De bescherming van algoritmische groepen bij profilering en datagedreven politiewerk: van individuele naar group privacy?

Schermer, B.W.; Galič, M.

Artikel

De bescherming van algoritmische groepen bij profilering en datagedreven politiewerk

Van individuele naar group privacy?

prof. mr. dr. B.W. (Bart) Schermer en dr. M. (Maša) Galič*

1. Inleiding

De beschikbaarheid van grote hoeveelheden gegevens en de snelle ontwikkeling van kunstmatige intelligentie (*artificial intelligence*, hierna: AI) heeft ervoor gezorgd dat het werk van de politie steeds meer 'informatiegestuurd' en 'datagedreven' is. Naast het optimaliseren van de inzet van beperkte middelen (*intelligence led policing*)[1] speelt grootschalige gegevensanalyse ook een steeds belangrijker rol bij het voorspellen en voorkomen van crimineel gedrag (*predictive policing*) en bij het verkrijgen van een breder zicht op criminele organisaties en strafbare feiten.[2] Om crimineel gedrag beter te begrijpen, vroegtijdig te detecteren en zelfs te voorspellen maakt de politie in het bijzonder gebruik van profilering.[3]

Datagedreven politiewerk in het algemeen en profilering in het bijzonder is echter niet zonder risico's. Om deze risico's te beperken zijn er de bepalingen uit het Wetboek van Strafvordering en de Wet politiegegevens. De nadruk ligt hierbij op de bescherming van de persoonlijke levenssfeer en de persoonsgegevens van het individu. De vraag is echter of deze individuele benadering toereikend is wanneer het opstellen en toepassen van profielen in eerste instantie is gericht op algoritmische groepen en er dus nog geen 'aangrijppunt' is voor de wettelijke bescherming. In deze bijdrage verkennen wij de bescherming van individuen en meer in het bijzonder algoritmische groepen bij de toepassing van profilering.

De opbouw van deze bijdrage is als volgt. Allereerst bespreken we de ontwikkeling en het gebruik van profilering binnen de politie. Vervolgens bekijken wij het wettelijk kader voor profilering en beschrijven wij waarom dit kader onvoldoende bescherming biedt voor de rechten en vrijheden van burgers. Ten slotte doen wij enkele suggesties voor verbetering van het huidige juridische kader. Daarbij staat het concept *group privacy* centraal.

* Bart Schermer is hoogleraar Privacy & Cybercrime bij eLaw-Centrum voor Recht en Digitale technologie. Maša Galič is universitair docent privacy en strafprocesrecht bij Vrije Universiteit Amsterdam.

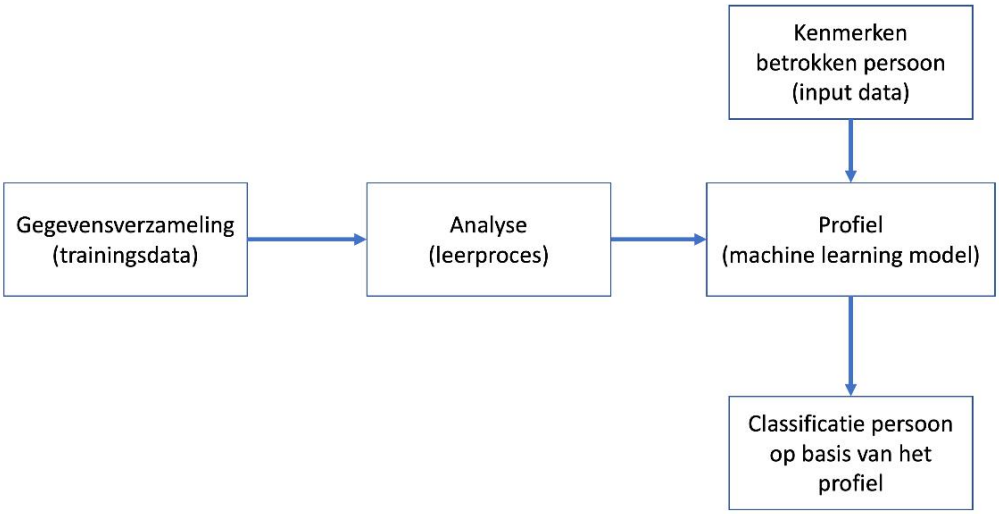
1 Informatiegestuurd werken (oftewel *intelligence-led policing*) betekent dat '*op basis van actuele en betrouwbare informatie en analyses, rationele keuzes worden gemaakt, waardoor mensen en middelen optimaal worden ingezet en de bedrijfsdoelen worden bereikt*'; zie Inspectie openbare orde en veiligheid (2008), *Informatiegestuurde politie*. Via https://zoek.officielebekendmakingen.nl/blg-16729.pdf.

2 Zie o.a. M.F.H. Hirsch Ballin, *Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States*, Den Haag: T.M.C. Asser Press, 2012; en M.I. Fedorova e.a., *Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Nijmegen: Radboud University Press, 2022.

3 Zie bijvoorbeeld J. Bachner, *Predictive Policing: Preventing Crime with Data and Analytics*, Washington, DC: IBM, Centre for the Business of Government, 2013.

doi: 10.5553/BSb/266669012023004002002

Figuur 1 *Schematische voorstelling van het proces voor profilering van personen*



2. Modellen als basis voor datagedreven politiewerk

Datagedreven werken impliceert dat de politie een model van de werkelijkheid heeft dat haar in staat stelt 'ruwe' gegevens te vertalen naar relevante informatie om het handelen te sturen. Zo kunnen modellen (in het populaire spraakgebruik 'algoritmen' genoemd) worden gebouwd die inzicht geven in de tijd en plaats waar delicten plaatsvinden, en modellen die betrekking hebben op de (persoonlijke) kenmerken en gedragingen die indicatief zijn voor het plegen of gepleegd hebben van een misdrijf.[4] Deze modellen functioneren tegenwoordig vaak op basis van *machine learning*, waarmee grote hoeveelheden gegevens worden geanalyseerd om patronen in het gedrag van groepen vast te stellen en op basis daarvan beslissingen te nemen.[5]

Computers creëren een model op basis van grote hoeveelheden gegevens ('trainingsdata'). Daarbij gaat het niet alleen om het gebruik van enkele standaardvariabelen (bijvoorbeeld geslacht, leeftijd, burgerlijke staat, inkomen en woonplaats), maar om grote hoeveelheden variabelen waaruit voorspellende informatie over groepen mensen valt af te leiden.[6] Het resultaat van de trainingsfase is een *machine learning model*. Vervolgens wordt het model gevoed met nieuwe gegevens ('inputdata') op basis waarvan het een antwoord geeft: een voorspelling, een classificatie op basis van een risicoprofiel et cetera. Het doel is gemakkelijk beschikbare gegevens, die meestal niet bijzonder privé of gevoelig zijn en vaak ook geanonimiseerd zijn, te gebruiken om meer gevoelige informatie over groepen te voorspellen die moeilijk te vinden is ('targetdata').

Profilering is een veelgebruikte toepassing van machine learning. Door profilering kunnen op basis van grote hoeveelheden gegevens algoritmische groepsprofielen worden opgesteld. Deze groepsprofielen kunnen dan worden gebruikt voor het maken van risico-inschattingen waardoor de politie kan optreden tegen een in principe onbeperkt aantal personen die niets hebben gedaan om de aandacht van de politie te trekken. Predictive policing – het proactieve gebruik van algoritmisch gemedieerde gegevensanalyse om patronen te vinden in datasets teneinde risico-inschattingen te maken – is een schoolvoorbeeld van een dergelijke gegevensanalyse.

Profilering brengt een opmerkelijke verandering teweeg: mensen worden door profileringstechnieken niet meer als individuen, maar als leden van specifieke, door algoritmen samengestelde (risico)groepen (potentiële bijstandsfraudeurs, jeugdcriminelen, drugskoeriers et cetera) aangemerkt.

Schematisch ziet dit proces voor profilering van personen eruit als weergegeven in figuur 1.

3. Het wettelijk kader voor profilering

Bij profilering kunnen we twee handelingen onderscheiden: 1) het opstellen van het model, en 2) het toepassen van het model. Het verschil tussen de twee is kunstmatig, omdat het opstellen van het profiel impliceert dat het ook wordt gebruikt, maar voor de beoordeling

4 R. Mühlhoff, 'Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI', in M. Friedewald, A. Roßnagel, J. Heesen, N. Krämer en J. Lamla (Red.), *Künstliche Intelligenz, Demokratie und Privatheit*, Baden Baden: Nomos, 2022, pp. 31-58.

5 Zie bijvoorbeeld A. Mantelero, 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection', *Computer Law & Security Review*, 2016; R. Mühlhof, 'Predictive privacy: towards an applied ethics of data analytics', *Ethics and Information Technology*, 2021; zie ook de bijdragen in M. Hildebrandt en S. Gutwirth (Red.), *Profiling the European citizen: cross-disciplinary perspectives*, Berlin: Springer, 2008.

6 Mantelero 2016, p. 239.

doi: 10.5553/BSb/266669012023004002002

van de legitimiteit van profilering is het wel van belang dit onderscheid te maken. De reden hiervoor is dat de wettelijke grondslagen voor het opstellen en het toepassen van het profiel niet noodzakelijkerwijs gelijk zijn.

3.1 Wettelijk kader voor het opstellen van het profiel

Om een profiel te creëren heeft de politie gegevens nodig. Hierbij zijn de verwerking van gegevens die eerder door de politie bij haar taakoefening en door opsporingsonderzoeken zijn verzameld en het doorlopend combineren en verrijken van verschillende datasets van de politie van groot belang.[7] Deze datasets bevatten immers onbekende inzichten die blootgelegd moeten worden, zoals verbanden tussen personen, groepen van personen, organisaties of voorwerpen. Ook kunnen gegevens van burgers worden verzameld uit openbare bronnen (denk bijvoorbeeld aan *social media feeds*) en kunnen de bewegingen van personen in de fysieke wereld worden gevolgd door middel van bijvoorbeeld stille sms en *Automatic Number Plate Recognition* (ANPR).

Het staat de politie in beginsel vrij alle mogelijke gegevens te gebruiken zolang daarmee maar geen inbreuk wordt gemaakt op de rechten en vrijheden van personen, vooral het recht op privacy en het verwante maar afzonderlijke recht op gegevensbescherming (art. 8 Handvest van de Grondrechten van de Europese Unie). Wanneer de politie bijvoorbeeld gegevens over het weer wil gebruiken (gegevens die geen betrekking hebben op een individu; 'niet-persoonlijke gegevens'), staat daar weinig aan in de weg, omdat er nog geen inbreuk wordt gemaakt op individuele rechten zoals het recht op privacy en gegevensbescherming.

Wanneer er bij het verzamelen van gegevens wél inbreuk wordt gemaakt op de rechten op privacy en gegevensbescherming, moet daarvoor een basis worden gevonden in de wet. Bij relatief beperkte inbreuken kan deze basis worden gevonden in het algemene artikel 3 Politiewet, te weten de taak tot daadwerkelijke handhaving van de rechtsorde. Wanneer sprake is van zwaardere inbreuken, moet een meer specifieke basis worden gevonden in het Wetboek van Strafvordering (of in een bijzondere wet, zoals de Wet wapens en munitie of de Wet op de economische delicten). Bij het beoordelen van de 'inbreukmakendheid' van een handeling wordt in eerste instantie gekeken naar de wijze waarop de gegevens worden verzameld (bijvoorbeeld het doen van een huiszoeking kan als ingrijpender worden gezien dan het observeren van sociale media). Verder wordt gekeken naar de aard van de gegevens. Zo wordt bijvoorbeeld bij het vorderen van gegevens onderscheid gemaakt tussen abonneegegevens, verkeersgegevens en inhoudelijke gegevens, waarbij het vorderen van deze laatste categorie als het meest inbreukmakend wordt gezien, gegeven de mogelijke gevoeligheid van de gegevens.[8] Ten slotte speelt de omvang van de verzameling een rol, waarbij bulkverzameling begrijpelijkerwijs meer inbreukmakend is dan een beperkte verzameling van gegevens.

Wanneer de gegevens die de politie gebruikt betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon, zijn die aan te merken als 'politiegegevens' (oftewel 'persoonsgegevens') en moet de verwerking voldoen aan de vereisten uit de Wet politiegegevens (Wpg). Politiegegevens mogen alleen worden verwerkt wanneer dit noodzakelijk is (art. 3 Wpg) en wanneer de verwerking gebaseerd kan worden op een van de grondslagen genoemd in de artikelen 8 tot en met 13 van de Wpg (waaronder de uitvoering van de dagelijkse politietaak, de handhaving van de rechtsorde in een concreet geval en de *intelligence*-taak). Deze artikelen stellen echter weinig concrete grenzen, omdat ze breed zijn geformuleerd. Dit en het feit dat gegevens verzameld voor de ene taak doorgaans ook voor andere taken mogen worden gebruikt, laat veel ruimte voor het (her)gebruik van politiegegevens. Zo kunnen bijvoorbeeld gegevens die zijn verzameld in het kader van een opsporingsonderzoek worden gebruikt voor de uitvoering van de dagelijkse politietaak (art. 9 lid 3 Wpg) en kunnen gegevens die zijn verzameld van getuigen en slachtoffers ook worden gebruikt om misdrijven te onderzoeken of te voorkomen waarbij zij als verdachten worden beschouwd.[9]

De politie kan ook gebruikmaken van statistische en demografische gegevens. Veel van deze gegevens zijn geaggregeerd of geanonimiseerd en hebben geen betrekking op een individu.[10] Dit betekent dat het gebruik ervan buiten het bereik van gegevensbeschermingsrecht valt.

Met betrekking tot de daadwerkelijke bouw van het model (het profiel) is de aankomende AI Verordening relevant.[11] Deze verordening gaat (onder andere) eisen stellen aan de kwaliteit en representativiteit van de gebruikte gegevens, de wijze waarop de modellen worden gebouwd en de wijze waarop ze in bedrijf worden genomen. Deze vereisten moeten ervoor zorgen dat AI-modellen op een zorgvuldige wijze worden ontwikkeld en toegepast. Hierbij is het van belang om aan te tekenen dat de AI Verordening – met uitzondering van de verboden praktijken beschreven in artikel 5 AI Verordening –

7 M.F.H. Hirsch Ballin en J.J. Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden', *Delikt & Delinkwent* 2023, afl. 2, p. 18-38.

8 In het Smartphone-arrest (HR 4 april 2017, ECLI:NL:HR:2017:592) heeft de Hoge Raad zich ook uitgelaten over de gevoeligheid van de gegevens en de inbreuk die het kennisnemen van deze gegevens kan opleveren. Zie verder bijvoorbeeld EHRM, 30 september 2014, no. 8429/05 (*Prezhdarovi t. Bulgarije*).

9 Zie de recente zaak voor het Hof van Justitie van de Europese Unie, 8 december 2022, C-180/21 (*Inspektor t. Inspektorata kam Visshia sadeben savet*).

10 Wanneer deze gegevens vervolgens gerelateerd worden aan een individu, is er uiteraard wel sprake van verwerking van persoonsgegevens.

11 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 21.4.2021, COM(2021) 206 final, 2021/0106(COD).

doi: 10.5553/BSb/266669012023004002002

géén bepalingen kent over de legitieme toepassing van profilering.[12]

3.2 Wettelijk kader voor het gebruiken van het profiel

Wat de consequenties van het gebruik van het profiel zijn, is afhankelijk van het doel van het profiel en de impact die het gebruik ervan heeft. De wettelijke bescherming om de negatieve impact van profielen te adresseren kan op twee manieren worden 'geactiveerd': 1) het verzamelen van de gegevens die als input dienen (niet te verwarren met de trainingsdata die zijn verzameld om het model op te bouwen) maakt inbreuk op de rechten van het individu, en/of 2) de handelingen die worden gedaan naar aanleiding van een match met het profiel hebben (negatieve) gevolgen voor het individu.

- *Ad 1) het verzamelen en matchen van input data*

Om personen te kunnen matchen met een profiel is het verzamelen van gegevens die als inputdata dienen voor het model noodzakelijk. Dit kan bijvoorbeeld gebeuren door middel van directe observatie (een persoon met bepaalde uiterlijke of gedragskenmerken voldoet aan een profiel), het matchen van gegevens uit (politie)systemen met het profiel, of het verzamelen en matchen van openbaar beschikbare gegevens (bijvoorbeeld likes, berichten, vrienden, lidmaatschap van een groep) tegen het profiel. Het verzamelen en gebruiken van dergelijke inputdata kan een inbreuk vormen op de persoonlijke levenssfeer en moet daarom wederom gebaseerd kunnen worden op een deugdelijke wettelijke grondslag. Zoals uit de gegeven voorbeelden blijkt, zijn de inputdata echter meestal gegevens die openbaar of anderzijds gemakkelijk beschikbaar zijn, zodat zij over het algemeen niet als bijzonder privé of gevoelig worden beschouwd en dus gezien worden als niet erg inbreukmakend.[13]

Er bestaat geen expliciete beschrijving van profilering als (opsporings)bevoegdheid in het Wetboek van Strafvordering.[14] Met de implementatie van de Europese Richtlijn politie en justitiegegevens[15] is profilering wel beschreven in de Wpg (art. 1 lid u):

> "*elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van die gegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met de bedoeling met name aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.*"

Wat daarbij opvalt, is dat profilering in de Wpg niet als bevoegdheid is beschreven, en geen concrete regels worden gesteld voor het rechtmatig gebruik van profielen, maar dat hoofdzakelijk is beschreven wat niét mag in de context van profilering. Zo is geautomatiseerde besluitvorming op basis van profilering zonder menselijke tussenkomst verboden (art. 7a lid 1 Wpg) en mag profilering niet leiden tot discriminatie op grond van bijzondere categorieën politiegegevens zoals etniciteit en religie (art. 7a lid 3 Wpg jo art. 5 Wpg). We mogen uit deze beschrijving van profilering in de Wpg *a contrario* afleiden dat profilering in ieder geval niet verboden is. Afhankelijk van het gebruik van het profiel moet de wettelijke basis voor de toepassing gevonden worden in de uitvoering van de dagelijkse politietaak (art. 3 Politiewet jo. art. 8 Wpg), de handhaving van de rechtsorde in een concreet geval (art. 132a Sv jo. art. 9 Wpg) of de *intelligence*-taak van de politie (art. 132a Sv jo. art. 10 Wpg).[16]

- *Ad 2) Vervolgstappen naar aanleiding van een match*

Wanneer een individu gematcht wordt met een profiel, leidt dat doorgaans tot een vervolgstap. De overeenkomst met het profiel is dan mogelijk aanleiding om dat individu staande te houden, vormt de opmaat voor nader onderzoek naar een persoon, of kan worden gebruikt als argument om een persoon op een risicolijst te zetten (denk bijvoorbeeld aan de TopX-lijsten die worden gehanteerd bij de bestrijding van jeugdcriminaliteit).[17] Deze vervolgstappen kunnen inbreuk maken op het recht op privacy, het recht op een eerlijk proces en het recht op gelijke behandeling.[18]

Het nemen van vervolgstappen, zoals bijvoorbeeld het staande houden van een persoon (art. 52 Sv) of de inzet van opsporingsbevoegdheden, is alleen mogelijk in het geval van een verdenking. De vraag is of het matchen met een groepsprofiel een dergelijke verdenking kan opleveren.[19] Wanneer dit niet het geval is en er op grond van het profiel toch vervolgstappen worden genomen, is er sprake van een vormverzuim in de zin van artikel 359a Sv.

Op grond van artikel 27 Sv wordt enkel als verdachte aangemerkt de persoon "*te wiens aanzien uit feiten of omstandigheden een redelijk vermoeden van schuld aan een strafbaar feit voortvloeit*". Wanneer sprake is van een

12 Verboden toepassingen zijn bijvoorbeeld grootschalige biometrische surveillance of '*social credit*' systemen zoals die in China worden gebruikt.

13 Mühlhoff 2022, pp. 34-5.

14 Daarbij moet ook worden aangetekend dat niet elk gebruik van profilering door de politie plaatsvindt in de context van de opsporing.

15 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.

16 In gevallen waarbij het verzamelen van de inputdata op zichzelf inbreukmakend is (bijvoorbeeld omdat iemand gedurende langere tijd wordt geobserveerd, of de gegevens door middel van bijvoorbeeld afluisteren worden verzameld) is daarenboven een opsporingsbevoegdheid noodzakelijk die deze verzameling legitimeert. Maar dat zal vaak niet het geval zijn.

17 Zie bijvoorbeeld F. Jansen, *Top400: A top-down crime prevention strategy in Amsterdam*, The Public Interest Litigation Project, 2022.

18 R.A. Hoving, 'Verdacht door een algoritme: Kan predictive policing leiden tot een redelijke verdenking', *Delikt en Delinkwent*, 2019, afl. 7, p. 530-546.

19 Zie in dit kader bijvoorbeeld ook: A.R. Lodder e.a., *Big Data, Big Consequences*, WODC, 2014, p. 67.

doi: 10.5553/BSb/266669012023004002002

verdenking, is niet bijzonder helder afgebakend in het strafrecht. In ieder geval moet het gaan om een vermoeden dat op zichzelf redelijk is.[20] Sikkema merkt op dat het accepteren van een vermoeden dat is gebaseerd op een kenmerk dat een zeer groot aantal personen gemeen heeft, onverenigbaar is met de rechtsbeschermende functie van de verdenkingseis. Er moeten bepaalde bezwaren tegen een concreet aan te wijzen verdachte zijn.[21] Een profiel dat onvoldoende specifiek is of anderszins niet accuraat is, kan dus geen aanleiding geven tot een redelijk vermoeden van schuld.[22] Wanneer profilering wordt toegepast om tot een verdenking te komen, moet het profiel dusdanig accuraat en concreet zijn dat de rechtsbeschermende functie van de verdenkingseis niet in het gedrang komt.[23] Maar dit is op zichzelf niet genoeg. Hoving concludeert dat een match met een profiel (de voorspelling van het model) in beginsel niet voldoende is om een redelijke verdenking te laten ontstaan. Er moeten aanvullende observaties zijn op basis waarvan in een concreet geval kan worden vastgesteld dat vermoedelijk een strafbaar feit is gepleegd.[24] Precies dit is het risico bij profilering: deze aanvullende observaties zijn er vaak niet, of worden pas gedaan na het toepassen van het profiel in een concreet geval, wat tot een selectieve toepassing van vervolgstappen kan leiden.

4. Analyse wettelijk kader

Op basis van het hierboven beschreven juridische kader springen wat ons betreft twee zaken in het oog:

1. De juridische bescherming is volledig gericht op het individu.
2. Er is geen integrale regeling voor profilering.

- *Ad 1) Juridische bescherming gericht op het individu*

Het eerste wat opvalt is dat de juridische bescherming vertrekt vanuit het individu. Wanneer geen politiegegevens worden verwerkt of geen sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer, is er geen echt aangrijppunt voor de wettelijke bescherming. De wettelijke bescherming komt pas in beeld wanneer het individu wordt geraakt (bijvoorbeeld door een match met een profiel, of omdat de toepassing van het model anderszins consequenties heeft voor het individu).

Wanneer het gaat om het gebruik van modellen om politieoptreden te sturen (waar moet extra gesurveilleerd worden, waar is een verkeerscontrole het meest effectief?) of als onderbouwing voor interventies richting bijvoorbeeld wijken of groepen (in welke wijken wordt het meest ingebroken, welke groepen zijn oververtegenwoordigd in bepaalde vormen van criminaliteit?), is het Wetboek van Strafvordering doorgaans niet van toepassing omdat nog géén sprake is van strafvorderlijke beslissingen. Ook de Wet politiegegevens is nog niet van toepassing omdat normaliter geen politiegegevens worden verwerkt.

- *Ad 2) Geen integrale regeling profilering*

Wanneer we kijken naar de juridische regeling van profilering, zien we dat een duidelijke juridische basis ontbreekt en sprake is van een lappendeken aan bepalingen die bescherming moeten bieden aan het individu. Bij het verzamelen van gegevens over individuen voor het trainen van de modellen komen het Wetboek van Strafvordering en de Wet politiegegevens in beeld, bij de bouw van het model is de aankomende AI Verordening relevant en bij de toepassing van het model komen het Wetboek van Strafvordering en de Wet politiegegevens wederom in beeld. Ten slotte speelt bij het matchen van personen met een profiel het verdenkingscriterium van artikel 27 Sv nog een rol. Schematisch geeft dit het beeld zoals weergegeven in figuur 2.

4.1 Schiet het wettelijk kader tekort?

De vraag is of de focus op het individu en de versnipperde regeling van profilering problematisch is. Naar onze mening is dat het geval.

Een eerste probleem met het huidige kader is dat de samengestelde handeling van het profileren (het verzamelen van trainingsdata, het bouwen van het model, het verzamelen van inputdata en het classificeren van personen) juridisch telkens vanuit één perspectief wordt beoordeeld (of gegevensbescherming, of strafvordering of de (aankomende) AI Verordening). Dit betekent dat er met name 'aan de voorkant' (bij de bouw van het model) weinig beperkingen en waarborgen zijn, omdat er in dat stadium nog geen individu in beeld is.

20 E. Sikkema, Wetboek van Strafvordering, A. L. Melai / M.S. Groenhuijsen e.a., artikel 27 Sv.

21 E. Sikkema, Wetboek van Strafvordering, A.L. Melai / M.S. Groenhuijsen e.a., artikel 27 Sv, aant. 10.5:10.5 Collectieve verdenking; abstracte indicaties.

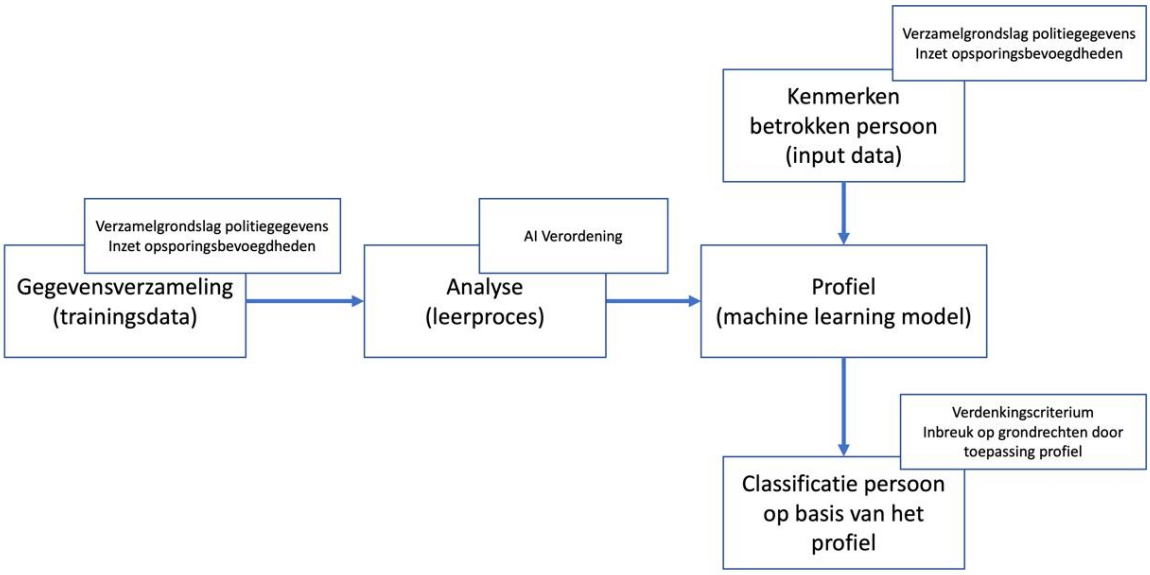
22 Nog los van het feit dat dergelijke profielen ook aanleiding kunnen geven tot discriminatie. Zie in dit kader bijvoorbeeld: M. van der Woude en J. van der Leun, 'De Nederlandse veiligheidscultuur als katalysator voor etnisch profileren?', *Tijdschrift over Cultuur & Criminaliteit*, 2013/3, afl. 2, p. 123-136; P. DeAngelis, 'Racial Profiling and the Presumption of Innocence', *Netherlands Journal of Legal Philosophy* 2014, afl. 1, p. 43-58.

23 Deze aanname kan overigens op gespannen voet staan met de eis van minimale gegevensverwerking uit het gegevensbeschermingsrecht.

24 Hoving 2019.

doi: 10.5553/BSb/266669012023004002002

Figuur 2 Schematische weergave van het wettelijk kader



Met het toenemende gebruik van anonimiseringstechnieken en de beschikbaarheid van openbaar beschikbare gegevens is de mogelijkheid om profielen op te stellen (vooral) op basis van niet-persoonlijke gegevens aanzienlijk uitgebreid.[25] Maar zoals privacywetenschappers in toenemende mate hebben aangetoond, zulke profielen kunnen wel degelijk een (belangrijke) impact hebben op personen.[26] Neem het eerdergenoemde voorbeeld van het verwerken van gegevens betreffende het weer. Purtova beargumenteert dat hoewel waarschijnlijk niemand weerberichten zal zien als persoonsgegevens, deze informatie wel gebruikt kan worden om het handelen van overheidsinstanties te sturen, hetgeen vervolgens weer invloed kan hebben op de persoonlijke levenssfeer van burgers.[27] Denk bijvoorbeeld aan een situatie waarbij op warme dagen extra gesurveilleerd wordt, omdat er dan een grotere kans is op geweldsmisdrijven.[28]

Deze praktijken stellen de politie in staat om onder het mom van anonimiteit in te grijpen in het leven van mensen. 'Leden van een groep' hoeven niet te worden geïdentificeerd (althans niet tot de allerlaatste stap in het profileringsproces: het nemen van een besluit met betrekking tot een individu op basis van het profiel), ze hoeven alleen te worden geclassificeerd om de politie in staat te stellen tegen hen op te treden (hetzij als groep, hetzij als individu). Barocas en Nissenbaum beschrijven dit probleem als volgt:

> *'Even when individuals are not "identifiable", they may still be "reachable", may still be comprehensively represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis."*[29]

Met andere woorden, de 'lens' waarmee naar het vraagstuk van profilering wordt gekeken, is met name die van de bescherming van de informationele privacy van het individu; deze informationele privacy komt pas in beeld wanneer sprake is van een geïdentificeerde of identificeerbare persoon. De individualistische focus van de bestaande privacybescherming suggereert ten onrechte dat de privacy en in het verlengde daarvan andere grondrechten niet geschonden kunnen worden zonder identificeerbaarheid. Dit terwijl door de profilering wel degelijk inbreuk kan worden gemaakt op de rechten van individuen, maar ook op de rechten van groepen. De profielen en andere toepassingen van data-analyse kunnen immers worden gebruikt om algemeen beleid te ontwikkelen (bijvoorbeeld het nemen van specifieke maatregelen met betrekking tot een groep op basis van

25 Zie bijvoorbeeld Mühlhoff 2022, 2021; Mantelero 2016; B. Mittelstadt, 'From individual to group privacy in big data analytics', *Philosophy & Technology*, 2017, afl. 30, p. 475-494.

26 Zie bijvoorbeeld de bijdragen in L. Taylor, L. Floridi en B. van der Sloot (Red.), *Group privacy: new challenges of data technologies*, Cham: Springer International, 2017; M. Galič en R. Gellert, 'Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab', *Computer Law & Security Review*, 2021, afl. 40; B. van der Sloot, 'The quality of life: protecting non-personal interests and non-personal data in the age of big data', *European Review of Private Law*, 2021, afl. 5.

27 N. Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', *Law, Innovation and Technology*, 2018, afl. 40; zie ook Van der Sloot 2021.

28 Voor een discussie over de invloed van het weer op criminaliteit zie: Corcoran, J. en Zahnow, R. (2022), 'Weather and crime: a systematic review of the empirical literature', *Crime Science*, (2022) jg. 11, afl. 16.

29 S. Barocas en H. Nissenbaum, 'Big data's end run around anonymity and consent', in: J. Lane e.a. (Red.), Privacy, big data, and the public good: frameworks for engagement, Cambridge: Cambridge University Press, 2014, p. 45.

de vastgestelde kernkenmerken van die groep).[30] Zo kan de kwalificatie van een risicogroep gevolgen hebben voor alle individuen die onderdeel zijn van die groep of met die groep geassocieerd worden; en kunnen interventies gericht op een wijk consequenties hebben voor bewoners en bezoekers van die wijk.[31]

Dit heeft vooral te maken met het bredere effect op specifieke groepen en delen van de samenleving. De gevolgen van *group profiling* kunnen vanuit individueel oogpunt soms gering zijn, maar het verspreidingseffect van een geautomatiseerde toepassing van profielen op talrijke personen kan wel aanzienlijke gevolgen voor (delen) van de samenleving hebben.[32] Het risico ligt dus niet alleen in de voorspelling met betrekking tot concreet getroffen personen, maar ook in de automatische voorspelling van informatie over grote groepen personen. Dit maakt namelijk een geautomatiseerde en systematisch ongelijke behandeling ('sortering') van bepaalde segmenten van de samenleving mogelijk. Het sorteren van mensen zonder hun medeweten kan leiden tot risico's op groepsniveau, met name in (verdere) discriminatie, *chilling effects* die het gedrag van burgers kunnen beïnvloeden en een toename van sociale onrechtvaardigheid.[33] Noch het Wetboek van Strafvordering, noch de Wet politiegegevens adresseert dit probleem.

Het nadeel van het behoren tot een bepaalde groep wordt uiteraard met name zichtbaar als het profiel uiteindelijk op een concrete persoon (als lid van een groep) wordt toegepast. Een voorbeeld van een dergelijk nadelig gevolg is het vaker onderworpen worden aan controles. Hoewel de onschuldpresumptie de leden van de groep hiertegen zou moeten beschermen, is deze bescherming niet waterdicht. De rechtsbeschermende functie van de onschuldpresumptie bij het gebruiken van profielen kan bijvoorbeeld 'omzeild' worden door de inzet van het profiel in het kader van een controlebevoegdheid. Het profiel wordt dan gebruikt voor een selectie van mogelijke (dan nog niet) verdachten. Op basis van de omstandigheden van het geval kan dan tijdens de uitoefening van de controlebevoegdheid een nadere verdenking worden geconstrueerd. Zo kan tijdens een verkeerscontrole een match ontstaan met een profiel; het zenuwachtige gedrag van de bestuurder kan dan aanleiding geven tot een verdenking en een grond om de wagen van de persoon te doorzoeken. De Hoge Raad heeft in het arrest *Dynamische verkeerscontrole* deze praktijk toegestaan.[34] Een ander voorbeeld is wanneer een 'match' met een profiel aanleiding geeft om een persoon te observeren, tijdens welke observatie aanvullende feiten en omstandigheden worden gevonden die leiden tot een redelijk vermoeden van schuld.[35] Het profiel dient in deze situaties dan als het ware als 'opstapje' voor de daadwerkelijke verdenking.[36] Ten opzichte van de niet-leden van de groep ondervinden de leden van de groep dus meer hinder omdat zij eerder op de radar van de politie komen.[37]

Nu het profiel zo'n cruciale rol speelt in de voorselectie, is het van groot belang dat het profiel accuraat is en er geen sprake is van ongelijke behandeling.[38] In het eerder aangehaalde arrest *Dynamische verkeerscontrole* heeft de Hoge Raad ook overwogen dat controles die uitsluitend of in overwegende mate zijn gebaseerd op etnische of religieuze kenmerken, onrechtmatig zijn. Meer recentelijk oordeelde het gerechtshof Den Haag dat het gebruik van aan ras of etniciteit ontleende uiterlijke kenmerken door de Koninklijke Marechaussee ten behoeve van het Mobiel Toezicht Veiligheid onrechtmatig was.[39] Hoewel het discriminatieverbod dus bescherming kan bieden, staat dit verbod niet direct gelijk aan een expliciete verplichting tot het opstellen van accurate profielen.

De Wet politiegegevens kent wél vereisten op het gebied van accuraatheid, maar wij roepen in herinnering dat de vereisten van die wet alleen van toepassing zijn wanneer sprake is van geïdentificeerde of identificeerbare personen. Bij anonieme profielen is dit nog niet het geval. We kunnen betogen dat op het moment dat een profiel wordt toegepast op een persoon, er sprake is van de verwerking van politiegegevens, omdat op dat moment de kenmerken van het profiel betrekking krijgen op een geïdentificeerde of identificeerbare persoon.[40] Het valt dan ook te betogen dat de Wet politiegegevens reeds in de fase van het opstellen van het profiel van toepassing moet zijn. Hiermee wordt het toepassingsbereik van die wet echter wel heel ver opgerekt.[41] Dit is in het bijzonder

30 Van der Sloot 2021, p. 761.
31 Zie in dit kader Galič en Gellert 2021.
32 Mühlhoff 2022, p. 47.
33 Zie in dit kader M. Büchi et al., 'The chilling effects of algorithmic profiling: Mapping the issues', *Computer Law & Security Review*, 2020, afl. 36; Mühlhoff 2021, 2022.
34 Zie Hoge Raad, 1 november 2016, ECLI:NL:HR:2016:2454 (*Dynamische verkeerscontrole*). Wanneer de inzet van het profiel enkel opsporing tot doel heeft en niet de verkeerscontrole, is er sprake van *détournement de pouvoir*.
35 Rechtbank Amsterdam, 3 augustus 2022, ECLI:NL:RBAMS:2022:4626 (*ANPR referentielijst*).
36 Een contra-argument is dat een profiel juist objectiever is en het probleem van de 'onderbuikgevoelens' van een vooringenomen opsporingsambtenaar oplost. Hoewel dit een positief aspect van profilering kan zijn, moeten we er daarbij wel van uit kunnen gaan dat het profiel objectief is. Is dit niet het geval, dan worden 'onderbuikgevoelens' via het profiel juist op schaal ingevoerd.
37 Dit is natuurlijk zowel een 'bug' als een 'feature'. Het idee is juist dat bepaalde personen die een bedreiging vormen voor de rechtsorde, eerder op de radar komen dan onschuldige burgers. Het probleem ontstaat wanneer de leden van de groep ten onrechte eerder op de radar komen (vals positieven) en/of wanneer de focus op de groep ervoor zorgt dat daadwerkelijke daders buiten beeld blijven (vals negatieven). Een bijkomende vraag is wat de invloed van profilering op de autonome waarneming van de politieagent is. Zo kan een (inaccuraat) profiel een bestaand onderbuikgevoel juist versterken of kan het ervoor zorgen dat de politieagent niet het eigen instinct volgt (wanneer het profiel afwijkt van het eigen oordeel).
38 Zie ook de uitspraak van het Duitse Bundesverfassungsgericht over geautomatiseerde data-analyse; BVerfG, 1 BvR 1547/19, Rn. 1-178, 16 februari 2023, ECLI:DE:BVerfG:2023:rs20230216.1bvr154719.
39 Zie gerechtshof Den Haag, 14 februari 2023, ECLI:NL:GHDHA:2023:173.
40 Zie bijvoorbeeld W. Schreurs e.a., 'Cogitas, Ergo Sum. The Role of Data Protection Law and Non-Discrimination Law in Group Profiling in the Private Sector', in M. Hildebrandt en S. Gutwirth (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Baden Baden: Springer, 2008.
41 Cf. Galič en Gellert 2021; Purtova 2018.

doi: 10.5553/BSb/266669012023004002002

het geval wanneer een model niet direct gericht is op het classificeren van personen (een profiel) maar gebruikt wordt voor het sturen van bijvoorbeeld de capaciteit van de politie. Ook dit kan (bij een verkeerde toepassing) invloed hebben op groepen en individuen, maar het is de vraag of het gegevensbeschermingsrecht dan het juiste instrument is om deze problematiek te adresseren.

Mogelijk biedt de aankomende AI Verordening in de toekomst enig soelaas, omdat daarin vereisten worden gesteld aan de representativiteit van de gegevens en de accuraatheid van geautomatiseerde beslissingen. Binnen de politie en het OM wordt verder gebruikgemaakt van het *Kwaliteitskader Big Data*, dat eisen stelt aan de accuraatheid en representativiteit van data-analyses, maar dit betreft vooralsnog een interne regeling, geen wettelijke verplichting.[42]

Het laatste punt betreft de onvoorzienbaarheid van de toepassing van profilering. Profilering is immers op verschillende wettelijke kaders gestoeld (de Politiewet, het Wetboek van Strafvordering en de Wet politiegegevens).[43] Hierdoor is het bijvoorbeeld niet altijd duidelijk of profilering onderdeel vormt van de opsporing, een opmaat vormt voor de opsporing, of dat het onder handhaving of toezicht moet worden geschaard. Omdat de grondslagen voor het gebruik over verschillende regelingen zijn verspreid, is ook de rechtsbescherming versnipperd. Daarbij komt dat deze rechtsbescherming gekoppeld is aan de uitgangspunten van het betreffende juridische kader, wat de uniformiteit en de consistentie van de rechtsbescherming niet ten goede komt. Denk bijvoorbeeld aan het toezicht: in het Wetboek van Strafvordering is er de toetsing vooraf door de officier van justitie en waar van belang de rechter-commissaris en achteraf door de zittingsrechter. In de Wet politiegegevens is het hoofdzakelijk de Autoriteit Persoonsgegevens die toezicht houdt.[44] De versnipperde regeling maakt het werk voor de politie overigens ook niet per se makkelijker. Wanneer zij bijvoorbeeld gegevens wil verzamelen met het oog op de uitvoering van de dagelijkse politietaak, of om inzicht te krijgen in criminele fenomenen, zit ze voor wat betreft de verzamelbevoegdheden al snel in de context van een strafrechtelijk onderzoek, omdat de bevoegdheden tot het verzamelen van gegevens enkel zijn beschreven in het Wetboek van Strafvordering.

4.2 *Group privacy* als richtinggevend?

Gegeven de hierboven beschreven beperkingen van het huidige juridische kader lijkt het zinvol om te kijken naar een meer 'holistische' beoordeling van de toepassing van profilering, waarbij de impact van het opstellen en toepassen van het profiel in samenhang wordt bekeken. Daarbij kan het concept *group privacy*[45] (soms ook *collective*,[46] *inferential*[47] of *predictive privacy*[48] genoemd) mogelijk een rol spelen.

Recente conceptualiseringen van *group privacy* zijn een reactie op de opkomst van Big Data en ontwikkelingen in *predictive analytics* die tot een opmerkelijke verandering hebben geleid: mensen worden door *machine learning*-technieken steeds vaker niet als individuen (Alice of Bob), maar als leden van specifieke algoritmisch samengestelde groepen benaderd. Deze ontwikkeling is ook zichtbaar in datagedreven politiewerk en profilering dat zich richt op fenomenen, groepen en de samenleving als geheel. Zoals al aangegeven zet de manier waarop dit gebeurt privacybescherming die op individuele rechten gebaseerd is onder druk. Omdat het koppelen van de classificaties of andere voorspellingen van het model aan de persoonsgegevens bij de bron (trainings- en inputdata) moeilijk is, valt het moeilijk hard te maken dat een meer dan geringe inbreuk op de privacy heeft plaatsgevonden.

De *group privacy*-wetenschap benadrukt daarbij de misvatting van de atomistische ontologie die ten grondslag ligt aan de huidige Europese wetgeving inzake gegevensbescherming: dat de bescherming van groepen vanzelf gaat als we persoonsgegevens die individuen identificeren beschermen.[49] Als zodanig is het concept van *group privacy* een oproep om de sociale en culturele conceptualisering van privacy uit te breiden met rechten die op groepsniveau worden geformuleerd. Dit moet helpen de tekortkomingen in de regelgeving die gestoeld zijn op individuele rechten aan te pakken. Hier komt ook de infrastructurele rol van privacy naar voren: privacy is niet alleen een recht in zichzelf, het is ook een belangrijke voorwaarde voor de bescherming en realisatie van andere rechten en vrijheden (bijvoorbeeld de vrijheid van vergadering en vereniging). Zonder privacy wordt het immers moeilijk om sommige andere rechten te genieten.[50] Privacy is dus een 'onderdeel van een pakket verweven grondrechten' dat niet alleen onze individuele, maar ook onze maatschappelijke en politieke

42 *Kwaliteitskader Big Data*, 2020. Via www.rijksoverheid.nl/documenten/rapporten/2020/05/29/tk-bijlage-2-kwaliteitskader-big-data; zie ook M. Galič, A. Das en M. Schuilenburg, 'Predictive policing in the Netherlands: a report on AI and administration of justice', *Revue internationale de droit penal* (forthcoming 2023).

43 L. Stevens et al., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling', *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2021, p. 234-245.

44 Voor een antwoord op de vraag waarom dit problematisch is zie: B.W. Schermer en M. Galič, 'Biedt de Wet politiegegevens een stelsel van "end-to-end" privacywaarborgen?', *Nederlands Tijdschrift voor Strafrecht*, 2022, afl. 3.

45 L. Floridi, 'Open data, data protection, and group privacy', *Philosophy & Technology*, 2014, afl. 27; Taylor, Floridi en Van der Sloot 2017; Mittelstadt 2017.

46 Mantelero 2016; A. Mantelero, 'From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era', in L. Taylor, L. Floridi en B. van der Sloot (Red.), *Group privacy: new challenges of data technologies*, Cham: Springer, 2017.

47 M. Loi en M. Christen, 'Two concepts of group privacy', *Philosophy & Technology*, 2020, afl. 33.

48 Mühlhoff 2021, 2022.

49 Floridi 2014, p. 2.

50 B.J. Koops, 'Privacy spaces', *West Virginia Law Review* 2018, afl. 121, p. 621.

emancipatie waarborgt.[51] In de context van profilering, zoals bij *predictive policing*, met het belangrijke risico van discriminerende gegevensverwerking, komt vooral het recht op gelijke behandeling in beeld. Om die reden dient de rechtsbescherming zich ook te richten op het bredere kader van de mensenrechten en zich niet te beperken tot privacy en gegevensbescherming.[52]

Wanneer deze gedachtegang wordt toegepast op het strafprocesrecht, kunnen enkele suggesties worden gedaan voor de regulering van profilering in het kader van informatiegestuurd en datagedreven politiewerk.

De eerste suggestie heeft te maken met de wijze waarop in het strafrecht de mate van inbreuk op de persoonlijke levenssfeer wordt beoordeeld. Momenteel wordt enkel gekeken hoe diep het overheidshandelen ingrijpt in de persoonlijke levenssfeer van het individu.[53] Het kan daarbij grofweg gaan om een geringe inbreuk of een meer dan geringe inbreuk.[54] Er is sprake van een meer dan geringe inbreuk wanneer er een min of meer compleet beeld wordt verkregen van bepaalde aspecten van het persoonlijk leven.[55] Maar zoals wij betogen in deze bijdrage, is dit criterium moeilijk toepasbaar in de context van profilering.

Bij een beoordeling van de zwaarte van een bevoegdheid en het effect op de persoonlijke levensfeer moet daarom niet alleen rekening worden gehouden met individuele maar ook met collectieve privacyrisico's die voortvloeien uit voorspellingen van toekomstig collectief gedrag. Dit betekent dat de beoordeling van de inmenging in de persoonlijke levenssfeer minder gericht moet zijn op het type en de omvang van de (gevoelige) gegevens met betrekking tot individuen die worden gebruikt en geproduceerd door voorspellende modellen (en die kunnen worden gebruikt om een nauwkeurig beeld van het privéleven van een individu te scheppen). Zoals aangetoond kan ook de verwerking van grote hoeveelheden niet-persoonlijke gegevens leiden tot een inbreuk op iemands privéleven, bijvoorbeeld door uit de verwerking (gevoelige) persoonsgegevens te creëren. Verder moet ook rekening worden gehouden met de verschillende soorten kennis over collectieve gedragingen en kenmerken die via de modellen kunnen worden geproduceerd – op basis van niet-persoonlijke en/of niet-gevoelige persoonlijke gegevens – en die een negatief effect kunnen hebben op bepaalde groepen. Hierbij dient ook een beoordeling van de mogelijke gerelateerde gevolgen voor het recht op gelijke behandeling gemaakt te worden. Dit maakt een uitgebreidere beoordeling van de privacyrisico's van profilering mogelijk.

In aansluiting op de eerste suggestie zou onze tweede suggestie zijn om een specifieke rechtsgrondslag voor profilering vast te stellen, bij voorkeur in het Wetboek van Strafvordering zelf.[56] Een alternatief is om de bevoegdheid op te nemen in de Politiewet, mits met voldoende waarborgen omkleed, zodat de toepassing in de context van de handhaving van de openbare orde ook gereguleerd wordt. Toch betogen wij dat profilering gewoonlijk tot een meer dan geringe inbreuk op het recht op privacy leidt, vooral wanneer rekening wordt gehouden met de impact op groepen. Dit zou de opname in het Wetboek van Strafvordering rechtvaardigen, zelfs in gevallen waarin profilering niet zou worden gebruikt voor opsporing in enge zin.[57] Dat profilering een groot risico inhoudt voor de rechten op privacy en de bescherming van persoonsgegevens, komt voort niet alleen uit theoretische overwegingen in verband met het begrip *group privacy*, maar ook uit de redenering van het Duitse Bundesverfassungsgericht in een recente zaak betreffende geautomatiseerde data-analyse.[58] Hoewel het Bundesverfassungsgericht vasthield aan de individuele benadering van het recht op privacy, was het Duitse hof toch van oordeel dat geautomatiseerde data-analyse die profilering mogelijk maakt, een groot risico inhoudt voor het recht op informationele zelfbeschikking (de Duitse opvatting van het recht op privacy) wat een concrete en specifieke wettelijke basis vereist. Een belangrijke overweging van het Bundesverfassungsgericht heeft te maken met de vraag hoe 'open' de gegevensanalyse met het oog op preventie is. Hoe meer deze open is (bijvoorbeeld als het doel is statistische anomalieën in de gegevensverzameling te ontdekken of de analyse niet is gericht op personen die nader kunnen worden omschreven en er geen feitelijk verband bestaat tussen het bedreigde rechtsbelang en de door de geautomatiseerde analyse getroffen personen), hoe groter de inbreuk op de persoonlijke levenssfeer is.[59] Dit verhoogt immers het risico dat personen die niets hebben gedaan om de aandacht van de politie te trekken, onder verder toezicht zullen komen. Het risico werd nog groter geacht naarmate de gebruikte modellen complexer zijn en gevoeliger voor fouten en discriminatie.[60] Als zodanig werden de vrij algemene rechtsgrondslagen voor geautomatiseerde

51 S. Gutwirth, *Privacy and the information age*, Lanham: Rowman & Littlefield, 2002, p. 45.

52 A. Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', *Computer Law & Security Review*, 2018, jg. 34, afl. 4, p. 754-772.

53 Zie voor een uitgebreide toelichting: Europees Hof voor de Rechten van de Mens, *Guide on Article 8, of the European Convention on Human Rights, Right to respect for private and family life, home and correspondence*, augustus 2022.

54 In het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (Boek 8) is naar aanleiding van het Smartphone-arrest en de adviezen van de commissie-Koops gekozen voor een drieledig criterium. Bij onderzoek kan er sprake zijn van: een beperkte inbreuk op de persoonlijke levenssfeer (niet-stelselmatig onderzoek), een min of meer compleet beeld van bepaalde aspecten van iemands privéleven (stelselmatig onderzoek) en een ingrijpend beeld van iemands privéleven (ingrijpend stelselmatig onderzoek). Zie: Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, Memorie van Toelichting, p. 264 (versie Raad van State).

55 HR 4 april 2017, ECLI:NL:HR:2017:592 (*Smartphone-arrest*).

56 Cf. Stevens e.a. 2021.

57 Ibid.

58 BVerfG, 1 BvR 1547/19, Rn. 1-178, 16 februari 2023, ECLI:DE:BVerfG:2023:rs20230216.1bvr154719.

59 Ibid., para. 93-5.

60 Ibid., para. 90-3.

doi: 10.5553/BSb/266669012023004002002

gegevensanalyse in de Duitse deelstaten van Hesse en Hamburg ontoereikend en ongrondwettelijk verklaard.

Een derde suggestie is het uitbreiden van de rechtsbescherming van individuen en groepen door de introductie van een recht op een 'redelijke gevolgtrekking' (*reasonable inferences*).[61] Dit door Wachter en Mittelstadt ontwikkelde concept behelst een plicht voor de gebruiker van het profiel om aan te tonen:

1. dat het ethisch/normatief verantwoord is om op basis van bepaalde gegevens aannames te doen over groepen en individuen;
2. waarom het ethisch/normatief verantwoord en relevant is om deze aannames te gebruiken voor (geautomatiseerde) besluitvorming;
3. dat de gegevens en de methoden gebruikt om deze aannames te doen accuraat en statistisch relevant en betrouwbaar zijn.[62]

Dit recht zou het probleem dat de rechtsbescherming pas aangrijpt als een identificeerbare persoon wordt geraakt, adresseren.[63] Een recht op redelijke gevolgtrekking zou de politie niet alleen dwingen om verantwoording af te leggen over haar gebruik van profilering, maar het individu (en mogelijk groepen) het recht geven om zich te beroepen op dit recht op redelijke gevolgtrekking.

5. Conclusie

Om de openbare orde effectief te handhaven en criminaliteit te bestrijden wordt het werk van de politie steeds meer 'datagedreven'. *Machine learning*-modellen spelen een belangrijke rol in deze ontwikkeling.

Hoewel datagedreven werken een belangrijke bijdrage kan leveren aan de efficiëntie en effectiviteit van de politie, is datagedreven werken niet zonder risico's. Met name profilering kan een (onevenredige) inbreuk op de persoonlijke levenssfeer vormen, tot discriminatie leiden, *chilling effects* hebben en de onschuldpresumptie onder druk zetten.

Het Wetboek van Strafvordering en de Wet politiegegevens moeten het hoofd bieden aan deze bedreigingen voor het individu en de samenleving, maar deze kaders zijn naar onze mening daar niet toe uitgerust. Niet alleen is de wettelijke bescherming versnipperd, zij grijpt ook pas aan wanneer een identificeerbare persoon in beeld komt. Dit terwijl risico's zoals discriminatie en *chilling effects* al kunnen ontstaan voordat het profiel op een individueel niveau wordt toegepast. Zelfs al is sprake van een identificeerbare persoon, dan nog ligt de nadruk momenteel op het beoordelen van de inbreuk die wordt gemaakt door het matchen van de persoon met het profiel. Omdat die handeling doorgaans niet heel inbreukmakend is (omdat voor de koppeling vaak niet heel gevoelige gegevens nodig zijn), kan worden volstaan met algemene grondslagen zoals de uitvoering van de politietaak (art. 3 Politiewet), die weinig houvast en concrete waarborgen bieden.

Informatiegestuurd en datagedreven politiewerk in het algemeen en profilering in het bijzonder dwingen ons dus tot een omslag in het denken over het beschermen van grondrechten in de context van handhaving en opsporing. De vanuit het individu ingestoken rechtsbescherming is niet alleen versnipperd over diverse regelingen, maar zorgt er ook voor dat de rechtsbescherming mogelijk te laat of in het geheel niet aangrijpt. Hierdoor ontstaan niet alleen risico's voor het individu wanneer een match met het profiel aanleiding geeft tot (strafvorderlijke) beslissingen, maar ook voor groepen en de samenleving als geheel.

Het verdient naar onze mening aanbeveling om profilering te beschouwen als een handhavings- en opsporingsmethode en te kijken naar de gehele impact van deze methode (en dus niet enkel te kijken naar de impact op het individu in een concreet geval). Mogelijke eerste suggesties voor een meer 'holistische' benadering van de regulering van profilering zijn een bredere interpretatie van het recht op privacy (*group privacy*), het vormgeven van profilering als een specifieke (opsporings)bevoeghdheid en/of het formuleren van een recht op 'redelijke gevolgtrekking' (*reasonable inferences*).

61 S. Wachter en B. Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review*, 2019, afl. 2.

62 Ibid.

63 Hoewel de AI Verordening naar alle waarschijnlijkheid punt 3 gaat adresseren, is er momenteel geen 'harde' juridische plicht om de punten 1 en 2 te onderbouwen. Instrumenten zoals de gegevensbeschermingseffectbeoordeling (*data protection impact assessment*) uit art. 5c Wpg en de recent geïntroduceerde Impact Assessment Mensenrechten en Algoritmen (IAMA) dragen wel bij aan het beantwoorden van de vragen 1 en 2, maar zij bieden individuen en groepen geen afdwingbaar recht.

doi: 10.5553/BSb/266669012023004002002