MASTER'S THESIS

Predictive Policing Welke rol speelt transparantie ingeval van inzet van Predictive Policing instrumenten bij de beoordeling van de vereiste voorwaarden uit artikel 8 EVRM?

Anoniem

Award date:
2021

Awarding institution:
Department of Public Law

Link to publication

Predictive Policing

Welke rol speelt transparantie ingeval van inzet van Predictive Policing instrumenten bij de beoordeling van de vereiste voorwaarden uit artikel 8 EVRM?

NAAM STUDENT:
STUDENTNUMMER:

SCRIPTIEBEGELEIDER: EMILE KOLTHOFF
EXAMINATOR: LITSKA STRIKWERDA

UNIVERSITEIT: OPEN UNIVERSITEIT
MASTER: RECHTSGELEERDHEID
AFSTUDEERRICHTING: STRAFRECHT

DATUM: 05-05-2021

AANTAL GEBRUIKTE WOORDEN: 13.341
(EXCLUSIEF VOORBLAD, INHOUDSOPGAVE, BRON- EN LITERATUURVERWIJZINGEN)

VOORWOORD

In mijn voorwoord wil ik u graag meenemen in mijn ervaringen in de periode van het schrijven van mijn masterscriptie.

De uitspraak van de zaak SyRI in februari 2020 kwam als geroepen. Een uitspraak binnen het sociaal domein, mijn huidige werkveld. En juist deze uitspraak zou wel eens het startpunt kunnen zijn voor mijn masterscriptie. Niet veel later – in maart 2020 – meldde ik mij aan voor de masterscriptie. Dit viel precies samen met de eerste intelligente lockdown. Twee bijzondere momenten die voor mij altijd aan elkaar verbonden zijn. En hoe wreed en ingrijpend de lockdown voor de één was, zo aangenaam en rustig was het voor mij.

De lockdown betekende namelijk veel minder tijd voor sociale aangelegenheden. Geen vakantie, geen zomerfeesten, geen voetbal, geen fitness en veel minder kraambezoek. Dat klinkt behoorlijk ingrijpend zou je toch zeggen? Niets is minder waar. Het gaf mij – samen met mijn vriendin - de tijd en ruimte om onze nieuwe woning bewoonbaar te maken en met volle teugen te genieten van de geboorte van onze zoon. En daarnaast heb ik de tijd goed kunnen gebruiken voor mijn onderzoek en het schrijven van de masterscriptie.

Mijn eerste woord van dank gaat uit naar mijn scriptiebegeleider Emile Kolthoff voor zijn waardevolle feedback. De feedback was kritisch en scherp en de positieve opmerkingen gaven mij een enorme boost om weer door te gaan. Tot slot wil ik mijn ouders, mijn vrienden en met name mijn vriendin bedanken. Zij hebben mij in de lange weg die ik heb moeten afleggen altijd gesteund.

Ik wens u veel leesplezier!

Wijchen, 05 mei 2021

LIJST VAN GEBRUIKTE AFKORTINGEN

ABRvS	Afdeling Bestuursrechtspraak van de Raad van State
AI HLEG	Deskundigengroep op hoog niveau inzake kunstmatige intelligentie
AVG	Algemene Verordening Gegevensbescherming
CAS	Criminaliteits Anticipatie Systeem
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
MvT	Memorie van Toelichting
PredPol	Predictive Policing systeem in Amerika
Rb	Rechtbank
SyRI	systeem risico inventarisatie
Sv	Wetboek van Strafvordering
WODC	Het Wetenschappelijk Onderzoek- en Documentatiecentrum
WWR	Wetenschappelijke Raad voor het Regeringsbeleid

Samenvatting

De digitalisering binnen de opsporing is volop in ontwikkeling. Enorme hoeveelheden data kunnen een belangrijke rol spelen bij de opsporing en vervolging van een verdachte. Binnen deze grote vergaarbakken aan data staat vaak de privacy van de burger ter discussie. Ingeval van de opsporing is het de vraag in hoeverre de privacy beperkende maatregel in verhouding staat met het recht op privacy. In het onderzoek staat één specifieke vorm van opsporing centraal, namelijk Predictive Identification zoals ingezet in Roermond. De centrale vraag van het onderzoek luidt als volgt: doorstaat Predictive Identification de subsidiariteits- en proportionaliteitstoets uit artikel 8 lid 2 EVRM en zo ja wanneer?

In het onderzoek is een vergelijking gemaakt tussen de instrumenten SyRI en Predictive Identification. De instrumenten vertonen grote gelijkenissen met elkaar. En uit het onderzoek is gebleken dat zij beiden voldoen aan de definitie van Predictive Policing. Beiden zijn een systeem die een voorspelling maakt van normoverschrijdend gedrag waarbij grootschalige monitoring van data plaatsvindt met behulp van techniek met als doel om criminaliteit te voorkomen. En voor SyRI heeft de rechtbank Den Haag in februari 2020 de lijnen uitgezet waaraan een Predictive Policing instrument moet voldoen.

Aan de hand van het speelveld van artikel 8 lid 2 EVRM en de handvatten uit de SyRI-zaak is onderzocht of Predictive Identification de subsidiariteits- en proportionaliteitstoets doorstaat. De belangrijkste bevindingen uit het onderzoek zijn met name:

- in een gerechtelijke procedure waarin Predictive Identification ter discussie staat zal de rechter tot de conclusie (moeten) komen, dat deze onvoldoende transparant is. Eenzelfde conclusie als bij SyRI. De werking van het risicomodel en een lijst met indicatoren van Predictive Identification is niet bekend. Ook is niet bekend welke indicator welke bijdrage heeft in de classificatie van de risicoprofilering.

- indien Predictive Identification voldoende transparant zou zijn, dan bevat het ogenschijnlijk onvoldoende waarborgen tegen (onbedoelde) discriminerende uitvloeisels.

- in de kern gaat het bij *fair balance* om de vraag naar proportionaliteit en subsidiariteit van Predictive Identification. De *fair balance* bij de inzet van Predictive Identification is mijns inziens niet aanwezig of althans in onvoldoende mate. Het belangrijkste argument hiervoor is dat de verhoudingen zijn zoekgeraakt. Er wordt immers bergen met data binnengehaald, maar het resultaat is zeer beperkt. Eén op de 1.000 voorbijgangers levert een hit op. Maar een hit is nog geen verdachte of dader van mobiel banditisme, dus dat aantal ligt nog (veel) lager. Ook kunnen no-hits gebruikt worden voor andere lopende

politieonderzoeken, waarbij de data van Predictive Identification dus ineens interessant kan worden voor ieder politieonderzoek.

Predictive Identification voldoet nu (nog) niet aan de *fair balance*. De staat zal enkele maatregelen moeten nemen om de balans terug te brengen. Te denken valt aan het direct verwijderen van no-hit gegevens. Of het (rigoureus) beperken van datadeling binnen lopende politieonderzoeken.

De grootste uitdaging ligt echter in de transparantie. Het gebruik van algoritmen zal een steeds grotere en belangrijkere rol innemen in de opsporing. De manier waarop de Staat nu inzicht geeft in haar opsporingsmethode is onvoldoende transparant. De staat verschuilt zich mijns inziens achter het (te eenvoudige) argument van het opsporingsbelang. De Staat zal op zoek moeten naar een oplossing om de kloof tussen het opsporingsbelang en de transparantie te overbruggen.

INHOUDSOPGAVE

1. Inleiding

Het gebruik van algoritmen bij de opsporing van fraude is een *hot item.* De afgelopen periode stond het gebruik en de werking van algoritmen frequent op de agenda bij het politieke debat in Den Haag. De meest bekende – en wellicht ook het meest tot de verbeelding sprekende – voorbeelden zijn de kinderopvangtoeslagaffaire bij de Belastingdienst en het Systeem Risico Inventarisatie (SyRI). Het algoritme van de Belastingdienst is een zelflerend risicomodel. Daarbij wordt gekeken naar enkele tientallen indicatoren die bij elkaar een totaalscore opleveren.[1] Een hogere score leidt tot een handmatige controle door een medewerker van Toeslagen. Een belangrijke ter discussie staande indicator is; een niet-Nederlandse nationaliteit is van invloed op de risicoscore. Enkel in combinatie met andere indicatoren kan dit leiden tot een hoge risicoscore. Eén enkele indicator levert geen kans op extra controle op, het gaan namelijk om de totaalscore. In beide gevallen leidde de uitkomsten van het algoritme tot landelijke verontwaardiging. Deze verontwaardiging komt tot stand vanwege de mogelijkheid van discriminatie en oneerlijke behandeling door het algoritme.[2] Bij de toepassing van algoritmes kan er sprake zijn van een zogenaamde bias, een bepaalde vooringenomenheid. Simpel uitgelegd: als je crimineel gedrag van mensen wilt voorspellen en in de data zitten veel mensen die langer zijn dan 1.90 meter, dan zal het algoritme snel(ler) mensen met een lengte van 1.90 meter als crimineel aanmerken. Op deze manier kan – onbewust en onbedoeld – directe of indirecte discriminatie in het algoritme sluipen.

Een coalitie van eiseres in de procedure tegen de Staat inzake de inzet en het gebruik van SyRI stellen de inrichting van het algoritme ter discussie. Zij eisen opheldering en uitleg. Vanwege het gebrek daaraan noemen zij SyRI een black box. Het zijn termen die verwijzen naar transparantie, of beter gezegd: het gebrek aan transparantie daarvan. In het rapport *'Big Data in een vrije en veilige samenleving* van de Wetenschappelijke raad voor het regeringsbeleid is al enige tijd geleden de nodige aandacht geschonken aan het risico van – het gebrek aan – transparantie. De algoritmen an sich worden steeds complexer, waardoor het steeds moeilijker wordt om deze uit te leggen.[3] Het begrip transparantie wordt dus beschouwd als de sleutel tot het succes.[4] De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) schrijft in haar rapport dat: ''de transparantie van de gegevensverwerking moet worden vergroot, en er moet een beter evenwicht komen tussen het vereiste van geheimhouding en het belang van openbaarheid over Big Data-

[1] Autoriteit Persoonsgegevens, *de verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag*, z2018-22445, 17 juli 2020, p. 14.
[2] WRR, *Big Data in een vrije en veilige samenleving*, Den Haag/Amsterdam: Amsterdam University Press 2016, p. 12.
[3] WRR, *Big Data in een vrije en veilige samenleving*, Den Haag/Amsterdam: Amsterdam University Press 2016, p. 69.
[4] M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht' (Preadvies NJV), *Wolters Kluwer* 2016, p. 93.

toepassingen die aan fundamentele vrijheden raken.''[5] [6] Een uitspraak van Den Haag over SyRI sluit hierop naadloos aan.

1.1 Aanleiding

De rechtbank Den Haag boog zich begin 2020 over de transparantie van het systeem SyRI. Kort en simpel uitgelegd: SyRI is een computersysteem dat persoonsgegevens van burgers uit verschillende overheidssystemen koppelt met de intentie om diverse vormen van fraude, misbruik en overtredingen op te sporen.[7] Het resultaat van SyRI is een op individueel niveau weergegeven verhoogd risico op oneigenlijk gebruik c.q. fraude.

De rechtbank Den Haag stelde zich - onder meer - op het standpunt dat: "dat in de SyRI-wetgeving onvoldoende wordt voorzien in waarborgen ter bescherming van het recht op respect voor het privéleven in relatie tot de risico-indicatoren en het risicomodel die in een concreet SyRI-project kunnen worden gebruikt. De SyRI-wetgeving biedt zonder inzicht in de risico-indicatoren en het risicomodel, althans zonder nadere wettelijke waarborgen die dit gebrek aan inzicht compenseren, onvoldoende handvatten voor de conclusie dat met de inzet van SyRI de inmenging in het privéleven in het licht van het misbruik en de fraude die wordt beoogd te bestrijden steeds proportioneel en daarmee noodzakelijk is, zoals artikel 8 lid 2 EVRM vereist."[8]

Bij SyRI ontbreekt aldus de balans tussen het maatschappelijk belang ter voorkoming van fraude, misbruik en overtreding enerzijds en de inbreuk op het privéleven van burgers anderzijds. Het gevolg? SyRI mag niet meer als handhavingsinstrument worden ingezet. Hoger beroep wordt niet ingesteld. De uitspraak van de rechtbank Den Haag blijft dus onaangetast en daarmee blijft dus ook SyRI onbruikbaar als handhavingsinstrument.

1.2 Doel- en probleemstelling

SyRI vertoont gelijkenissen met vormen van Predictive Policing zoals PredPol en CAS. PredPol – een afkorting van Predictive Policing – is een politiesysteem uit Amerika dat basis van gegevens over het type criminaliteit, plaats en tijd uit het verleden een voorspelling kan doen over de toekomst. PredPol richt zich op de voorspelling van verkeersongevallen,

[5] WRR, *Big Data in een vrije en veilige samenleving*, Den Haag/Amsterdam: Amsterdam University Press 2016, p. 146.
[6] AI HLEG, *Ethische richtsnoeren voor betrouwbare KI*, 08 april 2019.
[7] *Kamerstuk II* 2012/2013, 33 579, nr. 3.
[8] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.95.

drugscriminaliteit en diefstal.[9] De Nederlandse politie gebruikt een soortgelijk systeem, namelijk het criminaliteits anticipatiesysteem (CAS). Naast vergelijkbare informatie die PredPol verzamelt, verzamelt CAS ook andere variabelen. Denk hierbij aan de dichtstbijzijnde snelwegoprit en sociaal-demografische zaken van inwoners.[10] Vervolgens deelt het systeem een aangewezen gebied op in vakjes gevuld met een voorspelling of er een bepaalde vorm van criminaliteit zal plaatsvinden.

De belangrijkste vraag die is gerezen, is of Predictive Policing instrumenten voldoende transparant zijn zodat kan worden afgewogen of de inbreuk op het recht op privacy subsidiair en proportioneel is.

In het onderzoek wordt één specifieke vorm van Predictive Policing nader onderzocht, namelijk Predictive Identification. In Roermond is een proef met Predictive Identification gaande om mobiel banditisme tegen te gaan. Het OM legt het mobiel banditisme als volgt uit: ‘’mobiel banditisme is een vorm van internationaal georganiseerde criminaliteit. Het gaat hierbij om rondtrekkende bendes die delicten plegen als babbeltrucs, zakkenrollerij, inbraken, winkel-, metaal- en autodiefstal.’’[11] Een manier om mobiel banditisme tegen te gaan is om de potentiele daders zo snel mogelijk in beeld te krijgen. Camera’s moeten potentiele daders op weg naar het outletcentrum van Roermond al signaleren. De camera’s en sensoren screenen auto’s op de snelwegen rondom Roermond en brengen de herkomst en de (afgelegde) route van de auto in beeld gebracht.[12] Op basis van de (geautomatiseerde) data-analyse kan een *red flag* afgegeven worden. Is er gerede twijfel over de situatie? Dan wordt een politie-eenheid op de gekenmerkte situatie afgestuurd.

In het onderzoek wordt onderzocht of Predictive Identification - een vorm van Predictive Policing - hetzelfde lot staat te wachten als SyRI. Met andere woorden: doorstaat Predictive Identification de subsidiariteits- en proportionaliteitstoets uit artikel 8 lid 2 EVRM en zo ja wanneer?

[9] Rienks, *Predictive policing, kansen voor een veiligere toekomst,* Apeldoorn: Politieacademie 2015, p. 6.
[10] Rienks, *Predictive policing, kansen voor een veiligere toekomst,* Apeldoorn: Politieacademie 2015, p. 7.
[11] Openbaar Ministerie, *Onderwerp: mobiel banditisme,* https://www.om.nl/onderwerpen/mobiel-banditisme geraadpleegd op 03 oktober 2020.
[12] *Plan van aanpak: Operationele Proef Tuin Sensing Roermond*, Politie, 12 oktober 2017.

Ter beantwoording van de hoofdvraag zijn een aantal deelvragen geformuleerd.

1. Wat is Predictive Policing en vallen het Systeem Risico Indicatie (SyRI) en Predictive Identification (proef Roermond) onder deze definitie?
2. Wat houdt het transparantiebeginsel in?
3. In hoeverre speelt het transparantiebeginsel een rol bij de beoordeling van de vraag of Predictive Policing instrumenten voldoen aan de waarborgen van artikel 8 EVRM?
4. Voldoet Predictive Identification als ingezet in Roermond aan de waarborgen van artikel 8 EVRM?

1.3 Onderzoeksmethode

Het onderzoek bestaat uit een juridisch- dogmatisch onderzoek. Daarbij wordt gebruik gemaakt van verschillende bronnen, zoals boeken, internetbronnen, jurisprudentie, kamerstukken en wetenschappelijke artikelen.

1.4 Leeswijzer

In het eerste hoofdstuk wordt de eerste deelvraag behandeld. Daarin staat de term Predictive Policing centraal. Aan de hand van literatuuronderzoek wordt nagegaan wat daaronder kan worden verstaan en of de systemen SyRI en Predictive Identification als Predictive Policing instrumenten bestempeld kunnen worden.

In het tweede en derde hoofdstuk worden de tweede en derde deelvraag behandeld. De deelvragen liggen in elkaars verlengde, want de term transparantie staat centraal. Aan de hand van literatuuronderzoek en jurisprudentie wordt in hoofdstuk twee nader toegelicht wat het transparantiebeginsel inhoudt. In hoofdstuk drie wordt vervolgens uiteengezet welke rol het transparantiebeginsel speelt bij de beoordeling of de inbreuk op het recht op privacy (artikel 8 EVRM) subsidiair en proportioneel is.

In het vierde hoofdstuk wordt nagegaan of Predictive Identification voldoet aan de waarborgen van artikel 8 EVRM waarbij vooral wordt ingegaan op de vraag of Predictive Identification voldoende transparant is.

Ten slotte zal er in de conclusie een antwoord worden gegeven op de hoofdvraag.

2. Wat is Predictive Policing en vallen SyRI en Predictive Identification (proef Roermond) onder deze definitie?

Alvorens beoordeeld kan worden of SyRI en Predictive Identification gedefinieerd kunnen worden als Predictive Policing instrumenten is het van essentieel belang om helder te hebben wat onder Predictive Policing wordt verstaan. Dat betekent dat in dit hoofdstuk in eerste instantie de definitie van Predictive Policing aan bod komt. Nadien worden de kenmerken van SyRI en Predictive Identification uiteengezet. In het slot van dit hoofdstuk wordt een antwoord gegeven op de vraag of SyRI en Predictive Identification (proef Roermond) onder de definitie vallen van Predictive Policing.

2.1 Definitiebepaling van Predictive Policing

De moderne technologie neemt een enorme vlucht. Niet alleen in het gebruik door de burger en bedrijven, ook door de overheid. Met behulp van techniek kan bepaalde data geautomatiseerd worden onderzocht. Binnen de opsporing van de politie wordt gebruik gemaakt van algoritmen die trachten een verband te leggen tussen data en criminaliteit. De term Predictive Policing is gelanceerd door William Bratton in functie als politiechef bij Los Angeles Police Department.[13] William Bratton lanceerde in zijn korps hedendaagse wiskundige methoden om criminaliteit in Los Angeles te voorspellen waarmee politie-inzet effectief en efficiënt kon worden ingezet.[14] Het Amerikaanse model krijgt de term Predpol, een afkorting van Predictive Policing. De Nederlandse equivalent is CAS. De uitkomst van het algoritme is een voorspelling over de kans dat op een bepaalde plaats en tijd een misdrijf zal plaatsvinden.[15] De doelstelling van CAS is de preventie van criminaliteit en optimalisatie van de inzet van politie.[16] Het is Predictive Policing software.

Een zoektocht in relevante literatuur levert de volgende definities van Predictive Policing op. Een eerste definitie van de term Predictive Policing is afkomstig van de politie zelf. Logisch, aangezien vanuit de politie immers ook de term Predictive Policing is gelanceerd. In het boek van Rutger Rienks, intellegenceprofessional binnen de politie, wordt Predictive Policing gedefinieerd als: ‘’Predictive Policing is de wetenschap die met (computer)modellen en relevante (politie)data risico’s in relatie tot criminaliteit berekent en op basis daarvan politiële

[13] Perry et. al., *Predictive Policing, the Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica: RAND Corporation, 2013, p. 4.
[14] Perry et. al., *Predictive Policing, the Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica: RAND Corporation, 2013, p. 4.
[15] WODC, ‘De toekomstbestendigheid van de politie’, *Justitiële verkenningen* 2017/4, p. 71.
[16] D. Willems & R. Doeleman 2014. ‘Predictive policing: Wens of werkelijkheid?’, *Het Tijdschrift voor de Politie* 76(4) 2014, p. 42.

acties voorstelt om deze risico's te verkleinen''[17] Een nagenoeg gelijke definitie wordt gehanteerd door de Wetenschappelijk Raad voor Regeringsbeleid (WRR). De WRR definieert Predictive Policing als volgt: ''omvat elke politiestrategie of -tactiek die gebaseerd is op het gebruik van grote hoeveelheden data en de geavanceerde methoden om deze data te analyseren en hiermee vooruitstrevende misdaadpreventie te realiseren''[18]

De hierboven gepresenteerde definities kennen een aanwijsbare afbakening in de definitiebepaling, aangezien in beide definities het ten gunste komt van politiële acties. Betekent dit dat de term Predictive Policing enkel is voorbehouden aan methoden van de politie? Dat valt te betwijfelen. Predictive Policing wordt namelijk in Perry et al gedefinieerd als: ''Predictive Policing is het voorspellen van crimineel en normoverschrijdend gedrag door middel van grootschalige monitoring en slimme data-analyses, met als belangrijkste doel criminaliteit te voorkomen.''[19] Een essentieel verschil met de eerder gegeven definities is dat deze definitie geenszins is voorbehouden aan politiële acties. In de definitie van Mayer-Schoonberger & Cukier ontbreekt eveneens een verwijzing naar politiële acties: ''Predictive Policing: using big-data analysis to select what streets, groups and individuals to subject to extra scrutiny, simply because an algorithm pointed to them as more likely to commit a crime''[20]

De strafbaarstelling van gedragingen is niet enkel voorbehouden aan het wetboek van strafrecht. In verschillende andere wetten zijn strafbepalingen opgenomen. Denk hierbij onder meer aan strafbepalingen in Milieuwetgeving, de Algemene wet inzake rijksbelastingen en de Participatiewet.

Anders gezegd: strafbare feiten zijn zowel in het wetboek van strafrecht alsmede in sectorale wetgeving geformuleerd. De overheid kan daartegen verschillende instrumenten c.q. bevoegdheden inzetten. Daarbij heeft de politie geen exclusieve handhavingspositie in Nederland, immers ook andere personen c.q. instanties kunnen belast worden met (bepaalde vormen van) handhaving. Denk daarbij aan de opsporingsambtenaren binnen de Belastingdienst of de gemeenten. Een definitiebepaling van Predictive Policing waarbij enkel

[17] Rienks, *Predictive policing, kansen voor een veiligere toekomst,* Apeldoorn: Politieacademie 2015, p. 21.
[18] Van Brakel, *Pre-emptive Big Data surveillance and its (dis)empowering consequences: The case of predictive* policing. In Van der Sloot & Schrijvers, *Exploring the boundaries of Big Data,* Den Haag/ Amsterdam: WRR/ Amsterdam University, p. 119.
[19] Perry et. al., *Predictive Policing, the Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica: RAND Corporation, 2013, p. 1.
[20] Mayer-Schonberger & Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Eamon Dolan/ Houghton Mifflin Harcourt, p. 158.

en alleen wordt verwezen naar politiële acties is mijns inziens onvolledig gelet op de huidige handhavingsmodaliteiten.

De definitie van Perry et al is daarom mijns inziens het meest geschikt. De definitie van Perry et al: ‘’Predictive Policing is het voorspellen van crimineel en normoverschrijdend gedrag door middel van grootschalige monitoring en slimme data-analyses, met als belangrijkste doel criminaliteit te voorkomen.’’[21] Uit deze definitiebepaling kunnen een aantal criteria gedestilleerd worden waaraan een systeem moet voldoen wil er sprake zijn van Predictive Policing. Deze criteria zijn:

- voorspelling van normoverschrijdend c.q. strafbaar gedrag; en
- grootschalige monitoring van data met behulp van (digitale) techniek; en
- met als doel het voorkomen van criminaliteit.

Aan de hand van deze criteria wordt beoordeeld of SyRI en Predictive Identification (proef Roermond) onder de hierboven beschreven definitie van Predictive Policing valt.

2.2 Valt SyRI onder de definitie van Predictive Policing?

In paragraaf 1.1 is het begrip Predictive Policing gedefinieerd. Daarbij zijn criteria geformuleerd waaraan een systeem moet voldoen wil er sprake zijn van Predictive Policing. In deze paragraaf wordt nagegaan of SyRI daaronder valt. Eerst wordt – voor zover mogelijk – nader toegelicht hoe het systeem SyRI werkt. Vervolgens wordt per criterium uitgewerkt of SyRI daaraan voldoet. Het slot van deze alinea bevat een antwoord op de vraag of SyRI voldoet aan de definitie van Predictive Policing als gegeven in hoofdstuk 1.

Het systeem SyRI werkt in grote lijnen als volgt. SyRI verzamelt allerlei (persoons)gegevens van burgers.[22] Deze gegevens worden gekoppeld door Stichting Inlichtingenbureau.[23] Een – door de minister vastgesteld – risicomodel dient ervoor te zorgen dat burgers met een verhoogd risico op fraude naar voren komen.[24] Indien een burger met een verhoogd risico naar voren komt dan wordt deze gemeld en nader geanalyseerd.[25] Indien de gegevens daartoe aanleiding geven bestaat tevens een grondslag om deze informatie te delen met het Openbaar Ministerie en/ of de politie.[26]

[21] Perry et. al., *Predictive Policing, the Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica: RAND Corporation, 2013, p. 1.
[22] Artikel 5a.2 lid 3 Het Besluit SUWI.
[23] Artikel 5a.3 Het Besluit SUWI.
[24] Artikel 1.1 Het Besluit SUWI.
[25] Artikel 5a.3 Het Besluit SUWI.
[26] Artikel 65, derde lid, onderdeel b, van de Wet SUWI.

Hoe ziet het risicomodel en/ of diens indicatoren eruit? Dat blijft een groot raadsel, aangezien de Staat hieromtrent niets heeft gepubliceerd. Evenmin heeft de Staat hieromtrent een verklaring afgegeven in de gerechtelijke procedure aangaande het gebruik van SyRI.[27] Het ontbreken van deze informatie is jammerlijk, maar niet onoverkomelijk voor de beantwoording van de deelvraag. Aan de hand van de reeds beschikbare informatie zal worden nagegaan of SyRI voldoet aan de criteria van Predictive Policing.

Het eerste criterium waaraan moet worden voldaan is een voorspelling van normoverschrijdend c.q. strafbaar gedrag. De werking van SyRI is reeds eerder uiteengezet. Simpelweg komt het erop neer dat SyRI de aangeleverde data analyseert. Aansluitend op de richtlijnen van de overheid bij het gebruik van algoritmen door de overheid zijn er vier type analyses te onderscheiden, namelijk: beschrijvend, diagnostisch, voorspellend en voorschrijvend.[28] Een diagnostisch en voorschrijvende analyse is niet aan de orde, dus is de vraag of SyRI een beschrijvende of een voorspellende analyse maakt. Een beschrijvende analyse beschrijft een kenmerk zonder verdere interpretatie.[29] Een voorspellende analyse maakt op basis van bepaalde kenmerken een voorspelling over een individu.[30]

De Staat betoogde in de gerechtelijke procedure dat SyRI expliciet geen tool is bij het voorspellen van normoverschrijdend c.q. strafbaar gedrag. De Staat stelt dat SyRI enkel bestanden met elkaar vergelijkt en de discrepanties toont.[31] De Staat is consequent in haar visie omtrent de vraag of hier sprake is van een voorspellend systeem. Immers bij de totstandkoming van Het Besluit SUWI is reeds het standpunt ingenomen dat de verwerkte gegevens niet worden verwerkt om te voorspellen.[32] Al met al kan worden aangenomen dat de Staat van mening is dat SyRI beschrijvende analyses maakt.

Het standpunt van de Staat aangaande een beschrijvende analyse is twijfelachtig. Vanuit het perspectief van data science – een vakgebied dat gericht is op het verkrijgen van inzichten uit data – kan betoogd worden dat er sprake is van een voorspellende analyse.[33] Ook specialisten op het gebied van het strafrecht – onder meer Das & Schuilenburg - zijn van

[27] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.49.
[28] Bijlage bij de brief van Minister voor Rechtsbescherming van 8 oktober 2019 (Kamerstukken II 2019, 2717062), p. 3.
[29] WRR, *Big Data in een vrije en veilige samenleving*, Den Haag/Amsterdam: Amsterdam University Press 2016, p. 44.
[30] WRR, *Big Data in een vrije en veilige samenleving*, Den Haag/Amsterdam: Amsterdam University Press 2016, p 44.
[31] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.48.
[32] Hoofdstuk 6 in Het Besluit SUWI (p. 19).
[33] Meer informatie over voorspellende analyses met data: Provost, F., & Fawcett, T. *Data Science for Business: What you need to know about data mining and data-analytic thinking,* O'Reilly Media, Inc, 2013.

mening dat SyRI gebruik maakt van een voorspellende analyse, omdat SyRI op basis van historische gegevens een nog onbekende strafbare gedraging van een individueel persoon zal inschatten[34]. Mijns inziens zijn de argumenten over een voorspellende analyse sterker dan die van een beschrijvende analyse. SyRI maakt gebruik van een risicotaxatiemodel.[35] Het gebruik van een risicotaxatiemodel duidt op een voorspellende analyse.[36] De verzamelde data wordt in een model gegoten waaraan risico-indicatoren zijn gekoppeld.[37] Het systeem SyRI geeft vervolgens een uitkomst of er sprake is van een verhoogde kans op onrechtmatigheden c.q. fraude.[38] Dit is geen louter beschrijvende analyse, het is verdergaand. SyRI analyseert de persoonlijke data en voegt daar – vooralsnog onbekende – indicatoren aan toe met als doel individuele personen met een verhoogd risico op normoverschrijdend c.q. strafbaar gedrag naar voren te schuiven. SyRI voorspelt dus als het ware de individuele persoon waar het normoverschrijdend c.q. strafbaar gedrag het grootst is.

Over de term voorspellen nog enige twijfel bestond, bestaat er geen twijfel dat het gaat om normoverschrijdend c.q. strafbaar gedrag. Een verwijzing naar artikel 1.1. onder z Het Besluit SUWI volstaat als argument. In het betreffende artikel staat namelijk:
‘’risicomodel: een model dat bestaat uit vooraf bepaalde indicatoren en aangeeft of er sprake is van een verhoogd risico op:

- onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van sociale zekerheid en de inkomensafhankelijke regelingen,
- belasting- en premiefraude, of
- het niet naleven van arbeidswetten.’’

Aan het eerste in hoofdstuk 1 onderscheiden criterium, er moet sprake zijn van een voorspelling van normoverschrijdend c.q. strafbaar gedrag, is dus voldaan.

Het tweede criterium waaraan moet worden voldaan is grootschalige monitoring van data met behulp van techniek. Evident is er sprake van grootschalige monitoring. Deze is zelfs zo grootschalig dat de Raad van State bij haar advies over het systeem SyRI een kanttekening plaatst bij de potentiele gegevens: ‘’*deze categorieën zijn ruim en veelomvattend en de gegevens die eronder vallen kunnen in een aantal gevallen diep ingrijpen in iemands*

[34] Das & Schuilenburg, *‘Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht’*, Strafblad 2018(4), p. 21.
[35] Artikel 1 lid 1 onder aa Het Besluit SUWI.
[36] Bijlage bij de brief van Minister voor Rechtsbescherming van 8 oktober 2019 (Kamerstukken II 2019, 2717062), p. 8.
[37] Artikel 1 lid 1 onder x en z Het Besluit SUWI.
[38] Artikel 1 lid 1 onder aa Het Besluit SUWI.

persoonlijke levenssfeer. De opsomming van gegevens is weliswaar bedoeld om de gegevensverwerking in te perken (beginsel van dataminimalisatie), maar is in feite zo ruim dat er nauwelijks een persoonsgegeven te bedenken is dat niet voor verwerking in aanmerking komt. De opsomming lijkt niet bedoeld om in te perken, maar om zoveel mogelijk armslag te hebben."[39] De techniek in deze is het systeem SyRI. Uit artikel 65 lid 1 Het Besluit SUWI blijkt namelijk dat SyRI de risicoanalyses uitvoert.

Het derde criterium waaraan moet worden voldaan is het voorkomen van criminaliteit. Uit de nota van toelichting blijkt glashelder dat SyRI het voorkomen van criminaliteit als doelstelling heeft. In de nota van toelichting staat namelijk*: een belangrijke manier om dit te bereiken is door gebruik te maken van gegevens die de overheid of andere organisaties met een publieke taak al beschikbaar hebben. De mogelijkheden van gegevensuitwisseling moeten daarom optimaal worden benut. Dit draagt bij aan het draagvlak in de sociale zekerheid en een adequate fraudebestrijding. Dit is het uitgangspunt van SyRI."*[40]

Al met al kan worden geconcludeerd dat SyRI voldoet aan de criteria van een Predictive Policing systeem. Er is een kleine ruimte voor discussie of SyRI voldoet aan het criterium van een voorspellend vermogen, maar de argumenten dat SyRI voorspelt zijn sterker en steekhoudender dan dat SyRI louter beschrijft.

2.3 Valt Predictive Identification (proef Roermond) onder de definitie van Predictive Policing?

Predictive Identification, zoals wordt toegepast in de strijd tegen mobiel banditisme in de outlet winkelcentra van Roermond werkt in grote lijnen als volgt. Predictive Identification analyseert de verkregen data op 'verdachte' omstandigheden. De data die worden aangeleverd zijn afkomstig uit camera's en sensoren die kentekens van auto's, routes van de auto's en telefoons van de inzittenden die met een wifi-netwerk zijn verbonden registreren.[41]

Hoe ziet het risicomodel en/ of diens indicatoren eruit? Dat is niet precies te zeggen. Waarom niet? Omdat eenzelfde strategie als bij SyRI wordt toegepast, namelijk in het belang van het (opsporings)onderzoek kan deze informatie niet worden prijsgegeven. Een WOB verzoek inzake de proef in Roermond heeft daarin niets veranderd. Uit de openbaar

[39] Advies van Raad van State inzake Ontwerpbesluit houdende regels voor fraudeaanpak door gegevensuitwisseling en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Besluit SyRI), met nota van toelichting (*Stcrt*. 2014, 26306).
[40] Hoofdstuk 2.1 in Het Besluit SUWI in *Stb* 2014, 320 (NvT).
[41] Schuilenburg, '*De camera maakt op eigen gezag van de burger een verdachte',* NRC 21 september 2018.

gemaakte stukken kan namelijk niet worden gedestilleerd welke omstandigheden een situatie verdacht maakt. Uit een interview met het Rathenau Instituut kan alsnog een tipje van de sluier worden weergegeven: ‘’*een informatieprofiel van mogelijke daders is opgesteld welke antwoord geeft op vragen zoals: welke mensen zijn het, van welke leeftijdscategorie, met welke auto’s komen ze, wat is hun land van afkomst en op welke tijdstippen zijn ze actief? Het profiel bestaat uit meer dan tien kennisregels, die de kenmerken van daders beschrijven. Iedere regel heeft een bepaalde score. De optelsom van al die scores haalt een bepaalde grens. Vanaf een bepaalde score hebben we te maken met een verdachte situatie. Vervolgens wordt nagegaan of een team op straat ingaat op deze verdachte situatie”*[42] Het ontbreken van deze informatie is jammerlijk, maar niet onoverkomelijk voor de beantwoording van de deelvraag. Aan de hand van de reeds beschikbare informatie zal worden nagegaan of Predictive Identification voldoet aan de criteria van Predictive Policing.

Het eerste criterium waaraan moet worden voldaan is een voorspelling van normoverschrijdend c.q. strafbaar gedrag. Een antwoord op een Kamervraag aangaande Predictive Identification geeft een aanknopingspunt: ‘’*de politie maakt gebruik van (klassieke) risicotaxatiemodellen om inschattingen te kunnen maken ten aanzien van het potentieel gebruik maken van geweld of het optreden van recidive bij personen met antecedenten zoals vastgelegd in de politiesystemen. Het taxatiemodel geeft alleen een inschatting of er een verhoogd risico is op het gebruik van geweld of het optreden van recidive bij een geselecteerde groep personen.”*[43] In de vorige paragraaf zijn de verschillende typen analyses reeds uitvoerig aan de orde gekomen. Kort gezegd is hier sprake van een voorspellende analyse, omdat het Predictive Identification systeem een individu naar voren schuift zodra deze een bepaalde score heeft gehaald op basis van vooraf vastgestelde normen. Deze score geeft aan in hoeverre er sprake is van een verhoogd risico op normoverschrijdend c.q. strafbaar gedrag, zoals: winkel- en ladingdiefstal, inbraak in woningen en bedrijven, zakkenrollerij en oplichting,[44] op basis van vooraf vastgestelde kenmerken.

Het tweede criterium waaraan moet worden voldaan is grootschalige monitoring van data met behulp van techniek. Camera’s en sensoren worden ingezet in de omgeving Roermond om kentekens en routes van auto’s in kaart te brengen. Het systeem maakt gebruik van

[42] Rathenau Instituut, ‘*Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan’,* geraadpleegd op 16 augustus 2020, https://www.rathenau.nl.
[43] Kamerstukken 26 643 en 32 761, nr 669, p. 17.
[44] Politie eenheid Limburg, *‘Mobiele bendes aan het roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond’’,* in Programma Mobiel Banditisme proeftuin Roermond, geraadpleegd op 6 augustus 2020, www.politie.nl/wob/korpsstaf/.

onder andere twee technische ontwikkelingen, namelijk artificial intelligence en machine learning.[45] Een algoritme is in feite een beslisboom. Artificial intelligence is een soort super algoritme, het kan namelijk zelfstandig leren en acties ondernemen. Machine learning is weer een stap verder, in die zin dat het op zoek kan naar patronen en voorspellingen door een enorme hoeveelheid data. Met andere woorden: Predictive Identification maakt gebruik van technologieën om een grote hoeveelheid aan data te verwerken tot behapbare proporties voor de ‘’echte’’ agenten op straat.

Het derde criterium waaraan moet worden voldaan is het voorkomen van criminaliteit. Blijkens de doelstelling van de proeftuin Roermond is er sprake van het voorkomen van criminaliteit. In de doelstelling staat namelijk: ‘’*eerder in de dreigingsontwikkeling van mobiel banditisme worden ingegrepen. Dit ter voorkoming, opsporing en beëindiging van strafbare feiten.’’*[46] Al met al kan worden geconcludeerd dat Predictive Identification voldoet aan de criteria van een Predictive Policing systeem.

[45] E. de Jonge, *‘’Projectplan Smart City Security Concept. Landelijk Project Operationele Proeftuinen. Programma Sensing’’,* in Programma Mobiel Banditisme proeftuin Roermond, geraadpleegd op 8 augustus 2020, www.politie.nl/wob/korpsstaf/.
[46] Politie, *‘’Criteria referentiebestanden en het opslaan van no-hits in verband met operationele proeftuin Sensing in de gemeente Roermond’’,* in Programma Mobiel Banditisme proeftuin Roermond, geraadpleegd op 11 augustus 2020, www.politie.nl/wob/korpsstaf/.

3. Wat houdt het transparantiebeginsel in?

In voorgaande paragraaf is nader toegelicht waarom Predictive Identification zoals ingezet in Roermond valt onder het begrip Predictive Policing. De inzet van zo'n systeem maakt een inbreuk op de privacy van burgers. Deze inbreuk kan legitiem zijn. Eén van de voorwaarden is dat het Predictive Policing instrument transparant moet zijn. Als het instrument transparant is, kan namelijk worden afgewogen of de inbreuk op het recht op privacy subsidiair en proportioneel is. De term transparantie(beginsel) staat daarom in dit hoofdstuk centraal. Het transparantiebeginsel is een containerbegrip. Een begrip zonder een scherp afgebakende betekenis. In dit hoofdstuk wordt nadere invulling gegevens aan het begrip transparantiebeginsel. Meer specifiek gaat het over het transparantiebeginsel bij het gebruik van algoritmen. Eerst zal vanuit een theoretisch kader worden nagegaan wat het transparantiebeginsel inhoudt. Vervolgens zal aan de hand van praktijkvoorbeelden worden geïllustreerd dat algoritmen niet zonder meer transparant zijn. Dit hoofdstuk wordt afgesloten met de grenzen aan het transparantiebeginsel.

3.1 Wat betekent het transparantiebeginsel bij het gebruik van algoritmen?

Wet- en regelgeving is het startpunt van de zoektocht naar de betekenis van het transparantiebeginsel. Bij de inzet van algoritmen waarbij gebruik wordt gemaakt van persoonsgegevens is de Algemene Verordening Gegevensbescherming (AVG) van toepassing.[47] De AVG is Europese privacywetgeving. Primair bedoeld om de rechten van de (getroffen) individuele burger te beschermen. Artikel 5 lid 1 sub a AVG is het belangrijkste artikel ingeval van inzet van algoritmen. Dit artikel geeft simpelweg aan dat de verwerking van persoonsgegevens transparant moet gebeuren. Hieruit vloeien een aantal informatieverplichtingen voort die uiteindelijk tot doelstelling hebben dat de informatie beknopt, begrijpelijk en gemakkelijk toegankelijk moet zijn.[48] Indien nodig kan met visualisaties worden gewerkt.[49] Met andere woorden: de AVG schrijft voor welke persoonsgegevens worden verwerkt, het doel van deze verwerking en de wijze waarop deze worden verwerkt.[50] Enkel in de gevallen waarbij sprake is van geautomatiseerde besluitvorming op basis van profilering gaat de AVG een stap verder. In die situaties moet de burger ook geïnformeerd worden over de onderliggende logica (artikel 13 lid 2 sub f AVG). Risico-modellen – zoals gebruikt bij SyRI – zijn geen onderdeel van geautomatiseerde

[47] Sommige verwerkingen van persoonsgegevens vallen niet onder de AVG. Deze worden hier buiten beschouwing gelaten.
[48] Brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 21 december 2018, kenmerk 2370000, p. 5.
[49] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679'.
[50] AP, ''*Toezicht op AI & Algoritmes''*, 17 februari 2020, p. 5.

besluitvorming, waardoor geen wettelijke verplichting bestaat tot uitleg van de onderliggende logica.[51] De verplichtingen omtrent de transparantie uit de AVG geldt primair voor de individuele burger. Dit betekent dat de transparantieverplichtingen uit de AVG niet inhouden dat het algoritme publiekelijk transparant moet zijn.

De wet- en regelgeving is vrij summier in de transparantieverplichtingen bij het gebruik van algoritmen. Sander Dekker, Minister voor Rechtsbescherming, heeft in een kamerbrief verkondigd dat bij het gebruik van algoritmen ook niet juridische aspecten kunnen meewegen. Niet juridische aspecten zijn bijvoorbeeld de technische transparantie en uitlegbaarheid.[52] Op deze manier kan in meer algemene zin een algoritme worden uitgelegd.[53] In de hiervoor aangehaalde kamerbrief van Minister Sander Dekker wordt verwezen naar de activiteiten van de Europese Commissie op dit onderdeel. Eén van die activiteiten is het oprichten van de deskundigengroep op hoog niveau inzake kunstmatige intelligentie (AI HLEG) door de Europese Commissie. AI HLEG is een onafhankelijke deskundigengroep en heeft in *Ethics Guidelines for Trustworthy AI* begrippen zoals technische transparantie en uitlegbaarheid beschreven. Niet geheel onbelangrijk om daarbij te vermelden is dat de *Ethics Guidelines for Trustworthy AI* geen bindend voorschrift is. De *Ethics Guidelines for Trustworthy AI* trachten uniforme richtsnoeren te geven voor betrouwbare kunstmatige intelligentie. Transparantie geldt voor zowel de gegevens, het systeem als de modellen.[54] Transparantie omvat traceerbaarheid, verklaarbaarheid en communicatie.[55] Traceerbaarheid houdt in dat de data, processen en de gebruikte algoritmen moeten worden vastgelegd. Op deze manier is controle mogelijk. Verklaarbaarheid ten aanzien van de technische ontwikkeling alsmede de (menselijke) beslissingen die worden genomen. Voor wat betreft de technische ontwikkeling dient inzicht gegeven te worden in het proces van besluitvorming, de totstandkoming en de keuzes bij het ontwerp van het algoritme. Communicatie houdt in dat het algoritme herkenbaar moet zijn. In de zin van: de burger moet weten dat hij of zij te maken heeft met een algoritme. Tevens moet er een mogelijkheid zijn van menselijke interactie.

In voorgaande alinea's is het transparantiebeginsel bij algoritmen in een theoretisch perspectief geplaatst. Het transparantiebeginsel moet bijdragen aan het vertrouwen in het systemen die hen raken, de (getroffen) burgers moeten deze kunnen begrijpen en daartegen

[51] Brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 21 december 2018, kenmerk 2370000, p. 7 en 8.
[52] Brief van de Minister voor Rechtsbescherming van 9 oktober 2019, kenmerk 2370000, p. 9
[53] Brief van de Minister voor Rechtsbescherming van 9 oktober 2019, kenmerk 2370000, p. 3.
[54] AI HLEG, *Ethics Guidelines for Trustworthy AI, Chapter II,* p. 21.
[55] AI HLEG, *Ethics Guidelines for Trustworthy AI, Chapter II,* p. 17.

bezwaar kunnen maken.[56] Een belangrijke vervolgstap is hoe het in de praktijk werkt. Is een algoritme transparant en dus duidelijk voor de getroffen burger?

3.2 Het transparantiebeginsel en algoritmen: waar gaat het mis?

Lodder waarschuwde in haar rapport aan het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) reeds in 2014 voor de risico's van het gebrek aan transparantie bij de inzet van big data. Eén van die risico's hield in dat personen zouden moeten weten welke analyses met hun gegevens gemaakt worden.[57] Diverse auteurs wijzen ook op andere potentiele risico's die het gebrek aan transparantie van algoritmen met zich meebrengen. Zo schrijven Kulk en Van Deursen dat het recht op rechtsbescherming in gevaar komt, omdat het algoritme niet altijd goed uitlegbaar is.[58] En Das en Schuilenburg wijzen op het risico van 'social sorting', omdat algoritmen risicogroepen op bepaalde specifieke kenmerken en/ of categorieën selecteert.[59] Onvoldoende inzicht in en toezicht op algoritmen kunnen deze risico's laten uitkomen tot werkelijkheid. Of het is gelukt om algoritmen transparant te laten zijn en dus de risico's te minimaliseren zal worden geïllustreerd aan de hand van twee voorbeelden. De gekozen voorbeelden zijn situaties waarin geen sprake bleek te zijn van transparantie, maar dat zegt niets over de vraag of algoritmen nooit transparant kunnen zijn. Een rechterlijke uitspraak waarbij het algoritme van de overheid transparant is bevonden is voor zover bekend niet voorhanden, maar ondenkbaar is het zeker niet. Weliswaar niet binnen een strafrechtrechtelijk kader, maar aanknopingspunten over transparante algoritmen zijn vindbaar. Bij de Afdeling bestuursrechtspraak van de Raad van State en de Hoge Raad zijn reeds toetsingskaders afgegeven bij het gebruik van een algoritme.[60] [61] En zodra een gebruiker van het algoritme voldoet aan het toetsingskader, dan is het algoritme in zekere zin transparant.

Een eerste en tevens belangrijkste voorbeeld waaruit blijkt dat er geen sprake is van een transparantie algoritme is de SyRI uitspraak. De rechtbank uit Den Haag is van oordeel dat het algoritme welke gebruikt wordt bij SyRI onvoldoende transparant is. Redenen voor de rechtbank om tot dit oordeel te komen zijn gelegen in de volgende feiten:

[56] Article 29 Data Protection Working Party,'Guidelines on transparency under Regulation 2016/679'.
[57] A.R. Lodder et. al, '*Big Data, Big Consequences? Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolging en rechtspraak',* Amsterdam: Vrije Universiteit Amsterdam 2014, p. 39.
[58] S. Kulk & S. van Deursen, '*Juridische aspecten van algoritmen die besluiten nemen Een verkennend onderzoek',* UU, 2 juni 2020, p. 192.
[59] Das & Schuilenburg, *'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht'*, Strafblad 2018(4), p. 24.
[60] ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454, Computerrecht 2018/253, m.nt. N. Jak & T. Barkhuysen.
[61] HR 17 augustus 2018, ECLI:NL:HR:2018:1316, AB 2018/388, m.nt. P. Flutsch.

- Een burger waarvan de persoonsgegevens zijn verwerkt, maar waar geen risico wordt aangetroffen is niet op de hoogte van de omstandigheid dat zijn gegevens zijn verwerkt.[62] De burger wordt niet in staat gesteld om zijn informatie te volgen. In feite is hier niet voldaan aan de informatieverplichting uit artikel 13 en 14 van de AVG. Het risico dat Lodder beschrijft is derhalve niet in de kiem gesmoord bij het gebruik van SyRI.
- De werking van het model is niet uitlegbaar. Het risicomodel en de methode van analyse is niet bekend.[63] Een enkel voorbeeld in de memorie van toelichting van de Wet SyRI is ontoereikend om te kunnen spreken van transparantie van het systeem en het model. In hoeverre selecteert het algoritme op specifieke kenmerken en/ of categorieën, waardoor er mogelijk sprake is van 'social sorting'? Deze vraag is vooralsnog niet met een ja of nee te beantwoorden, omdat het model en het systeem niet uitlegbaar is.

Een ander voorbeeld is te vinden in de rechtspraak van de Afdeling Bestuursrechtspraak Raad van State (ABRvS) welke is bevestigd door de Hoge Raad. Overheden maakten gebruik van AERIUS. Een systeem (het algoritme) berekent of stikstofnormen in een bepaald gebied niet worden overschreden als gevolg van de nieuwe activiteit die is aangevraagd. Het oordeel van de ABRvS is glashelder. Het algoritme is onvoldoende transparant, hetgeen het benutten van rechtsmiddelen bemoeilijkt. Immers is het niet duidelijk welke factoren en in welke mate deze meewegen tot een bepaalde beslissing.[64] Uit de uitspraak blijkt dat op het bestuursorgaan de verplichting rust om de gemaakte keuzes en de gebruikte data openbaar te maken.[65]

3.2 Grenzen aan het transparantiebeginsel

In beide procedures ontbrak het aan technische transparantie van het algoritme. Immers niet is uitgelegd hoe het systeem en/ of het model werkt. Het gebrek aan transparantie kan allerlei redenen hebben. Enerzijds leidt transparantie tot andere risico's zoals openbaring van handelsgeheimen, schendingen van auteursrechten en tot vormen van 'gaming the system'.[66] [67] Dit betekent dat burgers hun gedrag in overeenstemming brengen met het systeem. Anderzijds kunnen algoritmen – zeker degene met *machine en deep learning* – complex en ondoorgrondelijk zijn, hetgeen de transparantie bemoeilijkt. Welke van de mogelijk soms duizenden variabelen worden gebruikt? En welke factor is van

[62] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.90.
[63] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.87.
[64] ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 (St. Werkgroep Behoud de Peel/GS Noord Brabant), r.o. 14.3.
[65] ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 (St. Werkgroep Behoud de Peel/GS Noord Brabant), r.o. 14.4.
[66] R. van den Hoven van Genderen, '*Algoritmen en AI: distopische black box of glazen bol? Is een wettelijk kader voor transparantie van algoritmen mogelijk en wenselijk?',* Computerrecht 2020/5, p. 9.
[67] Kamerstukken II 2019/20, 26643 en 32761, 641, p. 8.

doorslaggevend belang? Vragen die in feite enkel bedoeld zijn voor bepaalde experts. [68] Is een algoritme dan nooit transparant? Neen, transparantie is mogelijk want het wordt immers door mensen gedefinieerd, maar het kent zijn grenzen. Het eigenlijk doel – transparantie voor de individueel getroffen burger – wordt niet bereikt door een technische uitleg van het systeem en/ of het model. De uitlegbaarheid van de uitkomst van het algoritme kan dit gebrek aan technische transparantie compenseren. Volgens de *Ethics Guidelines for Trustworthy AI* is een vereiste voor betrouwbare kunstmatige intelligentie de uitlegbaarheid van het model. Ingeval van uitlegbaarheid gaat het om het verklaren van de uitkomst van het algoritme in begrijpelijke taal.[69] Dus gericht op de uitleg van het doel van het gebruik van algoritmen.

Niet onbesproken mag blijven dat een wettelijke beperking van transparantie tot de mogelijkheden behoort. Op grond van artikel 23 AVG kunnen bepaalde informatieverplichtingen buitenspel gezet worden, zodra de nationale veiligheid, de openbare veiligheid en de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten in het geding zijn. Het buitenspel zetten van deze informatieverplichtingen is mogelijk in sectorspecifieke wetgeving en als deze voldoet aan de vereisten van artikel 23 AVG.

[68] R. van den Hoven van Genderen, '*Algoritmen en AI: distopische black box of glazen bol? Is een wettelijk kader voor transparantie van algoritmen mogelijk en wenselijk?',* Computerrecht 2020/5, p. 2.
[69] Bijlage bij de brief van Minister voor Rechtsbescherming van 8 oktober 2019 (Kamerstukken II 2019, 2717062), p. 5.

4. In hoeverre speelt het transparantiebeginsel een rol bij de beoordeling van de vraag of Predictive Policing instrumenten voldoen aan de waarborgen van artikel 8 EVRM?

Artikel 8 EVRM geeft de burger het recht op privacy. Het is een vrijheidsrecht welke uitgaat van bescherming van het individu op inbreuken van buitenaf op zijn privéleven. Dat recht is echter niet onbeperkt in haar omvang. Artikel 8 EVRM biedt immers ook de mogelijkheid tot een beperking van het recht op privacy. In dit hoofdstuk wordt nader ingegaan op de juridische grondslag van het Predictive Policing instrument zoals ingezet in Roermond. Vervolgens wordt uiteengezet onder welke voorwaarden een inbreuk op de privacy gerechtvaardigd is. Ten slotte wordt uitgelegd welk gevolg – in het kader van artikel 8 EVRM – een gebrekkige transparantie van het Predictive Policing instrument kan hebben voor de inzet van Predictive Policing instrumenten.

4.1 Proef Roermond: de juridische grondslag voor de inzet van Predictive Policing instrumenten

De Nota Rechtmatigheid is het startpunt van het onderzoek naar de juridische grondslag van de inzet van Predictive Policing instrumenten. In de Nota wordt gesteld dat: ‘*’indien en voor zover die inbreuk gering kan worden geacht, volstaat volgens vaste jurisprudentie (HR 19 december 1995, LJN: ZD 0328, Zwolsmanarrest) de wettelijke algemene taakomschrijving van de politie van artikel 3 Politiewet*.’’[70] Dat artikel 3 Politiewet als voldoende grondslag geldt voor niet-specifiek in de wet geregelde opsporing is reeds meermaals bevestigt in jurisprudentie.[71] Nieuwe opsporingshandelingen, zoals Predictive Policing instrumenten, hebben hun grondslag in artikel 3 Politiewet. Pas zodra de opsporingshandeling ter discussie wordt gesteld en de rechter een oordeel heeft gevormd over de onbevoegdheid van de opsporingshandeling is dit aanleiding voor de wetgever om een expliciete wettelijke grondslag te formuleren.[72] Bestaat er reeds een expliciete grondslag voor Predictive Policing zodra de inbreuk op de grondrechten van burgers groter is waardoor artikel 3 Politiewet niet meer volstaat?

Predictive Policing kent een proactief karakter, aangezien één van de criteria van Predictive Policing is het voorkomen van criminaliteit. Predictive Policing vindt dus doorgaans plaats in een (zeer) vroeg stadium. Er is (nog) geen sprake van een redelijk vermoeden van schuld

[70] Politie 2019C, document nr. 083, ‘Nota rechtmatigheid OPTR en GPV’, p. 1.
[71] ECLI:NL:RBBRE:2006:AY7442; HR 1 juli 2014, *NJ* 2015/114 (Stille sms) en *NJ* 2015/115 (IMSI-catcher), m.nt. Van Kempen.
[72] E. Muller e.a., Politie. Studie over haar werking en organisatie (Handboeken veiligheid), Deventer: Kluwer 2014, p. 292-294.

aan een strafbaar feit (artikel 27 Sv).[73] Daarbij dient opgemerkt te worden dat dit ook niet (meer) vereist is voor de toepassing van artikel 132a Sv. Mijns inziens is er ruimte voor discussie of ingeval van Predictive Policing sprake is van een onderzoek in verband met strafbare feiten (artikel 132a Sv). Het is afhankelijk van de mate van gerichtheid van het onderzoek of het gekenmerkt kan worden als een onderzoek in verband met strafbare feiten.[74] De gerichtheid van het onderzoek in Roermond zou – volgens de uitleg van de politie over de werking van het Sensing project – vrij gericht zijn, omdat het pretendeert te kunnen voorspellen welke burgers de grootste risico vormen met betrekking tot het mobiel banditisme. Een bijzonder interessant vraagstuk waar de rechter tot zover bekend nog geen uitspraak over heeft gedaan.

Das & Schuilenburg bevelen aan dat bij de modernisering van het Wetboek van Strafvordering een expliciete grondslag opgenomen moet worden voor het gebruik van Predictive Policing instrumenten.[75] De Commissie Koops heeft in haar rapport *regulering van opsporingsbevoegdheden in een digitale omgeving* expliciet aandacht voor artikel 132a Sv en het proactieve karakter van onder meer Predictive Policing. De Commissie Koops stelt daarom een nieuwe definitie van het opsporingsbegrip voor, hetgeen betekent dat er meer ruimte ontstaat voor opsporingsonderzoek dat is gericht op het beëindigen van het strafbare feit.[76] De standpunten van Das & Schuilenburg en de Commissie Koops lijken te insinueren dat de huidige in het wetboek opgenomen opsporingsmethode(n) waarschijnlijk niet voldoen als inzet van Predictive Policing zodra de inbreuk op de privacy groter is en artikel 3 Politiewet dus niet meer volstaat.

Hierboven is met name de juridische grondslag voor de verkrijging van de gegevens uiteengezet. De wijze van verwerking van deze gegevens is vastgelegd in de Wet politiegegevens (Wpg). Het moet gaan om een persoonsgegeven dat in het kader van de politietaak wordt verwerkt, aldus artikel 1 sub a Wpg. De politie gaat uit van het feit dat de gegevens die worden verwerkt in het project van Roermond dat het politiegegevens betreft.[77] Artikel 3 Wpg bepaalt dat politiegegevens enkel verwerkt mogen worden indien: (a) voor zover zij rechtmatig zijn verkregen, (b) noodzakelijk is voor bij of krachtens die wet bepaalde doeleinden en (c) gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake

[73] B. Vulto & D. Sander, '*Predictive identification. Tussen instrumentaliteit en rechtsbescherming*', Ars Aequi 2019/827, p. 1.
[74] Das & Schuilenburg, *'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht'*, Strafblad 2018(4), p. 25.
[75] Das & Schuilenburg, *'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht'*, Strafblad 2018(4), p. 26.
[76] Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Koops), 'Regulering van opsporingsbevoegdheden in een digitale omgeving, juni 2018, p. 23.
[77] Politie 2019C, document nr. 083, 'Nota rechtmatigheid OPTR en GPV', p. 2.

dienend en niet bovenmatig is. In dit artikel lezen we dus een noodzakelijkheids- en evenredigheidsbeginsel terug welke rechtstreeks voortvloeit uit artikel 8 EVRM.[78] In de volgende paragraaf zal dit nader worden uitgewerkt.

4.2 Hoe luiden de waarborgen uit artikel 8 EVRM?

In de voorgaande paragraaf is de juridische grondslag voor de proef in Roermond toegelicht. Hierbij is met name aandacht geweest voor het nationale wettelijke kader, namelijk het Wetboek van Strafvordering en de Wpg. Zoals aangegeven speelt artikel 8 EVRM een cruciale rol zodra het recht op privacy van burgers wordt geschonden. Maar wat valt onder het recht op privacy? Het beschermingsbereik van artikel 8 EVRM strekt zich uit over de gebieden privéleven, familieleven, de woning en correspondentie. In het geval van algoritmen bij Predictive Policing instrumenten geldt dat deze een inbreuk kunnen maken op het privéleven.[79] In het specifieke geval van de proef in Roermond wordt gebruik gemaakt van ANPR camera's en sensoren. Deze verzamelen systematisch gegevens, leggen deze vast voor een eventuele analyse en worden bewaard zodra het relevant is. Daarmee wordt het privéleven van burgers geraakt.[80] [81] Dit betekent dat de proef van Roermond een inbreuk maakt welke valt onder de reikwijdte van artikel 8 EVRM. Een inbreuk op het recht kan geoorloofd zijn, want het recht op privacy is niet absoluut. Anders geformuleerd: er is dus ruimte voor een belangenafweging op landelijk niveau.[82] Dit betekent dat een beperking op het recht op privacy mogelijk is wanneer is voldaan aan een bepaald aantal vereisten. Deze vereisten vormen een zogenaamd drietrapsraket. Eerst dient beoordeeld te worden of de inbreuk is gebaseerd op een wetsbepaling, vervolgens of het een legitiem doel dient en ten slotte ook als noodzakelijk kan worden beschouwd in een democratische samenleving.[83]

Het eerste criterium, bij wet voorzien, wordt door het EHRM ruim uitgelegd. Bij wet voorzien betekent niet enkel een wet in formele zin, maar ook lagere wetgeving en jurisprudentie.[84] [85] [86] De HR heeft daar aan toegevoegd dat ook richtlijnen, bijvoorbeeld aanwijzingen van het OM, als 'bij wet voorzien' kunnen worden geïnterpreteerd.[87] Essentieel is dat de grondslag

[78] Kamerstukken II 2012/13, 33 542, nr. 3, p. 16 (MvT).
[79] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.6.
[80] EHRM 2 september 2010, Uzun vs. Germany, nr. 35623/05, par. 44 e.v.
[81] HR 24 februari 2017, ECLI:NL:HR:2017:286, r.o.v. 2.3.3.
[82] T. de Jong, '*Het onderscheid tussen absolute rechten en relatieve rechten en de invloed van het materiële recht op de procedurele waarborgen'*, Procedurele waarborgen in materiële EVRM-rechten, Wolters Kluwer 2017/8.3, p. 1.
[83] Artikel 8 lid 2 EVRM.
[84] Zie EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568 (Sunday Times t. Verenigd Koninkrijk), paragraaf 87-88.
[85] EHRM 2 augustus 1984, nr. 8691/79 (Malone tegen het Verenigd Koninkrijk).
[86] Gerards e.a., Grondrechten. De nationale, Europese en internationale dimensie, Nijmegen: Ars Aequi Libri 2013, p. 165.
[87] HR 19 juni 1990, ECLI:NL:HR:1990:ZC8556 (Richtlijn en recht).

toegankelijk en voorzienbaar is.[88] De inbreuk makende regeling dient 'voldoende precies' geformuleerd te zijn, zodat de burger kan herleiden in welke omstandigheden en onder welke voorwaarden de beperking van artikel 8 EVRM is toegestaan.[89] In de SyRI-zaak wordt eveneens stilgestaan bij de begrippen toegankelijk en voorzienbaar: '*'Uit het arrest van S. en Marper tegen het Verenigd Koninkrijk blijkt dat de nationale wet, om aan de eisen van toegankelijkheid en voorzienbaarheid te voldoen, voldoende bescherming moet bieden tegen willekeur en met voldoende duidelijkheid de discretionaire ruimte die aan de bevoegde autoriteiten wordt toegekend en de wijze waarop daarvan gebruik mag worden gemaakt moet bepalen. In hoeverre de wettelijke waarborgen toereikend zijn, hangt volgens het EHRM dus af van de concrete omstandigheden en komt neer op een weging van het geheel van wettelijke waarborgen. De mate waarin en de gedetailleerdheid waarmee waarborgen in de wet moeten zijn vastgelegd, hangt af van de ingrijpendheid van de inmenging".*[90]

Het tweede criterium houdt in dat de inbreuk gerechtvaardigd kunnen zijn zodra de overheid een doel nastreeft zoals limitatief opgesomd in artikel 8 lid 2 EVRM. Doelen zijn bijvoorbeeld het voorkomen van strafbare feiten en het economisch welzijn. De rechtvaardiging op grond van een legitiem doel levert in de praktijk nauwelijks problemen op, omdat het legitiem doel vrij algemeen geformuleerd is.[91]

Het derde en tevens laatste criterium is de beoordeling of de inbreuk noodzakelijk is in een democratische samenleving. Het begrip noodzakelijk wordt uitgelegd als een *pressing social need.*[92] Het noodzakelijkheidsbeginsel loopt uiteen in twee criteria, namelijk het proportionaliteits- en subsidiariteitsbeginsel. Gerards legt het proportionaliteitsbeginsel als volgt uit: '*'de inbreuk op de privacy van de betrokkene mag niet onevenredig zijn in verhouding met het doel dat met de verwerking wordt verwezenlijkt. Het proportionaliteitsbeginsel vergt ook dat er steeds een belangenafweging plaatsvindt, waarbij gekeken moet worden naar de omstandigheden van het geval, het algemeen belang en de op het spel staande belangen van het individu. Op dit punt komt aan de verdragsstaten volgens vaste rechtspraak van het Hof een margin of appreciation toe*.''[93] Dit betekent in het geval van de inzet van Predictive Policing instrumenten dat het doel – het voorkomen van strafbare feiten – in verhouding moet staat met de inbreuk op de privacy. Het

[88] EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, nummer 6538/74 (Sunday Times tegen het Verenigd Koninkrijk), paragraaf 49.
[89] EHRM 29 juni 2006, nr. 54934/00 (Weber en Saravia t. Duitsland).
[90] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.68 t/m 6.70.
[91] EHRM 26 maart 1987, nr. 9248/81 (Leander t. Zweden), paragraaf 49.
[92] EHRM 25 juli 2013/25 oktober 2013,
ECLI:NL:XX:2013:365, nummer 27183/04 (Rousk tegen Zweden), paragraaf 136.
[93] Gerards e.a., Grondrechten. De nationale, Europese en internationale dimensie, Nijmegen: Ars Aequi Libri 2013, p. 166.

subsidiariteitsbeginsel houdt in dat er geen ander – lichter ingrijpend middel – beschikbaar is om het doel te bereiken. Anders geformuleerd: er moet sprake zijn van een '*fair balance'* tussen de doelen van de wetgeving die een inbreuk mogelijk maakt en de inbreuk op het privéleven die de wetgeving oplevert.[94] Een antwoord op deze vraag wordt behandeld in hoofdstuk vijf.

4.3 Wat is het gevolg van een gebrekkige transparantie van het algoritme in het licht van artikel 8 EVRM?

Wat mij betreft kan hier een parallel worden getrokken met de SyRI-uitspraak. Vergelijkend met de SyRI-uitspraak kan de vraag gesteld worden of het Predictive Policing instrument – zoals ingezet bij de proef in Roermond – objectieve feitelijke gegevens bevat welke gerechtvaardigd tot de conclusie kunnen leiden dat sprake is van een verhoogd risico van een bepaalde burger?[95] En voorziet het Predictive Policing instrument informatie over de werking van het risicomodel, zoals het type algoritme en de informatie over de methode van risicoanalyse?[96] Deze vragen hebben te maken met de transparantie, oftewel de controleerbaarheid. Het belang hiervan is groot, omdat er risico's aan zijn verbonden zoals (onbedoelde) discriminerende uitvloeisels.[97]

Als blijkt dat (ook) bij het Predictive Policing instrument in Roermond deze informatie ontbreekt en het onvoldoende waarborgen bevat ter bescherming van de privacy in relatie tot het Predictive Policing instrument, dan staat het hetzelfde lot te wachten als SyRI. De rechter kan dan geen oordeel vellen of de inbreuk op het recht op privacy subsidiair en proportioneel is.[98] Met andere woorden: de rechter kan geen zinnig woord zeggen of de inbreuk die door de overheid wordt gepleegd subsidiair en proportioneel is. Het heeft immers te weinig informatie over de werking van het systeem. En het gevolg daarvan kan zijn dat het Predictive Policing instrument niet meer ingezet mag worden. Of de proef in Roermond discriminerende uitvloeisels bevat en hetzelfde lot staat te wachten als SyRI zal nader uiteen worden gezet in het volgende hoofdstuk.

[94] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.80.
[95] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865, m.nt. Van Kolfschooten r.o.v. 6.87.
[96] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865, m.nt. Van Kolfschooten r.o.v. 6.89.
[97] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865, m.nt. Dommering, 11.
[98] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.95.

5. Voldoet Predictive Identification als ingezet in Roermond aan de waarborgen van artikel 8 EVRM?

In voorgaande hoofdstukken is uitvoerig stilgestaan bij de term Predictive Policing, Predictive Identification en de waarborgen van artikel 8 EVRM. Deze hoofdstukken waren essentieel voor het goed en volledig kunnen beantwoorden van de laatste deelvraag. In dit hoofdstuk zal namelijk de vraag worden beantwoord of de inzet van Predictive Identification in Roermond voldoet aan de waarborgen van artikel 8 EVRM. Het hoofdstuk is opgebouwd in volgorde van de vereisten van het zogenaamde drietrapsraket.[99] Eerst wordt beoordeeld of de inbreuk is gebaseerd op een wetsbepaling. Vervolgens of Predictive Identification een legitiem doel dient. Ten slotte wordt beoordeeld of Predictive Identification noodzakelijk is in een democratische samenleving.[100]

5.1 De wettelijke grondslag voor een inbreuk op de privacy door het gebruik van Predictive Identification

Predictive Identification – en ook Predictive Policing - als opsporingsinstrument is nog niet specifiek in de wet geregeld. Artikel 3 Politiewet geldt als voldoende grondslag voor niet-specifiek in de wet geregelde opsporing. Dit is meermaals bevestigt in jurisprudentie.[101] In hoofdstuk 2.3 is uitvoerig besproken dat Predictive Identification als een Predictive Policing systeem aangemerkt kan worden. Dit is van belang, omdat bepaalde standpunten van auteurs ten aanzien van Predictive Policing dus naar analogie mijns inziens ook van toepassing zijn op Predictive Identification. Lodder is van mening dat de algemene grondslag in beginsel volstaat bij de inzet van Predictive Policing.[102] Ook Brinkhoff onderschrijft deze wettelijke grondslag, en voegt daaraan toe dat artikel 3 Politiewet volstaat zolang daardoor slechts een beperkte inbreuk op grondrechten van burgers wordt gemaakt.[103] Of in de specifieke situatie van Predictive Policing slechts een beperkte inbreuk wordt gemaakt, daar laat Brinkhoff zich – helaas – niet over uit. Of er sprake is van slechts een beperkte inbreuk is zeker geen strak omlijnde materie, dus iedere situatie dient apart bekeken te worden. Jurisprudentie (zaak *Stille SMS)* geeft ons wel aanknopingspunten. Uit de zaak *Stille SMS* blijkt een belangrijk criterium, namelijk of door het gebruik van de techniek een 'min of meer compleet beeld van bepaalde aspecten van het persoonlijk leven van de betrokkene' wordt

[99] D. van Toor, *'Rechtvaardiging van de inbreuk op grond van artikel 8 lid 2 EVRM',* SteR, 2017, nr. 32, pargraaf III.6.2.4.
[100] Artikel 8 lid 2 EVRM.
[101] ECLI:NL:RBBRE:2006:AY7442; HR 1 juli 2014, *NJ* 2015/114 (Stille sms) en *NJ* 2015/115 (IMSI-catcher), m.nt. Van Kempen.
[102] A.R. Lodder et. al, '*Big Data, Big Consequences? Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolging en rechtspraak',* Amsterdam: Vrije Universiteit Amsterdam 2014, p. 63.
[103] S. Brinkhoff, *'Big data datamining door de Politie – IJkpunten voor een toekomstige opsporingsmethode',* NJB 2016/994, afl. 20, p. 1400 – 1407.

gevormd. De onderdelen zoals de duur, de intensiteit en de frequentie van het gebruik zijn daarbij essentieel.[104] En Gritter doet daar nog een schepje bovenop door te stellen dat een vorm van ongericht automatisch vergaren op grond van artikel 3 Politiewet rechtmatig is, ondanks dat de verzamelde gegevens óók informatie bevat van burgers die geen doel van onderzoek zijn of worden.[105] Deze vorm van inbreuk op de informationele privacy is inherent aan de politietaak.[106] Zoals aangegeven kunnen deze standpunten naar analogie ook worden gebruikt voor wat betreft de wettelijke grondslag voor de inzet van Predictive Identification. Geenszins lijkt bij deze vorm van Predictive Identification sprake te zijn van meer dan beperkte inbreuk, omdat geen of in zeer beperkte mate een beeld van het persoonlijk leven van de betrokkene wordt verkregen. In beginsel volstaat artikel 3 Politiewet voor de inzet van Predictive Identification. Dit betekent dat de inbreuk op de privacy is 'voorzien bij wet'. Er is nog geen jurisprudentie beschikbaar ten aanzien van de vraag of de inbreuk op de privacy door Predictive Identification – of Predictive Policing – zodanig groot is dat artikel 3 Politiewet niet meer voldoet. Met andere woorden: de inzet van Predictive Identification kan vooralsnog op grond van artikel 3 Politiewet worden gebaseerd, voor zolang niet anders besloten is door een rechter. Indien door een rechter in de toekomst anders wordt beoordeeld en de wet ongewijzigd blijft, dan is artikel 3 Politiewet ontoereikend en ontbreekt een specifieke wettelijke grondslag.[107] De tweede vraag van de zogenaamde drietrapsraket komt in de volgende paragraaf aan de orde.

5.2 Dient Predictive Identification een legitiem doel?

In artikel 8 EVRM staan expliciet legitieme doelen geformuleerd. Het voorkomen van strafbare feiten is één van die expliciet geformuleerde doelen. Er bestaat mijns inziens geen twijfel over de vraag of Predictive Identification in Roermond een legitiem doel dient. Een eenvoudige bevestiging is terug te lezen in de doelstelling van het project, namelijk: ''*eerder in de dreigingsontwikkeling van mobiel banditisme worden ingegrepen. Dit ter voorkoming, opsporing en beëindiging van strafbare feiten.''*[108] In de jurisprudentie wordt betrekkelijk eenvoudig de aangevoerde doelstelling geaccepteerd.[109] [110] De beantwoording van dit criterium blijft derhalve betrekkelijk kort. Meer nadruk wordt gelegd op het volgende criterium,

[104] HR 01-07-2014, ECLI:NL:HR:2014:1563, r.o.v. 2.5.
[105] E. Gritter, *'De rechtmatigheid van datamining door de politie',* TBS&H, 2018, nr. 2, p. 113.
[106] E. Gritter, *'De rechtmatigheid van datamining door de politie',* TBS&H, 2018, nr. 2, p. 115.
[107] Zie hoofdstuk 4.1.
[108] Politie, *''Criteria referentiebestanden en het opslaan van no-hits in verband met operationele proeftuin Sensing in de gemeente Roermond'',* in Programma Mobiel Banditisme proeftuin Roermond, geraadpleegd op 11 augustus 2020, www.politie.nl/wob/korpsstaf/.
[109] D. van Toor, ''*Het schuldige geheugen?*'', SteR nr. 32, 2017/III.6.2.4.2.
[110] Bijlage bij de brief van Minister van Justitie en Veiligheid van 11 december 2020 (Kamerstukken II 2020, 3090936), p. 9.

namelijk of Predictive Identification geschikt is om het doel te dienen. Oftewel een noodzakelijkeidstoets.

5.3 Is Predictive Identification noodzakelijk in een democratische samenleving?

Of het noodzakelijk is in een democratische samenleving is afhankelijk van het antwoord op de vraag of er sprake is van een *fair balance.* En deze *fair balance* moet er zijn tussen de doelen van de wetgeving die een inbreuk mogelijk maakt en de inbreuk op het privéleven die het oplevert. In de kern gaat het bij *fair balance* om de vraag naar proportionaliteit en subsidiariteit van Predictive Identification. Een aantal factoren zijn (mede) bepalend of sprake is van een *fair balance.* Uit de SyRI-zaak kunnen een aantal factoren worden gedestilleerd die relevant zijn voor deze beoordeling. Deze factoren gelden eveneens als leidraad bij de beoordeling over de vraag of er sprake is van *fair balance* bij de inzet van Predictive Identification.

Een eerste relevante vraag die beantwoord moet worden is of de hit een aanmerkelijk effect heeft op betrokkene, en zo ja in welke mate en ernst.[111] Volgens artikel 29 Data Protection Working Party, is sprake van een aanmerkelijk effect als het besluit het potentieel heeft om de omstandigheden, het gedrag of de keuzen van de betrokken burger in aanmerkelijke mate treft, een langdurig of blijvend effect op de burger heeft of tot uitsluiting of discriminatie van personen leidt. Het outletcentrum Roermond trekt jaarlijks ruim 5 miljoen bezoekers. Bij de proef in Roermond wordt een techniek toegepast die niet alle voertuigbewegingen vastlegt, maar enkel op specifieke wegen en voertuigen met specifieke kenmerken.[112] De waarneming omtrent de specifieke kenmerken kan pas worden gedaan, zodra een voertuig geregistreerd wordt. Zonder registratie kan immers ook niet vastgesteld worden of het om specifieke kenmerken gaat. Vanzelfsprekend gaan niet alle bezoekers per voertuig en ook niet iedere automobilist neemt de weg waarop het project Roermond zich richt, maar het leidt geen twijfel dat een ongekend aantal voertuigen voor verwerking in aanmerking komen. En het gegeven dat in het kader van een lopend politieonderzoek ook ‘no hits’ opgeslagen kunnen worden, betekent dat informatie uit het project Roermond met politie en Openbaar Ministerie gedeeld kan worden. De inzet van Predictive Identification heeft derhalve de potentie – of beter gezegd daadwerkelijk – een effect te hebben op de burger. Dit kan op verschillende manieren, zoals het beïnvloeden van het gedrag van de burger door bepaalde wegen wel of juist niet te nemen. Ook kan een no-hit dienen als (ondersteunend) bewijs in een lopend politieonderzoek, hetgeen een langdurig of blijvend effect kan hebben op de

[111] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.82.
[112] Brief van de Minister van Justitie en Veiligheid van 11 december 2020, kenmerk 3090936, p. 6.

betrokken burger. Al met al leidt dit tot de conclusie dat er sprake is van een (grote) impact op het privéleven van de burger.

De tweede vraag is of er voldoende waarborgen zijn om misbruik en willekeur tegen te gaan. Het transparantiebeginsel is het leidende hoofdbeginsel.[113] Transparantie is zo zwaarwegend, omdat aan het gebruik van het risicomodel en de daaropvolgende analyse het risico heeft dat (onbedoelde) discriminerende effecten optreden.[114] En daar zou zomaar eens sprake van kunnen zijn. Volgens de Minister van Justitie en Veiligheid is de dadergroep van mobiel banditisme met name afkomstig uit Roemenië, Bulgarije en Groot Brittannië.[115] Mijns inziens bevat deze stelling al (onbedoelde) discriminerende effecten. De bron waar de Minister van Justitie en Veiligheid naar verwijst is een rapport met de titel *Mobiele bendes aan het roer*. In dat rapport wordt de volgende definitie gehanteerd voor een mobiele bandiet, te weten: ‘’iemand die geen Nederlandse Nationaliteit bezit, niet in Nederland is geboren en zijn woonplaats niet in Nederland is.’’[116] Deze definitiebepaling door de politie is – zoals weergegeven in paragraaf 1.2 van dit onderzoek – een afwijkende definitie ten opzichte van de definitie van het OM. Bij de definitiebepaling van het OM gaat het om internationaal georganiseerde criminaliteit, hetgeen niet betekent dat Nederlanders zijn uitgesloten.[117] In het rapport *Mobiele bendes aan het roer* wordt dus een grote dadergroep van winkeldiefstallen en zakkenrollerij niet geschaard onder de definitie van mobiele bandiet. En wat blijkt uit de cijfers van het rapport *Mobiele bendes aan het roer?* Bij winkeldiefstallen en zakkenrollerij blijkt dat deze het vaakst worden gepleegd door personen met de Nederlandse nationaliteit en dus helemaal niet door de mobiele bandiet.[118] De politie is bij de proef in Roermond op zoek naar een Roemeense, Bulgaarse of Britse mobiele bandiet, terwijl dit slechts een kleine(re) groep is van de winkeldiefstallen en zakkenrollerij. Het heeft er alle schijn van dat de veronderstelling van onze Minister van Justitie en Veiligheid een (indirect) gevolg is van (onbedoelde) discriminerende effecten.

Kan een Nederlander – of een persoon met een willekeurig andere nationaliteit – wel een hit opleveren? Deze vraag is relevant, want het kan iets zeggen over de openbaarheid en kenbaarheid van het algoritme en haar indicatoren. De kenmerken bij het project Roermond zijn – voor zover bekend – het voertuig (o.a. merk, model, herkomst), het aantal inzittenden

[113] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.86.
[114] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.91.
[115] Brief van de Minister van Justitie en Veiligheid van 11 december 2020, kenmerk 3090936, p. 8.
[116] Politie, *‘’Eindversie Mobiele Bendes aan het Roer ’’,* in Programma Mobiel Banditisme proeftuin Roermond, geraadpleegd op 30 november 2020, www.politie.nl/wob/korpsstaf/, p. 17.
[117] Zie paragraaf 1.2 voor de definitie van het OM.
[118] Politie, *‘’Eindversie Mobiele Bendes aan het Roer ’’,* in Programma Mobiel Banditisme proeftuin Roermond, geraadpleegd op 30 november 2020, www.politie.nl/wob/korpsstaf/.

en de richting c.q. route van de auto. Een soortgelijke situatie deed zich voor in de SyRI-zaak waar ook enkele voorbeelden werden aangehaald die relevant konden zijn voor het algoritme. Het enkele feit dat een aantal voorbeelden zijn gegeven doet daar niets aan af nu de voorbeelden zonder objectief verifieerbare informatie op grond waarvan de voorbeelden berusten niet zijn toegelicht.[119] En er is een grotere lijst met criteria maar deze wordt niet gedeeld, omdat dit het opsporings- en handhavingsbelang doorkruist.[120] Evenmin is bekend in welke mate de indicatoren bijdragen aan een hit. Het algoritme en de factoren kunnen derhalve niet als openbaar en kenbaar worden gekwalificeerd. Echter kunnen er grenzen gesteld worden aan de openbaarheid. Beperkingen kunnen worden aanvaard, maar dat geldt alleen wanneer er goede redeneren bestaan en de beperkingen daaraan evenredig zijn.[121] Het algoritme draagt bij aan de opsporing en onderzoek van de politie en het OM, evident dus dat het een goede reden heeft. Of het evenredig is valt te betwijfelen. Het gebrek aan transparantie zorgt ervoor dat het moeilijk is om deze evenredigheid te toetsen. De kans dat er een discriminerend en stigmatiserend effect optreedt is reëel. De kans dat een Nederlander als mobiele bandiet wordt aangemerkt lijkt uitgesloten en een Roemeen als mobiele bandiet des te groter. De risico's van discriminatie en stigmatisering zijn in onvoldoende mate geborgd. En ook de Minister van Veiligheid en Justitie slaagt er niet in om in zijn antwoorden mij anders te doen geloven.

Een laatste relevante vraag is of er ruimte bestaat om het algoritme aan te passen. Het project in Roermond is een pilot. Binnen de pilot bestaat er ruimte – mede op basis van de resultaten - om het algoritme aan te passen. De Minister van Justitie en Veiligheid zegt hier het volgende over: ''*Vervolgens is eerst geanalyseerd onder welke condities het profiel een hit oplevert. Op basis daarvan is het opgestelde algoritme aangepast, zodat de hits voldoende relevant zouden zijn. De werkwijze omvat een zogenaamde leerlus. Het profiel omvat een aantal kenmerken van mobiel banditisme. Wanneer in de praktijk blijkt dat bepaalde kenmerken niet worden aangetroffen of wanneer bepaalde kenmerken wel worden aangetroffen, maar na opvolging blijkt dat voertuigen die worden stil gehouden niet bij de dadergroep passen, vindt er analyse en aanpassing van het profiel plaats"*.[122]

Of de effectiviteit van een project relevant is bij het noodzakelijkheidscriterium is interpretabel. In de SyRI zaak is het standpunt door de rechtbank ingenomen dat de effectiviteit niet vooraf hoeft vast te staan om te voldoen aan de eis van een *'pressing social*

[119] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.88.
[120] Brief van de Minister van Justitie en Veiligheid van 11 december 2020, kenmerk 2020Z17814, p. 2
[121] J. Gerards, R. Nehmelman & M. Vetzo, '*Algoritmes en grondrechten*, Den Haag: Boom Juridisch 2018, p. 81.
[122] Brief van de Minister van Justitie en Veiligheid van 11 december 2020, kenmerk 3090936, p. 5.

need'.[123] Custers is van mening dat bij de beoordeling van de noodzakelijkheid naar effectiviteit gekeken kan worden.[124] [125] De vraag in deze is of ze hetzelfde zeggen of dat er nuanceverschillen zijn. Hetgeen mijns inziens de strekking is, is dat de opsporingsmethode voorafgaand aan de invoering een bepaalde mate van effectiviteit moet hebben welke in verhouding staat met de inbreuk. Dus kan het instrument daadwerkelijk een bijdrage leveren en, zo ja, is dat substantieel? Predictive Identification in Roermond heeft zijn effectiviteit achteraf (nog) niet bewezen, maar deze vraag is ook minder van belang. Relevanter is de vraag of Predictive Identification vooraf effectief zou zijn? Mijns inziens had voorafgaand aan de implementatie van Predictive Identification redelijkerwijs ingeschat kunnen worden dat een enorme dataset verzameld en geanalyseerd moet worden alvorens een potentiele dader naar voren komt. Het aantal inbreuken op privélevens is enorm en het resultaat relatief gering. Met andere woorden: vooraf zou men in feite al zijn bedenkingen kunnen hebben over de verhouding tussen het aantal geanalyseerde data en de (weinige) hits. Mijns inziens kunnen er dus terecht vraagtekens geplaatst worden bij de substantiële bijdrage van Predictive Identification in Roermond. Achteraf blijkt dit ook zo te zijn, aangezien slechts één op de duizend reisbewegingen een hit oplevert.[126] Dus tegenover één hit – waarvan allerminst zeker is dat het ook een mobiele bandiet is – staan 999 inbreuken op het privéleven. En deze inbreuken zijn reel, omdat de gegevens ook voor andere doeleinden gebruikt kunnen worden.[127] De gegevens van no-hits worden dus niet direct vernietigd, maar pas na verloop van tijd én als ze niet relevant zijn voor andere politieonderzoeken.

Al met al kan worden geconcludeerd dat Predictive Identification zoals ingezet in Roermond niet aan de waarborgen voldoet van artikel 8 EVRM. Ondanks dat er een toereikende wettelijke grondslag is en het een legitiem doel dient, doorstaat het niet de toets van de noodzakelijkheid in een democratische samenleving. Het ontbreekt Predictive Identification aan een *fair balance.* De inbreuk op de vele privélevens is aanwezig, waarbij slechts een gering inbreuken ook een potentiele hit zou opleveren. Ook kan informatie van alle geanalyseerde gegevens worden gebruikt voor andere doeleinden, waaronder een lopend politieonderzoek. Het risicomodel dat wordt gebruikt is aanpasbaar, niet transparant en dus ook niet controleerbaar. Het risico op (onbedoelde) discriminerende effecten is zeer reëel. Een strikt theoretisch antwoord vanuit het perspectief van de rechter luidt dat het gebrek aan transparantie en controleerbaarheid niet kan worden beoordeeld en daarom niet voldoet in de waarborgen ter bescherming van het recht op respect voor het privéleven. En vanuit een

[123] Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865 r.o.v. 6.77.
[124] B. Custers, '*Nieuwe online opsporingsbevoegdheden en het recht op privacy',* JV 2018/05, p. 111.
[125] ECLI:CE;ECHR:2020:0611JUD007444017, EHRM 11 juni 2020, m.nt. Custers, paragraaf 11.
[126] Brief van de Minister van Justitie en Veiligheid van 11 december 2020, kenmerk 3090936, p. 6.
[127] Nota Rechtmatigheid OPTR en GPV, versie 1.3, 15 aug 2018. Bewaartermijn gegevens OPTR, p. 4.

minder neutrale positie dan die van een rechter is het haast onvermijdelijk om een voorzichtige conclusie te trekken dat Predictive Identification (onbedoelde) discriminerende effecten heeft.

6. Conclusie

De inzet van algoritmen bij de opsporing staat nog in de kinderschoenen. Een eerste belangrijke uitspraak volgde in februari 2020 toen de rechtbank Den Haag oordeelde dat SyRI – een zelflerend risicomodel dat scores geeft aan potentiele fraudeurs – onvoldoende waarborgen bevat ter bescherming van het recht op het privéleven. De rechtbank Den Haag heeft daarmee belangrijke eerste lijnen uitgezet voor het speelveld van algoritmen en opsporing. En dus rijst de vraag of, en zo ja in welke mate, andere algoritmen binnen de opsporing passen binnen de uitgezette lijnen van de rechtbank Den Haag. SyRI vertoont gelijkenissen met Predictive Identification. Deze gelijkenis is onder meer te vinden in het gegeven dat zij beiden voldoen aan de criteria van Predictive Policing. Zowel SyRI als Predictive Identification is een systeem met een (veronderstelde) voorspelling van normoverschrijdend gedrag, grootschalige monitoring van data met behulp van techniek en heeft als doel om criminaliteit te voorkomen. Om die reden is in dit onderzoek nagegaan of Predictive Identification past binnen de uitgezette lijn van de rechtbank Den Haag.

De inzet van instrumenten zoals SyRI en Predictive Identification maken een inbreuk op het privéleven van burgers. Burgers worden hiertegen beschermd door artikel 8 EVRM, maar die bescherming is niet onbeperkt in haar omvang. Een inbreuk is slechts toegestaan als aan de voorwaarden wordt voldaan van artikel 8 lid 2 EVRM, een zogenaamde drietrapsraket. Eerst dient beoordeeld te worden of de inbreuk is gebaseerd op een wetsbepaling, vervolgens of het een legitiem doel dient en ten slotte ook of de inbreukals noodzakelijk kan worden beschouwd in een democratische samenleving. De eerste twee criteria leveren geen problemen op. Het derde criterium is het cruciale criterium. Dit criterium – ook wel het noodzakelijkheidscriterium – valt uiteen in een subsidiariteits- en proportionaliteitstoets. In de SyRI-zaak was de rechtbank van oordeel dat onvoldoende transparantie aanwezig was om deze beoordeling te maken. De vraag die vervolgens opkomt is of dit ook geldt voor Predictive Identification?

Ik kom tot de conclusie dat in een gerechtelijke procedure een rechter eveneens tot het oordeel zou komen dat Predictive Identification onvoldoende transparant is. Onvoldoende transparant om te beoordelen of voldaan is aan de subsidiariteits- en proportionaliteitstoets. Het gebrek aan transparantie is het meest zichtbaar bij het risicomodel en diens indicatoren. Op het voorbeeld van de herkomst van een kenteken en het type auto, is niet inzichtelijk gemaakt hoe het risicomodel werkt. Bij Predictive Identification kan niet op objectieve gronden worden vastgesteld of er risico's zijn verbonden aan (onbedoelde) discriminerende uitvloeisels. De kans dat een Nederlander in aanmerking komt als mobiele bandiet lijkt zeer

miniem. De kans dat een Roemeen of Bulgaar als mobiele bandiet wordt aangemerkt is veel aanzienlijker, vanwege de herkomst van het kenteken. Andere indicatoren zijn onbekend of onderbelicht. Tevens is niet bekend welke indicator welk aandeel heeft in de classificatie van het risicoprofiel. Deze situatie toont op dit onderdeel veel gelijkenissen met SyRI. De rechter zal daarom eenzelfde conclusie nemen als in de SyR-zaak. Als ik – op basis van mijn onderzoek – een standpunt moet innemen of er sprake is van (onbedoelde) discriminerende uitvloeisels, dan ben ik geneigd deze vraag met een ja te beantwoorden. De Minister schrijft dat schuldigen aan mobiel banditisme in Roermond hoofdzakelijk afkomstig zijn uit Groot-Brittannië, Roemenië en Bulgarije. De Minister baseert zich daarbij op een rapport van de politie met de titel '*Mobiele bendes aan het roer'*. En in het rapport *Mobiele bendes aan het roer* schuilt een groot (onbedoeld) discriminerend uitvloeisel, omdat een rechtvaardiging op basis van criminaliteitscijfers risicovol is. Want hoe objectief zijn deze criminaliteitscijfers? Is deze doelgroep vaker schuldig aan mobiel banditisme of zoekt de politie vaker naar daders in deze doelgroep? Daarnaast voegt het rapport *Mobiele bendes aan het roer* eigenhandig een aantal criteria toe, waardoor het begrip mobiele bandiet afwijkt ten aanzien van de definitie van het OM. Het komt er – in het kort op neer – dat in het rapport *Mobiele bendes aan het roer* een Nederlander geen mobiele bandiet kan zijn. Het OM heeft deze beperkende definitie niet. In het geval van het rapport *Mobiele bendes aan het roer* betekent het dus per definitie dat alle verdachten van mobiel banditisme in het rapport *Mobiele bendes aan het roer* geen Nederlander. Op deze cijfers – en dus tevens misvatting – is het project Predictive Identification gebaseerd. En daar hebben we mijns inziens een (onbedoeld) discriminerend uitvloeisel te pakken.

Betekent dit het einde van de inzet van Predictive Identification? Dat hoeft niet. De inzet van algoritmen in de opsporing staat in de kinderschoenen, maar zal ongetwijfeld in de toekomst een wezenlijk onderdeel gaan (blijven) uitmaken van de opsporing. Om die reden is het belangrijk dat Predictive Identification in overeenstemming wordt gebracht met de lijnen zoals deze zijn uitgezet door de rechtbank Den Haag. In het geval van Predictive Identification kan meer inzicht gegeven worden in het model en diens indicatoren. Welke indicatoren dragen bij aan een hogere score op het profiel en welke indicatoren zijn ondergeschikt? Op deze manier kan namelijk ondervangen worden dat er onvoldoende waarborgen zijn tegen risico's van discriminatie en stigmatisering. Het argument van de Staat dat dit onwenselijk is in het kader van het opsporingsbelang zal ongetwijfeld zo zijn, maar de huidige inzet is sowieso ontoelaatbaar. De Staat kan zich niet steevast verschuilen achter het argument van het opsporingsbelang. De Staat zal een manier moeten bedenken om de transparantie te vergroten, zonder daarbij de potentiele daders in hun kaarten te laten

kijken. Op welke manier de Staat dit kan bewerkstellingen is geen onderdeel van het onderzoek geweest.[128]

In de hypothetische situatie dat Predictive Identification voldoende waarborgen bevat, betekent dat niet ook automatisch dat het de subsidiariteits- en proportionaliteitstoets doorstaat. Het stelt de rechter in ieder geval in staat om op objectieve gronden een inhoudelijk oordeel te vellen. En stel – in dezelfde hypothetische situatie – dat Predictive Identification voldoende transparant is, kunnen er mijns inziens terechte vraagtekens geplaatst worden bij de subsidiariteit en proportionaliteit. Het aantal dagelijkse inbreuken op privélevens is hoog, het aantal (betrouwbare) hits is gering en de verzamelde informatie van no-hits kan worden gebruikt in (andere) politieonderzoeken. De verhouding tussen het doel en het middel is daarmee zoekgeraakt. Mijns inziens slaat de *fair balance* dus in het nadeel uit voor de Staat. Predictive Identification moet – wil het voldoen aan de proportionaliteitseis - het aantal betrouwbare hits in relatie met de hoeveelheid geanalyseerde data groter maken. En het voorkomen van informatie-uitwisselingen voor andere politieonderzoeken zorgt er eveneens voor dat de impact op het privéleven van de burger kleiner wordt. Op deze manier komt er daadwerkelijk meer balans komen tussen de doelen van wetgeving die een inbreuk mogelijk maakt en de inbreuk op het privéleven die het oplevert. Op deze manier geraken we een stap dichterbij een transparante en proportionele inzet van algoritmen bij de opsporing.

[128] Voorbeelden zijn: wettelijke bepaling voor het ontwerp en inrichting van de systemen. Een toezichterhouder op deze datagestuurde systemen. Y. Buruma, ‘De criminele homo digitalis’, NJB 2016/22.

Literatuurlijst

Boeken

Broeders, D., E. Schrijvers & E. Hirsch Ballin 2017
Broeders, D., E. Schrijvers & E. Hirsch Ballin, *Big Data and Security Policies: Serving Security, Protecting Freedom*, Den Haag: WRR.

Commissie Koops 2018
Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Koops), *'Regulering van opsporingsbevoegdheden in een digitale omgeving,* juni 2018

Gerards e.a. 2013
Gerards e.a., Grondrechten. De nationale, Europese en internationale dimensie, Nijmegen: *Ars Aequi Libri 2013, p. 166.*

Gerards, Nehmelman & Vetzo 2018
J. Gerards, R. Nehmelman & M. Vetzo, '*Algoritmes en grondrechten*, Den Haag: Boom Juridisch 2018.

Lodder, van der Meulen, Wisman, Meij & Zwinkels 2014
A.R. Lodder, N. S. van der Meulen, T.H.A. Wisman, L. Meij, C.M.M. Zwinkels, *Big Data, Big Consequences? Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolging en rechtspraak,* Amsterdam: Vrije Universiteit Amsterdam 2014.

Muller e.a.
E. Muller et al, *Politie. Studie over haar werking en organisatie* (handboeken veiligheid), Deventer: Kluwer 2014.

Rienks 2015
R. Rienks, *Predictive Policing; Kansen voor een veiligere toekomst,* Apeldoorn: Lectoraat Intelligence Politieacademie 2015.

Sietsma 2006
R. Sietsma, *Gegevensverwerking in het kader van de opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy,* Den Haag: *Sdu* 2006.

WRR 2016
WRR, *Big Data in een vrije en veilige samenleving*, Den Haag/Amsterdam: Amsterdam University Press 2016.

Artikelen

Autoriteit Persoonsgegevens Onderzoeksrapport 2020
Rapport Autoriteit Persoonsgegevens, Belastingdienst/ Toeslagen: de verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, z2018-22445, 17 juli 2020.

Brakel 2016
R. van Brakel, 'Pre-emptive Big Data surveillance and its (dis)empowering consequences: The case of Predictive Policing. In Van der Sloot & Schrijvers, Exploring the boundaries of Big Data, Den Haag/ Amsterdam: *WRR/ Amsterdam University* 2016.

Brinkhoff 2016
S. Brinkhoff (2016), 'Big data datamining door de Politie – IJkpunten voor een toekomstige opsporingsmethode', *NJB* 2016/994, afl. 20.

Custers 2018
B. Custers, 'Nieuwe online opsporingsbevoegdheden en het recht op privacy', *JV* 2018/05.

Das & Schuilenburg 2018
A. Das & M.B. Schuilenburg, 'Predictive Policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht', *Strafblad* 2018(4).

Dijkstra e.a. 2016
M. Dijkstra, S. Joosten, E. Stamhuis & M. Visser, 'Beginselen digitaal. Digitalisering en de beginselen van de strafrechtspleging', Den Haag: *WODC* 2016.

Gritter 2018
E. Gritter, 'De rechtmatigheid van datamining door de politie', *TBS&H* 2018 nr. 2.

Hildebrandt 2016
M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht' (Preadvies NJV), *Wolters Kluwer* 2016.

van den Hoven van Genderen 2020
R. van den Hoven van Genderen, 'Algoritmen en AI: distopische black box of glazen bol? Is een wettelijk kader voor transparantie van algoritmen mogelijk en wenselijk?', *Computerrecht* 2020/5.

de Jong 2017
T. de Jong, 'Het onderscheid tussen absolute rechten en relatieve rechten en de invloed van het materiële recht op de procedurele waarborgen', Procedurele waarborgen in materiële EVRM-rechten, *Wolters Kluwer* 2017/8.3, p. 1

Kulk & van Deursen 2020
S. Kulk & S. van Deursen, 'Juridische aspecten van algoritmen die besluiten nemen Een verkennend onderzoek', *UU*, 2 juni 2020, p. 192.

Mayer-Schoonberger & Cukier 2013
V. Mayer-Schonberger & K. Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think, *Eamon Dolan/ Houghton Mifflin Harcourt,* 2013.

Perry e.a. 2013
Perry et. al., Predictive Policing, the Role of Crime Forecasting in Law Enforcement Operations, Santa Monica: *RAND Corporation*, 2013.

Provost & Fawcett 2013
Provost, F., & Fawcett, T. Data Science for Business: What you need to know about data mining and data-analytic thinking, *O'Reilly Media, Inc*, 2013

Schendel & van der Sloot 2019
S. van Schendel & B. van der Sloot, 'De modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving', Den Haag, *WODC* 2019.

Schendel 2020
S. van Schendel, 'Inzet SyRI onvoldoende inzichtelijk en controleerbaar en strijdig met fundamentele rechten', *Penl* 2020/2.

Schermer & Oerlemans 2019
B. Schermer & J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3.

Schuilenburg 2016
M. Schuilenburg, 'Predictive Policing: De opkomst van de gedachtenpolitie?', *Ars Aequ*i 2016 nr. 65, p. 931.

Schuilenburg 2018
M. Schuilenburg, 'De burger moet kunnen weten hoe de misdaadvoorspeller werkt', *NRC Handelsblad* 18 juni 2018.

Schuilenburg 2020
M. Schuilenburg, 'De camera maakt op eigen gezag van de burger een verdachte', *NRC* 21 september 2018.

van Toor 2017
D. van Toor, ''Het schuldige geheugen?'', *SteR* nr. 32, 2017/III.6.2.4.2.

van Toor 2017
D. van Toor, 'Rechtvaardiging van de inbreuk op grond van artikel 8 lid 2 EVRM', *SteR*, 2017, nr. 32, pargraaf III.6.2.4.

de Vries & Smit 2016
A. de Vries & S. Smit, 'Predictive Policing: politiewerk aan de hand van voorspellingen', *Justitiële Verkenningen* 42(3) 2016.

Vulto & Sander 2019
Vulto, B & Sander, D., 'Predictive Identification. Tussen instrumentaliteit en rechtsbescherming', *Ars Aequi* 2019/827.

Willems & Doeleman 2014
D. Willems & R. Doeleman 2014. 'Predictive Policing: Wens of werkelijkheid?', *Het Tijdschrift voor de Politie* 76(4) 2014.

WODC 2017
WODC, 'De toekomstbestendigheid van de politie', *Justitiële verkenningen* 2017/4.

Kamerstukken

- *Kamerstukken* II 2012/13, 33 542, nr. 3 (MvT).
- *Kamerstukken* II 2012/2013, 33 579, nr. 3.
- *Kamerstukken* II 2015/2016, 26643, nr 426.
- *Kamerstukken* II 2019, 2717062.
- *Kamerstukken* II 2019/2020, 26543 en 32761, nr. 641
- *Kamerstukken* I26 643 en 32 761, nr 669

- Brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 21 december 2018, kenmerk 2370000.
- Brief van de Minister voor Rechtsbescherming van 9 oktober 2019, kenmerk 2370000.
- Brief van de Staatssecretaris Sociale Zaken en Werkgelegenheid van 23 april 2020, 2020-0000052759.
- Brief van de Minister van Justitie en Veiligheid van 11 december 2020, kenmerk 3090936.
- Brief van de Minister van Justitie en Veiligheid van 11 december 2020, kenmerk 2020Z17814.

Internetbronnen

Alston 2019
Philip Alston, VN-rapporteur; *extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./ De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388)*.

AI HLEG 2019
AI HLEG, *Ethics Guidelines for Trustworthy AI, Chapter II*.

Autoriteit Persoonsgegevens
AP, ''Toezicht op AI & Algoritmes'', *AP* 17 februari 2020.

Korpschef Politie 2019
Sensing Mobiel Banditisme 2019; *Programma Mobiel Banditisme (Proeftuin Roermond)*, https://www.politie.nl/wob/, geraadpleegd op 20 juni 2020.

Openbaar Ministerie
Openbaar Ministerie, Onderwerp: *mobiel banditisme*, https://www.om.nl/onderwerpen/mobiel-banditisme, geraadpleegd op 03 oktober 2020.

PredPol How Predictive Policing works 2019
PredPol, How Predictive Policing works, 2019, https://www.predpol.com/how-predictivepolicing-works/, geraadpleegd op 15 juni 2020.

Rathenau Instituut
Rathenau Instituut, ‘Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan’, https://www.rathenau.nl, geraadpleegd op 16 augustus 2020.

***Jurisprudentielijst**:*

EHRM

- EHRM 26 april 1979, nr. 6538/74 (*Sunday Times/ VK)*
  ECL:NL:XX:1979:AC6568
- EHRM 2 augustus 1984, nr. 8691/79 (*Malone/ VK)*
  ECLI:NL:XX:1984:AB8061
- EHRM 26 maart 1987, nr. 9248/81 (*Leander/ Zweden)*
  ECLI:CE;ECHR:1987:0326JUD000924881
- EHRM 29 juni 2006, nr. 54934/00 (*Weber en Saravia/ Duitsland)*
  ECLI:CE:ECHR:2006:0629JUD005493400
- EHRM 2 september 2010, nr. 35623/05 (*Uzun/ Duitsland)*
  ECLI:CE:ECHR:2010:0902JUD003562305
- EHRM 25 juli 2013, nr. 27183/04 (*Rousk/ Zweden)*
  ECLI:NL:XX:2013:365:0725JUD002718304
- EHRM 4 december 2015, nr. 47143/06, (*Roman Zakharov/ Rusland*)
  ECLI:CE:ECHR:2015:1204JUD004714306.
- EHRM 12 januari 2016, nr. 37138/14, (*SzabóenVissyt/ Hongarije).*
  ECLI:CE:ECHR:2016:0112JUD003713814
- EHRM 22 oktober 2018, nr. 35553/12, (*S., V. en A. / Denemarken)*
  ECLI:CE;ECHR:2018:1022JUD003555312
- EHRM 11 juni 2020, nr. 74440/17 (*PN/ Duitsland)*
  ECLI:CE;ECHR:2020:0611JUD007444017

Hof van Justitie

- HvJEU 8 april 2014, zaak C-293/12 en C-594/12, *(Digital Rights Ireland)*,
  ECLI:EU:C:2014:238.

Hoge Raad

- HR 19 juni 1990, ECLI:NL:HR:1990:ZC8556 (*Richtlijn en recht*).
- Hoge Raad, 01 juli 2014, ECLI:NL:HR:2014.1563 *(Stille SMS)* en (*IMSI-Catcher)*
- HR 24 februari 2017, ECLI:NL:HR:2017:286
- HR 17 augustus 2018, ECLI:NL:HR:2018:1316

Rechtbank

- Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865
- JB 2020/63, Rechtbank Den Haag, 05-02-2020, ECLI:NL:RBDHA:2020:865, nr. C-09-550982-HA ZA 18-388 (annotatie)

Afdeling bestuursrechtspraak van de Raad van State

- ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 (*St. Werkgroep Behoud de Peel/GS Noord Brabant*)
- ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454