MASTER'S THESIS

Verstoren van criminele activiteiten op het dark web.

Een onderzoek naar de verenigbaarheid met het recht op privacy uit artikel 8 EVRM

Trommelen, K.

Award date:
2022

Awarding institution:
Department of Public Law

Link to publication

Verstoren van criminele activiteiten op het *dark web*.

Een onderzoek naar de verenigbaarheid met het recht op privacy uit artikel 8 EVRM

Naam: Karin Trommelen
Studentnummer: 839085815
Scriptiebegeleider: Dhr. prof. dr. W. P. Stol en mw. mr. S. Naber
Examinator: Mw. mr. dr. L. Strikwerda
Aantal woorden: 12.948
Inleverdatum: 10 mei 2022

VOORWOORD

Voor u ligt mijn masterscriptie welke ik heb geschreven ter afronding van de opleiding Rechtsgeleerdheid aan de Open Universiteit. Voor deze scriptie heb ik deelgenomen aan de projectgroep *Police Detectives on the Tor Network (PDTOR),* een projectgroep van het Cyber Science Center, en heb ik onderzocht in hoeverre de verstorende activiteiten door de politie van criminele werkzaamheden op het *dark web*, welke bijvoorbeeld ingezet kunnen worden als er geen opsporingsbevoegdheid is, in strijd zijn met het recht op privacy uit artikel 8 EVRM.

Ruim vijftien jaar geleden ben ik vol goede moed aan deze opleiding begonnen, in eerste instantie aan de Universiteit van Tilburg, drie avonden per week in de collegebanken, naast een fulltime baan. Dat heb ik vier jaar volgehouden. Ik was halverwege de bachelor toen ik er geen zin meer in had en ik besloot te stoppen. Maar na een jaar of twee begon het weer te kriebelen en wilde ik toch graag mijn mastertitel halen, maar wel met iets meer vrijheid. Dus de overstap gemaakt naar de Open Universiteit. Maar dat bleek wel heel vrijblijvend te zijn en voor dat ik het wist waren er weer een aantal jaren voorbij voordat ik dan eindelijk aan het integratiepracticum ter afsluiting van de bachelor mocht deelnemen. Dat ging ook niet zonder slag of stoot en na twee pogingen heb ik een mail naar de begeleider gestuurd met de mededeling dat ik er mee stop. Dat was niet de bedoeling en met heel veel overredingskracht heeft hij er tenslotte voor gezorgd dat ik voor een derde poging ben gegaan en dit keer lukte het wel. Ik had mijn bachelor gehaald en daar zou ik het bij laten. Maar dan sta je daar, bij de diploma-uitreiking, zo'n trots gevoel dat het was gelukt, ik werd weer enthousiast. Nog diezelfde avond heb ik me ingeschreven voor de master.

September 2020 ben ik gestart met deze afstudeerscriptie, met het goede voornemen om het in een half jaar tijd af te ronden. We zijn nu anderhalf jaar verder, corona gooide roet in het eten. Daar zat ik thuis met een basisschoolkind dat ik onderwijs moest geven, naast mijn baan en deze scriptie. Bijna in tranen heb ik op een gegeven moment mevrouw Naber gebeld, dit ging hem niet worden. Gelukkig was ze erg begripvol en mocht ik voor enkele maanden een pauze inlassen. Daarna heb ik het weer opgepakt, maar corona was echter nog steeds niet voorbij en na enkele quarantaine verplichtingen en nog een schoolsluiting, is het tenslotte toch gelukt mijn scriptie af te ronden. Zeker ook door de hulp van mijn scriptiebegeleiders, die regelmatig stukken van mij doorlazen en van commentaar voorzagen, meerdere keren een online sessie via teams welke naast leerzaam ook gezellig waren. Mevrouw S. Naber en de heer W. Stol, heel erg bedankt hiervoor.

Daarnaast wil ik ook mijn ouders bedanken, die vele malen op mijn zoontje hebben gepast, zodat ik bij hen op zolder kon werken aan mijn scriptie. En mijn vriend, die vrijwel iedere zondagmiddag met ons zoontje op pad ging, zodat ik het huis voor mijzelf had en in alle rust enkele uren aan mijn scriptie kon schrijven.

Ik wens u hierbij veel leesplezier.

Karin Trommelen

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Dagelijks wordt er op grote schaal gebruik gemaakt van het internet. Het gedeelte van het internet dat voor de meeste internetgebruikers toegankelijk is, is het *surface web*. Het *surface web* is geïndexeerd en doorzoekbaar via diverse browers zoals Safari, Edge en Firefox.[1]

Het *surface web* is ongeveer 10% van het gehele internet, daarnaast kent het internet nog het *deep web* en het *dark web*. Het *deep web* is het gedeelte waar niet iedereen toegang toe heeft, alleen met behulp van inloggegevens is het toegankelijk, zoals bijvoorbeeld bankrekeningen, medische gegevens et cetera. Het *dark web* is een ander verhaal omdat het niet te bereiken is via de gebruikelijke browsers zoals Safari, Edge en Firefox. Om toegang te krijgen tot het *dark web* is een andere browser nodig dan voor het *surface web*. Een heel bekende is de Tor-browser: The Onion Router, welke door iedereen te downloaden is. Met deze browser kunnen op het *dark web* sites gevonden worden met het achtervoegsel *.onion.*[2]
Het gebruik van een Tor-browser of surfen op het *dark web* is in geen enkele wettelijke bepaling strafbaar gesteld, het is niet verplicht dat je online traceerbaar bent en daarnaast is niet alles wat op het *dark web* gebeurt illegaal.[3] Hieruit kan geconcludeerd worden dat het downloaden van een Tor-browser en vervolgens webpagina's bezoeken op het *dark web* niet illegaal is, met uitzondering van het bezoeken van kinderpornosites hetgeen wel strafbaar is. Bij gebruik van de Tor-browser worden gegevens versleuteld verstuurd, maar ook verstuurd via tussenstations. Hierdoor kunnen berichten anoniem verstuurd en websites anoniem bezocht worden zolang men zelf zijn of haar identiteit niet onthult zodat niet te zien is van welk ip-adres berichten verstuurd worden. Dat maakt het *dark web* ideaal voor journalisten en mensen die leven onder een dictatoriaal regime waardoor hun vrijheid beperkt is. Facebook heeft op het *dark web* een *mirror* zodat in landen waar Facebook niet vrij toegankelijk is toch een account aangemaakt kan worden.[4] Maar het maakt het *dark web* ook ideaal voor mensen die zich bezig willen houden met illegale activiteiten.[5]

[1] 'What is Surface Web, Deep Web and Dark Web?', medium.com 9 april 2018 (laatst geraadpleegd 11 maart 2022).
[2] C. Asher, 'Een korte uitleg van het dark web', avg.com 14 september 2021 (laatst geraadpleegd 11 maart 2022).
[3] 'Surfen op het dark web: mag dat?', privacy-escaperoom.nl 9 mei 2019 (laatst geraadpleegd 11 maart 2022).
[4] T. Marks, 'Wat heb ik op het dark web te zoeken?', vpngids.nl 2 december 2021 (laatst geraadpleegd 25 maart 2022).
[5] 'Het dark web. Wat is het en hoe werkt het?', ewmagazine.nl 22 maart 2017 (laatst geraadpleegd 11 maart 2022).

Omdat cybercrime en gedigitaliseerde criminaliteit[6] enorm toenemen, wil de politie fors meer gaan investeren in de aanpak van cybercriminaliteit[7]. Maar het mag wel duidelijk zijn dat dit soort activiteiten zich niet hoeven te beperken tot de landsgrenzen van de nationaliteit van de gebruiker of van de criminelen. Of er ook daadwerkelijk sprake is van grensoverschrijdende cybercriminaliteit, daarover zijn de meningen verdeeld. Zo is te lezen in een brief van de minister van Justitie en Veiligheid dat daders van georganiseerde cybercriminaliteit zich vooral buiten Nederland bevinden terwijl zij wel Nederlandse slachtoffers maken of de Nederlandse digitale infrastructuur gebruiken voor hun criminele activiteiten.[8] Maar in het artikel van Van Erp, Stol en Wilsem is echter te lezen dat uit onderzoek blijkt dat criminaliteit in cyberspace, waarbij sprake is van Nederlandse slachtoffers, de criminelen zich vaak gewoon in Nederland bevinden.[9] Terwijl landsgrenzen bij cybercriminaliteit geen rol spelen.

Bij criminele activiteiten in cyberspace heeft de politie regelmatig moeite met de bestrijding hiervan wanneer deze vanuit een ander land dan Nederland gepleegd worden.[10] Opsporing door de Nederlandse politie of het Openbaar Ministerie (verder te noemen OM) is in sommige gevallen zelfs in zijn geheel niet mogelijk, bijvoorbeeld wanneer de dader opereert vanuit een land waar Nederland juridisch niet mee samenwerkt. In zo'n geval zou het voor de politie of het OM een optie zijn om de criminele activiteiten op het *dark web* te verstoren. Het probleem dat zich hierbij voor kan doen, is dat met dit vestoren de politie ingrijpt in het privéleven van de verdachte of betrokken personen hetgeen volgens het eerste lid van artikel 8 van het Europese Verdrag voor de Rechten van de Mens (verder te noemen EVRM) niet is toegestaan. Het tweede lid brengt hier echter wel een nuancering op aan door enkele voorwaarden te noemen die een inbreuk rechtvaardigen, waarvan de belangrijkste is dat voor een inbreuk een wettelijke grondslag aanwezig moet zijn. Het knellende vraagstuk bij de politie en OM is nu of deze wettelijke grondslag er voor verstoren eigenlijk wel is.

Enkele jaren geleden is het project *Police Detectives on the Tor Network (PDTOR)* gestart. Dit is een internationale onderzoeksgroep waar naast het Verenigd Koninkrijk, Zweden en Noorwegen ook Nederland aan mee doet. Deze onderzoeksgroep is bezig onderzoek te verrichten naar bepaalde aspecten op het *dark web* en ieder deelnemend land heeft hierin zijn eigen onderwerp. Het onderwerp waar Nederland zich mee bezig houdt, is het feitelijk

[6] Bij cybercrime gaat het om delicten waarbij ICT (Informatie- en communicatietechnologie) het middel en doel is, zoals bijvoorbeeld het hacken van een computer of het plaatsen van randsomware. Bij gedigitaliseerde criminaliteit gaat het om traditionele delicten maar wordt ICT als hulpmiddel in gezet, zoals bijvoorbeeld het oplichten van burgers via marktplaats. (M.G.J. Beerthuizen, T. Sipma en A.M. van der Laan, *Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland.* Cahier 2020-15, WODC, p. 12-13).
[7] 'Investeer in aanpak cybercrime', politie.nl 15 april 2021 (laatst geraadpleegd 11 maart 2022).
[8] *Kamerstukken* II 2017/18, 28684, nr. 522, p. 3.
[9] Erp, Stol & Wilsem, *Tijdschrift voor Criminologie* 2013 (55) 4, p. 327.
[10] Erp, Stol & Wilsem, *Tijdschrift voor Criminologie* 2013 (55) 4, p. 329.

handelen van de politie op het *dark web.*[11] De Nederlandse organisatie bestaat uit de Open Universiteit, de Politieacademie en de NHL Stenden Hogeschool. Binnen het onderwerp dat door de Nederlandse groep wordt onderzocht, is de vraag ontstaan of de politie met het verstoren van criminele activiteiten op het *dark web* geen inbreuk maakt op het recht op privacy voortkomend uit artikel 8 EVRM. In deze scriptie wordt deze vraag beantwoord. Als eerste zal onderzocht worden of er sprake is van een inbreuk op het privacy recht. Mocht dat inderdaad zo zijn, dan wordt verder onderzocht of er misschien voldaan wordt aan de voorwaarden van het tweede lid waardoor de inbreuk gerechtvaardigd is.

1.2 Centrale vraag, opbouw en gebruikte onderzoeksmethoden

De centrale vraag die in deze scriptie beantwoord wordt is:

Is het verstoren van criminele activiteiten op het TOR-netwerk door de politie een geoorloofde inbreuk op artikel 8 EVRM?

1.2.1 Opbouw, methodologie en bronnen

Deze scriptie is als volgt opgebouwd. In hoofdstuk 2 wordt uiteengezet wat onder verstorende activiteiten wordt verstaan, hierbij wordt uitgegaan van een glijdende schaal van intensiviteit[12], van generaal naar specifiek verstorende activiteiten, tot activiteiten gericht op reputatieschade. Dit zal voornamelijk gebeuren aan de hand van literatuuronderzoek. De activiteiten gericht op reputatieschade worden, naast de toetsing aan artikel 8 EVRM, ook beknopt getoetst aan smaad en laster opgenomen in de artikelen 261 en 262 van het Wetboek van Strafrecht (verder te noemen Sr). De reden hiervoor is dat buiten het feit of er een schending van artikel 8 EVRM is, de politie zich niet schuldig mag maken aan strafbare feiten. Hoofdstuk 3 is een uiteenzetting van artikel 8 EVRM. Wat houdt het privacybegrip nu precies in en aan welke voorwaarden moet voldaan zijn wil een inbreuk op dit recht gerechtvaardigd zijn, hetgeen veelal door middel van jurisprudentie uitgelegd wordt. Hoofdstuk 4 is de toetsing van de verschillende verstorende activiteiten aan de eisen van artikel 8 EVRM om zo tot een conclusie te komen of er nu wel of niet sprake is van schending van dit artikel bij het verrichten van verstorende activiteiten. In dit hoofdstuk worden de verstorende activiteiten, ondanks het feit dat de bijzondere opsporingsbevoegdheden buiten het bereik van deze scriptie vallen zoals vermeld in de volgende paragraaf, toch getoetst aan de stelselmatige observatie van artikel 126g Wetboek

[11] 'Seminar Policing the Dark Web: Onderzoekers en politie bundelen krachten', ou.nl 21 november 2017 (laatst geraadpleegd 11 maart 2022).
[12] Met glijdende schaal van intensiviteit wordt bedoeld dat de verstorende activiteiten steeds ingrijpender worden voor de crimineel.

van Strafvordering (verder te noemen Sv). Hoofdstuk 5 tenslotte zal de eindconclusie bevatten en enkele aanbevelingen.

Voor het literatuuronderzoek zal gebruik gemaakt worden van verschillende bronnen. Deze bronnen zijn boeken, tijdschriftartikelen, wetenschappelijke artikelen, jurisprudentie van het Europese Hof van de Rechten van de Mens (verder te noemen EHRM) en de Hoge Raad, kamerstukken zoals de memorie van toelichting van de Wet computercriminaliteit II en internetbronnen zoals de site van de politie en het OM. De bronnen zijn gevonden via de online catalogus WordCat Discovery van de bibliotheek van de Universiteit van Tilburg, via Kluwer Navigator en de zoekmachine Google. Maar ook door literatuurlijsten in gevonden bronnen, zijn er bronnen gevonden, de zogenoemde sneeuwbalmethode.

1.3 Afbakening

Het recht op privacy is in meerdere wetten vastgelegd, het is niet alleen opgenomen in artikel 8 EVRM, maar ook artikel 10 van onze eigen Grondwet bevat het recht op privacy en artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (verder te noemen IVBPR). Voor de beantwoording van de onderzoeksvraag van deze scriptie, wordt echter alleen aan het EVRM getoetst. Het recht op privacy opgenomen in artikel 10 Grondwet en artikel 17 IVBPR wordt buiten beschouwing gelaten.

Opsporing zelf kan ook al gezien worden als een verstorende activiteit, maar deze vorm van verstoren valt buiten het bereik van deze scriptie.

Een van de vereisten waaraan voldaan moet zijn wil een inbreuk gerechtvaardigd zijn, is de wettelijke grondslag. Van belang hierbij is de bevoegdheid van de politie welke geregeld is in artikel 3 Politiewet. Daarom zal in deze scriptie voornamelijk getoetst worden aan dit artikel. Daarnaast zijn er nog andere wetten waar politiebevoegdheden geregeld worden waarvan de Wet Bijzondere opsporingsbevoegdheden (verder te noemen Wet BOB) een hele bekende is. Echter, deze bevoegdheden zijn gericht op het opsporingsonderzoek waardoor toetsing aan deze wet buiten het bereik van deze scriptie valt.

2. Verstorende activiteiten: wat houdt dat precies in?

2.1 Inleiding

Na een inventarisatie van de verstorende activiteiten, zag ik dat er sprake was van een verschillende mate van intensiviteit ten opzichte van de crimineel. Hier bedoel ik het volgende mee. Sommige activiteiten hadden vooral als doel het voorkomen dat er criminele activiteiten kunnen plaatsvinden. Andere waren voornamelijk gericht tegen de werkzaamheden van criminelen. En dan was er nog een groep verstorende activiteiten die echt gericht is tegen de persoon zelf. Daarom heb ik er voor gekozen de verstorende activiteiten in te delen in verschillende gradaties waarbij sprake is van een glijdende schaal van intensiviteit. Ik heb voor de volgende indeling gekozen: generaal verstorende activiteiten - specifiek verstorende activiteiten - *Naming & Shaming* activiteiten. Naar mijn mening moet onder deze verdeling het volgende worden verstaan. De generaal verstorende activiteiten zijn de activiteiten die zich richten op de maatschappij. Het gaat om activiteiten die erop gericht zijn de legale bovenwereld sterker te maken tegen illegale praktijken waardoor er een preventieve werking vanuit gaat. Hierbij kan worden gedacht aan maatregelen ter voorkoming van witwassen van criminele gelden. Met specifiek verstorende activiteiten bedoel ik activiteiten die gericht zijn op het verstoren of zelfs onmogelijk maken van de criminele activiteiten zelf, zoals het offline halen van een criminele website. En onder de *Naming & Shaming* activiteiten laat ik de activiteiten vallen die de crimineel persoonlijk raken, deze zijn gericht op hem als persoon, zoals het schaden van zijn reputatie.

In de volgende paragrafen zullen deze verstorende activiteiten toegelicht worden en zal er ook aangegeven worden wat nog net wel toelaatbaar is en wat niet meer.

2.2 Generaal verstorende activiteiten

2.2.1 De illegale onderwereld kan niet zonder de legale bovenwereld

Criminelen zijn voor het uitvoeren van hun illegale praktijken afhankelijk van de legale bovenwereld.[13] Het kan hierbij om hele basale zaken gaan zoals de crimineel die een auto koopt bij een dealer die vervolgens als vluchtauto gebruikt wordt of de aanschaf van een pak papier en toner of een notitieblok. Er kan ook gedacht worden aan huis-tuin-en-keukenmiddelen die gebruikt worden als grondstof voor de productie van drugs. Of het gebruik van een Tor-browser, ook de Tor-browser is een product van de legale bovenwereld

[13] *Integraal, tenzij …. Leidraad om samen het criminele ondernemingsklimaat te verslechteren* 2013, p. 3.

die gebruikt wordt door de illegale onderwereld. Maar om dit soort afhankelijkheid met de legale bovenwereld gaat het hier niet. Het lijkt mij dat het voor de politie vrijwel onmogelijk is dit soort activiteiten te verstoren aangezien deze producten en middelen ook aangeschaft kunnen worden voor legitieme doeleinden, zowel door criminelen als niet-criminelen.

Waar het hier om gaat is dat criminelen bijvoorbeeld financiële dienstverleners zoals banken en financieel adviseurs nodig hebben voor het witwassen van hun criminele inkomsten, een elektricien voor de aanleg van een hennepkwekerij, pakketdiensten voor het versturen van hun xtc-pillen, de containeroverslag in de haven van Rotterdam voor drugs- en mensensmokkel, eigenaren van ontroerend goed voor illegale wapenhandel en vakantiehuisjes voor illegale prostitutie. Mensen worden hierbij afgeperst, onder druk gezet of verleid met grote sommen geld om als legale partij zich in te laten met deze illegale criminele activiteiten. Normen en waarden vervagen, hetgeen niet ten goede komt aan de veiligheid in buurten.[14]

Het hinderen van criminelen in hun werkwijze, al dan niet op het *dark web,* het frustreren van de criminele bedrijfsprocessen of het bemoeilijken van deelneming aan criminele organisaties, kan bijdragen aan het verminderen van criminaliteit.[15] Ook het onaantrekkelijk maken van het criminele ondernemingsklimaat kan hiertoe aan bijdragen.[16] Criminelen zijn creatief en verzinnen steeds nieuwe constructies om hun activiteiten voort te kunnen zetten. Een voorbeeld hiervan werd gegeven in de nieuwsuitzending van NPO begin april 2021. Hierin werd vermeld dat het voor criminelen eenvoudig is een zorginstelling op te zetten en deze instelling vervolgens te gebruiken om criminele gelden wit te wassen. Een zorginstelling is makkelijk te beginnen en politie en gemeenten mogen maar weinig informatie met elkaar delen of men heeft niet de juiste bevoegdheden om iets aan dit probleem te kunnen doen.[17] Een ander voorbeeld is de bitcoin waarvan blijkt dat dit een makkelijk middel is om geld wit te wassen, omdat de bitcoin namelijk, net zoals andere cryptovaluta, anoniem overgeboekt kan worden buiten het zicht van de politie en opsporingsdiensten.[18]

2.2.2 Het verstoren van de relatie legale bovenwereld – illegale onderwereld

Zoals in de vorige paragraaf vermeldt, maken criminelen op verschillende manieren gebruik van de legale bovenwereld bij de uitvoering van hun criminele activiteiten. Echter, deze

[14] 'Ondermijnende criminaliteit', rijksoverheid.nl (laatst geraadpleegde datum 11 maart 2022).
[15] B. Berghuis, 'Verstoring van criminele netwerken', ccv-secondant.nl 2 september 2019 (laatst geraadpleegde datum 11 maart 2022).
[16] *Integraal, tenzij …. Leidraad om samen het criminele ondernemingsklimaat te verslechteren* 2013, p. 10.
[17] 'Veel criminele zorgaanbieders actief in Nederland', beveiligingsnieuws.nl 7 april 2021 (laatst geraadpleegde datum 11 maart 2022).
[18] T. Hofmans, 'De Nederlandse Bank registreert drie officiële aanbieders van cryptovaluta', tweakers.net 6 november 2020 (laatst geraadpleegde datum 11 maart 2022); R. Baurichter, 'Nieuwe anti-witwaswet zaait verwarring in de crypto-wereld', dejurist.com 12 mei 2020 (laatst geraadpleegde datum 11 maart 2022).

activiteiten kunnen verstoord worden waarbij gedacht kan worden aan het aanpakken van gelegenheidsstructuren, het wegnemen van bepaalde vitale faciliteiten, het onaantrekkelijk maken om als facilitator op te treden en het verstoren van logistieke voorzieningen en processen.[19] De machtsposities, op economisch niveau, van criminele organisaties moeten worden afgebroken wat mogelijk is door te voorkomen dat legale sectoren misbruikt kunnen worden voor het faciliteren van de criminele markt.[20] De overheid moet effectief gaan optreden wat bij gaat dragen aan het vertrouwen en rechtvaardigheidsgevoel van burgers.[21] Maar wat houdt dit concreet in? Hieronder volgt een niet-limitatieve opsomming van vijf voorbeelden van activiteiten die erop gericht zijn de interactie tussen boven- en onderwereld te verstoren.

De eerste soort van verstorende activiteiten is het geven van voorlichting aan burgers, ondernemers en bedrijven waardoor voorkomen moet worden dat zij zich inlaten met criminele activiteiten. Burgers, ondernemers en bedrijven moeten weerbaarder gemaakt worden tegen criminele organisaties.[22]
Hierbij kan gedacht worden aan het informeren van boeren over drugshandel in hun schuren zodat zij hun schuren niet meer verhuren aan drugscriminelen. Of het geven van instructies aan baliemedewerkers van hotels hoe ze illegale prostitutie kunnen herkennen zodat de hotelkamers daar niet meer voor gebruikt gaan worden. Het informeren van makelaars over de werkwijze van criminelen hoe zij gelden witwassen door ze bijvoorbeeld te instrueren geen contant geld aan te nemen.[23] Maar ook burgers inlichten over diverse oplichtingspraktijken zoals WhatsApp fraude, Microsoft-fraude, fraude met QR-codes en phising, bijvoorbeeld via tv-spotjes. Of door in programma's zoals Radar hier aandacht aan te besteden, zodat burgers met dit soort oplichtingspraktijken bekend raken en voorkomen wordt dat ze er slachtoffer van worden.

Een tweede soort van verstorende activiteiten zijn de activiteiten die het witwassen van crimineel verworven gelden tegen gaan. Criminelen kunnen hun verworven inkomen niet zomaar uitgeven aan dure auto's, huizen of andere zaken zonder dat zij in het oog springen bij Justitie of de Belastingdienst.[24] Door het witwassen van criminele gelden moet voorkomen worden dat er een direct verband gelegd kan worden tussen het vermogen en de criminele activiteiten en wordt er een legale herkomst van het vermogen gecreëerd.[25]

[19] *Integraal, tenzij …. Leidraad om samen het criminele ondernemingsklimaat te verslechteren* 2013, p. 10.
[20] *Integraal, tenzij …. Leidraad om samen het criminele ondernemingsklimaat te verslechteren* 2013, p. 14.
[21] *Integraal, tenzij …. Leidraad om samen het criminele ondernemingsklimaat te verslechteren* 2013, p. 14.
[22] Van der Steen 2016, p. 25.
[23] 'Dit doet de politie tegen ondermijning', politie.nl (laatst geraadpleegd 11 maart 2022)
[24] OESO 2019, p. 13.
[25] OESO 2019, p. 13.

Het voorkomen van het witwassen van criminele gelden is daarom een belangrijke verstorende activiteit. Dit kan door medewerkers van de Belastingdienst goed op te leiden waardoor hun kennis en bewustwording over witwaspraktijken worden vergroot, zodat zij weten waar ze op moeten letten en zo mogelijke gevallen van witwaspraktijken kunnen aanmelden voor strafrechtelijke beoordeling.[26] Ook het uitwisselen van informatie tussen de belastingdiensten van verschillende landen is van groot belang bij de bestrijding van witwaspraktijken.[27]

Jachthavens en recreatieparken zijn ideale locaties voor criminele activiteiten of witwaspraktijken, vanwege de anonimiteit, beperkte verplichting van registratie van vaartuigen, de waarde van de vaartuigen en geringe barrières in wet- en regelgeving.[28] Door deze locaties beter in kaart te brengen en de kwetsbaarheden te inventariseren kunnen zwakke plekken aangepakt worden en worden criminelen belemmerd in hun witwaspraktijken.[29]

Sinds maart van dit jaar is er een nieuwe campagne “Blijf Alert”. Deze campagne is op initiatief van onder andere het ministerie van Justitie en Veiligheid, met als doel ondernemers alert te maken op pogingen van criminele die ‘hulp’ willen bieden door te investeren in hun bedrijf.[30] Dit kan namelijk duiden op het witwassen van criminele gelden.

Bitcoins en andere cryptovaluta[31] kunnen gebruikt worden om criminele opbrengsten wit te wassen. Het registreren van bitcoinaanbieders zou dat moeten voorkomen. In Nederland geldt een officieel register, dat beheerd wordt door De Nederlandse Bank, waaraan crypobedrijven verplicht moeten voldoen willen ze in Nederland handelen.[32] Dit register moet voor transparantie zorgen om witwassen tegen gaan.[33]

De derde soort van verstorende activiteiten is het verhinderen dat burgers verleid worden tot criminele activiteiten. Door risicojongeren in kaart te brengen en tijdig de juist hulp te bieden, kan voorkomen worden dat zij toetreden tot criminele organisaties.[34] De wijkagent speelt hierbij een rol doordat hij de buurt kent. Hij bezoekt veelplegers, voert overleg met scholen over bepaalde leerlingen en heeft contact met de leerplichtambtenaar bij spijbelende

[26] OESO 2019, p. 28.
[27] OESO 2019, p. 31.
[28] *Jaarverslag 2019* 2020, p. 20.
[29] *Jaarverslag 2019* 2020, p. 20.
[30] ‘Campagne ‘Blijf Alert’ waarschuwt ondernemers voor fout geld’, rijksoverheid.nl 10 maart 2021 (laatst geraadpleegd 11 maart 2022).
[31] Ook al kort vermeld in paragraaf 2.2.1.
[32] T. Hofmans, ‘De Nederlandse Bank registreert drie officiële aanbieders van cryptovaluta’, tweakers.net 6 november 2020 (laatst geraadpleegd 11 maart 2022).
[33] S. Trompert & M. Veeger, ‘Cryptoplatform Etoro stopt in Nederland, gebruikers moeten verkopen’, rtlnieuws.nl 30 december 2020 (laatst geraadpleegd 11 maart 2022).
[34] Van der Steen 2016, p. 25.

scholieren[35]. Kortom, de wijkagent weet wat er in een wijk speelt en weet welke jongeren misschien een probleem gaan opleveren. Maar ook door de samenwerking tussen het OM, gemeenten, politie en andere ketenpartners kunnen criminele jeugdgroepen aangepakt worden[36], zodat voorkomen wordt dat zij zich aansluiten bij een criminele organisatie of dat ze benaderd worden voor drugshandel.
Mensen met financiële problemen laten zich makkelijker door criminelen ompraten thuis een hennepkwekerij te beginnen.[37] Door deze mensen in kaart te brengen en tijdig te helpen met hun financiële problemen zijn zij minder vatbaar voor dit soort verzoeken van criminele organisaties.

Inwoners van wijken zijn de oren en ogen van de wijk, zij weten vaak bij welke winkels, bedrijven of horecagelegenheden er verdachte zaken plaatsvinden, of op vreemde tijdstippen vreemde mensen bijeenkomen.[38] Deze kennis van inwoners kan gebruikt worden als een bron van informatie.[39]

Over mensenhandel, zowel arbeidsuitbuiting als seksuele uitbuiting, hebben regio's vaak te weinig informatie waardoor de omvang en de aard van dit probleem moeilijk is in te schatten.[40] Ook is de aangiftebereidheid van slachtoffers laag.[41] Betere voorlichting, training en samenwerking tussen diverse organisaties zoals het OM, politie, gemeenten en maatschappelijke organisaties, moeten er voor zorgen dat er beter zicht is op deze vorm van criminaliteit zodat het aangepakt kan worden.[42]

De vierde soort verstorende activiteiten moeten gezocht worden in de vastgoedsector. De vastgoedsector is een risicovolle sector voor criminele activiteiten omdat illegale activiteiten toch ergens plaats moeten vinden, zoals bijvoorbeeld het op locatie produceren van drugs.[43] Vastgoedbedrijven hebben er op hun beurt belang bij dat hun ruimte wordt verhuurd.[44] Er is vaak sprake van illegale huur en onderhuur of huurders die uitgebuit worden.[45] Door een betere samenwerking tussen de vastgoedpartijen, de overheid, makelaars, woningcorporaties, e.d. zal het voor een criminele organisatie moeilijker worden om hun illegale activiteiten uit te voeren.[46]

[35] Miltenburg, van Steden & Boutellier, *Het Tijdschrift voor de Politie* jg.76/nr.8/14, voetnoten.
[36] https://www.om.nl/onderwerpen/jeugdcriminaliteit (laatst geraadpleegd 11 maart 2022).
[37] *Jaarverslag 2019* 2020, p. 15.
[38] Van der Steen 2016, p. 25.
[39] Van der Steen 2016, p. 25.
[40] *Jaarverslag 2019* 2020, p. 17.
[41] *Jaarverslag 2019* 2020, p. 17.
[42] *Jaarverslag 2019* 2020, p 18.
[43] Van der Steen 2016, p. 30.
[44] Van der Steen 2016, p. 30.
[45] *Jaarverslag 2019* 2020, p 16.
[46] Van der Steen 2016, p. 31.

Voor het terugdringen en bestrijden van malafide horecaondernemingen moeten er meer gezamenlijke controles worden uitgevoerd waarin interventies zoals boekenonderzoek, boetes van Inspectie SZW (Het Nederlandse Ministerie van Sociale Zaken en Werkgelegenheid) en sluitingen in verband met de openbare orde.[47]

De laatste soort verstorende activiteiten zijn gericht op de overheid. Niet alleen burgers, maar ook overheden kunnen ongewild betrokken raken bij criminele activiteiten. De Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (verder te noemen: Wet Bibob) zorgt ervoor dat een bestuursorgaan de eigen integriteit kan beschermen door te voorkomen dat de overheid criminele activiteiten faciliteert.[48] Indien hier sprake van is, kan het overheidsorgaan een beschikking weigeren of intrekken, een opdracht niet gunnen, een vastgoedtransactie niet door laten gaan of een overeenkomst ontbinden.[49] Om de toepassing van deze wet te versterken is er een wetsvoorstel ingediend waarin overheden meer informatie over mogelijk crimineel misbruik kunnen delen. Dit wetsvoorstel heeft als doel de vermenging van de boven- en onderwereld tegen te gaan.[50]

De verstorende activiteiten zoals hierboven genoemd zijn gericht op de legale bovenwereld, het weerbaarder maken van de maatschappij. Dit soort activiteiten zijn niet zozeer gericht op de crimineel zelf of zijn activiteiten, maar op het beter informeren van burgers, hen weerbaarder maken of begeleiden naar een maatschappelijk sterkere positie. Daardoor hebben criminelen minder vat op hen waardoor zij belemmerd worden bij de uitvoering van hun criminele activiteiten.

2.3 Specifiek verstorende activiteiten

2.3.1 Verstorende activiteiten gericht op criminele werkzaamheden

Er zijn verstorende activiteiten die verder gaan dan de hierboven genoemde activiteiten. In de vorige paragraaf ging het namelijk vooral over activiteiten die erop gericht zijn de legale bovenwereld weerbaarder te maken tegen de illegale onderwereld, de verstorende maatregelen die in deze paragraaf worden besproken, zijn specifiek op de criminele werkzaamheden gericht. Gedacht kan worden aan het uit de lucht halen van een website of een gerichte DDoS aanval op criminele websites. Van dit soort verstoringen volgt hieronder een opsomming van zes voorbeelden welk ook zeker niet limitatief is, maar wel een beeld geeft van wat ermee bedoeld wordt.

[47] *Jaarverslag 2019* 2020, p. 13.
[48] MvT Wet Bibob 2e trance. p. 1.
[49] MvT Wet Bibob 2e trance, p. 1.
[50] 'Crimineel misbruik via legale structuren voorkomen door meer informatiedeling overheden', rijksoverheid.nl 15 maart 2021.

2.3.2 Voorbeelden specifieke verstorende activiteiten

Een eerste voorbeeld is een *DDos*-aanval. Een *DDoS-aanval*, hetgeen staat voor *Distributed Denial of Service*, is het versturen van een groot aantal berichten vanaf meerdere computers naar een bepaalde server zodat de website overbelast raakt waardoor hij in de meeste gevallen niet meer bereikbaar is of zelfs crasht.[51] Normaliter voeren criminelen een *DDoS*-aanval uit op legale websites, maar de politie kan ook een *DDoS*-aanval uitvoeren op een illegale website. Het gevolg is de onbereikbaarheid van de illegale website waardoor de crimineel gehinderd wordt in zijn criminele activiteiten.

Een tweede voorbeeld is de verkoop van illegale goederen op het *dark web*, al dan niet tijdelijk, stop te zetten door de website offline te halen. Het lukt de politie en andere opsporingsinstanties steeds beter om de encryptie en anonimiteit van deze marktplaatsen op het *dark web* te verbreken en uit de lucht te halen.[52] Mochten de criminelen die achter zo'n site zitten niet opgespoord worden, zullen ze ongetwijfeld een nieuwe website lanceren. Maar ze zullen dan wel een nieuwe reputatie op moeten bouwen.[53] Criminelen verliezen in één keer hun reputatie en klantenkring, waardoor ze weer van voren af aan kunnen beginnen met de opbouw hiervan.[54] De verstoring heeft dan maar een tijdelijk karakter, maar het hindert de crimineel toch zeker in de uitvoering van zijn handel.

Een derde voorbeeld is het ongedaan maken van de anonimiteit op het *dark web*. Zoals in paragraaf 1.1 al genoemd kan er op het *dark web* anoniem gesurft worden, tenminste, dat was tot voor kort de gedachte. In 2016 heeft het OM een website op het Tor-netwerk gelanceerd waarop een lijst vermeld staat van kopers en verkopers van illegale goederen. Hieruit blijkt dat criminelen die handel drijven op het *dark web* minder anoniem zijn dan aanvankelijk werd gedacht. Op deze manier wordt geprobeerd de infrastructuur en de handel van criminelen te verstoren.[55]

Een vierde voorbeeld is de aanpak van illegale marktplaatsen op het *dark web.* Op deze illegale marktplaatsen is het belangrijk dat koper en verkoper elkaar kunnen vertrouwen, maar omdat de omgeving anoniem is, is het nooit zeker of je wel handel drijft met degene wie hij zegt dat hij is. De politie kan hier gebruik van maken door illegale verkoopplatforms over te nemen zodat ze gedurende langere tijd mee kan kijken en zo een enorme hoeveelheid data kan verzamelen. Na een tijd maakt de politie zich bekend en de twijfel is

[51] Stol en Strikwerda 2017, p. 57 (nr. 59 voetnoot).
[52] 'Internationale operatie tegen drugsverkopers op het dark web leidt tot 179 arrestaties', politie.nl 22 september 2020.
[53] Libbenga, *Emerce* 2020 #177.
[54] 'Infiltratie door politie op dark web lijkt succesvol', nos.nl 28 augustus 2017.
[55] 'Openbaar Ministerie start website op darknet om criminelen te waarschuwen', 31 oktober 2016.

gezaaid, ook al vluchten de criminelen vervolgens naar andere illegale marktplaatsen, de angst is aanwezig dat de politie ook daar meekijkt.[56]

Een volgend voorbeeld is het onderscheppen van versleutelde berichten via speciale telefoons. Criminelen maken vaak gebruik van telefoons waarmee versleutelde berichten verstuurd kunnen worden, de zogeheten *Pretty Good Privacy-telefoon*, afgekort PGP-telefoon, waar vaak de camera, microfoon en belfunctie zijn uitgezet.[57] Het lukt de politie soms deze chatberichten te onderscheppen en te ontsleutelen.[58] Aangezien in 2020 de topcrimineel Ridouan Taghi mede hierdoor is opgepakt[59], zal bij criminelen het besef doordringen dat het versturen van berichten via speciale telefoons, ondanks de versleuteling, toch een risico is. Alle voorzorgsmaatregelen ten spijt is het toch mogelijk dat verzonden berichten door politie worden onderschept en gelezen, hetgeen in het achterhoofd gehouden moet worden.

Een laatste voorbeeld is het blokkeren, filteren of afsluiten van criminele websites, waardoor degene die de criminele website wil bezoeken, wordt doorgestuurd naar de 'stoppagina' van het Landelijk Politiekorps.[60] Elke website heeft een domeinnaam en die domeinnaam verwijst naar een IP-adres. Voor het blokkeren en doorsturen van een website hoeft alleen de koppeling tussen de domeinnaam en het IP-adres gewijzigd te worden.[61] Hierbij moet wel een balans gevonden worden tussen *overblocking* (het ten onrechte blokkeren van websites) en *underblocking* (onvoldoende sites blokkeren).[62]

De verstorende activiteiten die in deze paragraaf zijn opgesomd, raken direct de werkzaamheden van de criminelen. Deze activiteiten zijn daardoor een stuk ingrijpender dan de activiteiten genoemd in de tweede paragraaf. Hun website wordt overbelast met eventueel een crash als gevolg of de website wordt uit de lucht gehaald, chatberichten blijken gekraakt te kunnen worden ondanks versleuteling en ook de anonimiteit wordt aangetast.

[56] R. Van Wegberg, 'TNO en opsporingsdiensten schijnen licht op het dark web', tno.nl 1 mei 2019.
[57] 'PGP-telefoon: wat is het en hoe werkt het?', electronica.infonu.nl (laatst geraadpleegd op 12 maart 2022).
[58] J.J. Oerlemans, '(Poging tot) Huurmoord via het dark web', jjoerlemans.nl 17 december 2021 (laatst geraadpleegd op 12 maart. 2022).
[59] T. Hofmans, 'Politie las in real time mee met otr-berichten op cryptotelefoons van Encrochat', tweakers.net 2 juli 2020 (laatst geraadpleegd op 12 maart. 2022).
[60] Leukfeldt e.a., *Tijdschrift voor de veiligheid* 2009, p. 36 en p. 40.
[61] Leukfeldt e.a., *Tijdschrift voor de veiligheid* 2009, p. 40.
[62] Leukfeldt e.a., *Tijdschrift voor de veiligheid* 2009, p. 40.

2.4 Naming and Shaming

2.4.1 Verstorende activiteiten als aanval op de crimineel zelf

Een nog verdergaande verstorende activiteit is het ondermijnen van de reputatie van criminelen. Verkopers van illegale goederen op het *dark web*, zoals drugs en wapens, worden online beoordeeld via reviews van kopers en zo kunnen zij een betrouwbare reputatie opbouwen.[63] Ondanks dat er gebruik gemaakt wordt van een pseudoniem, een *nick name*, zijn deze reviews nuttig omdat bij langdurig gebruik deze naam toch op verschillende markten opduikt en misschien ook wel op webforums.[64] De politie kan zich echter ook onder een pseudoniem op het *dark web* begeven en reviews achterlaten. Dit zullen echter geen positieve reviews zijn maar meer in de trant van *'bij die verkoper xtc-pillen gekocht, wat een troep!'.* Als er meerdere van dit soort reviews worden geschreven, onder verschillende pseudoniemen, wordt op een gegeven moment de verkopende crimineel niet meer als betrouwbaar gezien en lijkt zijn handeltje te gaan mislukken.

2.4.2 Belediging

2.4.2.1 De artikelen 261 en 262 Wetboek van Strafrecht

Ondanks dat in deze scriptie het toetsen van de verstorende activiteiten aan artikel 8 EVRM centraal staat, wil ik in deze paragraaf toch beknopt de verstorende activiteiten die de persoon van de crimineel raken toetsen aan belediging, opgenomen in Titel XVI van het Wetboek van Strafrecht. Deze titel bevat onder andere de artikelen 261 en 262 waarin smaad en laster zijn opgenomen. Het is namelijk de vraag of het plaatsten van onjuiste negatieve reviews niet onder belediging valt. Van smaad is sprake wanneer opzettelijk iemands eer of goede naam wordt aangetast door een negatief feit openbaar te maken, van laster is sprake wanneer dat feit onjuist is. Iemands goede naam is aangetast wanneer er feitelijke onjuistheden over diegene verspreid worden, zowel mondelinge als schriftelijke of online uitlatingen via *social media* zoals facebook.[65]

Voor wat betreft smaad is in het derde lid van artikel 261 Sr een uitzondering opgenomen. Er is geen sprake van smaad wanneer de dader heeft gehandeld uit noodzakelijke verdediging of te goeder trouw heeft gehandeld en het algemeen belang deze uitlating eiste. Anders gezegd "De dader die te goeder trouw heeft kunnen aannemen dat het ten laste gelegde feit waar was en ook te goeder trouw heeft kunnen aannemen dat het algemeen belang het

[63] Oerlemans en van Wegberg, *Strafblad* 2019/500 (5), p. 26.
[64] Oerlemans en van Wegberg, *Strafblad* 2019/500 (5), p. 26.
[65] 'Wanneer gaat het Openbaar Ministerie over tot vervolging van smaad?', om.nl 19 oktober 2018.

openbare ervan eiste, gaat vrijuit".[66] Er is sprake van cumulatie van voorwaarden. De dader moet hebben gehandeld uit noodzakelijke verdediging of te goeder trouw én het algemeen belang moet er mee gediend zijn. Een beroep op het in artikel 10 lid 2 EVRM opgenomen vrijheid van meningsuiting heeft geen kans van slagen aangezien deze niet absoluut is en haar begrenzing heeft in artikel 261 Sr.[67] Of een beroep op het derde lid kans van slagen heeft, wordt beoordeeld aan de hand van de feiten en omstandigheden zoals die bestonden op het moment dat de uitspraken werden gedaan.[68]

2.4.2.2 Toepast op de activiteiten van de politie

De politie die op het *dark web* slechte, negatieve recensies schrijft om criminelen zwart te maken, maakt zich naar mijn mening schuldig aan smaad en naar grote waarschijnlijkheid zelfs aan laster, omdat er bewust onjuistheden worden verspreid. Van de rechtvaardigingsgrond opgenomen in het derde lid is geen sprake. De politie handelt niet te goeder trouw, het is zelfs hun doel onjuistheden te verspreiden. Aan de toetsing aan het algemeen belang wordt niet meer toegekomen, ondanks mijn mening dat het algemeen belang hiermee gediend zou zijn.

Smaad en laster zijn echter klachtdelicten (artikel 269 Sr). Dit houdt in dat het OM alleen tot vervolging overgaat wanneer het slachtoffer aangifte doet.
De kans lijkt mij klein dat de crimineel wiens goede naam is aangetast door deze opzettelijk onjuiste aantijgingen naar de politie stapt om aangifte te doen, maar dit betekent mijn inziens niet dat de politie zich schuldig mag maken aan enig misdrijf, ook al zou de politie er mee weg komen.

2.4.2.3 Bereik van de bevoegdheden van de politie op grond van artikel 3 Politiewet

Hoever reiken de bevoegdheden van de politie? Is er een wettelijke bevoegdheid waardoor de politie toch deze verstorende activiteiten kan uitvoeren zonder dat ze onder de artikelen van belediging vallen?
Een belangrijk artikel is artikel 3 van de Politiewet. Dit artikel beschrijft de taak van de politie en luidt als volgt:

> *De politie heeft tot taak in ondergeschiktheid van het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven."*

[66] *Kamerstukken II* 1975/76, 11249, nr. 6, p. 6.
[67] Rb. Amsterdam 22 november 2007, ECLI:NL:RBAMS:2007:BB8525, r.o. 4.
[68] Rb. Amsterdam 22 november 2007, ECLI:NL:RBAMS:2007:BB8525, r.o. 5.

Echter, niet alles wat onder de politietaak valt is wettelijk geregeld.[69] Zo heeft de Hoge Raad bijvoorbeeld In het Zwolsman-arrest[70] geoordeeld dat een beperkte inbreuk op de persoonlijke levenssfeer door de politie toelaatbaar is op grond van artikel 3 Politiewet. Als je deze mate van inbreuk op laster toepast, zou hieruit de conclusie getrokken kunnen worden dat 'een beetje laster' mogelijk is toegestaan op grond van artikel 3 Politiewet. De vraag die hierbij gesteld kan worden is in hoeverre de reputatieschade, waar het bij de verstorende activiteiten omgaat, nog wel vallen onder 'een beetje laster'. Bij laster is al sprake van de meest vergaande vorm van belediging omdat er bewust onjuiste informatie verspreid wordt. Wanneer de politie eenmalig bewust een onjuiste slechte review plaatst, zal dit vermoedelijk nog wel toelaatbaar zijn op grond van artikel 3 Politiewet, maar zodra het een frequenter karakter krijg, is er naar mijn mening geen sprake meer van 'een beetje laster' en valt het niet meer onder de politiebevoegdheid van artikel 3 Politiewet.

[69] Stol en Strikwerda, *Tijdschrift voor Veiligheid* 2018 Aflevering 1-2, § 1.
[70] HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, r.o. 6.4.5. (*Zwolsman*).

3. Artikel 8 EVRM

3.1 Inleiding

Het recht op privacy is in meerdere wetten en verdragen geregeld en is een belangrijk recht omdat je daarmee vrij bent om te zijn wie je bent en wat je doet.[71] In artikel 8 EVRM staat "*een ieder"* wat inhoudt dat dit recht voor iedere burger geldt, dus ook voor burgers die zich bezig houden met criminele activiteiten, zo blijkt uit een uitspraak van het Gerechtshof Amsterdam.[72]

Criminele activiteiten op internet, dus ook op het *dark web*, kunnen op eigen grondgebied plaatsvinden, dus zowel de crimineel als het slachtoffer bevinden zich in Nederland. Uit onderzoek blijkt dat dat ook vaak gebeurt[73]. Maar aangezien het internet geen grenzen kent, kan het ook in een ander land plaatsvinden, maar wie wordt nu precies beschermd door het EVRM en hoever gaat die bescherming? Voor dit verdrag is de uitoefening van de rechtsmacht van belang en niet zozeer het grondgebied van de staat.[74] In de meeste gevallen heeft een staat alleen rechtsmacht op haar eigen grondgebied, maar in een enkel geval kan er ook sprake zijn van rechtsmacht buiten het eigen grondgebied, bijvoorbeeld wanneer er autoriteiten als politiek vertegenwoordigers in het buitenland opereren.[75]
Het verdrag geldt in de verhouding tussen overheid en burger, ook wel verticale werking genoemd, waardoor alleen een staat verantwoordelijk gehouden kan worden voor schending van het EVRM.[76] Hieronder vallen overheidsorganisaties, dus alle publieke autoriteiten die belast zijn met besturende, wetgevende en rechtsprekende bevoegdheden, zowel op centraal als decentraal niveau.[77] Aangezien de politie een overheidsinstelling is, is de politie gebonden aan het EVRM en doordat in het verdrag 'een ieder' is opgenomen, geldt het recht op privacy ook voor criminelen en zal de politie in beginsel geen handelingen mogen verrichten die dit recht schenden.

Voor de beantwoording van de centrale vraag uit het eerste hoofdstuk is het van belang te weten wat het recht op privacy uit artikel 8 EVRM precies inhoudt. In de volgende paragraaf wordt eerst de tekst van dit artikel vermeld om vervolgens in paragraaf drie een beschrijving

[71] Artikel 10 Grondwet, artikel 17 Internationaal verdrag inzake burgerrechten en politieke rechten, artikel 16 Kinderrechtenverdrag; 'Waarom is privacy belangrijk?', autoriteitpersoonsgegevens.nl (laatst geraadpleegd 12 maart 2022).
[72] Hof Amsterdam 8 maart 2011, ECLI:NL:GHAMS:2011:BP6989.
[73] Erp, Stol & Wilsem, *TvCr* 2013 (55) 4, p. 327.
[74] Barkhuysen & Emmerik 2011, p. 16.
[75] Barkhuysen & Emmerik 2011, p. 16.
[76] Barkhuysen & Emmerik 2011, p. 17.
[77] Barkhuysen & Emmerik 2011, p. 17.

te geven van het privacybegrip. Paragraaf vier is een uiteenzetting van de eisen opgenomen in het tweede lid die een inbreuk rechtvaardigen.

3.2 Artikel 8 EVRM – Recht op eerbiediging van privé, familie- en gezinsleven

De Nederlandse vertaling van de letterlijke wettekst is als volgt:

> *" Lid 1*
> *Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
> *Lid 2*
> *Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economische welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."*

Uit het tweede lid blijkt dus dat het recht op respect voor het privéleven en dergelijke geen absoluut recht is, omdat er een limitatieve opsomming is gegeven waaraan voldaan moet worden wil een inbreuk op het recht genoemd in het eerste lid gerechtvaardigd zijn.[78] Er moet een wettelijke grondslag voor de inbreuk zijn, de inbreuk moet een legitiem doel dienen en moet noodzakelijk zijn in een democratische samenleving. Een voorbeeld hiervan is een inval in een woning als na gedegen onderzoek blijkt dat zich daar een verdachte van kinderporno bevindt. Het onverwachts binnenvallen in de woning is een schending van het recht op privacy, de persoonlijke levenssfeer wordt hierbij aangetast doordat vreemden zijn privéwoning binnenvallen. Maar deze inbreuk is gerechtvaardigd omdat zo'n woninginval in de wet is geregeld, het dient een legitiem doel, namelijk het voorkomen van strafbare feiten en de bescherming van de gezondheid en goede zeden van kinderen en het is noodzakelijk in een democratische samenleving. Het is niet zo dat elk bestuursorgaan of ieder ander belast met openbaar gezag maar zijn gang kan gaan.

[78] Harteveld e.a. 2004, p. 150.

3.3 Het privacy begrip uit artikel 8 EVRM

Het recht op privacy valt onder de klassieke grondrechten hetgeen betekent dat het individu beschermd moet worden tegen inbreuken van buitenaf op zijn privéleven.[79] Klassieke grondrechten zijn rechten die de vrijheden van mensen garanderen en dan met name tegen de overheid.[80] Dit impliceert dat de overheid zich moet onthouden van bepaalde handelingen, zoals bijvoorbeeld discriminatie op grond van geslacht of opleidingsniveau, beperking van de persvrijheid of het tegen gaan van de oprichting van een bepaalde politieke partij of andersoortige vereniging.[81] Overigens betekent dit niet dat de overheid zich nergens mee mag bemoeien, uit EVRM vloeien ook positieve verplichtingen voort zoals bijvoorbeeld artikel 2 EVRM waarin het recht op leven is geregeld.[82] De overheid moet er voor zorgen dat haar onderdanen in leven blijven door mensen die een moord hebben gepleegd of zich schuldig hebben gemaakt aan doodslag, te berechten.

Het privacy begrip wordt door het EHRM ruim uitgelegd, hetgeen blijkt uit het feit dat het hof reputatierechten, rechten die verband houden met bescherming van de leefomgeving alsook aspecten die nauw samenhangen met persoonlijke autonomie zoals abortus en hulp bij zelfdoding onder dit artikel heeft gebracht.[83] Voor wat betreft de reputatierechten moet er wel een nuancering aangebracht worden. In het Karakó-arrest heeft het Hof namelijk geoordeeld dat artikel 8 EVRM geen recht op reputatie beschermt, alleen persoonlijke identiteit en persoonlijke integriteit.[84] Volgens het Hof is de privacy alleen geschonden als de aanval op de reputatie zo'n ernstige inbreuk op het privéleven is dat dit een aantasting is van de persoonlijke integriteit.[85] Uit jurisprudentie van het EHRM blijkt dat onder het privacy begrip de fysiologische en psychologische integriteit van een individu valt.[86] Verder vallen diverse andere zaken onder het privacy begrip zoals onder andere de seksuele voorkeur, iemands geslacht, identiteit, et cetera.[87]

[79] Van der Jagt 2013, p. 163.
[80] Akkermans, Bax & Verhey 2005, p. 33.
[81] Akkermans, Bax & Verhey 2005, p. 33.
[82] EHRM 9 oktober 1979, nr. 6289/73, m.nt. E.A. Alkema *(Airey t. Ierland)*.
[83] 'Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden', merelkoning.nl (laatst geraadpleegd 20 januari 2022).
[84] EHRM 28 april 2009, nr. 39311/05, r.o. 22 en 23 (*Karakó t. Hongarije)*.
[85] R. Van der Zaal, 'Europees Hof voor de Rechten van de Mens (Karako arrest): art. 8 EVR omvat geen recht op reputatie', mediareport.nl 8 juni 2009.
[86] EHRM 29 april 2002, ECLI:CE:ECHR:2002:0429JUD000234602, r.o. 61 *(Pretty t. Verenigd Koninkrijk)*.
[87] EHRM 6 februari 2001, ECLI:CE:ECHR:2001:0206JUD004459998 (*Bensaid t. Verenigd Koninkrijk)* en EHRM 4 december 2008, ECLI:ECHR:2008:1204JUD003056204 (*S. en Marper t. Verenigd Koninkrijk)*.

Daarnaast heeft het EHRM geoordeeld dat het privéleven zich niet beperkt tot de privésfeer van een persoon, maar dat de werkvloer en het publieke domein hier ook onder vallen.[88] Dit is van belang voor de beantwoording of de privacy van een verdachte wordt geschonden bij het verstoren van zijn of haar criminele activiteiten op het *dark web*, daarmee bevindt de verdachte zich namelijk in het publieke domein. Uit het voorgaande blijkt dat ook die activiteiten van een persoon onder het recht op privacy vallen waardoor het verstoren van deze activiteiten een inbreuk hierop zou kunnen zijn. Zeker omdat een persoon mag verwachten dat zijn identiteit verborgen blijft als hij zich op internet bevindt en dat zijn privacy gewaarborgd is.[89] Dat zijn IP-adres hierbij bekend wordt gemaakt, al dan niet bewust, en de persoon daardoor identificeerbaar is, heeft hierbij geen betekenis[90] en personen die zich op het *dark web* bevinden zijn al helemaal in de veronderstelling dat ze daar anoniem zijn. Het recht op privacy wordt ook geschonden wanneer gegevens die herleidbaar zijn tot een persoon systematisch worden verzameld, vastgelegd, bewerkt en lang worden bewaard.[91]

3.4 Voorwaarden gerechtvaardigde inbreuk

Het recht op privacy is geen absoluut recht aangezien in het tweede lid voorwaarden zijn opgenomen wanneer een inbreuk op dit recht gerechtvaardigd is. Van een absoluut recht kan namelijk nooit afgeweken worden, niet in een normale situatie en ook niet in een uitzonderingssituatie. [92] De in het tweede lid genoemde voorwaarden is een limitatieve opsomming, waardoor een inbreuk alleen gerechtvaardigd is wanneer a) dit bij wet is voorzien, b) een legitiem doel dient en c) in een democratische samenleving noodzakelijk is. Deze voorwaarden zijn cumulatieve vereisten, als aan één van deze voorwaarden niet is voldaan, dan is een inbreuk niet gerechtvaardigd en is het recht op privacy geschonden. In de volgende subparagrafen worden deze voorwaarden besproken.

3.4.1 Bij wet voorzien

Bij wet voorzien betekent dat nationale wetgeving een grondslag voor de inmenging moet bevatten waarbij wordt voldaan aan de rechtstatelijke vereisten.[93] Dit hoeft niet altijd een wet in formele zin te zijn, jurisprudentie kan ook als wettelijke grondslag dienen, evenals richtlijnen, zoals beleidsregels van het OM.[94] Wel van belang is dat aan de voorwaarden van

[88] EHRM 16 december 1992, ECLI:CE:ECHR:1992:1216JUD001371088, r.o. 29 *(Niemietz t. Duitsland)* en EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD04464798 *(Peck t. Verenigd Koninkrijk)*.
[89] EHRM 16 juni 2015, ECLI:CE:EC HR:2015:0616JUD006456909 (*Delfi AS t. Estland)*.
[90] EHRM 24 april 2018, WCLI:CE:ECHR:2018:0424JUD006235714 *(Benedik t. Slovenië)*.
[91] HR 10 april 2020, ECLI:NL:HR:2020:639, r.o. 2.4.4.
[92] Akkermans, Bax & Verhey 2005, p. 147.
[93] Van der Jagt 2013, p.165.
[94] Van der Jagt 2013, p. 165; EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, m. nt. E.J. Dommering *(Kopke t. Duitsland)*: noot 3; HR 19 juni 1990, ECLI:NL:HR:1990:ZC8556, r.o. 5.1, m. nt. M. Scheltema, Th. W. van Veen *(Richtlijn en recht in artikel 99 RO)*.

toegankelijkheid (accessibility) en voorzienbaarheid (foreseeability) wordt voldaan, hetgeen inhoudt dat de grondslag toegankelijk moet zijn voor betrokkene zodat hij weet wat de consequenties van zijn gedrag zijn en zijn gedrag hierop kan afstemmen.[95] De betrokkene moet in staat zijn om kennis te nemen van deze wetgeving.[96] De eis van voorzienbaarheid houdt ook in dat de wettelijke regeling met voldoende precisie moet zijn geformuleerd in het nationale recht.[97]

Het is echter niet altijd handig als betrokkene op voorhand op de hoogte is van het toepassen van diverse maatregelen, bijvoorbeeld wanneer de politie iemand in de gaten wil houden bij een vermoeden van criminele activiteiten. In het geval van heimelijk toezicht kunnen de eisen van toegankelijkheid en voorzienbaarheid worden afgezwakt, maar hiervoor gelden echter wel strenge voorwaarden omdat het afzwakken van de voorzienbaarheid het risico van willekeur met zich meebrengt.[98] Het Hof heeft in enkele arresten minimumvoorwaarden opgesteld waaraan heimelijk toezicht moet voldoen om te waarborgen dat er geen misbruik van bevoegdheden wordt gemaakt.[99] De aard van de wetsovertreding die aanleiding kan geven voor de toezichtsmaatregel moet omschreven worden. Er moet een definitie komen van de categorieën van personen die onderworpen kunnen zijn aan de toezichtsmaatregel. Daarnaast moet de duur van de maatregel beperkt worden en er moet een beschrijving van de te volgen procedures voor het onderzoek komen, hoe de gegevens worden verkregen, gebruikt en opgeslagen. Er moet een beschrijving komen van de voorzorgsmaatregelen die genomen moeten worden als gegevens van derden worden doorgegeven en er moet aangegeven worden hoe gegevens verwijderd mogen worden en hoe deze dan verwijderd of vernietigd moeten worden. Als aan deze voorwaarden wordt voldaan mag er dus toezicht plaatsvinden zonder dat volledig aan de voorwaarden van toegankelijkheid en voorzienbaarheid is voldaan.

3.4.2 Een legitiem doel dienen

Om een inbreuk te rechtvaardigen moet er ook sprake zijn van een legitiem doel, welke in het tweede lid limitatief zijn opgesomd. Dit zijn de nationale veiligheid, de openbare veiligheid of het economische welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Voorbeelden hierbij zijn het voorkomen van terroristisch geweld of het voorkomen van verspreiding van massavernietigingswapens.[100] Deze doelen moeten restrictief worden uitgelegd zodat de hoofdregel van het eerste lid ook

[95] Van der Jagt 2013, p. 165; EHRM 26 april 1979, *NJ* 1980/146, nr. 6538/74, r.o. 49 (*Sunday Times t. Verenigd Koninkrijk)*.
[96] EHRM 2 augustus 1984, Apll. Nr. 8691/79, r.o. 81 (*Malone)*.
[97] Harteveld e.a. 2004, p. 165.
[98] Harteveld e.a. 2004, p. 166-167; Van der Jagt 2013, p. 165; Van der Jagt 2013, p. 165 en Harteveld e.a., p. 167.
[99] EHRM 29 juni 2006, ECLI:CE:ECHR:2006:0629DEC005493400, r.o. 77-79 *(Weber en Saravia t. Duitsland)* en EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204 JUD004714306, r.o. 231 *(Roman Zakharov t. Rusland)*.
[100] 'Wat is nationale veiligheid?', aivd.nl (laatst geraadpleegd 20 januari 2022).

echt hoofdregel blijft.[101] Het hof rekent hiertoe ook preventieve maatregelen ter voorkomen van wanordelijkheden en ter bevordering van de waarheidsvinding.[102]

3.4.3 Noodzakelijk democratische samenleving

Een maatregel is noodzakelijk wanneer er een dwingend maatschappelijke behoefte bestaat[103], zodat met de maatregel het nagestreefde doel bereikt kan worden en de maatregel evenredig is met het doel.[104] Er moet hierbij voldaan worden aan het subsidiariteitsbeginsel en het proportionaliteitsbeginsel. Het subsidiariteitsvereiste houdt in dat als er een minder ingrijpend middel voor handen is waarmee hetzelfde kan worden bereikt, dit middel toegepast moet worden. Het proportionaliteitsvereiste houdt in dat met de maatregel de inbreuk op het privéleven evenredig moet zijn in verhouding met het doel dat moet worden verwezenlijkt.[105] Hierbij moet steeds een belangenweging plaatsvinden waarbij naar de omstandigheden van het geval, het algemeen belang en het belang van de betrokkene wordt gekeken.[106] Er moet gezocht worden naar een *"fair balance"* tussen de belangen van het individu en de maatschappelijke belangen.[107] Belangrijk bij de beoordeling van de noodzaak van de inbreuk op het recht op privacy is de beoordeling van de subsidiariteit en de proportionaliteit van het overheidsoptreden ten opzicht van de inbreuk op het recht op privacy van de betrokkene.[108] Als niet aan de voorwaarden van de subsidiariteit en de proportionaliteit wordt voldaan, is er geen noodzaak tot inbreuk.[109]

De betrokken staat heeft hier wel enige *"margin of appreciation"* (beoordelingsruimte) om een afweging te maken tussen het recht op privacy van de betrokkene en de noodzaak om het gestelde doel te behalen.[110] Het hof heeft in een aantal arresten de *pressing social need* getoetst aan urgentie.[111] Daarbij werd bekeken of de inmenging op het moment van ingrijpen als urgent aangemerkt kon worden.[112] Van belang hierbij is dat als een bepaalde situatie enige tijd ongemoeid is gelaten door de overheid er geen sprake is van urgentie en dus geen sprake van *"pressing social need".*[113] Ook heeft het hof bij uitspraken over wel of geen schending van artikel 8 EVRM het vereiste toegevoegd dat voor een bepaalde inmenging

[101] Harteveld e.a. 2004, p. 160.
[102] Harteveld e.a. 2004, p. 160.
[103] *Pressing social need.*
[104] Van der Jagt 2013, p. 165 en EHRM 22 oktober 1981, nr. 7525/76 (*Dudgeon t. Verenigd Koninkrijk)*.
[105] Van der Jagt 2013, p. 165.
[106] Van der Jagt 2013, p. 166.
[107] Harteveld e.a. 2004, p. 177.
[108] Harteveld e.a. 2004, p. 178.
[109] Harteveld e.a. 2004, p. 178.
[110] Harteveld e.a. 2004, p. 177.
[111] Nieuwenhuis, *NTM/NJCM-Bull.* Jrg. 2014, nr.1, p. 14.
[112] Nieuwenhuis, *NTM/NJCM-Bull.* Jrg. 2014, nr.1, p. 14.
[113] Nieuwenhuis, *NTM/NJCM-Bull.* Jrg. 2014, nr.1, p. 16.

een *"particular strong reasons"* dient te zijn, een vergaande inbreuk zou slechts gerechtvaardigd kunnen worden als er sprake is van een bijzonder sterke reden.[114]

3.5 Tussenconclusie

'Een ieder' heeft recht op privacy, dus ook criminelen. Het verdrag regelt de betrekking tussen overheid en burger, zoals de betrekking tussen politie en criminelen, hetgeen inhoudt dat de politie het privacyrecht van criminelen moet eerbiedigen, althans in eerste instantie. Het privacybegrip is ruim uitgelegd en beperkt zich niet alleen tot de privésfeer, maar bestrijkt ook de werkvloer en het publiek domein waar het *dark web* een onderdeel van is. Burgers mogen er daarom vanuit gaan dat hun identiteit verborgen blijft op internet alsook de activiteiten die zij op het web, inclusief *dark web*, verrichten.
Het recht op privacy is echter geen absoluut recht doordat in het tweede lid een limitatieve opsomming is gegeven wanneer een inbreuk op dit recht gerechtvaardigd is. Hiervan is sprake wanneer de inbreuk bij wet is voorzien, een legitiem doel treft en noodzakelijk is in een democratische samenleving.
Bij wet voorzien kan een wet in formele zin zijn, maar kan ook jurisprudentie, richtlijnen of beleidsregels van het OM, zolang aan de eisen van toegankelijkheid en voorzienbaarheid is voldaan.
Een legitieme doel is de nationale veiligheid, openbare veiligheid of het economisch welzijn van een land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.
De noodzakelijkheid in een democratische samenleving houdt in dat er sprake moet zijn van een dwingend maatschappelijke behoefte waarbij de eisen van subsidiariteit en proportionaliteit in acht moeten worden genomen, waardoor er een "*fair balans"* is tussen de maatschappelijke behoefte en het individu.

[114] Nieuwenhuis, *NTM/NJCM-Bull.* Jrg. 2014, nr.1, p. 16.

4. Toetsing

4.1 Inleiding

In de voorgaande hoofdstukken is besproken wat onder verstorende activiteiten wordt verstaan. De verstorende activiteiten kunnen naar mijn idee in drie categorieën onderverdeeld worden en in de volgende paragraaf zal eerst per categorie bekeken worden of ze een inbreuk op het recht op privacy opleveren. Mocht er namelijk geen sprake zijn van schending, dan hoeft er niet meer getoetst te worden aan de vereisten voor een gerechtvaardigde inbreuk welke opgenomen zijn in het tweede lid van artikel 8 EVRM. In de derde paragraaf worden de categorieën die wel een inbreuk opleveren op het recht op privacy getoetst aan de rechtvaardigingsgronden om zo te kunnen beoordelen of er sprake is van een gerechtvaardigde inbreuk.

4.2 Wel of geen schending van de privacy

4.2.1 Het privacy-begrip

Het recht op privacy geldt voor iedereen, het geldt tussen de overheid en de burger, het wordt ruim uitgelegd waardoor bijvoorbeeld ook aspecten die samenhangen met persoonlijke autonomie er onder vallen en is niet alleen van toepassing in het privédomein maar ook in het publiekdomein en op de werkvloer. Het recht op privacy geldt dus in de verhouding politie – crimineel en geldt ook wanneer de crimineel zich op internet bevindt waar het *dark web* een onderdeel van is. De crimineel vertrouwt erop dat zijn identiteit verborgen en zijn persoonlijke integriteit behouden blijft en er niet systematisch gegevens die herleidbaar zijn tot hem als persoon worden verzameld, bewaard en bewerkt.

4.2.2 De generaal verstorende activiteiten

De generaal verstorende activiteiten zijn gericht op het weerbaarder maken van de legale bovenwereld.[115] Criminelen hebben de legale bovenwereld, zoals financiële dienstverleners, verhuurders van onroerend goed, jongeren zonder toekomst en geld nodig om hun criminele activiteiten uit te kunnen voeren. Als deze doelgroep door middel van informatie, begeleiding en andere soorten hulp zich bewuster is van de praktijken en werkwijze van criminelen en eventuele strafrechtelijke gevolgen, wordt het voor criminelen steeds moeilijker om hun werkzaamheden uit te blijven oefenen. Dit soort verstorende activiteiten zijn niet direct gericht op de criminele activiteiten of de persoon van de crimineel zelf, maar op de

[115] Zie paragraaf 2.2.

maatschappij. Om van een schending van het privacyrecht te kunnen spreken moet de persoonlijke identiteit en integriteit aangetast worden en daar is bij dit soort activiteiten geen sprake van. Er is geen sprake van het stelselmatig verzamelen, bewaren en verwerken van gegevens die herleidbaar zijn tot een bepaald persoon (de crimineel). Hieruit kan naar mijn mening de conclusie getrokken worden dat de generaal verstorende activiteiten geen schending van het recht op privacy uit artikel 8 lid 1 EVRM oplevert.

4.2.3 De specifiek verstorende activiteiten

De specifiek verstorende maatregelen zijn, in tegenstelling tot de generaal verstorende activiteiten, wel gericht op de werkzaamheden van criminelen. Hun website wordt uit de lucht gehaald door een *DDos*-aanval, websites worden in het geheim overgenomen waardoor de politie gedurende enige tijd mee kan kijken en data kan verzamelen of verstuurde chat-berichten via een *Pretty Good Privacy* telefoon worden onderschept en ontsleuteld.
Het *dark web*, waar zowel criminele werkzaamheden als verstorende activiteiten van de politie plaatsvinden, is publiek domein. Het is voor iedereen toegankelijk. Tevens is het *dark web* de werkvloer van criminelen en het EHRM heeft in een arrest Niemiets t. Duitsland en het arrest Peck t. Verenigd Koninkrijk[116] geoordeeld dat het recht op privacy zich niet beperkt tot het privédomein maar zich ook uitstrekt in het publiek domein en op de werkvloer.
Zoals we in paragraaf 3.3 zagen, is het recht op privacy geschonden wanneer er gegevens die herleidbaar zijn tot een persoon systematisch verzameld en bewaard worden. Daarnaast mag degene die zich op het web bevindt er vanuit gaan dat zijn identiteit verborgen blijft.
Als de politie een criminele website overneemt om zo gedurende enige tijd mee te kunnen kijken en data te verzamelen, vermoed ik dat de politie hierbij ook achter de identiteit van de beheerder van de criminele website kan komen. Ook bij het onderscheppen en ontsleutelen van berichten verstuurd via de *Pretty Good Privacy* telefoons zal de politie gegevens verkrijgen die herleidbaar zijn tot bepaalde criminelen. Bij de *DDos*-aanval zal er van te voren ook gedegen onderzoek hebben plaatsgevonden om te beoordelen of desbetreffende website gebruikt wordt voor illegale praktijken. Ook hierbij kan de identiteit van criminelen bekend worden.
Hieruit blijkt dat de persoonlijke identiteit, levenssfeer en integriteit niet gewaarborgd kan worden en het privacy recht geschonden wordt of kan worden. Het zal misschien niet altijd gebeuren, maar er is een reële kans dat het wel gebeurt.

[116] EHRM 16 december 1992, ECLI:CE:ECHR:1992:1216JUD001371088, r.o. 29 *(Niemietz t. Duitsland)* en EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD04464798 *(Peck t. Verenigd Koninkrijk)*.

4.2.4 *Naming and Shaming* activiteiten

De meest vergaande vorm van verstorende activiteiten zijn persoonlijk, gericht op de crimineel zelf[117], door het schaden van zijn reputatie. Het Hof heeft in een arrest uit 2009[118] echter geoordeeld dat reputatieschade niet onder de bescherming van artikel 8 EVRM valt, dit artikel beschermt namelijk persoonlijke identiteit en persoonlijke integriteit. Het recht op privacy is alleen geschonden als de aanval op de reputatie zo'n ernstige inbreuk is op het privéleven, dat het de persoonlijke integriteit raakt. Het is de vraag of daar sprake van is als de politie onder pseudoniem negatieve nep-reviews plaatst. Persoonlijke integriteit houdt in dat een persoon, ondanks druk van buitenaf, bij zijn waarden en normen blijft.[119] Over het algemeen wordt iemand als integer gezien die eerlijk en betrouwbaar is en zich niet om laat kopen.[120] In hoeverre zijn criminelen integer? Mijn vermoeden is dat de aanval op de reputatie van de crimineel niet zo'n ernstige inbreuk is dat het de integriteit van de crimineel raakt, aangezien hijzelf niet helemaal integer handelt[121]. Dus ondanks dat dit soort verstorende activiteiten een aanval op hem persoonlijk zijn, raakt het niet zijn privacyrecht waardoor er geconcludeerd kan worden dat deze verstorende activiteiten geen schending van het recht op privacy opleveren, bezien vanuit het EVRM.

De conclusie die hieruit getrokken kan worden, is dat alleen in geval van de specifiek verstorende activiteiten er sprake kan zijn van schending van het recht op privacy. In de volgende paragraaf zal getoetst worden of deze inbreuk gerechtvaardigd is.

4.3 Specifiek verstorende activiteiten toetsen aan vereisten voor een gerechtvaardigde inbreuk

4.3.1 Voorwaarden gerechtvaardigde inbreuk

Voor een gerechtvaardigde inbreuk moet er aan een aantal cumulatieve voorwaarden zijn voldaan, de inbreuk moet bij wet zijn voorzien, een legitiem doel dienen en noodzakelijk zijn in een democratische samenleving. Zodra aan een van de voorwaarden niet wordt voldaan, is er geen gerechtvaardigde inbreuk en is er sprake van een schending van het privacy recht uit artikel 8 EVRM.

---

[117] In de toekomst is het niet ondenkbaar dat een crimineel zich verschuilt achter een digitale entiteit, zoals een avatar. Valt een avatar ook onder 'een ieder' in de zin van artikel 8 lid 1 EVRM zodat de reputatie van die avatar ook bescherming geniet? Een antwoord op deze vraag heb ik niet, dat gaat ook deze scriptie te buiten, maar het is denk ik wel iets om over na te denken aangezien het naar mijn idee een realistisch scenario is.

[118] EHRM 28 april 2009, nr. 39311/05 (*Karakó t. Hongarije)*.

[119] 'Wat is de betekening van integriteit?', handhavingsacademie.info 20 mei 2015.

[120] 'Wat is de betekening van integriteit?', handhavingsacademie.info 20 mei 2015.

[121] Integer kan ook nog anders opgevat worden. Een crimineel is voor wat betreft zijn criminele werkzaamheden heel integer, hij zal bijvoorbeeld zijn leveringsverplichtingen altijd nakomen. Hij zal zorgvuldig omgaan met zijn reputatie want daarmee verkopen ze hun waar. Criminelen hebben dus in dit opzicht belang bij integer handelen. Maar dit is een ander soort integerheid dan die ik bedoel. Ik bedoel het meer ten opzichte van de (legale) maatschappij.

4.3.2 Gerechtvaardigde inbreuk – Eis bij wet voorzien

Voor een gerechtvaardigde inbreuk moet er in nationale wetgeving een grondslag te vinden zijn. Dit kan door middel van een wet in formele zin, maar ook via richtlijnen of beleidsregels van het OM. Deze nationale wetgeving moet wel toegankelijk en voorzienbaar zijn hetgeen inhoudt dat een betrokkene in staat moet zijn kennis te nemen van deze wetgeving en de wetgeving moet ook met voldoende precisie zijn geformuleerd. Bij heimelijk toezicht kunnen de eisen van toegankelijkheid en voorzienbaarheid enigszins wat afgezwakt worden maar hiervoor gelden wel enkele minimum voorwaarden welke in paragraaf 3.4 zijn genoemd.

4.3.2.1 De politietaak

Voor de beoordeling of er een grondslag is in nationale wetgeving, zal eerst gekeken worden wat de politietaak inhoudt. De politietaak is opgenomen in artikel 3 Politiewet en bepaalt dat de politie moet zorgdragen voor de handhaving van de rechtsorde en aan degenen die hulp nodig hebben, hulp verstrekken. Dit alles ondergeschikt aan het bevoegd gezag en met in acht neming van de geldende rechtsregels. De HR heeft hier aan toegevoegd dat niet alles wat onder de politietaak valt wettelijk is geregeld door in het Zwolsman-arrest[122] aan te geven dat bij de uitoefening van de politietaak een beperkte inbreuk op de persoonlijke levenssfeer toelaatbaar is. Bij een verdergaande inbreuk is een afzonderlijke wettelijke bevoegdheid nodig zoals opgenomen in de Wet BOB. De Wet BOB bevat echter bevoegdheden die bedoeld zijn voor opsporing, terwijl het nu juist gaat om verstorende activiteiten als opsporing niet mogelijk is. Daarom is de kans klein dat in de bijzondere opsporingsbevoegdheden een grondslag gevonden kan worden. Tevens valt de Wet BOB buiten het bereik van deze scriptie zoals in paragraaf 1.3 is aangegeven. Toch wil ik één bijzondere opsporingsbevoegdheid verder onderzoeken om te kijken of deze toch niet van toepassing kan zijn op verstorende activiteiten, namelijk de stelselmatige observatie uit artikel 126g Sv.

4.3.2.2 Stelselmatige observatie van artikel 126g Sv

De bevoegdheid ‘stelselmatige observatie’ zou ingezet kunnen worden bij het overnemen van een illegale marktplaats op het *dark web* om zo gedurende enige tijd mee te kunnen kijken en data te verzamelen. Zo kan er een bijna volledig beeld worden verkregen van de illegale praktijken waar criminelen zich mee bezig houden. Bij stelselmatige observatie gaat het om “*het verkrijgen van een min of meer volledig beeld van bepaalde aspecten van*

[122] HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, r.o. 6.4.5. (*Zwolsman*).

iemands leven" hetgeen verder gaat dan een gewone observatie.[123] Hoe ver de inbreuk gaat is afhankelijk van bepaalde factoren zoals duur, plaats, intensiteit en frequentie.[124]
Voor deze stelselmatige observatie mag volgens het derde lid gebruik gemaakt worden van een technisch hulpmiddel, maar deze mag niet gebruikt worden voor het opnemen van communicatie. Het technisch hulpmiddel moet voldoen aan de kwaliteitseisen die opgenomen zijn in het Besluit technische hulpmiddelen strafvordering.[125] Het technisch hulpmiddel dat de politie in kan zetten voor de verstorende activiteiten is een computer zoals een pc of laptop, waardoor dit derde lid geen probleem oplevert.
In het eerste lid is opgenomen dat deze bevoegdheid ingezet kan worden bij de verdenking van een misdrijf in het belang van het onderzoek door een opsporingsambtenaar. Dat er sprake is van een misdrijf, daar zal geen twijfel over bestaan. En ook dat de politie een opsporingsambtenaar is, zal duidelijk zijn. Op de site van de politieacademie is te lezen dat een algemeen opsporingsambtenaar belast is met een algemene opsporingsbevoegdheid wat inhoudt dat hij alle strafbare feiten opgenomen in wetten en verordeningen mag opsporen.[126] Maar de eis 'in het belang van het onderzoek' levert een probleem op. Om te kunnen verstoren op een illegale marktplaats moet er onderzoek plaatsvinden. Er moet bijvoorbeeld onderzocht worden wat voor soort illegale handel er wordt gedreven. Maar dit is niet het soort onderzoek waar het in de Wet BOB om gaat. Dit soort onderzoek valt onder strategische criminaliteitsanalyse en niet onder het opsporingsonderzoek. Daaruit kan geconcludeerd worden dat er niet aan deze eis wordt voldaan. Hierdoor wordt het naar mijn mening toch wel moeilijk om in de BOB-wetgeving een wettelijke grondslag te vinden voor de specifiek verstorende activiteiten.

4.3.2.3 Artikel 3 Politiewet

In de vorige subparagraaf is geconcludeerd dat er in de BOB-wetgeving geen grondslag gevonden kan worden voor verstorende activiteiten. Maar het belangrijkste artikel waar eventueel een grondslag in gevonden kan worden is artikel 3 Politiewet waar deze paragraaf mee startte. Als er sprake is van een beperkte inbreuk op de persoonlijke levenssfeer is dit artikel toereikend. Zolang er bij het observeren geen sprake is van stelselmatigheid, dan wordt er geen volledig beeld van bepaalde aspecten van iemands leven in kaart gebracht en kan er sprake zijn van een beperkte inbreuk.[127] De algemene taakstelling van dit artikel biedt een voldoende wettelijke basis voor observaties die geen of een beperkte inbreuk op iemands persoonlijke levenssfeer zijn.[128] Een voorbeeld waarbij geen sprake is van

[123] Nieuwenhuis e.a. 2007, p. 179.
[124] Nieuwenhuis e.a.2007, p. 179.
[125] 'Besluit technische hulpmiddelen strafvorering', wetten.overheid.nl geldend van 01-01-2019 t/m heden (laatst geraadpleegd op 18 maart 2022).
[126] 'Algemeen opsporingsambtenaar', thesaurus.politieacademie.nl (laatst geraadpleegd 18 maart 2022).
[127] Nieuwenhuis e.a. 2007, p. 179.
[128] Nieuwenhuis e.a. 2007, p. 179.

stelselmatige observatie is een observatie door middel van camera's opgehangen in uitgaansgebieden. Hierbij is geen sprake van een stelselmatige observatie van een persoon aangezien de observatie in deze situatie niet gericht is op een specifiek persoon.[129] Er is wel sprake van stelselmatige observatie wanneer de observatie zich herhaaldelijk voordoet op een besloten plaats, niet zijde een woning maar bijvoorbeeld de werkplek of loods, om het gedrag van een specifiek persoon vast te kunnen stellen.[130] Uit jurisprudentie blijkt dat als de observatie plaatsvindt op openbare plaatsen waar verdachte zich bevindt, er geen sprake is van stelselmatige observatie en artikel 3 Politiewet toereikend is voor deze vorm van observatie.[131] Het *dark web* is in principe een openbare plaats, welke dan misschien wel niet met een gangbare browser zoals Safari, Edge of Firefox is te raadplegen, maar door de juiste browser te installeren voor iedereen toegankelijk. Als de politie op het *dark web* rondneust en illegale marktplaatsen bekijkt, is deze observatie in eerste instantie niet gericht op een specifiek persoon. Maar komt de politie hierbij een interessant persoon tegen en wordt deze persoon, bewust of onbewust, frequenter gevolgd of geobserveerd, dan komt je toch al gauw bij stelselmatige observatie uit. Er blijkt dus een dunne scheidingslijn te zijn tussen waarbij nog net geen sprake is van stelselmatige observatie en net wel. Artikel 3 Politiewet kan dus toereikend zijn voor observatie maar er moet voor gewaakt worden dat de observatie niet overgaat in stelselmatige observatie. Zodra daar sprake van is, en dat kan al wanneer er tweemaal informatie over een specifiek persoon verzameld wordt, biedt dit artikel geen grondslag meer. Er zullen situaties zijn waarbij dit artikel voldoende grondslag biedt, maar ik vermoed dat er ook situaties zullen voorkomen waarbij dit artikel geen grondslag biedt.

Ook het afluisteren en onderscheppen van versleutelde berichten via een PGP-telefoon zijn verstorende activiteiten waarbij het discutabel is of deze nu wel of niet gericht zijn op een bepaald persoon. Het versturen van versleutelde berichten via een PGP-telefoon kan niet gezien worden als een openbare plaats en ondanks dat de verstorende activiteiten gericht zijn op de inhoud van de berichten, wordt het toestel wel gebruikt door een bepaald persoon en ook kunnen de berichten een inhoud bevatten die over een bepaald persoon gaan. Dus ook bij deze activiteiten, het afluisteren en het onderscheppen van versleutelde berichten, kan de conclusie getrokken worden dat ze gericht zijn op een bepaald persoon waardoor er geen sprake meer is van een beperkte inbreuk op de persoonlijke levenssfeer.

[129] Nieuwenhuis e.a. 2007, p. 190.
[130] Nieuwenhuis e.a. 2007, p. 190.
[131] HR 29 maart 2005, ECLI:NL:HR:2005:AS2752.

4.3.2.4 Artikel 125o Wetboek van Strafvordering

Een andere specifiek verstorende activiteit is het uit de lucht halen van een criminele website op het *dark web.* In art. 125o Sv is deze bevoegdheid opgenomen in het kader van opsporing. Dit artikel bepaalt dat als bij het doorzoeken van geautomatiseerde werken gegevens worden gevonden waarmee strafbare feiten worden gepleegd, deze gegevens ontoegankelijk gemaakt mogen worden. Onder 'ontoegankelijk maken van gegevens' wordt verstaan dat er maatregelen getroffen worden waardoor de beheerder van de gegevensdrager of derden de gegevens niet meer kunnen raadplegen of verder verspreiden.[132] Het ontoegankelijk maken houdt onder andere in het verwijderen van de gegevens, maar andere wijzen van ontoegankelijk maken zijn ook toe gestaan zolang ze er maar toe strekken dat verdere verspreiding van de gegevens wordt voorkomen.[133] Naar mijn mening kan dit gezien worden als een vorm van verstoren waardoor er dus al sprake is van een wettelijke regulering van 'verstoren', waarbij preventie centraal staat. Dit artikel is nu nog ontoereikend voor verstorende activiteiten waarbij geen sprake is van opsporing, maar mij lijkt dat deze bevoegdheid uitgebreid zou kunnen worden zodat er een wettelijke grondslag ontstaat voor specifiek verstorende activiteiten. Het *dark web* kan mijn inziens gezien worden als een geautomatiseerd werk. De politie kan het *dark web* doorzoeken en als het daarbij vervolgens op een website waar kinderpornografische afbeeldingen worden aangeboden stuit, dan zou de politie op grond van dit artikel de bevoegdheid hebben desbetreffende website offline te halen. Het offline halen voorkomt verdere verspreiding van de kinderpornografische afbeeldingen. Overigens hierbij wel vermeld dat het offline halen van een website waar een enkel pornografisch plaatje op gevonden wordt, disproportioneel is. In zo'n geval is het een optie dit enkele plaatje te blokkeren.
Naast het offline halen van een website kan er ook een *DDOS*-aanval plaatsvinden waarbij aan een criminele website zoveel schade wordt toegebracht dat daardoor een site niet meer bereikbaar is en de gegevens niet langer meer toegankelijk zijn. Bij uitbreiding van artikel 125o Sv zoals hierboven voorgesteld zou in dit artikel ook voor dit soort specifiek verstorende activiteiten een grondslag gevonden kunnen worden.

4.3.2.5 Tussenconclusie

Een van de eisen waaraan voldaan moet zijn wil een inbreuk gerechtvaardigd zijn is dat de inbreuk bij wet moet zijn voorzien. Hiervoor zijn een aantal wetsartikelen beoordeeld. De belangrijkste hierbij is artikel 3 Politiewet aangezien hierin de politietaak is geregeld. Het blijkt dat een beperkte inbreuk op de persoonlijke levenssfeer toelaatbaar is op grond van dit artikel waarbij gedacht kan worden aan het observeren van illegale marktplaatsen met als

[132] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 20.
[133] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 20.

doel ze offline te halen. Maar deze marktplaatsobservatie kan overgaan in de observatie van een bepaald persoon, bijvoorbeeld de oprichter of iemand die daar wel heel vaak iets koopt. Zodra de observatie stelselmatig wordt, waarvan al sprake is bij tweemaal gericht informatie opzoeken van een specifiek persoon, biedt dit artikel geen grondslag meer. Dit artikel kan dus een grondslag bieden, waardoor voldaan zou zijn aan de eis 'bij wet voorzien', maar ik ben van mening dat dit artikel in de meeste gevallen van verstoren niet toereikend is. Om te kunnen beoordelen of er een grondslag gevonden kan worden in de BOB-wetgeving is artikel 126g Sv onderzocht. Hierbij is geconcludeerd dat deze wetgeving geen grondslag biedt omdat bevoegdheden uit de Wet BOB echt bedoeld zijn voor opsporingsonderzoek waar hier geen sprake van is. In artikel 125o Sv is een verstorende bevoegdheid opgenomen. Echter, ook deze bevoegdheid is alleen toepasbaar in het kader van opsporing. Met een uitbreiding naar verstoren zou deze dit artikel wel een bevoegdheid kunnen geven voor een gerichte *DDOS*-aanval of het offline halen van een website.
Hieruit kan de conclusie getrokken worden dat er voor de meeste specifiek verstorende activiteiten geen wettelijke grondslag is.

4.3.3 Gerechtvaardigde inbreuk – Eis van een Legitiem doel

De legitieme doelen waar aan voldaan moet zijn zijn de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Preventieve maatregelen ter voorkoming van wanordelijkheden vallen hier ook onder.
Het doel van het verstoren van criminele activiteiten op het *dark web* is voorkomen, of in elk geval beperken, dat er strafbare feiten gepleegd worden alsook, of juist daardoor, het beschermen van de rechten en vrijheden van anderen. Bij dat laatste kan gedacht worden aan het voorkomen dat mensen slachtoffer worden van mensenhandel, mensen verslaafd raken aan drugs, het milieu ernstige schade oploopt door het illegaal dumpen van drugsafval, er afrekeningen plaatsvinden, et cetera. De verstorende activiteiten zorgen er dus voor dat de nationale veiligheid toeneemt, wanordelijkheden verminderden of voorkomen worden, er minder strafbare feiten gepleegd worden, de gezondheid wordt beschermd doordat er geen of minder chemisch afval in het milieu terecht komt, burgers beschermd worden en hun vrijheden behouden en niet verstrikt raken in het criminele web doordat ze hun onroerend goed verhuurd hebben aan criminelen of zich op andere wijze in hebben gelaten met criminelen.
Ik wil hier wel een nuancering in aanbrengen. Er kan zich de situatie voordoen dat een scholier een eenmalige partij drugs verkoopt omdat deze even krap bij kas zit en graag naar een concert wil of iets dergelijks. Mij lijkt dat de verkoop van drugs niet eenmalig is, zeker

niet als de scholier ziet wat de opbrengsten hieruit zijn. In het hypothetische geval dat het bij een eenmalige verkoop blijft, zouden de verstorende activiteiten geen legitiem doel treffen, maar dit is een uitzondering waardoor naar mijn mening de conclusie getrokken kan worden dat aan de eis van legitiem doel is voldaan.

4.3.4 Gerechtvaardigde inbreuk – Eis van Noodzakelijkheid in een democratische samenleving

De inbreuk is gerechtvaardigd als de inbreuk een dwingende maatschappelijke behoefte nastreeft. De maatregel moet wel evenredig zijn met het doel, er moet aan het subsidiariteits- en proportionaliteitsbeginsel zijn voldaan. Dat betekent dat als er een minder ingrijpend middel voorhanden is om hetzelfde doel te bereiken, dat minder ingrijpende middel toegepast moet worden. Daarnaast moet de inbreuk op het privéleven in verhouding zijn met het doel dat verwezenlijkt moet worden, er moet dus sprake zijn van een belangenafweging tussen het individu en de samenleving. Wordt hier niet aan voldaan, dan is er geen noodzaak tot inbreuk.

De dwingend maatschappelijke behoefte die door de politie wordt nagestreefd is het veiliger maken van de maatschappij en bescherming van de burger. Dit doel kan bereikt worden door degenen die zich schuldig maken aan strafbare feiten op te sporen en te berechten. In situaties waarin opsporing niet mogelijk is, wil de politie criminele activiteiten verstoren met als doel criminaliteit te ontmoedigen.
Om te voldoen aan het proportionaliteitsbeginsel moet er een belangenafweging plaatsvinden tussen het individu (de crimineel) en de samenleving. De samenleving is erbij gebaat dat deze veilig is en door criminaliteit is er sprake van een afname van deze veiligheid. Daarnaast zijn de diverse criminele activiteiten strafbaar gesteld in het wetboek van strafrecht. De politie wil met de verstorende activiteiten deze illegale activiteiten verminderen. Omdat het belang van de samenleving prevaleert boven het belang van criminelen, is naar mijn mening voldaan aan de eis van proportionaliteit.
Dan is er nog de eis van subsidiariteit. De generale verstorende activiteiten zijn minder vergaand, minder ingrijpend, maar vermoedelijk wordt met deze activiteiten alleen criminelen niet tegengehouden. Daarmee worden de criminelen ongemoeid gelaten. Het verstoren van de criminele werkzaamheden is een volgende stap van verstorende activiteiten op de glijdende schaal van intensiviteit. Daarom wordt er naar mijn mening aan de eis van subsidiariteit voldaan en tevens aan de eis van noodzakelijkheid in een democratische samenleving. Uitgezonderd voor de situatie, zoals in de vorige paragraaf geschetst, van de scholier die eenmalig een partij drugs verkoopt omdat hij even krap bij kas zit.

4.3.5 Tussenconclusie

In deze paragraaf is bekeken of de specifiek verstorende activiteiten voldoen aan de voorwaarden voor een gerechtvaardigde inbreuk. Een van de voorwaarden is dat de inbreuk bij wet moet zijn voorzien maar het blijkt dat de wettelijke grondslag voor deze activiteiten ontbreekt. Artikel 3 Politiewet is niet toereikend omdat op grond van dit artikel een beperkte inbreuk toelaatbaar is, maar bij de specifiek verstorende activiteiten is er gemakkelijk sprake van stelselmatige observatie van een bepaald persoon hetgeen niet meer onder een beperkte inbreuk valt.
Ook in de BOB-wetgeving kan geen wettelijke grondslag gevonden worden omdat deze bevoegdheden echt bedoeld zijn voor het opsporingsonderzoek.
Artikel 125o Sv bevat een vorm van verstoren, alleen is deze bevoegdheid alleen te gebruiken in geval van opsporing. Dit artikel zou uitgebreid kunnen worden zodat het ook een bevoegdheid tot verstoren bevat in geval er geen sprake is van opsporing.
Ondanks dat aan de andere twee voorwaarden wel wordt voldaan, is er toch geen sprake van een gerechtvaardigde inbreuk omdat de voorwaarden cumulatief zijn.
Hieruit kan geconcludeerd worden dat de specifiek verstorende activiteiten geen gerechtvaardigde inbreuk op het recht op privacy uit artikel 8 EVRM opleveren omdat niet is voldaan aan de eis ‘bij wet voorzien’.

5 Conclusie en aanbevelingen

5.1 Inleiding

In de inleiding van deze scriptie is een korte uitleg gegeven van het *dark web*, een onderdeel van het internet, dat niet toegankelijk is met de gangbare browsers zoals Edge, Safari en Firefox. Om op het *dark web* te kunnen surfen is een andere browser nodig, een bekende is de Tor-brouwser, welke door iedereen te downloaden is. Het *dark web* is voor iedereen toegankelijk en een voordeel van surfen op het *dark web* is dat het anoniem kan gebeuren doordat gegevens versleuteld verstuurd worden. Daarom is het *dark web* tevens een ideale plek voor criminelen. Maar het internet, en dus ook criminaliteit, beperkt zich niet tot de landsgrenzen. Daarom kan het zo zijn dat de Nederlandse politie criminaliteit niet kan bestrijden omdat de criminelen opereren vanuit een land waar Nederland niet juridisch mee samenwerkt. Het enige dat de Nederlandse politie in zo'n geval kan doen, is deze criminele activiteiten verstoren, in de breedste zin van het woord.

5.2 Verstorende activiteiten

Omdat er bij de verstorende activiteiten een gradatie van intensiviteit is, is er door mij gekozen voor een indeling in drie categorieën.
De generale verstorende activiteiten zijn gericht op het weerbaarder maken van de legale bovenwereld, op de maatschappij. Een voorbeeld van dit soort activiteiten is medewerkers van de Belastingdienst opleiden waardoor zij witwasconstructies kunnen herkennen, burgers inlichten over alle vormen van fraude waaraan zij ten prooi kunnen vallen zoals WhatsApp fraude en phising of jongeren in probleemwijken monitoren en begeleiden zodat zij minder gauw toe zullen treden tot criminele organisaties.
De specifiek verstorende activiteiten zijn gericht op de criminele werkzaamheden. Dit kan bestaan uit het offline halen van criminele marktplaatsen op het *dark web* of het infiltreren in een illegale marktplaats om zo een tijdje mee te kijken en zich later bekend te maken. De bedoeling hiervan is criminelen angst in boezemen, hen laten weten dat ze toch niet zo anoniem te zijn als ze dachten.
De derde vorm en meest vergaande vorm is de *Naming & Shaming*. Deze activiteiten zijn gericht op de crimineel persoonlijk en bestaan voornamelijk uit reputatieschade door het plaatsen van negatieve reviews. Meerdere van dit soort reviews tast zijn reputatie aan waardoor hij niet meer als betrouwbaar wordt gezien en zijn criminele activiteiten moet staken.

5.3 Het recht op privacy uit artikel 8 EVRM

Een terechte vraag die de Nederlandse politie zich hierbij stelt, is of met deze verstorende activiteiten het recht op privacy wordt geschonden en dan met name het privacyrecht opgenomen in artikel 8 EVRM.
De probleemstelling van deze scriptie is of het verstoren van criminele activiteiten op het TOR-netwerk door de politie een geoorloofde inbreuk op artikel 8 EVRM is. Het recht op privacy geldt voor iedereen, maar het is geen absoluut recht. Een inbreuk is gerechtvaardigd als er een wettelijke grondslag is voor de inbreuk, het een legitiem doel dient en noodzakelijk is in een democratische samenleving.

5.3.1 Het privacybegrip

Het privacybegrip wordt ruim uitgelegd, het geldt niet alleen in het privéleven, maar ook op de werkvloer en in het publieke domein. Alleen voor wat betreft reputatierechten is er door de Hoge Raad een nuancering aangebracht waardoor de privacy alleen is geschonden als de aanval op de reputatie zo'n ernstige inbreuk op het privéleven is dat dit een aantasting van de persoonlijke integriteit is.
Bij het uitoefenen van de generaal verstorende activiteiten wordt het privacy recht niet geschonden omdat deze activiteiten niet persoonsgericht zijn.
De *Naming & Shaming* activiteiten raken wel de crimineel persoonlijk, maar deze vallen onder reputatieschade en door de Hoge Raad is geoordeeld dat dit niet onder de bescherming van artikel 8 EVRM valt, tenzij de persoonlijke integriteit wordt aangetast. Naar mijn mening is daar geen sprake van. Wat bij *Naming & Shaming* wel van belang is, is dat deze activiteiten onder laster vallen hetgeen strafbaar is gesteld in artikelen 261 en 262 Sr.
Voor wat betreft de specifiek verstorende activiteiten is geconcludeerd dat hierbij wel sprake is van een schending van het privacyrecht. De reden hiervoor is dat, ondanks dat bij deze activiteiten in eerste instantie geen sprake is van stelselmatige observatie, de activiteiten wel op een gegeven moment het karakter van stelselmatige observatie kunnen krijgen. En ook bij het onderscheppen en ontsleutelen van berichten verstuurd via een *Pretty Good Privacy* telefoon is het twijfelachtig of hier geen sprake is van een actie gericht op een bepaald persoon.

5.3.2 Gerechtvaardigde inbreuk?

Na geconcludeerd te hebben dat de secundair verstorende activiteiten een inbreuk zijn op het privacyrecht, zijn deze activiteiten getoetst aan de voorwaarden opgesomd in het tweede lid om te beoordelen of de inbreuk gerechtvaardigd is.

Van belang hierbij is of er een grondslag voor de inbreuk is in nationale wetgeving. Dit kan een wet in formele zin zijn, maar ook beleidsregels van het OM of richtlijnen vallen onder nationale wetgeving. Ondanks dat de BOB-bevoegdheden buiten het bereik van deze scriptie vallen, is er toch gekeken of er in deze wetgeving een grondslag te lezen is. Dat bleek niet zo te zijn en dat kwam omdat de BOB-bevoegdheden echt zijn opgesteld voor het opsporingsonderzoek en daar is nu juist geen sprake van in verband met het ontbreken van jurisdictie.
In de Politiewet, en dan met name artikel 3, zijn de bevoegdheden van de politie opgenomen. Uit jurisprudentie blijkt dat niet alles wat onder de politietaak valt, wettelijk is geregeld. Een beperkte inbreuk op de persoonlijke levenssfeer is toelaatbaar op grond van dit artikel, maar het is de vraag of er bij secundair verstorende activiteiten nog wel sprake is van een beperkte inbreuk. Van een beperkte inbreuk is sprake wanneer op een openbare plaats een camera wordt opgehangen waarbij geen sprake is van het volgen van een bepaald persoon. De infiltratie op een illegale marktplaats is in eerste instantie niet gericht op een specifiek persoon, maar als daarbij steeds dezelfde naam naar boven komt, kan die persoon interessant zijn en kan hij gerichter geobserveerd worden waardoor er sprake is van een overgang naar stelselmatige observatie en er dus geen sprake meer is van een beperkte inbreuk. Ook het onderscheppen van berichten verstuurd met de PGP-telefoon kan moeilijk van gezegd worden dat er geen sprake is van een actie gericht op een specifiek persoon. Alleen al om het feit dat de telefoon aan een specifiek iemand toebehoort. De conclusie die hieruit getrokken is, is dat er geen sprake is van een geringe inbreuk waardoor artikel 3 Politiewet geen grondslag biedt voor de inbreuk. In het tweede lid van artikel 8 EVRM gaat het om een cumulatie van voorwaarden. Dit houdt in dat als aan een van de voorwaarde niet wordt voldaan, er geen sprake is van een gerechtvaardigde inbreuk. Hierdoor kan geconcludeerd worden dat de specifiek verstorende activiteiten, zoals het offline halen van een criminele website, geen gerechtvaardigde inbreuk opleveren nu niet wordt voldaan aan de eis dat de inbreuk bij wet moet zijn voorzien.

5.4 Conclusie

Uit bovenstaande volgt dat de centrale vraag van deze scriptie niet eenduidig kan worden beantwoord. De verstorende activiteiten zijn ingedeeld in drie categorieën. De eerste categorie, het preventief verstoren levert geen problemen op. De politie kan dit soort activiteiten zonder problemen voortzetten. De *naming & shaming* activiteiten zijn ook een geoorloofde inbreuk. Maar ondanks dat ze geen schending van artikel 8 EVRM opleveren, leveren ze wel een schending van de artikelen 261 en 262 Sr op. Daardoor kunnen deze activiteiten naar mijn idee niet zomaar voortgezet worden. Voor wat betreft de tweede

categorie, de specifiek verstorende activiteiten, kan de centrale vraag ontkennend beantwoord worden. Deze activiteiten leveren een schending van het privacyrecht op en daarnaast voldoen ze ook niet aan de voorwaarden voor een gerechtvaardigde inbreuk. Dus om dit soort activiteiten te kunnen uitvoeren als verstoringsmaatregel zal er iets gewijzigd moeten worden in wet- en regelgeving.

5.5 Aanbevelingen

Wil criminaliteit op het *dark web* aangepakt kunnen worden, is het naar mijn mening toch belangrijk dat ook de in deze scriptie genoemde verstorende activiteiten uitgevoerd kunnen worden. Voor wat betreft de preventief verstorende activiteiten is dat geen probleem, maar mijn vermoeden is, is dat met alleen dit soort verstorende activiteiten het gewenste doel, het tegengaan van criminaliteit op het *dark web,* niet bereikt zal worden. Daarom wil ik in deze afsluitende paragraaf nog enkele aanbevelingen geven.

Zoals gezegd, de specifiek verstorende activiteiten leveren een schending op van het privacyrecht. Echter, deze schending zou gerechtvaardigd kunnen zijn als deze inbreuk bij wet is voorzien. Daar schort het momenteel aan waardoor nadere regelgeving noodzakelijk is. Dit hoeft niet meteen een wet in formele zin te zijn. Door middel van beleidsregels van het OM of een richtlijn kan dit al gerealiseerd worden. Mijn advies is om beleidsregels op te stellen waarin een bevoegdheid voor deze specifiek verstorende activiteiten is opgenomen. Dan is er een wettelijke grondslag waardoor voldaan wordt aan de voorwaarden voor een gerechtvaardigde inbreuk en kunnen deze activiteiten worden uitgevoerd.

Artikel 125o Sv bevat de bevoegdheid tot het ontoegankelijk maken van gegevens waarmee strafbare feiten worden gepleegd indien deze gegevens gevonden worden in geautomatiseerde werken. Deze bevoegdheid is beperkt tot de situatie waarin sprake is van opsporing, maar er is dus al een wettelijke bevoegdheid tot verstoren. Verstoren is dus geen nieuw fenomeen. Met een kleine aanpassing kan deze bevoegdheid ook van toepassing verklaard worden in situaties waarin nog geen sprake is van opsporing. Er zullen waarschijnlijk wel enkele waarborgen opgenomen moeten worden, maar mij lijkt dat hier de deur op een kier staat om verstorende activiteiten op te nemen in het wetboek van Strafvordering.

Ook zit er naar mijn idee een gat in de bevoegdheden opgenomen in artikel 3 Politiewet en de BOB-wetgeving. Artikel 3 Politiewet laat een geringe inbreuk op de persoonlijke levenssfeer toe, maar zodra er sprake is van een actie gericht op een specifiek persoon, dan

is dit artikel niet meer toereikend. Echter, de opsporingsbevoegdheden uit de BOB-wetgeving zijn alleen in te zetten als er sprake is van opsporing en daar is bij verstoren geen sprake van. Dit gat in bevoegdheden, of deze tekortkoming, kan opgevuld worden door middel van aanvullende wetgeving, door bijvoorbeeld een extra titel in het Wetboek van Strafvordering op te nemen met verstorings-bevoegdheden.

De *Naming & Shaming* activiteiten zijn dan wel geen schending van het recht op privacy, maar de politie maakt zich hierbij wel schuldig aan smaad en laster. Omdat naar mijn mening dit toch ook verstorende activiteiten zijn die bij kunnen dragen aan de bestrijding van internetcriminaliteit, zou hier aanvullende wetgeving voor moeten komen. Bijvoorbeeld door een aparte bevoegdheid in het wetboek van strafrecht of ook via een beleidsregel of richtlijn.

Tot slot wil ik u als lezer de volgende vraag voorleggen. De politie en andere opsporingsambtenaren zijn gebonden aan wettelijke bevoegdheden. Het blijkt dat deze bevoegdheden niet altijd toereikend zijn om criminaliteit te bestrijden. Burgers zijn vaak minder gebonden door allerlei wettelijke restricties, hun bevoegdheden worden in elk geval niet in de wet uitgekristalliseerd. In hoeverre zouden burgers ingezet kunnen worden bij het verstoren van criminaliteit op internet, meer specifiek het *dark web*, zonder dat zij zelf hierbij de wet overtreden?

Literatuurlijst

Boeken en tijdschriftartikelen

Akkermans, Bax & Verhey 2005
P.W.C. Akkermans, C.J. Bax & L.F.M. Verhey, *Grondrechten. Grondrechten en grondrechtsbescherming in Nederland*, Deventer: Kluwer 2005.

Barkhuysen & Van Emmerik 2011
T. Barkhuysen & M.L. van Emmerik, *Het EVRM en het Nederlandse bestuursrecht*, Deventer: Kluwer 2011.

Erp, Stol & Wilsem, *Tijdschrift voor criminologie* 2013 (55) 4
J. van Erp, W. Stol en J. van Wilsem, 'Criminaliteit en criminologie in een gedigitaliseerde wereld'*, Tijdschrift voor criminologie* 2013 (55) 4, p. 327-341.

Harteveld e.a. 2004
A.E. Harteveld e.a., *Het EVRM en het Nederlandse strafprocesrecht*. Deventer: Kluwer 2004.

***Integraal, tenzij… Leidraad om samen het criminele ondernemingsklimaat te verslechteren* 2013**
Integraal, tenzij ….: Leidraad om samen het criminele ondernemingsklimaat te verslechteren, (Stuurgroep Geïntegreerde aanpak Ondermijnende Criminaliteit (GOC), Rijksoverheid), januari 2013, J-16866.

***Jaarverslag 2019* 2020**
Jaarverslag 2019 (RIEC-LIEC), juni 2020.

Leukfeldt e.a., *Tijdschrift voor veiligheid* 2009, p. 36-50
R. Leukfeldt, e.a., 'Filteren op internet. De rol van de Nederlandse overheid in het blokkeren van kinderpornograische websites', *Tijdschrift voor veiligheid* 2009 (8) 4, p. 36-50.

Libbenga, *Emerce* 2020
J. Libbenga, 'Twintig jaar Dark Web: van drugshandel tot The Guardian', *Emerce* 2020, #177.

Miltenburg, van Steden & Boutelier, *Het Tijdschrift voor de Politie* jg.76/nr.8/14
E. Miltenburg, R. van Steden & H. Boutellier, 'Sturing binnen de wijk: de taken en positie van de wijkagent', *Het Tijdschrift voor de Politie* jg.76/nr.8/14, p. 24-29.

Nieuwenhuis, e.a. 2007
M. Nieuwenhuis e.a., *Handboek voor de Opsporingspraktijk – deel I*. Den Haag: Sdu Uitgevers 2007.

Nieuwenhuis, *NTM/NJCM-Bull. Jrg. 39 2014, nr.1*
A. Nieuwenhuis, 'Pressing social need; Op zoek naar het dringende karakter van de maatschappelijke behoefte', *NTM/NJCM-Bull.* Jrg. 39 2014, nr. 1.

Oerlemans & Van Wegberg, *Strafblad* 2019 /500 (5)
J.J. Oerlemans & R.S. van Wegberg, '45. Opsporing en bestrijding van online drugsmarkten', *Strafblad* 2019 /500 (5), p. 25-31.

OESO 2019
OESO, *Indicatoren van witwassen en terrorismefinanciering. Handboek voor medewerkers van de Belastingdienst*, Parijs: 2019.

Stol & Strikwerda 2017
W. Stol en L. Strikwerda, *Strafrechtspleging in een digitale samenleving*, Den Haag: Boom juridisch 2017.

Stol & Strikwerda, *Tijdschrift voor Veiligheid* 2018
W. Stol en L. Strikwerda, 'Online vergaren van informatie voor opsporingsonderzoek', *Tijdschrift voor Veiligheid* 2018, Aflevering 1-2.

Van der Jagt 2013
F. van der Jagt, 'Het recht op bescherming van persoonsgegevens', in: J. Gerards e.a. (red.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013, p. 163-167.

Van der Steen e.a. 2016
M. van der Steen, e.a. *Ondermijning ondermijnd. Hoe het rijk meer ruimte kan maken voor een (boven)lokale aanpak van georganiseerde criminaliteit* (Rapport van de Nederlandse School voor Openbaar Bestuur (NSoB)), 2016.

Parlementaire stukken

MvT Wet Bibob 2e tranche
Memorie van Toelichting Web Bibob 2e tranche, 19 december 2019

Kamerstukken II 1975/76, 11249.
Kamerstukken II 2015/16, 34372, nr. 3.
Kamerstukken II 2017/18, 28684.

Jurisprudentie

EHRM 26 april 1979, nr. 6538/74 (*Sunday Times t. Verenigd Koninkrijk)*.
EHRM 9 oktober 1979, nr. 6289/73 *(Airey t. Ierland)*.
EHRM 22 oktober 1981, nr. 7525/76 (*Dudgeon t. Verenigd Koninkrijk)*.
EHRM 2 augustus 1984, Apll. Nr. 8691/79 (*Malone)*.
EHRM 16 december 1992, ECLI:CE:ECHR:1992:1216JUD001371088 *(Niemiet t. Duitsland).*
EHRM 6 februari 2001, ECLI:CE:ECHR:2001:0206JUD004459998 (*Bensaid t. Verenigd Koninkrijk).*
EHRM 29 april 2002, ECLI:CE:ECHR:2002:0429JUD000234602 (*Pretty t. Verenigd Koninkrijk).*

EHRM 28 januari 2003, ECLI:CE:ECHR:2003:0128JUD04464798 (*Peck t. Verenigd Koninkrijk)*.
EHRM 29 juni 2006, ECLI:CE:ECHR:2006:0629DEC005493400 *(Weber en Saravia t. Duitsland)*
EHRM 4 december 2008, ECLI:ECHR:2008:1204JUD003056204 (*S. en Marper t. Verenigd Koninkrijk)*.
EHRM 28 april 2009, nr. 39311/05 *(Karakó t. Hongarije)*
EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, m. nt. E.J. Dommering *(Kopke t. Duitsland)*.
EHRM 16 juni 2015, ECLI:CE:EC HR:2015:0616JUD006456909 (*Delfi AS t. Estland)*.
EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204 JUD004714306 *(Roman Zakharov t. Rusland)*.
EHRM 24 april 2018, WCLI:CE:ECHR:2018:0424JUD006235714 *(Benedik t. Slovenië)*.

HR 19 juni 1990, ECLI:NL:HR:1990:ZC8556, m. nt. M. Scheltema, Th. W. van Veen *(Richtlijn en recht in artikel 99 RO)*.
HR 19 december 1995, ECLI:NL:HR:1995:ZD0328 (*Zwolsman*).
HR 29 maart 2005, ECLI:NL:HR:2005:AS2752.
HR 10 april 2020, ECLI:NL:HR:2020:639.

Hof Amsterdam 8 maart 2011, ECLI:NL:GHAMS:2011:BP6989.

Rb. Amsterdam 22 november 2007, ECLI:NL:RBAMS:2007:BB8525.