid (Buzzcapture) en de contacten met burgers, maar ook voor ondersteuning bij meldingen, aangiften, handhaving, Real Time Intelligence Center en opsporing (Coosto, OBI4wan en HowAboutYou). In 2013 antwoordde de minister voor Wonen en Rijksdienst Blok dat de politie en de ministeries slechts gebruikmaakten van de zoektechnologie van Coosto. Uit de Wob-stukken blijkt echter dat Coosto, evenals OBI4wan en HowAboutYou, wordt ingezet voor social media surveillance.

Die interesse in de databanken en de social media monitoring tools komt niet alleen van de overheid, maar ook van investeerders. Dat blijkt uit ontwikkelingen in de Verenigde Staten en in Nederland. In de Verenigde Staten werkt het social media monitoring bedrijf Geofeedia samen met een internationaal bedrijf, Everbridge, om

haar marktbereik te vergroten. Een ander bedrijf Snap Trends werkt samen met een groot private military contractor Chenega. De tools en databanken zijn belangrijke bezittingen van de bedrijven. Zo is het Amerikaanse Intrado overgenomen door het grote beursgenoteerde West Corporation, en vervolgens West Corporation door het hedgefonds Apollo Global Management.

De ontwikkelingen van internationalisering en overnames zijn ook in Nederland zichtbaar, maar vooralsnog op beperkte schaal. De eerste overname vond plaats in 2017 toen Buzzcapture werd overgenomen door OBI4wan. Buzzcapture probeert zelf het nieuws positiever te brengen door te stellen dat 'OBI4wan en Buzzcapture krachten bundelen.' Die overname wordt gefinancierd door Main Capital Partners B.V., een Nederlandse investeerder in de IT industrie. Regelmatig verkoopt het zijn belangen door aan grotere investeerders, dit kan in de toekomst dus ook gebeuren met het meerderheidsaandeel in OBI4wan.

OBI4wan was voor de overname van Buzzcapture een betrekkelijk kleine speler. De overname kwam echter niet als een verrassing omdat het bedrijf al in juli 2016 in zee was gegaan met Main Capital. De investeerder schrijft op haar website dat "Main Capital OBI4wan en OBILytics actief gaat ondersteunen met de internationale groei en de uitbouw van de productportfolio, onder meer door selectieve internationale acquisities." Main Capital omschrijft OBI4wan als een snelgroeiend bedrijf. Naast kennis en inzicht over de analyse-tools zal OBI4wan interesse hebben gehad in de klanten en de grotere database van Buzzcapture. Gezien de ontwikkelingen in de Verenigde Staten en Nederland is het reëel dat de archieven van de Nederlandse social media monitoring bedrijven op termijn in buitenlandse handen terecht komen.

Overheidssteun social media surveillance industrie

Ook overheden maken onderdeel uit van de social media surveillance industrie. Niet alleen als afnemers van de diensten, maar tevens als geldschieter. In de Verenigde Staten is bekend geworden dat diverse social media monitoring bedrijven zoals Geofeedia, Pathar en Dataminr worden gefinancierd door de

investeringsmaatschappij van de CIA: In-Q-Tel (In-Q-It). In hoeverre de CIA toegang heeft tot de data van die bedrijven, is niet bekend.

Of de Nederlandse inlichtingendiensten investeren in social media monitoring bedrijven als Coosto, OBI4wan en Buzzcapture wordt niet duidelijk uit de documenten. Wel op andere manieren is er overheidssteun voor de social media surveillance industrie.

Universiteiten ondersteunen de ontwikkeling van tools om online en social media gegevens te verzamelen en op te slaan. Ook wordt aan startups huisvesting aangeboden op campussen van universiteiten. Zo breidde Coosto in 2015 uit naar 150 talen en financierde dit uit eigen middelen. Het bedrijf was in staat dit te doen omdat het een groot deel van haar bestaan geholpen is door de TU Eindhoven die Coosto als startup op de campus liet groeien.

Ook het Ministerie van Veiligheid en Justitie heeft Coosto financieel ondersteund door in 2011 geen aanbesteding te doen, losse accounts af te nemen en vervolgens de aanbestedingsgrens te overschrijden. De Nationaal Coördinator Terrorisme en Veiligheid (NCTV) wilde de tool van Coosto blijven gebruiken terwijl de aanbestedingsgrens was overschreden, blijkt uit openbaar gemaakte documenten via een Wob-verzoek van Buro Jansen & Janssen bij het ministerie van Veiligheid en Justitie. De aanbestedingsgrens is de grens waarboven publiek opdrachten openlijk moeten worden gedaan, zodat ieder bedrijf kan meedingen naar die opdracht.

In 2013 schrijft een ambtenaar van het ministerie van Veiligheid en Justitie nog: "Binnen de kaders van het recent gewijzigde inkoopbeleid van VenJ c.q. Rijksbreed zie ik, na controle, geen beperkingen om de overeenkomst met Coosto te verlengen. Het VenJ inkoopbeleid schrijft voor dat er pas boven de 50K concurrentie gesteld dient te worden zie bijlage." Het contract dat het ministerie met Coosto sloot was een "vierjarige overeenkomst met een eventuele verlenging voor het jaar 2016." Dit herhaalt zich in 2014. In 2015 gaan de alarmbellen rinkelen.

Op 28 april 2015 schrijft een ambtenaar: een "volgende verlenging zal er voor zorgen dat de grens voor Europees aanbesteden bereikt gaat worden." Het contract van de NCTV loopt af op 31 december

2015. Toch is het ministerie Coosto blijven gebruiken hoewel in de correspondentie van februari 2016 staat dat het "allemaal moeilijker dan gedacht wordt want, jawel, we gaan met de factuur die nog betaald moet worden dit jaar de aanbestedingsgrens over. Dat betekent dat we de factuur die nu nog ligt niet kunnen betalen." Er wordt geconcludeerd dat er voor 2016 "al een nota onrechtmatigheid opgesteld moet worden."

Hoewel het ministerie verschillende documenten openbaar heeft gemaakt is er nog veel geheim. Uit de openbaar gemaakte documenten blijkt dat de NCTV in 2016 en in 2017 Coosto is blijven gebruiken. Op 17 april 2017 meldt een ambtenaar: "Coosto schijnt handig overal losse accountjes te verkopen en het is waarschijnlijker goedkoper om één aanbesteding te doen." Niet alleen via het vermijden van de aanbesteding, maar ook via extra accounts ondersteunt het ministerie van Veiligheid en Justitie Coosto.

Transparantie bij Surveillance

De social media monitoring tools worden door de politie en de NCTV ingezet voor social media surveillance doeleinden. Uit openbaar gemaakte documenten wordt duidelijk dat Coosto, Obi4wan en HowAboutYou hiervoor zijn ingezet. Over Buzzcapture is dit niet bekend. HowAboutYou heeft geen eigen technologie en gebruikt exclusief OBI4wan. Buro Jansen & Janssen heeft de betreffende bedrijven gevraagd naar de samenwerking met politie en de NCTV.

Twee vragen hadden expliciet betrekking op de samenwerking. "Werkt of werkte u samen met de Nationale politie?" En "wordt of werd de tool van u door de NCTV gebruikt?" Daarnaast vroeg Buro Jansen & Janssen naar de inzet van de tools. "Wij begrijpen dat uw tool bij de politie is ingezet bij in ieder geval het RTIC, opsporing en andere processen. Is dit juist of niet? Ziet u deze overheidsactiviteiten als surveillance van burgers door de overheid?" Tevens vroeg Buro Jansen & Janssen naar de archieven en de verwerking van persoonsgegevens. " U heeft een databank die teruggaat tot 2007/2009. Ziet u die data als persoonsgegevens? Hebt u de verwerking van die persoonsgegevens aangemeld bij de bevoegde instanties en wanneer en wordt daar een regelmatige

audit op uitgevoerd? Houdt u zich aan de wettelijke bewaartermijnen? Wordt informatie die door burgers op online en sociale media zelf wordt verwijderd ook uit uw archief verwijderd?" Tot slot vroeg Buro Jansen & Janssen naar de sentiment analyse en nep- of schaduwaccounts. "In uw tool maakt u gebruik van een zogenaamde sentiment analyse. Maken de politie en de NCTV ook gebruik van die sentiment analyse? Hoe nauwkeurig is die? Is er wetenschappelijk onderzoek dat die nauwkeurigheid bevestigt? Is dat openbaar?" En "Maakt u gebruik van nepaccounts op social media platformen om informatie te verzamelen? Of spreekt u van schaduwaccounts?"

Buzzcapture is zeer stellig door te antwoorden dat het "geen data beschikbaar stelt aan Nederlandse opsporings- en inlichtingendiensten en geen oplossing bieden voor opsporing of surveillance." Het bedrijf geeft aan dat het slechts tools levert voor "corporate communicatie en webcare." "Onze oplossingen worden niet door NCTV gebruikt. Onze oplossing worden ook niet voor opsporing- of inlichtingendiensten gebruikt," stelt het bedrijf. De Nationale Politie gebruikt Buzzcapture voor communicatiedoeleinden, en de politie wil daartoe "realtime social media analyseren, inzicht in sentimenten, geolocatie, stakeholders, en toegang tot historie/archief," blijkt uit openbaar gemaakte documenten. Uit de bedrijfsgegevens blijkt tevens dat Buzzcapture wel degelijk sentiment analyse en een historisch archief aanbiedt, data die teruggaan tot 2007. Het bedrijf stelt ook nog dat ze "communicatieafdelingen inzicht geven in wat er speelt rond hun organisatie in de publieke sfeer."

OBI4wan antwoordt dat hun reputatiemanagement en webcare tools "niet bedoeld zijn voor surveillance van individuen en daar ook niet voor gebruikt mogen worden." Het bedrijf zegt dat zij geen uitspraak mag doen over het al dan niet samenwerken met de Nationale Politie. Of OBI4wan tools dus door de politie voor social media surveillance doeleinden wordt gebruikt laat het bedrijf in het midden. Op de vraag of de tool van het bedrijf wordt ingezet bij het RTIC, de opsporing en of het bedrijf deze overheidsactiviteiten ziet als surveillance van burgers, antwoordt OBI4wan dat zij daar "geen uitspraak over doen." Het bedrijf antwoordt nog wel dat zij "geen data meer aanbieden die terug gaan tot 2009," maar of de politie toegang heeft tot historische data laat het bedrijf ook in het midden.

Uit de openbaar gemaakte documenten blijkt dat de politie daar wel toegang toe heeft. OBI4wan is het enige bedrijf da ingaat op de vraag over de sentiment analyse. Het bedrijf antwoordt, "niet van toepassing."

Transparantie van Coosto

Coosto antwoordt dat het bedrijf transparant wil zijn over de samenwerking met de overheid en social media surveillance. Het bedrijf verwijst naar haar privacyverklaring. "Zaken zoals de doorgifte van data aan derden en rechten die over de verzamelde data uitgeoefend kunnen worden, worden hierin tevens besproken," schrijft het bedrijf. Daarnaast verwijst Coosto naar haar persbericht van 29 juni 2017 waarin het bedrijf stelt dat het zich in de toekomst aan de voorwaarden van de social media platforms gaat houden. Het bedrijf schrijft in antwoord op vragen van Buro Jansen & Janssen dat in dat persbericht zij "hun standpunt rondom surveillance delen." In het persbericht geeft Coosto echter niet haar eigen standpunt ten aanzien van surveillance, maar dat van Facebook. "For example, the current conditions of Facebook state that Facebook data can't be used for surveillance purposes."

Het bedrijf antwoordt ook niet op de vraag of het voor de politie en de NCTV werkt. Coosto sluit de korte e/mail naar aanleiding van vragen van Buro Jansen & Janssen af met de opmerking dat het bedrijf "de voorwaarden van onze partners volgen (zoals Twitter en Facebook etc.) in combinatie met ons moreel kompas en regelgeving."

Buro Jansen & Janssen heeft ook Wob verzoeken ingediend bij zowel de politie als het Ministerie van Veiligheid en Justitie over de samenwerking met Coosto. Het Ministerie informeerde Buro Jansen & Janssen dat een belanghebbende in december 2016 een zienswijze op de openbaar te maken documenten had ingediend. De ambtenaar van het ministerie gaf telefonisch aan dat de indruk bestond dat deze belanghebbende tegenstander van openbaarmaking van documenten was. Deze belanghebbende kondigde aan ook in bezwaar te gaan tegen de beslissing van het ministerie om de stukken openbaar te maken.

Bij de Wob verzoeken ging het naast Coosto om enkele andere bedrijven. De documenten die het ministerie uiteindelijk openbaar maakte hadden in het algemeen betrekking op Coosto. Op 17 augustus 2017, bij het bezwaar op de beslissing, maakte het ministerie bekend dat Coosto op 15 februari 2017 een zienswijze had ingediend. Coosto heeft uiteindelijk geen bezwaar ingediend. Coosto verzette zich dus in eerste instantie tegen openbaarmaking.

Social media surveillance is een publiek private samenwerking. De politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) zijn afhankelijk van commerciële tools die beschikbaar worden gesteld door bedrijven als Coosto, OBI4wan, HowAboutYou en Buzzcapture. Alle vier de tools worden gebruikt voor communicatie doeleinden. Van Coosto, OBI4wan en HowAboutYou is ook bekend dat de politie en de NCTV ze gebruikt voor social media surveillance en de opsporing.

Daar waar in het verleden private inlichtingendiensten werden gezien als enigszins obscuur, zijn reputatiemanagement of risicomangement bedrijven volledig geaccepteerd. Zij worden door diverse overheidsorganen ingehuurd. Het feit echter dat bedrijven en de overheid weinig transparant zijn over social media surveillance geeft aan dat er in twintig jaar niet veel is veranderd. De reputatiemanagement bedrijven verschillen niet van de obscure private inlichtingendiensten uit het verleden.

[Reputatie management bedrijven, de nieuwe private inlichtingendiensten](#) (pdf)

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

Andere artikelen

[Social Media Surveillance in Nederland](#)

[Dagelijkse en structurele monitoring; De Nederlandse politie en social media surveillance](#)

[De burger als dreigingscore; 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

[Overheid ontmoedigde het protest rondom NSS-top](#)

[Wijkagent: Gaat u soms naar de NSS-top?](#)

[Beroepsverbod voor familielid activiste](#)

[De Telegraaf, Milieudefensie, en de oud papier-affaire](#)

[Liefdewerk, oud papier](#)

Bijlagen

AIVD

[AIVD besluit Global Open.pdf](#)

[ukhomeaffairscommitteeundercoverpolicingglobalopenmarkkennedy.pdf](#)

Coosto

[Product Changes Coosto 29 juni 2017 \(pdf\)](#)

[vragen aan Coosto \(pdf\)](#)

[antwoorden coosto \(pdf\)](#)

[vragen aan Wiseguys \(pdf\)](#)

[factsheet Coosto november 2014 \(pdf\)](#)

[Coosto Open factsheet NL 2014 \(pdf\)](#)

OBI4wan

[vragen aan OBI4wan \(pdf\)](#)

[antwoorden OBI4wan \(pdf\)](#)

[vragen aan Sitedata \(pdf\)](#)

[factsheet OBI4wan november 2014 \(pdf\)](#)

Buzzcapture

[vragen aan Buzzcapture \(pdf\)](#)

[antwoorden van Buzzcapture \(pdf\)](#)

[factsheet Buzzcapture november 2014 \(pdf\)](#)

Reputatiemanagement bedrijven

[reputatiemanagement bedrijven factsheets 2014 \(pdf\)](#)

[reputatiemanagement bedrijven 2012 \(pdf\)](#)

[Monitoring webcare tools 2012 \(pdf\)](#)

Politie

[politie besluit OBI4wan HowAboutYou \(pdf\)](#)

[politie besluit OBI4wan online media monitoring tool en proces \(pdf\)](#)

[politie besluit Buzzcapture \(pdf\)](#)

Ministerie van Veiligheid en Justitie

[besluit ministerie van V en J Coosto Buzzcapture primair \(pdf\)](#)

Autoriteit Persoonsgegevens

[persoonsgegevens op internet 2007 \(pdf\)](#)

[brief aan Autoriteit Persoonsgegevens \(pdf\)](#)

[aanvullende brief aan Autoriteit Persoonsgegevens \(pdf\)](#)

[Autoriteit Persoonsgegevens antwoord \(pdf\)](#)