**ARTIKELEN**

*PEER REVIEWED*

# Predictive identification als een moreel ondoorzichtig panopticon

*Litska Strikwerda**

## 1. Inleiding

In 2016 sloot de laatste van de drie koepelgevangenissen die Nederland rijk was haar deuren. Deze gevangenissen waren bijzonder, omdat ze gebouwd waren volgens het panopticon-principe, dat afkomstig is van de Britse filosoof Jeremy Bentham (1748-1832). Het panopticon dient om mensen op een efficiënte manier in de gaten te houden. De koepelgevangenissen waren zo ontworpen dat één cipier in de centrale hal volstond om alle gevangenen te bewaken, zonder dat de gevangenen de cipier konden zien. In zijn werk *Discipline, toezicht en straf* legt de Franse filosoof Foucault (1926-1984) uit dat gevangenen daardoor als het ware zichzelf gingen bewaken. Omdat ze nooit zeker wisten wanneer er op hen werd gelet, gedroegen ze zich voor de zekerheid altijd gedisciplineerd. Hij noemt dit 'slim toezicht'.[1] Met de sluiting van de koepelgevangenissen zijn het panopticon en slim toezicht niet uit onze samenleving verdwenen.

Technologische ontwikkelingen, vooral op het gebied van ICT, voorzien in allerlei nieuwe middelen voor slim toezicht. Een voorbeeld is *predictive policing*, een fenomeen dat in het kort omschreven kan worden als het gebruik van big-data-analyse om te voorspellen waar en wanneer strafbare feiten zullen plaatsvinden (*predictive mapping*) of wie ze zullen plegen dan wel daarvan slachtoffer zullen worden (*predictive identification*).[2] Deze paper richt zich op predictive identification en dan specifiek op de vorm die voorspelt wie een verhoogd risico loopt om crimineel gedrag te vertonen. Er zal veelvuldig worden gerefereerd aan twee Nederlandse instrumenten op het gebied van predictive identification die op dit moment om verschillende redenen in de belangstelling staan, te weten het Systeem Risico Indicatie (SyRI) en het Sensing-project.

SyRI en Sensing hebben beide te lijden onder een gebrek aan transparantie. Het is onduidelijk waarop de voorspellingen die zij genereren precies zijn gebaseerd. Dit

* Dr. Litska Strikwerda is universitair docent Metajuridica aan de Faculteit Rechtswetenschappen van de Open Universiteit.

1 M. Foucault, *Discipline and punish*, New York: Vintage Books 1975.

2 V. Mayer-Schonberger & K. Cukier, *Big Data. A revolution that will transform how we live, work and think*, Londen: John Murray 2013, p. 158; A. Drenth & R. van Steden, 'Ervaringen van Straatagenten met het Criminaliteits Anticipatie Systeem, *Het Tijdschrift voor de Politie* 2017, 3, p. 6.


PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

heeft tot gevolg dat zij 'moreel ondoorzichtig' zijn: er valt moeilijk te controleren welke waarden in het geding zijn of kunnen komen door het gebruik van deze predictive identification instrumenten.[3] Dat is niet alleen vanuit een moreel oogpunt problematisch, maar ook vanuit een juridisch oogpunt. Waarden vormen vaak de basis voor normen, ook voor juridische normen. Als niet duidelijk is of de onderliggende waarden in het geding zijn, valt ook niet goed te controleren of er bepaalde juridische waarborgen, regels of rechten geschonden worden.[4]

Het doel van deze bijdrage is om bloot te leggen welke waarden samenhangen met en onder spanning kunnen komen te staan door predictive identification op het individuele niveau van burgers en politiemensen.[5] Om dit doel te bereiken zal gebruik worden gemaakt van een methode afkomstig uit de computerethiek die *disclosive computer ethics* genoemd wordt.[6] Disclosive computer ethics kent drie verschillende niveaus van analyse. Het eerste niveau bestaat uit de onthulling van de relevante waarden. Op basis van recente relevante literatuur wordt geïnventariseerd welke waarden impliciet of expliciet met predictive identification in verband worden gebracht. Er wordt ook een definitie in algemene termen van die waarden gegeven. Het tweede niveau gaat dieper in op de definiëring van de gevonden waarden. Onderzocht wordt of predictive identification aanleiding geeft tot een herinterpretatie van deze waarden. Het derde niveau is van toegepaste aard en bestaat uit aanbevelingen.[7]

Deze paper is als volgt gestructureerd. Na een uitleg van wat predictive identification precies is en waarom het niet transparant is, zullen in paragrafen 3, 4 en 5 de drie hiervoor genoemde niveaus van analyse worden doorlopen. Het eerste analyseniveau draait om de vraag welke waarden bevorderd of juist geschaad kunnen worden door predictive identification. Het tweede analyseniveau draait om de vraag of predictive identification ertoe leidt dat de geïdentificeerde waarden anders geïnterpreteerd moeten worden. Het derde analyseniveau draait om de vraag hoe vanuit het oogpunt van de geïdentificeerde waarden beter met predictive identification omgegaan kan worden. Tot slot, in de conclusie, worden de uitkomsten en beperkingen van deze analyse besproken en worden suggesties gedaan voor verder onderzoek.

3 P. Brey, 'Values in technology and disclosive computer ethics', in: L. Floridi (red.), *The Cambridge Handbook of Information and Computer Ethics*, Cambridge: Cambridge UP 2010, p. 47-53.

4 Brey 2010.

5 De waarden die samenhangen met of onder spanning komen te staan door predictive identification kunnen ook worden benaderd op het niveau van de samenleving als geheel, bijv. vanuit de invalshoek van de democratische rechtsstaat zoals o.a. beschreven door S. Zouridis, M. van Eck & M. Bovens,, 'Automated discretion', in: T. Evans & P. Hupe (red.), *Discretion and the quest for controlled freedom*, Palgrave MacMillan 2020, p. 313-329. Deze paper beoogt hier met een andere invalshoek een aanvulling op te bieden.

6 Brey 2010.

7 Brey 2010, p. 52.

## 2. Wat is predictive identification en waarom is het niet transparant?

Predictive identification kan worden gedefinieerd als de toepassing van analysetechnieken, met name kwantitatieve technieken, om middels statistische voorspellingen te bepalen ten aanzien van wie waarschijnlijk politieoptreden nodig is om criminaliteit te voorkomen of gepleegde misdrijven op te lossen.[8] Het kan dan gaan om zowel potentiële daders als potentiële slachtoffers, maar zoals aangekondigd in de inleiding zal deze bijdrage zich alleen richten op predictive identification instrumenten die voorspellen wie een verhoogd risico loopt om crimineel gedrag te vertonen. Predictive identification is een vorm van kunstmatige intelligentie (beter bekend onder de Engelse term *artificial intelligence* of kortweg AI), die gebruikmaakt van een voorspellingsmodel. Zo'n voorspellingsmodel kan beschreven worden als een formule om een onbekende waarde (in dit geval het risico op het plegen van criminaliteit) in te schatten.[9] Een dergelijke formule noemt men een algoritme. Nederland is een van de landen die vooroplopen op het gebied van predictive policing, waar predictive identification onderdeel van uitmaakt.[10] Hierna worden twee predictive identification instrumenten die op dit moment om verschillende redenen in de belangstelling staan, uitgebreid besproken: het Systeem Risico Indicatie (SyRI) en het Sensing-project.

### *2.1 SyRI*

SyRI werd door de overheid gebruikt om fraude op het terrein van onder andere uitkeringen, toeslagen en belastingen te voorkomen en te bestrijden. Het systeem kende een wettelijke basis in artikel 65 van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI).[11] SyRI werd ingezet op verzoek van samenwerkende bestuursorganen, waaronder de Belastingdienst, en dus niet door de politie.[12] Maar indien nodig werden risicomeldingen wel doorgespeeld aan het Openbaar Ministerie en de politie.[13] In dat geval kon SyRI gezien worden als een predictive identification instrument.

SyRI koppelde gegevens en toetste deze aan een risicomodel met verschillende indicatoren dat voorspelde wie een verhoogd risico liep om fraude te plegen. Het risicomodel en de daarbij behorende indicatoren zijn niet openbaar gemaakt. Wel is bekend welk soort gegevens SyRI verwerkte. Het gaat onder meer om arbeidsgegevens, fiscale gegevens, inburgeringsgegevens, schuldenlastgegevens, zorgverzeke-

8 W.R. Perry e.a., *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, RAND, www.rand.org/pubs/research_reports/RR233.html, p. 1-2.

9 F. Provost & T. Fawcett, *Data Science for Business: What you need to know about data mining and data-analytic thinking*, Sebastopol: O'Reilly Media, Inc. 2013, p. 45.

10 Amnesty International, *We Sense Trouble. Automated Discrimination and Mass Surveillance in predictive policing in the Netherlands*, 2020, p. 4, te raadplegen van www.amnesty.org; *Halfjaarbericht politie 2019, bijlage 5, ICT-vernieuwing bij de politie*, Ministerie van Justitie en Veiligheid, Directoraat-Generaal Politie en Veiligheidsregio's 2019, p. 3.

11 Wet van 29 november 2001, *Stb*. 2001, 624.

12 Art. 65 lid 1 jo. art. 64 lid 1 Wet SUWI.

13 Art. 65 lid 3 sub b Wet SUWI.



PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

ringsgegevens (of iemand al dan niet een zorgverzekering heeft) en persoonsgegevens (naam, adres, geboortedatum enzovoort).[14]
Sinds februari 2020 wordt SyRI niet meer gebruikt, omdat de rechtbank Den Haag de wetgeving die het gebruik ervan mogelijk maakte onverbindend heeft verklaard.[15] Aan een opvolger voor SyRI wordt echter gewerkt. De wet die het gebruik daarvan mogelijk moet maken, heeft de titel Wet gegevensverwerking door samenwerkingsverbanden[16] en ligt op dit moment bij de Eerste Kamer.

*2.2 Sensing*

Sensing was een 'fieldlab', een operationele proeftuin bedoeld om vast te stellen wat de impact is van een nieuwe methode van politiewerk. Het betrof een predictive identification instrument dat zich richtte op 'mobiel banditisme': rondreizende bendes die zich bezighouden met verschillende vormen van vermogenscriminaliteit, zoals zakkenrollerij, winkeldiefstal, babbeltrucs en inbraken. Volgens de politie maken vooral Oost-Europese dadergroepen zich schuldig aan mobiel banditisme. Sensing werd ingezet in Roermond, omdat die stad kwetsbaar is voor mobiel banditisme door de ligging als grensstad en de aanwezigheid van veel winkels en de bezoekers daarvan in onder meer het Designer Outlet Centre. Het maakte gebruik van sensorinformatie afkomstig uit een netwerk van ANPR-camera's (automatische kentekenplaatherkenning). Daarvoor is gekozen omdat volgens de politie mobiele bendes zich meestal verplaatsen per auto. Het plan van aanpak rept ook over andere, niet openbaar gemaakte sensoren.[17] Volgens de minister van Justitie is daarvan echter uiteindelijk geen gebruik gemaakt.[18]
De in het kader van Sensing verkregen (kenteken)gegevens werden gekoppeld en getoetst aan een risicomodel met verschillende indicatoren dat voorspelde welke inzittenden van auto's een verhoogd risico liepen om zakkenrollerij, winkeldiefstal of andere vermogenscriminaliteit te plegen in de winkelcentra van Roermond. Net als bij SyRI zijn het betreffende risicomodel en de daarbij behorende indicatoren niet openbaar gemaakt. Volgens de minister zijn het merk, model en land van herkomst van de gebruikte auto voorbeelden van indicatoren.[19] Indien Sensing een treffer vaststelde, hield de politie de desbetreffende auto staande op grond van de algemene controlebevoegdheid die haar op grond van artikel 160 Wegenverkeerswet toekomt. Zo hoopte zij mobiel banditisme te voorkomen.[20]
Omdat er, waarschijnlijk onder invloed van de coronacrisis, in 2020 sprake was van een grote daling in het aantal incidenten, lag het Sensing-project sindsdien feitelijk stil.[21] Vervolgens kwam het onder vuur te liggen omdat Amnesty International een

14 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, par. 3.2, 4.17, 4.29 en 6.59.
15 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865.
16 Kamerstukken II 2019/20, 35447, nr. 2.
17 Politie, Plan van Aanpak Operationele Proeftuin Sensing Roermond, 12 oktober 2017, p. 4-9, te raadplegen van 045---plan-van-aanpak-opt-sensing-roermond-definitief-12-oktober-2017_def.pdf (politie.nl).
18 Brief van de minister van Justitie, 11 december 2020, 3090935.
19 Idem.
20 Amnesty International 2020, p. 35.
21 Brief van de minister van Justitie, 11 december 2020, 3090935.

vernietigend rapport uitbracht over dit predictive identification instrument.[22] Volgens berichtgeving in *De Limburger* zou het Sensing-project inmiddels definitief zijn gestopt.[23]

*2.3 Gebrek aan transparantie*

Sensing en SyRI hebben een belangrijke overeenkomst. Het is niet transparant waarop hun voorspellingen zijn gebaseerd door een gebrek aan *toegankelijkheid*: het gebruikte risicomodel en de daarbij behorende indicatoren zijn niet bekendgemaakt. Het gebeurt regelmatig dat algoritmes die gebruikt worden om beslissingen te nemen, in de (semi)publieke sector niet toegankelijk zijn, bijvoorbeeld omdat ze zijn ontwikkeld door commerciële partijen die er patent op hebben.[24] Specifiek in de strafrechtelijke context kan daar ook een andere reden voor zijn. In antwoord op Kamervragen naar aanleiding van het kritische rapport van Amnesty International over Sensing gaf de minister van Justitie bijvoorbeeld aan dat hij inzage had gehad in de lijst met indicatoren op grond waarvan Sensing de risicoscore van een auto bepaalt, maar deze informatie niet openbaar kon maken omdat dat het opsporings- en handhavingsbelang zou doorkruisen.[25] Overigens hoeft een gebrek aan transparantie van algoritmes niet voort te vloeien uit een gebrek aan toegankelijkheid; dit kan ook komen door een gebrek aan *uitlegbaarheid*. Daarvan is sprake indien de uitkomsten van analyses door algoritmes niet door mensen begrepen kunnen worden. Dit wordt het 'black-boxprobleem' genoemd.[26] Het black-boxprobleem doet zich vaak voor bij *machine learning*-algoritmes en dan vooral bij diep lerende neurale netwerken, zoals bijvoorbeeld ten grondslag liggen aan gezichtsherkenningstoepassingen. Bij gezichtsherkenningstoepassingen leert het model welke gezichtskenmerken belangrijk zijn, in plaats van dat de ontwikkelaar van het model de relevante kenmerken selecteert. De manier van leren van het model is echter zo complex dat deze voor mensen niet te begrijpen valt.[27]

## 3. Het eerste analyseniveau: welke waarden kunnen bevorderd of juist geschaad worden door predictive identification?

Predictive identification instrumenten zoals SyRI en Sensing hebben tot doel (een specifiek type) criminaliteit te voorkomen en te bestrijden.[28] Op die manier beogen ze de waarde veiligheid te bevorderen. Veiligheid kan worden omschreven als 'de effectieve bescherming tegen persoonlijk leed, dat wil zeggen effectieve bescher-

22 Amnesty International 2020.
23 G. Driessen, 'Mobiel banditisme. Stil einde project tegen zakkenrollers', *De Limburger* 12 november 2022, p. 6.
24 S. Giest & S. Grimmelikhuijsen, 'Introduction to special issue algorithmic transparency in government: Towards a multi-level perspective', *Information Polity* 2020, 24, p. 410.
25 Brief van de minister van Justitie, 11 december 2020, 3090935.
26 Giest & Grimmelikhuijsen 2020, p. 410.
27 A. Rai, 'Explainable AI: from black box to glass box', *J. of the Acad. Mark. Sci.* 2020, 48, p. 137-141, https://doi.org/10.1007/s11747-019-00710-5.
28 Zie respectievelijk Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, par. 3.1 en Amnesty International 2020, p. 26.


PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

ming tegen de aantasting van iemands lichamelijke of geestelijke integriteit'.[29] Iemands veiligheid kan niet alleen in het geding komen door een dreiging gericht tegen hem of haar persoonlijk, maar ook door een dreiging die uitgaat van problemen op het niveau van de samenleving als geheel.[30] Sensing had tot doel strafbare feiten te voorkomen die voornamelijk persoonlijk leed veroorzaken, zoals zakkenrollerij, babbeltrucs en inbraken, waar SyRI tot doel had strafbare feiten te voorkomen die de samenleving als geheel bedreigen, te weten fraude op het terrein van onder andere uitkeringen, toeslagen en belastingen. Of de waarde veiligheid ook daadwerkelijk bevorderd wordt, hangt echter af van twee factoren: of de voorspellingen die predictive identification instrumenten genereren kloppen en wat politiemensen er in de praktijk mee doen. Uit onderzoek blijkt dat big-datatoepassingen zoals predictive identification nog niet veel worden gebruikt door politiemensen en dat er nog een lange weg te gaan is voordat zij een breed verspreide praktijk zullen worden.[31] Daarnaast blijkt de vertaalslag van data naar kennis waar politiemensen iets aan hebben, vaak complex. Als die vertaalslag niet goed wordt gemaakt, kunnen politiemensen de informatie niet goed interpreteren, waardoor deze onvoldoende of de verkeerde betekenis krijgt.[32]

De meest voor de hand liggende waarde die op individueel niveau geschaad kan worden door predictive identification, is privacy. In juridische termen wordt privacy vaak 'de persoonlijke levenssfeer' genoemd.[33] Hoewel het vaak is geprobeerd, valt eigenlijk niet precies te beschrijven wat het concept privacy of persoonlijke levenssfeer inhoudt.[34] Een bekende definitie is die van de Amerikaanse juristen Warren en Brandeis, die privacy in de negentiende eeuw omschreven als 'the right to be let alone'.[35] Dit betreft allereerst een moreel recht. Morele rechten leggen mensen de plicht op om de belangen van anderen te respecteren,[36] in casu de plicht om je niet te mengen in (bepaalde aspecten van) de persoonlijke levenssfeer van een ander. Maar privacy is ook een recht in juridische zin. Het is onder andere vastgelegd in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). In de eerdergenoemde SyRI-uitspraak kwam de rechtbank tot de conclusie dat SyRI het recht op privacy als vastgelegd in artikel 8 EVRM schond.[37] Het gaat dan voornamelijk om een specifiek

29 W. Stol & L. Strikwerda, *Strafrechtspleging in een digitale samenleving*, Den Haag: Boom juridisch 2017, p. 51.

30 Stol & Strikwerda 2017, p. 51-52.

31 R. Spithoven & E. Foppen, 'Big Data, kleine rechtsstaat?', *Tijdschrift voor Veiligheid* 2021, 4, p. 37, doi:10.5553/TvV/.000032.

32 R. Spithoven & J. van de Pas, 'Bij voorbaat effectiever? Over de noodzaak van het herwaarderen van vakmanschap en de onvermijdelijkheid van actieonderzoek bij het gebruik van big-datatoepassingen door de politie', in: W. Hardyns & T. Snaphaan (red.), *Big data en innovatieve methoden voor criminologisch onderzoek*, Den Haag: Boom criminologie 2020.

33 Zie bijv. art. 10 Grondwet.

34 J. Cohen, 'Turning Privacy Inside Out', *Theoretical Inquiries in Law* 2019, 1, p. 1-31, doi:10.1515/til-2019-0002.

35 S.D. Warren & L.D. Brandeis, 'The right to privacy', *Harvard Law Review* 1890, 5, p. 193-220.

36 B. Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics', *Philos. Technol.* 2017, 30, p. 475-494, doi.org/10.1007/s13347-017-0253-7.

37 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, par. 6.7.

recht dat daar onderdeel van uitmaakt, namelijk het recht op bescherming van persoonsgegevens.[38] Volgens Amnesty International schond Sensing het recht op privacy ook, omdat dit predictive identification instrument kenteken- en andere gegevens die te relateren zijn aan individuen een maand lang opsloeg, terwijl ten aanzien van veel van die individuen geen enkele verdenking bestond.[39]

Een andere waarde die onder spanning kan komen te staan door predictive identification, is autonomie. Een gebruikelijke omschrijving van autonomie is de vrijheid om zelf beslissingen te nemen, zonder invloed van buitenaf.[40] Doordat de technologische ontwikkelingen op dit terrein snel gaan, worden door predictive identification instrumenten steeds meer data over steeds grotere groepen burgers, verdacht en niet verdacht, verzameld en geanalyseerd.[41] Burgers kunnen zich daardoor genoodzaakt voelen om hun gedrag aan te passen. Indien gebruikgemaakt wordt van camera's, zoals in het geval van Sensing, kunnen ze letterlijk, en anders figuurlijk, buiten beeld proberen te blijven.[42] Ze zijn dan dus niet meer geheel vrij om hun eigen beslissingen te nemen, maar worden daarin beïnvloed door een externe factor. De autonomie van politiemensen kan eveneens onder druk komen te staan door predictive identification. Hun discretionaire ruimte kan verminderen als zij steeds meer door informatie afkomstig uit predictive identification instrumenten gestuurd zouden worden in hun werk, en steeds minder over mogen laten aan hun eigen beoordelingsvermogen.[43]

Ook de waarde gelijkheid kan in het geding komen door predictive identification. Gelijkheid houdt in dat geen ongerechtvaardigd onderscheid tussen mensen gemaakt wordt: in situaties die hetzelfde zijn, worden mensen op dezelfde manier behandeld. Deze waarde is verankerd in artikel 1 van de Grondwet en een aantal andere wetten, zoals de Algemene wet gelijke behandeling.[44] Discriminatie, dat wil zeggen het anders behandelen, achterstellen of uitsluiten van mensen op basis van bepaalde (persoonlijke) kenmerken, is op grond van deze wetten verboden. Predictive identification brengt een reëel risico met zich mee dat op basis van de uitkomsten van analyses door algoritmes beslissingen worden genomen die discriminerend zijn.[45] Data en de analyse daarvan zijn niet neutraal. De verzameling en analyse van data gaat gepaard met menselijke keuzes, bijvoorbeeld met betrekking tot welke databronnen wel of niet worden gebruikt of welk algoritme wordt toegepast.[46] Daardoor kunnen onregelmatigheden en afwijkingen in de gebruikte data-

38 Zie o.a. EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (S. en Marper/Verenigd Koninkrijk). In art. 8 van het Handvest van de grondrechten van de Europese Unie is een zelfstandig recht op bescherming van persoonsgegevens opgenomen.

39 Amnesty International 2020, p. 12-13, 30.

40 G. Dworkin, 'The nature of autonomy', *Nordic Journal of Studies in Educational Policy* 2015, 2, doi:10.3402/nstep.v1.28479.

41 WRR, *Big Data in een vrije en veilige samenleving*, Amsterdam University Press 2016.

42 WRR 2016.

43 J. Terpstra & R. Salet, 'Big Data Policing als Sociale Praktijk - schets van een miskend, maar urgent onderzoeksterrein', *Cahiers Politiestudies* 2020 54, Gompel&Svacina.

44 Wet van 2 maart 1994, *Stb*. 1994, 230.

45 Giest & Grimmelikhuijsen 2020, p. 410.

46 L. Kool, J. Timmer & R. van Est, *De datagedreven samenleving*, Rathenau Instituut 2015.



PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

sets (bias) ontstaan die resulteren in voorspellingen die nadelig zijn voor bepaalde groepen in de maatschappij.[47]

Dit kan worden geïllustreerd aan de hand van het volgende voorbeeld. In de Amerikaanse stad Chicago werd van 2013 tot 2019 het Custom Notification Program ingezet: een predictive identification instrument bedoeld om potentiële slachtoffers en daders van vuurwapengeweld te voorspellen. Op basis van empirische gegevens werd een Strategic Subjects List (SSL) opgesteld: een ranglijst van personen die een verhoogde kans hadden om daarbij betrokken te raken.[48] De gebruikte gegevens omvatten onder andere gegevens over demografie, strafblad en socialenetwerkvariabelen.[49] Uiteindelijk had de meerderheid van de zwarte jonge mannen in Chicago een hoge risicoscore. Het Custom Notification Program is toen stopgezet.[50]

In Nederland speelde mogelijk iets soortgelijks met betrekking tot SyRI. Dit predictive identification instrument werd alleen in achterstandswijken ingezet. Daardoor bestaat het risico dat een bias is ontstaan en dat door SyRI bijvoorbeeld aan mensen met een lagere sociaaleconomische status of een migratieachtergrond een hogere risicoscore voor fraude is toebedeeld.[51] Volgens Amnesty International speelde dit probleem ook met betrekking tot Sensing. In het plan van aanpak wordt gesteld dat uit onderzoek blijkt dat mobiel banditisme vooral wordt gepleegd door Oost-Europese dadergroepen.[52] Amnesty International gaat er daarom van uit dat (sommige van) de indicatoren in het risicomodel erop waren gericht mensen van die afkomst te selecteren.[53]

Een aanpalend probleem is de mogelijke uitholling van de onschuldpresumptie die predictive identification teweeg kan brengen.[54] De onschuldpresumptie houdt in dat eenieder voor onschuldig wordt gehouden totdat zijn schuld in rechte is komen vast te staan.[55] Predictive identification maakt deel uit van een nieuwe manier van opsporing die 'niet zozeer wordt gestart naar aanleiding van een reeds gepleegd delict als wel op grond van gegevens die over bepaalde mensen bekend zijn geworden'.[56] Het doel is om groepen mensen te identificeren, classificeren en beheren op basis van risiconiveaus.[57] Daarbij wordt niet uitgegaan van onschuld, zoals de on-

47 WRR 2016.

48 J. Saunders, P. Hunt & J.S. Hollywood, 'Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot', *J Exp Criminol* 2016, 12, p. 347-351.

49 Saunders, Hunt & Hollywood 2016.

50 E.E. Joh, 'Reckless Automation in Policing', *Berkeley Technology Law Journal Online* 2022, http://dx.doi.org/10.2139/ssrn.4009911.

51 F. Çapkurt & Y.E. Schuurmans, 'Komt een fraude-opsporingssysteem bij de rechter', in: L.W. Verboeket e.a. (red.), *Bestuursrecht in het echt. Vriendenbundel voor prof. mr. drs. Willemien den Ouden*, Deventer: Wolters Kluwer 2021, p. 599.

52 Politie 2017, p. 7.

53 Amnesty International 2020, p. 39-41.

54 Zie bijv. E.E. Joh, 'Policing by numbers: big data and the fourth amendment', *Washington Law Review* 2014, 3, p. 35-68.

55 Art. 6 lid 2 EVRM.

56 Y. Buruma, *De dreigingsspiraal. Onbedoelde neveneffecten van misdaadbestrijding*, Den Haag: Boom Juridische uitgevers 2005, p. 81.

57 Y. Mehozay & E. Fisher, 'The epistemology of algorithmic risk assessment and the path towards a non-penology penology', *Punishment & Society* 2019, 5, p. 524, 531-533.

schuldpresumptie vereist, maar van (de grootte van) het risico dat iemand schuldig is. Mensen kunnen zelfs door een predictive identification instrument zelf verdacht worden gemaakt. Volgens Amnesty International kan Sensing bijvoorbeeld een 'feedback loop' veroorzaken omdat een auto die door de politie is gecontroleerd vanwege een treffer in Sensing, maar waarbij geen bijzonderheden zijn vastgesteld, wel in de politiesystemen komt te staan. Daardoor creëert de auto een volgende keer dat deze Roermond in rijdt weer een treffer in Sensing.[58] Volgens de minister gebeurt dit echter niet en worden auto's die door de politie zijn gecontroleerd, maar waarbij geen bijzonderheden zijn aangetroffen, door Sensing juist op een lijst geplaatst die voorkomt dat de auto nog een keer onder de aandacht komt.[59]
Tot slot kan de waarde verantwoordelijkheid door predictive identification onder spanning komen te staan. Vanuit moreel oogpunt betekent verantwoordelijkheid dat aan iemand bepaalde bevoegdheden en bekwaamheden worden toegekend en dat zijn gedrag wordt beschouwd als (op de juiste wijze) voortvloeiend uit het feit dat de persoon deze bevoegdheden en bekwaamheden heeft en heeft uitgeoefend.[60] Het probleem met predictive identification is dat de werking ervan zo complex is *dat* het lastig of zelfs onmogelijk is om, als er iets fout gaat, te achterhalen waar het is misgegaan of waarom.[61] In veel gevallen kan er dan niet iemand, bijvoorbeeld de producent van het predictive identification instrument in kwestie of de gebruiker, voor verantwoordelijk gehouden worden. Dit terwijl deze fouten wel heel tastbare gevolgen kunnen hebben, zoals, in het geval van respectievelijk Sensing en SyRI, onterechte staandehoudingen of onterechte strafrechtelijke onderzoeken naar fraude. Dit kan het vertrouwen van burgers, ook een waarde, schaden en daarmee de rechtsstaat bedreigen.[62]

## 4. Het tweede analyseniveau: leidt predictive identification ertoe dat de geïdentificeerde waarden anders geïnterpreteerd moeten worden?

Om de vraag te kunnen beantwoorden of predictive identification ertoe leidt dat de geïdentificeerde waarden anders geïnterpreteerd moeten worden, wordt eerst vanuit een breder perspectief naar predictive identification gekeken en onderzocht in hoeverre deze nieuwe computertechnologie veranderingen teweegbrengt waardoor deze waarden op een andere manier worden bevorderd of juist onder druk komen te staan. Predictive identification kan worden getypeerd als 'data-gedreven'[63] of 'algoritmische'[64] surveillance, en past in een bredere maatschappelijke trend. De samenleving als geheel kan namelijk worden getypeerd als 'data-gedre-

58 Amnesty International 2020, p. 31.
59 Brief van de minister van Justitie, 11 december 2020, 3090935.
60 M. Talbert, 'Moral Responsibility', in: E.N. Zalta & U. Nodelman (red.), The Stanford Encyclopedia of Philosophy,2022 https://plato.stanford.edu/archives/fall2022/entries/moral-responsibility/.
61 Kool, Timmer & Van Est 2015.
62 Ziosi e.a. 2022.
63 Joh 2022.
64 R. van Brakel, 'Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance', in: M. Schuilenburg & R. Peeters, *The Algorithmic Society. Technology, Power, and Knowledge*, Londen/New York: Routledge 2021.


PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

ven'.[65] Data-analyses en algoritmes spelen een steeds grotere rol, zowel in het bedrijfsleven als in het overheidsdomein.[66] In dit verband wordt wel gesproken van de dreiging van een 'algocratie'.[67] Algoritmes hebben steeds meer invloed op de besluitvorming door professionals binnen de overheid en andere organisaties, maar onduidelijk is waar die invloed precies uit bestaat.[68]

Ook binnen de politieorganisatie worden data-analyses en algoritmes breed ingezet.[69] Data en voorspellingen hebben altijd een rol gespeeld in het politiewerk.[70] Maar in de huidige tijdgeest wordt meer en meer gebruikgemaakt van toepassingen die grote databestanden aan elkaar koppelen en er zo voor zorgen dat informatie sneller kan worden gevonden.[71] Er is sprake van een steeds verdergaande koppeling van databronnen.[72] Dit wordt 'hyperconnectiviteit' genoemd.[73] Over het algemeen wordt positief gedacht over de mogelijkheden die deze datakoppelingen bieden in het politiewerk.[74] De geautomatiseerde analyse van grote, gecombineerde gegevensbestanden door middel van algoritmes levert een grote tijdwinst op en kan ook in andere of nauwkeuriger uitkomsten resulteren.[75] Er kunnen patronen worden ontdekt in de data die met menselijke vaardigheden niet, of niet volledig, zichtbaar zouden worden. Hierdoor ontstaat niet alleen een rijkere beeldvorming, maar kan ook de beschikbare politiecapaciteit gerichter worden ingezet.[76] Kortom, de politie wordt niet in staat gesteld iets te doen wat zij in de analoge wereld niet kon, maar wel om het anders, namelijk sneller, diepgaander en efficiënter, te doen.[77]

Overigens speelt niet alleen de grootschalige koppeling, maar ook de grootschalige beschikbaarheid van data hier een rol. Als gevolg van digitalisering zijn data onbeperkt beschikbaar gekomen.[78] Mensen genereren met de dag meer data die geanalyseerd kunnen worden. Ter illustratie: bij wijze van proef vroeg de NOS in 2018 alle data op die bedrijven zoals Google en Facebook hadden over drie mensen. Bij elkaar leverde dit drie miljoen A4-tjes aan data op.[79] Daarnaast zijn er tegenwoor-

65 Kool, Timmer & Van Est 2015.
66 Kool, Timmer & Van Est 2015.
67 A. Das & M. Schuilenburg, '"Garbage in, garbage out". Over predictive policing en vuile data', *Beleid en Maatschappij* 2020, 3, p. 254-268.
68 Das & Schuilenburg 2020, p. 254-268.
69 WRR 2016.
70 WRR 2016, p. 55.
71 M. Schuilenburg & M. Soudijn, 'Big data in het veiligheidsdomein: onderzoek naar big datatoepassingen bij de Nederlandse politie en de positieve effecten hiervan voor de politieorganisatie', *Tijdschrift voor Veiligheid* 2021, 4, doi:10.5553/TvV/.000028.
72 WRR 2016.
73 Schuilenburg & Soudijn 2021, p. 57.
74 Spithoven & Foppen 2021.
75 WRR 2016.
76 Schuilenburg & Soudijn 2021, p. 55-56.
77 A.G. Ferguson, 'Why digital policing is different', *Ohio State Law Journal* 2022, te raadplegen van https://ssrn.com/abstract=4133670.
78 Spithoven & Van de Pas 2020.
79 D. Simons, 'Miljoenen pagina's aan data over deze twee socialemediasterren', *NOS* 25 mei 2018, https://nos.nl/op3/artikel/2233420-miljoenen-pagina-s-aan-data-over-deze-twee-socialemediasterren.html, laatst geraadpleegd op 27 juni 2022.

dig allerlei surveillancetechnologieën in omloop die in vroegere tijden niet bestonden en die steeds meer data opleveren.[80] Denk bijvoorbeeld aan de ANPR-camera's waarvan Sensing gebruikmaakte. Maar er bestaan ook meer geavanceerde toepassingen zoals Shotspotter, een AI-toepassing die in de Amerikaanse stad Chicago wordt ingezet en via akoestische sensoren geluiden detecteert waarvan vervolgens binnen een minuut kan worden vastgesteld of het om schoten gaat.[81] En dan zijn er ook nog de slimme technologische toepassingen die, vooral in stedelijke omgevingen, worden ingezet om de leefbaarheid te vergroten ('smart cities').[82] Zo wordt er bijvoorbeeld gebruikgemaakt van slimme parkeersensoren die niet alleen aangeven wanneer een parkeerplek vrij is, maar bijvoorbeeld ook de gemiddelde parkeerduur meten en het aantal in- en uitgaande parkeerbewegingen per dag registreren.[83] Al deze technologische toepassingen leveren data op die voor predictive identification gebruikt kunnen worden.

De grootschalige datakoppeling en -analyse die aan predictive identification ten grondslag liggen, zijn activiteiten die tot een vergaande inbreuk op de persoonlijke levenssfeer kunnen leiden.[84] Zoals in de inleiding al werd gesteld, kan een soort panopticon ontstaan. Er zijn echter wel twee fundamentele verschillen tussen predictive identification en het panopticon dat Bentham in de achttiende eeuw bedacht. Ten eerste, waar de cipier in de koepelgevangenis slim toezicht hield op het gedrag van individuele gevangenen, richten predictive identification instrumenten en andere vormen van geautomatiseerde digitale gegevensanalyse zich op patronen. Gevonden patronen kunnen wel aanleiding geven om individuele personen te controleren of aan een strafrechtelijk onderzoek te onderwerpen. Ten tweede diende de cipier in de koepelgevangenis als een soort 'symbolische stand-in' voor een alwetende blik, terwijl geautomatiseerde digitale gegevensverzameling en -analyse niet zichtbaar zijn.[85] Daardoor dragen mensen er onbewust zelf aan bij: zonder het te beseffen leveren mensen allerlei data over zichzelf aan, bijvoorbeeld via hun smartphones.[86]

Het eerste verschil tussen predictive identification en het achttiende-eeuwse panopticon geeft aanleiding tot een herinterpretatie van de waarde privacy. Omdat predictive identification zich richt op patronen, worden gegevens verzameld over grote en ongedefinieerde groepen. Vaak gaat het om geaggregeerde gegevens; dat zijn data die van individuele data worden omgezet naar meer algemene data. Doel daarvan is het vinden van correlaties.[87] Naar aanleiding van gevonden correlaties

80 Idem.
81 Zie www.shotspotter.com.
82 M. Ziosi e.a., 'Smart cities: reviewing the debate about their ethical implications', *AI & Soc* 2022, https://doi.org/10.1007/s00146-022-01558-0.
83 www.smartcity-iot.nl/sensoren, laatst geraadpleegd op 24 oktober 2022.
84 M. Hirsch Ballin, Position paper d.d. 13 september 2021 t.b.v. rondetafelgesprek MIT d.d. 16 september 2021, te raadplegen van Rondetafelgesprek MIT | Tweede Kamer der Staten-Generaal.
85 M.B. Andrejevic, 'Automated surveillance', in: L. Lievrouw & B. Loader (red.), *Routledge Handbook of Digital Media and Communication*, Routledge 2020, https://doi.org/10.4324/9781315616551.
86 Ziosi e.a. 2022.
87 L. Stevens e.a., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling. Een analyse aan de hand van de casus "Sensingproject Outlet Roermond"', *Tijdschrift Bijzonder Strafrecht & Handhaving* 2021, 4, p. 234-245.


PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

met andere in het systeem, worden gegevens over individuen geclusterd in groepen.[88] De privacyrisico's komen in dit geval niet zozeer voort uit de toegang tot losse gegevens over mensen, maar vooral uit de mogelijkheid om conclusies te trekken uit de optelsom van een heleboel gegevens over een heleboel mensen op basis van correlaties.[89] Algoritmisch gegroepeerde individuen hebben een collectief belang bij de totstandkoming van informatie over de groep. Maar het concept van privacy zoals dat in de vorige paragraaf is gedefinieerd, is niet van toepassing omdat dat uitgaat van het individu. Met betrekking tot de datakoppeling en -analyse waar predictive identification gebruik van maakt, is een benadering van het concept privacy nodig die betrekking heeft op groepen en gedeelde identiteit. Dit wordt 'groepsprivacy' genoemd.[90] Het is een specifiek soort recht op gegevensbescherming dat niet aan individuen wordt toegekend, maar aan de ad-hocgroepen die predictive identification en andere vormen van geautomatiseerde digitale gegevensverzameling en -analyse creëren.[91] Groepsprivacy draait niet zozeer om de privacy van het 'geïdentificeerde individu', maar om de privacy van het 'nog niet zichtbare individu' als onderdeel van een risicogroep.[92] Het is nog niet wettelijk verankerd.[93]

Het tweede verschil tussen predictive identification en het achttiende-eeuwse panopticon, de onzichtbaarheid, geeft geen aanleiding tot een herinterpretatie van, maar wel tot nieuwe spanningsvelden rondom de waarden autonomie, gelijkheid, verantwoordelijkheid en vertrouwen. Burgers worden steeds transparanter voor de overheid, terwijl de algoritmes en datasets die overheidsinstanties gebruiken niet of nauwelijks transparant voor die burgers zijn.[94] Bovendien worden *voor* predictive identification niet alleen data ingezet die afkomstig zijn van surveillancetechnologieën, zoals de sensorinformatie uit ANPR-camera's die Sensing verwerkte en analyseerde, maar ook data afkomstig uit bronnen die daar oorspronkelijk niet voor bedoeld waren.[95] Denk bijvoorbeeld aan de arbeidsgegevens, fiscale gegevens, inburgeringsgegevens, schuldenlastgegevens, zorgverzekeringsgegevens (of iemand al dan niet een zorgverzekering heeft) en persoonsgegevens (naam, adres, geboortedatum enzovoort) waarvan SyRI gebruikmaakte. Dit wordt 'function creep'[96] genoemd. Burgers weten hierdoor niet welke en hoeveel data waar, hoe en door wie over hen verzameld en geanalyseerd worden. Daardoor staat hun 'digitale autonomie' op het spel: zij kunnen niet controleren hoe die data bij hen 'terugkomen'.[97] Ook kunnen zij niet controleren of er geen sprake is van etnisch profileren of discriminatie. Op dit moment wordt voor predictive identification nog vooral gebruikgemaakt van relatief eenvoudige algoritmes, maar het ligt

88 Mittelstadt 2017.
89 Stevens e.a. 2021.
90 Mittelstadt 2017.
91 Mittelstadt 2017.
92 Stevens e.a. 2021.
93 Mittelstadt 2017.
94 WRR 2016, p. 135.
95 Ziosi e.a. 2022.
96 WRR 2016.
97 Kool, Timmer & Van Est 2015, p. 12, 59.

in de lijn der verwachting dat in de toekomst complexere, zelflerende algoritmes zullen worden ingezet. Die zijn nog moeilijker te controleren.[98] Tot slot is voor het voor burgers onduidelijk wie waarvoor verantwoordelijk is met betrekking tot de verzameling en analyse van gegevens over hen. Daardoor kunnen zij er ook geen bezwaar tegen maken.[99] Het hiervoor omschreven gebrek aan controle- en bezwaarmogelijkheden kan het vertrouwen van burgers schaden.

Tot slot nog een opmerking over de waarde veiligheid. In de vorige paragraaf werd vastgesteld dat het gebruik van predictive identification deze waarde bevordert, mits de uitkomsten kloppen en in de praktijk (goed) worden gebruikt, maar ten koste kan gaan van andere waarden, zoals privacy, autonomie en gelijkheid. Dit geeft geen aanleiding tot een herinterpretatie van de waarde veiligheid, maar roept wel de vraag op hoe zwaar die waarde in onze samenleving moet wegen.[100] Met andere woorden: de positie van de waarde veiligheid ten opzichte van andere waarden moet opnieuw worden bepaald. Vragen die in dat kader opkomen zijn bijvoorbeeld hoeveel privacy en autonomie we willen inleveren om de waarde veiligheid te bevorderen. (Nieuwe) wetgeving op Europeesrechtelijk niveau geeft richting in de beantwoording van deze vragen. De EU-Richtlijn 2016/680,[101] die in Nederland is geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (WJG), heeft betrekking op het verzamelen, verwerken en delen van persoonsgegevens in de strafrechtelijke context en beoogt betrokkenen een betere bescherming te bieden op het vlak van privacy. Hoewel de richtlijn meer autonomie en controle suggereert dan betrokkenen daadwerkelijk hebben, omdat gebleken is dat de toestemming voor en controle van verwerking van persoonsgegevens in de opsporingspraktijk niet goed gerealiseerd kunnen worden,[102] legt deze richtlijn wel de nadruk op privacy en autonomie in de afweging tussen die waarden en de waarde veiligheid. Ook de voorgestelde Europese Wet op de artificiële intelligentie[103] maakt duidelijk dat de waarde veiligheid ten opzichte van andere waarden zoals privacy en autonomie niet te zwaar gewogen moet worden. Deze wet zal predictive identification instrumenten als 'hoog risico' kwalificeren,[104] hetgeen betekent dat ze zullen moeten gaan voldoen aan dwingende voorschriften die bedoeld zijn om grondrechten, zoals het recht op privacy, te waarborgen.[105]

98 Schuilenburg & Soudijn 2021.
99 Kool, Timmer & Van Est 2015, p. 25.
100 Zie o.a. Spithoven & Foppen 2021.
101 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, L 199/89 (4 mei 2016).
102 B. Custers & M. Leiser, 'Persoonsgegevens in het strafrecht', *NJB* 2019, 34, p. 2497.
103 Voorstel voor een verordening van het Europees parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (Wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie, Brussel, 21 april 2021 COM(2021), 206 final 2021/0106 (COD).
104 Overweging 39.
105 Toelichting, par. 1.1.


PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

## 5. Het derde analyseniveau: hoe kan vanuit het oogpunt van de geïdentificeerde waarden beter met predictive identification omgegaan worden?

De meest voor de hand liggende aanbeveling om beter met predictive identification instrumenten om te gaan is om de transparantie te vergroten van de risicomodellen en indicatoren waarop hun voorspellingen zijn gebaseerd, zodat ze moreel doorzichtiger worden en er beter kan worden gecontroleerd of en hoe ze de geïdentificeerde waarden bevorderen of schaden. Dit kan het vertrouwen van burgers vergroten. Regulering kan hierin een rol spelen. Transparantie is het hoofdbeginsel van de gegevensbeschermingswetgeving. Het transparantiebeginsel ligt ten grondslag aan en is vastgelegd in het Handvest van de grondrechten van de Europese Unie en de Algemene verordening gegevensbescherming (AVG).[106] Het is leidend geweest voor de SyRI-uitspraak waarin, zoals eerder genoemd, de rechter de wetgeving die het gebruik van SyRI regelde, onverbindend verklaarde wegens strijd met het recht op privacy. De rechter kwam tot dit oordeel omdat de betreffende wetgeving niet regelde dat inzicht werd geboden in het gebruikte risicomodel en de daarbij behorende indicatoren, en ook niet voorzag in nadere wettelijke waarborgen die een gebrek aan inzicht daarin compenseerden.[107]

Hierbij dient opgemerkt te worden dat de AVG niet van toepassing is op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek en de opsporing van strafbare feiten,[108] en dus in principe niet op predictive identification. (Deze uitzondering gold niet voor SyRI, omdat uit dit systeem voortvloeiende risicomeldingen weliswaar aan de politie of het OM konden worden doorgespeeld, maar de gegevens waarop die waren gebaseerd niet door deze instanties werden verwerkt. De uitzondering gold wel voor Sensing.) Niet de AVG, maar de Wpg[109] is daarop van toepassing. Deze wet stelt specifieke waarborgen, regels en rechten in verband met de verwerking van persoonsgegevens door opsporingsautoriteiten voor strafrechtelijke doeleinden. Ook in de Wpg is een transparantiebeginsel opgenomen.[110] Dit geldt echter niet indien daardoor het opsporingsbelang, of een ander strafrechtelijk belang, te veel in het gedrang zou komen.[111] In de praktijk kan, als een opsporingsonderzoek nog loopt, maar zeer beperkt informatie worden gedeeld met betrokkenen.[112]

Dit laatste betekent echter niet dat predictive identification niet controleerbaar hoeft te zijn. Controleerbaarheid kan ook bewerkstelligd worden op een andere manier dan door het gebruikte risicomodel en de daarbij behorende indicatoren transparant te maken. De inzet van predictive identification, die nu nog geschiedt op basis van het zeer algemene artikel 3 Politiewet, zou een afzonderlijke wettelijke

106 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, par. 6.87.
107 Idem, par. 6.90 en 6.95.
108 Art. 2 lid 2 sub d.
109 Wet van 21 juli 2007, *Stb*. 2009, 525.
110 Zie art. 24a en art. 24b.
111 Zie art. 24a lid 3 jo. art. 27.
112 Custers & Leiser 2019, p. 2495.

grondslag kunnen krijgen.[113] De wetgever heeft geen aanleiding gezien om zo'n afzonderlijke wettelijke grondslag op te nemen in het huidige wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering,[114] maar sluit dit in de toekomst niet uit.[115] Door het gebruik van predictive identification bijvoorbeeld afhankelijk te maken van een bevel van de officier van justitie, zou deze vooraf kunnen controleren of daardoor geen waarden of daarop gebaseerde wettelijke voorschriften op onaanvaardbare wijze geschonden worden. Daarnaast zou vastgelegd kunnen worden dat, indien predictive identification leidt tot het vervolgen van een verdachte, de gebruikte algoritmes in een strafproces voor de verdediging inzichtelijk moeten zijn, zodat die dit achteraf nog eens kan controleren.[116]
Hierbij moet wel een kritische kanttekening worden geplaatst. Om een algoritme te kunnen controleren, is technische kennis vereist die de meeste officieren van justitie of advocaten niet zullen bezitten. Zij zouden dan op de een of andere manier uitleg moeten kunnen krijgen over de werking van het algoritme, bijvoorbeeld van de ontwikkelaar van het betreffende predictive identification instrument. Er kan dan een probleem rijzen indien dit instrument gebruikmaakt van een algoritme dat lijdt aan een gebrek aan uitlegbaarheid. Daarvoor kan een oplossing gevonden worden in het technologische domein. Er bestaan *post hoc interpretability techniques* waarmee bijvoorbeeld nagegaan kan worden of kenmerken zoals ras of geslacht, of sociaaleconomische en lokale variabelen waaruit die afgeleid kunnen worden, direct of indirect in voorspellingsmodellen worden gebruikt.[117] Met deze technieken kan aan de hand van een ander, wel door mensen te begrijpen, voorspellingsmodel met dezelfde logica vastgesteld worden hoe de voorspelling tot stand is gekomen.[118] Het is echter belangrijk om te beseffen dat de strafrechtspleging niet alle technologische toepassingen die voorhanden zijn ook *hoeft* in te zetten. In een recent rapport over digitalisering concludeert de Raad van State: 'Voor zover gebruik wordt gemaakt van AI-technieken, rijst de vraag of hier voldoende grip op kan worden gehouden. Bestaat daarover geen zekerheid, dan kan het in voorkomende gevallen gerechtvaardigd zijn af te zien van digitalisering, dan wel de vormgeving of wijze van uitvoering te herzien.'[119] Een oplossing voor het probleem van niet uitlegbare algoritmes kan dus ook zijn dat ervoor wordt gekozen geen gebruik te maken van predictive identification instrumenten die daarop zijn gebaseerd.
Een tweede aanbeveling heeft te maken met de waarden veiligheid en verantwoordelijkheid. Zoals eerder gesteld, hebben predictive identification instrumenten tot doel de veiligheid te bevorderen. In verband daarmee is het van belang dat hun

113 A. Das & M.B. Schuilenburg, 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmes vraagt om aanpassing van het strafprocesrecht', Strafblad 2018, 4, p. 19-26.
114 *Kamerstukken II*, 36327, nr. 2.
115 Memorie van Toelichting, *Kamerstukken II*, 36327, nr. 3, par. 9.3.
116 J.J. Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', Platform Modernisering Strafvordering november 2018, doi:10.5553/PMSV/258950952018001018001.
117 Rai 2020.
118 Rai 2020, p. 139.
119 Raad van State, *Toetsingskader digitalisering en wetgeving*, mei 2021, p. 5, te raadplegen van Publicatie Raad van State over digitalisering in wetgeving en bestuursrechtspraak - Raad van State.

voorspellingen (zo veel mogelijk) kloppen en te vertalen zijn naar kennis waar politiemensen iets aan hebben in de praktijk; onjuiste en moeilijk te interpreteren voorspellingen bevorderen de veiligheid niet. Goede voorspellingen beginnen met goede data. Data zijn immers de grondstof waarop predictive identification drijft. Daarom moet bij de selectie van databronnen voor predictive identification niet worden gekeken naar de kwantiteit, maar vooral naar de kwaliteit van de data.[120] Het gebruik van vuile data, dat wil zeggen onjuiste of onrechtmatig verkregen data, kan ertoe leiden dat de uitkomsten ook vervuild zijn.[121] Het gebruik van vuile data voor predictive identification moet dus vermeden worden.

Ook hier kan regulering een rol spelen. De Wpg bevat verschillende voorschriften[122] die bepalen dat gegevens alleen (verder) mogen worden verwerkt als ze juist, nauwkeurig en rechtmatig verkregen zijn. De vraag rijst wie verantwoordelijk is voor het naleven van deze voorschriften. Volgens de Wpg is dat allereerst de politie zelf. Privacyfunctionarissen of beleidsmedewerkers zouden, al dan niet op verzoek van degenen op wie ze betrekking hebben, vuile data moeten verwijderen uit de datasets die voor predictive identification worden gebruikt.[123] De strafrechter zou, indien de voorspellingen tot een strafzaak leiden, een controle achteraf kunnen uitvoeren. In de praktijk zal een dergelijke controle echter slechts op een zeer beperkte schaal plaatsvinden, omdat maar weinig voorspellingen (aantoonbaar) tot een strafzaak zullen leiden en dit alleen zal gebeuren indien het de verdediging lukt de rechter te overtuigen de gebruikte data te controleren.[124] Van 'een sluitend en transparant mechanisme om vuile data (…) te identificeren en te verwijderen' is nog geen sprake.[125] Het wettelijk kader zou verbeterd kunnen worden door bijvoorbeeld de officier van justitie te betrekken bij de controle aan de voorkant (dus het verwijderen van vuile data uit de datasets).[126]

Een derde aanbeveling heeft betrekking op de waarde privacy. Zoals eerder gesteld, kan predictive identification potentieel tot een vergaande ingreep in de persoonlijke levenssfeer leiden. De wettelijke kaders die worden gebruikt om predictive identification te reguleren stammen uit een tijd waarin technisch gezien veel minder mogelijk was. Daarom is een nieuw wettelijk kader noodzakelijk.[127] Het Europees Hof voor de Rechten van de Mens (EHRM) heeft duidelijk gemaakt dat landen die vooroplopen bij de ontwikkeling en inzet van nieuwe opsporingstechnologieën, zoals Nederland, een bijzondere verantwoordelijkheid dragen voor het vinden van een balans tussen het belang van de preventie en vervolging van strafbare feiten

120 Th. Snaphaan & W. Hardyns, 'Handvatten voor een kwaliteitsbeoordeling van big data: De introductie van het Total Error raamwerk', *Tijdschrift voor Veiligheid* 2022, 20, p. 63-88, 10.5553/TvV/.000033.

121 Das & Schuilenburg 2020.

122 Art. 3 lid 2 en art. 4 Wpg.

123 Art. 4 jo. art. 1 onder f en art. 28 en 29 Wpg; Das & Schuilenburg 2020, p. 260-261.

124 Das & Schuilenburg 2020, p. 261-263.

125 Das & Schuilenburg 2020, p. 263.

126 Das & Schuilenburg 2020, p. 260.

127 Hirsch Ballin 2021.

enerzijds, en het belang van de bescherming van het recht op privacy anderzijds.[128] Hoewel het EHRM zich nog niet heeft uitgesproken over predictive identification, heeft het wel minimumwaarborgen vastgesteld met betrekking tot andere opsporingstechnologieën waarmee grote hoeveelheden gegevens kunnen worden verkregen en verwerkt, zoals bulkinterceptie. De regeling van dergelijke opsporingstechnologieën vereist volgens het EHRM 'end-to-end waarborgen'.[129] Dit betekent dat de noodzaak en de evenredigheid in elk stadium van het proces moeten worden beoordeeld, er vooraf onafhankelijke toestemming moet zijn verleend, en er sprake moet zijn van toezicht en onafhankelijke controle achteraf.[130] Deze eis toont aan dat de regulering van zulke potentieel zeer indringende bevoegdheden niet mag ophouden bij het verwerven van gegevens, waar het zwaartepunt van de huidige juridische regelgeving ligt, maar zich ook moet gaan uitstrekken tot de analyse en het gebruik van die gegevens, waarbij het risico van inmenging in de persoonlijke levenssfeer eigenlijk het grootst is.[131]

Niet alleen het risico van inmenging in de persoonlijke levenssfeer is het grootst in de fase van de analyse en het gebruik van gegevens, ook het risico op discriminatie doet zich in die fase het meest voor. Vanuit het oogpunt van de waarde gelijkheid verdient het daarom eveneens aanbeveling om de analyse en het gebruik van gegevens beter te reguleren. De voorgestelde nieuwe Europese Wet op de artificiële intelligentie bevat bepalingen die tot doel hebben bias in datasets te voorkomen teneinde discriminatie tegen te gaan.[132] De inzet van technologie kan ook helpen om de waarde gelijkheid te bevorderen. Er bestaan tegenwoordig toolkits die bias in datasets en voorspellingsmodellen kunnen aantonen.[133] Met behulp van zo'n toolkit kunnen onregelmatigheden en afwijkingen worden opgespoord die kunnen resulteren in voorspellingen die nadelig zijn voor bepaalde groepen in de maatschappij en daardoor kunnen leiden tot discriminatie.

Tot slot geldt voor alle waarden dat daar idealiter al in de ontwerpfase aandacht voor zou moeten zijn, zodat ze als het ware in predictive identification instrumenten kunnen worden ingebouwd door de bevordering of bescherming van bepaalde waarden en daarop gebaseerde normen te vertalen in ontwerpspecificaties.[134] Denk bijvoorbeeld aan een ontwerpspecificatie die tot doel heeft (groeps)privacy te beschermen. Een dergelijke manier van ontwerpen wordt *Value Sensitive Design* ge-

128 ECtHR 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204, appl. nrs. 30562/04 en 30566/04 (S. and Marper/United Kingdom); M.F.H. Hirsch Ballin & M. Galič, 'Digital investigation powers and privacy. Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure', *Boom Strafblad* 2021, 4, p. 148-159.

129 ECtHR 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, appl. nrs. 58170/13, 62322/14 en 24960/15 (Big Brother Watch and others/United Kingdom); Hirsch Ballin & Galič 2021, p. 153.

130 Idem.

131 Hirsch Ballin & Galič 2021, p. 156; WRR 2016, p. 9.

132 Overweging 44.

133 Zie bijv. R. Bellamy e.a., *AI Fairness 360: An Extensible Toolkit for Detecting, Understanding, and Mitigating Unwanted Algorithmic Bias*, doi.org/10.48550/arXiv.1810.01943.

134 M. Flanagan, D.C. Howe & H. Nissenbaum, 'Embodying Values in Technology: Theory and Practice', in: J. Van den Hoven & J. Weckert (red.), *Information Technology and Moral Philosophy*, Cambridge: Cambridge UP 2008, p. 322-353.



PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002

noemd.[135] Er is niet veel onderzoek gedaan naar de vraag hoe deze vertaalslag gemaakt kan worden.[136] Dit hangt af van het type technologie en is erg context-afhankelijk.[137] Wel duidelijk is dat dit alleen kan indien verschillende belanghebbenden ('stakeholders') bij het ontwerpproces betrokken zijn.[138] Indien een vertaling moet worden gemaakt van wetgeving naar een digitale uitvoeringspraktijk, is een multidisciplinaire en iteratieve samenwerking tussen juristen, uitvoeringsdeskundigen, modelleurs en softwareontwikkelaars essentieel.[139]

## 6. Conclusie

In deze bijdrage is met behulp van de uit de computerethiek afkomstige methode disclosive computer ethics transparant gemaakt welke waarden bevorderd of juist geschaad kunnen worden door predictive identification op het individuele niveau van burgers en politiemensen. De conclusie luidt dat allereerst transparantie zelf een belangrijke waarde is met betrekking tot predictive identification. Zonder transparantie is predictive identification als een moreel ondoorzichtig panopticon; een vorm van slim toezicht waarbij moeilijk valt te controleren welke waarden in het geding zijn of kunnen komen. Deze waarde heeft echter een bijzondere aard, omdat de betekenis ervan vooral duidelijk wordt in samenhang met andere waarden.

Data en voorspellingen, de twee pijlers van predictive identification, hebben altijd een rol gespeeld in het politiewerk. De politie wordt door predictive identification dan ook niet in staat gesteld iets te doen wat zij in de analoge wereld niet kon, maar wel om het anders te doen, namelijk sneller, diepgaander en efficiënter. De waarden die op het individuele niveau van burgers en politiemensen samenhangen met predictive identification, in deze paper geïdentificeerd als veiligheid, privacy, autonomie, gelijkheid, verantwoordelijkheid en vertrouwen, komen daardoor op een andere manier onder spanning te staan dan in het pre-digitale tijdperk. Onderzocht is vervolgens of ze daarom ook anders geïnterpreteerd moeten worden.

Voor de waarde privacy geldt dat het bestaande concept daarvan niet voldoet in relatie tot predictive identification. De privacyrisico's komen in dit geval niet zozeer voort uit de toegang tot losse gegevens over mensen, maar vooral uit de mogelijkheid om conclusies te trekken uit de optelsom van een heleboel gegevens over een heleboel mensen op basis van correlaties. Predictive identification vraagt derhalve om 'groepsprivacy': een concept van privacy dat niet draait om het geïdenti-

135 B. Friedman, P.H. Kahn & A. Borning, 'Value Sensitive Design and Information Systems', in: P. Zhang & D. Galletta (red.), *Human-Computer Interaction in Management Information Systems: Foundations*, New York: M.E. Sharpe 2006, p. 348-372.

136 I. van de Poel, 'Translating values into design requirements', in: D. Mitchfelder, N. McCarty & D.E. Goldberg (red.), *Philosophy and engineering: Reflections on practice, principles and process*, Dordrecht: Springer 2013, p. 253-266.

137 I. van de Poel, 'Design for value change', *Ethics Inf Technol* 2021, 23, p. 27-31, https://doi.org/10.1007/s10676-018-9461-9.

138 Flanagan, Howe & Nissenbaum 2008.

139 M. Lokin, A. Ausems & J. Bulles, Wetsanalyse: voor een werkbare uitvoering van wetgeving met ICT, Den Haag: Boom juridisch 2021.

ficeerde individu, maar om de privacy van het nog niet zichtbare individu als onderdeel van een risicogroep. Een dergelijk concept van privacy is nog niet wettelijk verankerd. Daarnaast geeft predictive identification aanleiding tot nieuwe spanningsvelden rondom de waarden autonomie, gelijkheid en verantwoordelijkheid. Voor burgers is niet transparant welke en hoeveel data waar, hoe en door wie over hen verzameld en geanalyseerd worden. Daardoor staat hun 'digitale autonomie' op het spel: zij kunnen niet controleren hoe die data bij hen 'terugkomen'. Ook kunnen zij niet nagaan of zij wel gelijk behandeld worden en wie waarvoor verantwoordelijk is met betrekking tot de verzameling en analyse van gegevens over hen. Dit kan hun vertrouwen, ook een belangrijke waarde, schaden en daarmee uiteindelijk de rechtsstaat bedreigen. Tot slot leidt het gebruik van predictive identification ertoe dat de positie van de waarde veiligheid ten opzichte van andere waarden opnieuw moet worden bepaald. (Nieuwe) Europese wetgeving geeft richting aan die afweging. Daaruit kan worden afgeleid dat de waarde veiligheid daarin niet te veel gewicht moet worden toegekend.

Deze paper eindigt met een aantal aanbevelingen om beter met predictive identification instrumenten om te gaan. De meest voor de hand liggende is om de transparantie te vergroten van de risicomodellen en indicatoren waarop hun voorspellingen zijn gebaseerd, zodat ze moreel doorzichtiger worden en er beter kan worden gecontroleerd of en hoe ze de hiervoor omschreven waarden schaden. Regulering kan hierin een rol spelen, maar ook technologische oplossingen kunnen soelaas bieden. Omdat goede voorspellingen beginnen met goede data, is het vanuit het oogpunt van de waarden veiligheid en verantwoordelijkheid belangrijk dat bij de selectie van databronnen voor predictive identification niet wordt gekeken naar de kwantiteit, maar vooral naar de kwaliteit van de data. Vanuit het oogpunt van de waarden privacy en gelijkheid ligt de nadruk juist meer op de fase van de analyse en het gebruik van die data en is het van belang dat deze beter wordt gereguleerd. Tot slot geldt voor alle waarden dat daar idealiter al in de ontwerpfase aandacht voor zou moeten zijn, zodat ze als het ware in predictive identification instrumenten kunnen worden ingebouwd door de bevordering of bescherming van bepaalde waarden en daarop gebaseerde normen te vertalen in ontwerpspecificaties (*Value Sensitive Design*).

In deze bijdrage is het fenomeen predictive identification slechts vanuit één perspectief, namelijk de computerethiek, bestudeerd. Het is van belang dat dit fenomeen onderwerp van discussie blijft en ook vanuit andere perspectieven belicht blijft worden, bijvoorbeeld vanuit politiestudies en de empirische rechtswetenschap. Wat agenten in de praktijk met informatie afkomstig uit predictive identification instrumenten doen en of en hoe die informatie uiteindelijk kan leiden tot een veroordeling, zijn voorbeelden van belangrijke vragen die, als predictive identification in de toekomst meer gebruikt gaat worden, aandacht behoeven.


PROCES 2023 (102) 3
doi: 10.5553/PROCES/016500762023102003002