Artikel

Strafvorderlijke normering van preventief optreden op basis van datakoppeling

Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond'

Prof. mr. L. Stevens, prof. mr. M. Hirsch Ballin, mr. dr. M. Galič, mr. dr. S.S. Buisman, mr. B. Groothoff, mr. Y. Hamelzky, mr. C. Lucas, mr. K. Rasul en mr. S. Verijdt*

1. Inleiding

De vraag die wij in deze bijdrage stellen – hoe moet preventief politieoptreden op grond van datakoppeling worden genormeerd? – komt voort uit het door de politie opgezette 'Sensingproject Outlet Roermond'. Het project beoogt 'mobiel banditisme' in het bij het winkelend publiek populaire Outletcentrum in Roermond te voorkómen.[1] Mobiel banditisme is geen scherpomlijnd begrip, maar lijkt in de kern te gaan om internationaal rondtrekkende criminele groepen – veelal uit Oost-Europa en kennelijk binnen de context van het Sensingproject Roermond in het bijzonder uit Roemenië[2] – die zich schuldig maken aan zakkenrollen, winkeldiefstal en woninginbraken. In het Roermondse project worden op basis van datakoppeling risicoanalyses gemaakt van auto's die in de buurt van de Outlet rijden – en die dus vermoedelijk 'mobiele bandieten' bevatten. Levert een risicoanalyse over een bepaalde auto een zeker puntenaantal op, dan is dat een 'hit' en wordt een surveillancewagen op de auto afgestuurd.

In een rapport uit 2020 heeft Amnesty International vanuit mensenrechtelijk perspectief kritiek geleverd op het Sensingproject Roermond. Die kritiek houdt kort gezegd in dat de wijze waarop de data worden gebruikt discriminerend is, dat met het gebruik van de data inbreuk wordt gemaakt op het recht op privacy en het recht op databescherming (verwante, maar afzonderlijke rechten) van grote groepen mensen zonder dat daarvoor een afdoende wettelijke grondslag voorhanden is, en dat (mede daardoor) onafhankelijk toezicht en afbakening van de inbreuk ontbreken.[3] Een belangrijk kritiekpunt is bovendien dat een dergelijke vorm van massasurveillance betekent dat elke burger wordt gezien als potentiële

* Prof. mr. L. Stevens is hoogleraar straf(proces)recht aan de Vrije Universiteit Amsterdam. Prof. mr. M. Hirsch Ballin is hoogleraar straf(proces)recht aan de Vrije Universiteit Amsterdam. Mr. dr. M. Galič is universitair docent straf(proces)recht aan de Vrije Universiteit Amsterdam. Mr. dr. S.S. Buisman is universitair docent straf(proces)recht aan de Vrije Universiteit Amsterdam. Mr. B. Groothoff is docent/onderzoeker aan de Vrije Universiteit Amsterdam. Mr. Y. Hamelzky is docent aan de Vrije Universiteit Amsterdam. Mr. C. Lucas is PhD-onderzoeker aan de Vrije Universiteit Amsterdam. Mr. K. Rasul is docent aan de Vrije Universiteit Amsterdam. Mr. S. Verijdt is docent aan de Vrije Universiteit Amsterdam.

1. Via een besluit op een Wob-verzoek zijn diverse politiedocumenten over de 'Proeftuin Roermond' openbaar geworden. Ze zijn alle te vinden via de website www.politie.nl/wob/korpsstaf/2019-programma-mobiel-banditisme-%E2%80%93-proeftuin-roermond.html. Over doel en aanpak is bijvoorbeeld te lezen in de brief van de burgemeester aan de korpschef, document (003) op de website.

2. In de berichtgeving van de NOS worden Roemenen als specifieke groep genoemd. Zie https://nos.nl/artikel/2250767-politie-wil-zakkenrollers-en-plofkrakers-vangen-met-data.html. In de juridische documenten van de politie worden Roemenen niet expliciet als direct doel genoemd, maar duidelijk wordt wel dat Roemenen worden gezien als belangrijke probleemgroep (naast overigens ook Bulgaren). Zie bijvoorbeeld document (002), 'Mobiele bendes aan het roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond'.

3. Rapport Amnesty International, 'We sense trouble, Automated discrimination and mass surveillance in predictive policing in the Netherlands', Amnesty International 2020, te vinden via amnesty.org.

doi: 10.5553/TBSenH/229567002021007004002

verdachte.[4] Het rapport van Amnesty International laat zien dat niet te gemakkelijk moet worden gedacht over het inzetten van een Sensingproject zoals dat in Roermond. Tegelijkertijd denken wij niet dat het voldoende is om te stellen dat we dan maar niet moeten beginnen aan projecten waarbij gebruikt wordt gemaakt van datakoppeling en risicoanalyses ter voorkoming van criminaliteit. Hoewel het Roermondse project inmiddels (voorlopig) is stopgezet,[5] biedt deze vorm van optreden interessante mogelijkheden voor de politie. De geschiedenis leert bovendien dat politiemethoden die eenmaal hun intrede hebben gedaan ondanks oproepen om er niet aan te beginnen of om ermee te stoppen, niet de neiging hebben weer te verdwijnen. Daar komt bij dat de inzet van politie en justitie juist ook steeds meer is gericht op het voorkómen van criminaliteit,[6] in plaats van dat wordt gereageerd op gepleegde strafbare feiten. De samenleving vraagt daar ook om, en de technologie biedt steeds weer nieuwe mogelijkheden.

Kortom, vanuit de gedachte dat preventief politieoptreden eerder een groter dan een kleiner aandeel van het politiewerk zal gaan beslaan, en vanuit de veronderstelling dat preventief politieoptreden met behulp van technologie ondergenormeerd is, werpen wij de vraag op hoe projecten zoals in Roermond gereguleerd zouden moeten worden. Die vraag stellen wij niet alleen opdat privacy en andere mensenrechten worden gewaarborgd, maar ook opdat dergelijk preventief politieoptreden de aansluiting vindt bij strafvorderlijke principes inzake de normering van opsporing. Het is namelijk onze overtuiging dat we hier te maken hebben met een nieuwe vorm van opsporing die veel meer strafvorderlijke aandacht verdient dan hij nu krijgt. Ter beantwoording van de reguleringsvraag analyseren wij allereerst de huidige grondslag van het Sensingproject Roermond en de tekortkomingen die wij daarbij zien (paragraaf 2). In paragraaf 3 gaan wij – mede in het licht van de analyse uit paragraaf 2 – dieper in op het recht op privacy. Vervolgens richten wij ons op de vraag of preventief optreden naar aanleiding van datakoppeling als opsporing moet worden gezien en welke consequenties dat heeft voor de regulering (paragraaf 4). Wij sluiten af met een beschouwing over de contouren van regulering van preventief politieoptreden op grond van datakoppeling.

In deze inleiding is ten slotte een belangrijke disclaimer op zijn plaats. Primaire of officiële bronnen over het Sensingproject zijn zeer beperkt beschikbaar en wij hebben de voor onze analyse relevante informatie voornamelijk bij elkaar gesprokkeld op basis van, en met behulp van secundaire bronnen.[7] Dat betekent dat het vrij zeker is dat we lang niet alles weten over het project, en dat er bovendien een kans bestaat dat dingen die wij denken te weten niet helemaal kloppen. Wij hebben geprobeerd die onzekerheden zoveel mogelijk duidelijk te maken in de tekst.

2. Waarom bestaande wettelijke bepalingen niet voldoen als grondslag voor het handelen in het Sensingproject

2.1 Om welke handelingen gaat het?

De data die in de Roermondse casus worden gebruikt, worden deels verkregen via Sensing-methoden. *Sensing* wordt door de politie gedefinieerd als 'het waarnemen of verzamelen van informatie met betrekking tot een object of persoon met een technisch hulpmiddel (de sensor)'.[8] De ANPR-camera (*automatic number plate recognition*), die automatisch kentekens en de route van auto's kan registreren, is een bekend voorbeeld van zo'n sensor. Welke sensoren in Roermond precies zijn gebruikt is niet met volledige zekerheid vast te stellen. Blijkens het door een Wob-verzoek 'vrijgegeven' plan van aanpak van het Sensingproject in Roermond, kunnen meerdere sensoren worden ingezet.[9] Bij de aankondiging van het project in de media worden naast ANPR-camera's bovendien sensoren genoemd die zouden kunnen meten hoeveel personen er in een auto zitten en welke telefoons ze op zak hebben.[10] Uiteindelijk lijkt echter 'alleen' gebruik te zijn gemaakt van ANPR-camera's en merk-model-kleurherkenningscamera's.[11] Wat dus door de sensoren lijkt te worden waargenomen, of beter 'geregis-

4. Zie bijvoorbeeld Marc Schuilenburg in een interview over het project www.amnesty.nl/wordt-vervolgd/criminaliteit-voorspellen-roermond-politie. Zie ook A. Das & M. Schuilenburg, 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht, *Strafblad* 2018, p. 21-22.
5. www.limburger.nl/cnt/dmf20201013_95388160.
6. Zie ook M.F.H. Hirsch Ballin, *Over grenzen bij bewijsvergaring* (oratie Amsterdam VU), Den Haag: Boom juridisch 2018, p. 27.
7. Een belangrijke vermelding krijgt daarbij de scriptie van Vera Prins van de Universiteit Utrecht. Op basis van het onderzoek van Prins (o.a. interviews) kregen wij een duidelijker beeld van wat er gebeurde en ook vormde haar scriptie een ontsluiting voor andere, niet makkelijk te vinden bronnen. Zie V.E. Prins, *Sensoren, risicoscores en mensenrechten. Een onderzoek naar de mensenrechtenimplicaties van het predictive-policingproject Sensing Mobiel Banditisme in Roermond*, scriptie Legal Research Master UU 2020, te vinden via www.uu.nl/sites/default/files/rebo-scriptie-Vera-Prins-Sensoren%2C%20risicoscores%20en%20mensenrechten%20%282020%29.pdf.
8. *Kamerstukken II* 2015/16, 29628, nr. 594, bijlage 626926 (visie op Sensing van de politie), p. 5; *Kamerstukken II* 2015/16, 29628, nr. 594, p. 2.
9. Politiedocument (045) 'Plan van aanpak Operationele Proef Tuin Sensing Roermond' van 12 oktober 2017, p. 8.
10. NOS 2018, 'Politie wil zakkenrollers en plofkrakers vangen met data', NOS 17 september 2018, www.nos.nl/artikel/2250767-politie-wil-zakkenrollers-en-plofkrakers-vangen-met-data.
11. Merk-model-kleurherkenningscamera's bevatten software die het merk, model en de kleur van de auto kunnen registreren; Prins 2020, p. 34-35. Naar ons idee gaat het hier om ANPR-camera's met een merkmodel-kleurherkenningssoftware, vgl. G. Homburg e.a., *ANPR: toepassingen en ontwikkelingen* (WODC-rapport), Amsterdam: Regioplan beleidsonderzoek 2016, p. 14.

treerd',[12] zijn het kenteken van een auto, het type en de kleur van een auto, en de route van een auto.[13]

De geregistreerde data (die dus in samenhang een bepaald beeld of profiel van de auto opleveren) worden door de sensoren verwerkt en tegelijkertijd gekoppeld aan een door de politie opgesteld risicoprofiel voor mobiel banditisme. Hoe dat profiel in de praktijk precies eruit heeft gezien blijft onduidelijk. Duidelijk is wel dat op enig moment de volgende zes regels (mede) het profiel bepaalden:[14]

- Mobiele bandieten rijden met meerdere passagiers in een auto.
- Mobiele bandieten rijden vaak in een witte, Duitse huurauto van drie tot vijf jaar oud. Het betreft vaak een niet te groot model.
- Mobiele bandieten rijden mogelijk in een auto met een kenteken van een bepaalde herkomst.[15]
- Mobiele bandieten rijden mogelijk in een auto die eerder gesignaleerd is in het kader van criminaliteit en/of een gestolen auto en/of een auto met een vals kenteken.
- Mobiele bandieten volgen een bepaald traject.
- Mobiele bandieten rijden op bepaalde tijdstippen.

Hoewel, zoals gezegd, niet helemaal duidelijk wordt welke regels van het risicoprofiel nu daadwerkelijk zijn ingezet en evenmin hoe dat is gebeurd (zijn bijvoorbeeld gegevens van Duitse autoverhuurbedrijven als referentiebestand gebruikt?), is wel duidelijk dat wordt beoogd dat de door de sensoren geregistreerde data inzake de auto zowel aan elkaar worden gekoppeld als aan diverse andere, elders reeds opgeslagen data over die auto (bij de politie, bij de RDW, maar in theorie ook bij private partijen).[16] De gecombineerde data kunnen een 'hit' opleveren als een bepaalde combinatie een bepaald aantal punten behaalt. Aan elke regel van het profiel is een hoeveelheid punten toegekend; voor ons is onduidelijk welke regel hoeveel punten kent. Is er een hit, dan wordt deze gepresenteerd bij de meldkamer van de politie in de regio en aldaar door politiemedewerkers geverifieerd (ook camera's maken fouten). Daarop wordt een 'inzetopdracht' gegeven aan agenten van het basisteam Roermond. Zij hebben een discretionaire bevoegdheid om te bepalen of en hoe wordt geïntervenieerd. Daarbij kan ook worden gedacht aan het waarschuwen van de beveiligers van de outlet, maar naar verwachting zal het in de meeste gevallen om een staandehouding gaan.[17]

2.2 Welke grondslagen en waarom passen die niet?

Voor het handelen zoals in het Sensingproject Roermond bestaat geen specifieke wettelijke grondslag. Volgens de politie moet de grondslag echter worden gevonden in artikel 3 Politiewet 2012 (hierna: Pw) dat de algemene politietaak beschrijft, en artikel 8 Wet Politiegegevens (hierna: Wpg) dat ziet op het verwerken van politiegegevens (die te herleiden zijn tot persoonsgegevens) met het oog op het uitvoeren van de dagelijkse politietaak.[18] Dat de politie naar deze algemene bepalingen grijpt, is op het eerste gezicht wel te begrijpen. In een specifieke grondslag voorziet de wet (Sv, Pw of Wpg) niet en het gaat om een koppeling van gegevens waarvan de vergaring op zichzelf niet als een vergaande ingreep in de persoonlijke levenssfeer wordt beschouwd. Een wat nadere blik maakt echter duidelijk dat het wringt bij beide grondslagen.

Voor wat betreft artikel 3 Pw geldt dat volgens vaste rechtspraak deze bepaling de grondslag kan vormen van niet expliciet geregelde opsporingsmethoden zolang die niet meer dan een geringe inbreuk maken op grondrechten van burgers.[19] Diverse 'nieuwe' opsporingsmethoden kunnen volgens die rechtspraak op artikel 3 Pw worden gebaseerd, zoals een warmtebeeldcamera (om te zien of een huis veel warmte uitstraalt, hetgeen kan wijzen op een hennepplantage), een IMSI-catcher of een stille sms (om de locatie van een verdachte te bepalen door middel van zijn telefoon).[20] In het Sensingproject stelt de politie op basis van deze rechtspraak dat de digitale waarnemingen van de sensoren slechts een geringe inbreuk maken op de persoonlijke levenssfeer (in de zin van bewegingsvrijheid) en dat aldus artikel 3 Pw volstaat als wettelijke grondslag. Hoewel een vergelijking met opsporingsmethoden zoals de warmtebeeldcamera en de IMSI-catcher te begrijpen is, gaat het hier echter om twee redenen mis.

In de eerste plaats is deze benadering van artikel 3 Pw als grondslag gebaseerd op het uitgangspunt dat het (normeren van het) *vergaren* van gegevens en het *verwerken* van gegevens gescheiden kan worden. Dat vergaren gebeurt in de context van de opsporing traditiegetrouw op basis van het Wetboek van Strafvordering en de Pw. Het verwerken vindt plaats op basis van de Wet politie-

12. Zie verder over deze terminologie paragraaf 2.2.
13. Uit het scriptieonderzoek van Prins, waarin interviews met de politie zijn afgenomen, komt naar voren welke inspanningen zijn verricht om andere, meer gecompliceerde sensoren mogelijk te kunnen maken en waarom dat (nog) niet lukte. Zie Prins 2020, p. 35-36.
14. Ontleend aan het onderzoek van Prins 2020, p. 36-38.
15. Het onderzoek van Prins laat zien dat niet helemaal duidelijk wordt welke waarde de politie hier hecht aan een Roemeens of ander Oost-Europees kenteken. Ook Duitse kentekens lijken relevant, maar leveren weer te veel matches op. Begin 2020 zijn er signalen dat ook Spaanse en Franse kentekens gebruikt worden voor mobiel banditisme. Prins 2020, p. 37.
16. Dit laatste suggereert althans de regel waarin wordt gesproken van huurauto's. Wij weten niet of die regel daadwerkelijk is gebruikt en waar die data dan vandaan zouden zijn gehaald.
17. De beschrijving van deze werkwijze hebben wij ontleend aan Prins 2020, p. 39-43. Zij heeft interviews met betrokken politiemedewerkers gehouden.
18. Zie Politiedocument (068) 'Juridische paragraaf OPT' van 23 april 2018. In een ander politiedocument (083) 'Nota Rechtmatigheid OPT en GPV' van 15 augustus 2018 is een tabel te vinden waarin de relevante bepalingen zijn gekoppeld aan te onderscheiden handelingen. Wij moeten na meerdere pogingen constateren dat wij deze tabel niet goed doorgronden.
19. Zie bijv. HR 1 juli 2014, ECLI:NL:HR:2014:1569 en HR 18 april 2017, ECLI:NL:HR:2017:725.
20. HR 9 december 2014, ECLI:NL:HR:2014:3537, HR 1 juli 2014, ECLI:NL:HR:2014:1562 en HR 1 juli 2014, ECLI:NL:HR:2014:1569.

doi: 10.5553/TBSenH/229567002021007004002

gegevens. Deze benadering miskent echter wat in het Sensingproject daadwerkelijk gebeurt. Het gaat in het project immers niet om het doen van een enkele digitale waarneming van een individu op de openbare weg. Het betreft het voortdurend combineren en verrijken van data – opdat deze vervolgens een startpunt voor preventief politieoptreden kunnen zijn. Aldus gaan vergaren en verwerken hand in hand en kunnen zij niet – niet in de praktijk en daarmee ook niet in de normering van die praktijk – van elkaar worden gescheiden. In die zin zou ook niet van 'waarneming' moeten worden gesproken maar eerder van 'registratie'.[21] De term waarneming (of in strafvorderlijke terminologie: observatie) impliceert dat wat de camera's doen vergelijkbaar is met een menselijke waarneming in de publieke ruimte. Wat de camera's echter doen – waarnemen, combineren en verrijken van data; op grote snelheid en in (potentieel) grote hoeveelheden – kunnen mensen niet. Het is vele malen gecompliceerder en verstrekkender. Kortom, het vinden van een grondslag in artikel 3 Pw gaat samen met een te beperkte voorstelling van zaken, die mede wordt ingegeven door de bestaande scheiding in de normering van vergaren en verwerken.

In de tweede plaats gaat een benadering waarin artikel 3 Pw als grondslag wordt genomen uit van een klassiek privacyconcept en dat wringt in deze casus. Privacyregelgeving gaat immers traditiegetrouw uit van de bescherming van het individu, ook artikel 3 Pw veronderstelt het 'geïdentificeerde individu' als de te beschermen entiteit. In het Sensingproject is daarentegen een groot deel van de handelingen niet gericht op het individu, maar op het selecteren van *groepen* personen (namelijk bepaalde weggebruikers). Het punt is juist dat bij een dataverzameling en -verwerking als in het Roermondse project individuen niet als individu worden geselecteerd, maar als onderdeel van een groep en dat dus de privacy niet enkel kan worden gewaarborgd door bepalingen die uitgaan van de bescherming van het individu.

Vergelijkbare problematiek doet zich voor ten aanzien van het eveneens als grondslag genoemde artikel 8 Wpg. Deze bepaling ziet op het verwerken van politiegegevens (die te herleiden zijn tot persoonsgegevens) met het oog op het uitvoeren van de dagelijkse politietaak.[22] De uitvoering van de dagelijkse politietaak wordt wel de oog- en oorfunctie, of het basispolitiewerk van de politie genoemd. Het werk omvat surveillance (in de zin van menselijk toezicht; geen surveillance met behulp van geavanceerde technologie), afhandeling van de verkeersproblematiek, eenvoudige opsporingsonderzoeken, hulpverlening en handhaving van wetten en regels.[23] Bij het verwerken van gegevens op basis van artikel 8 Wpg kan bijvoorbeeld worden gedacht aan een politieagent die een auto die hij net voor een verkeerscontrole heeft staande gehouden, laat natrekken in de politiesystemen.

Ten aanzien van het Sensingproject kan moeilijk worden volgehouden dat de gegevens worden verwerkt met het oog op de dagelijkse politietaak zoals hierboven omschreven. Ook dat is een te eenvoudige voorstelling van zaken die de aard van het project miskent. Het doel van het project in Roermond is immers veel gerichter dan het houden van menselijk toezicht en het uitvoeren van eenvoudige opsporingshandelingen zoals ze zich aandienen op straat: het gaat om het gericht opsporen en voorkómen van mobiel banditisme. Daarbij komt dat het middel, wij noemden het al in relatie tot artikel 3 Pw, verstrekkender is dan de menselijke waarneming van een agent én dat hier niet de bescherming van individuele privacy het probleem is. Op de situatie in het Sensingproject is artikel 8 Wpg kortom helemaal niet toegesneden. Dat geldt overigens ook voor de andere bepalingen van de Wpg. De wet kent in de artikelen 9, 10 en 11 meer specifieke regelgeving inzake verwerking van gegevens naar aanleiding van een concreet geval of in relatie tot bepaalde personen. Maar, het Sensingproject richt zich in hoofdzaak niet op een concreet geval of een bepaald persoon en ook die bepalingen gaan dus over andere situaties dan die in Roermond.[24]

3. Hoe moet het recht op privacy bij preventief optreden op grond van datakoppeling worden gewaarborgd?

3.1 Inleiding

In de voorgaande paragraaf hebben we uiteengezet waarom de bestaande wettelijke grondslagen voor het Sensingproject niet zijn toegesneden op de privacyproblematiek die in dat project speelt. In het licht van de vraag naar de regulering moet dan ook worden nagedacht over hoe privacy in dergelijke projecten wel goed kan worden gewaarborgd. In deze paragraaf gaan wij daarom dieper in op het recht op privacy. Allereerst kijken we daartoe naar artikel 8 EVRM en hoe en in hoeverre dit recht waarborgen biedt voor preventief optreden op grond van datakoppeling (paragraaf 3.2). Vervolgens gaan we in paragraaf 3.3 nader in op de

21. Als vertaling van het Engelse 'capture'.
22. In Politiedocument (068) 'Juridische paragraaf OPT' van 23 april 2018 spreekt de politie alleen over ANPR-gegevens in relatie tot artikel 8 Wpg. Dat suggereert dat andere data niet worden gezien als persoonsgegevens en dus geen beperkingen kennen wat betreft verwerking. In een ander politiedocument (083) 'Nota Rechtmatigheid OPT en GPV' van 15 augustus 2018 worden de door de politie verzamelde data niet gespecificeerd of beperkt maar wordt wel een onderscheid gemaakt tussen waarnemingen in het publieke domein door de politie en 'private sensoren'. Voor verwerking van die laatste geldt de Algemene Verordening Gegevensbescherming (AVG). Zie p. 2.
23. *Tekst & Commentaar Openbare Orde en Veiligheid*, aantekening 2 bij artikel 8 Wpg.
24. In het politiedocument (083) 'Nota Rechtmatigheid OPT en GPV' van 15 augustus 2018 wordt wel gerefereerd aan de mogelijkheid dat zich situaties als in artikel 9 en 10 Wpg voordoen.

doi: 10.5553/TBSenH/229567002021007004002

reeds in paragraaf 2.2 gesignaleerde spanning tussen bescherming van mensen in risicogroepen en het traditionele, op het individu gerichte concept van privacy. Ten slotte bespreken we welke waarborgen kunnen worden afgeleid uit het recht op bescherming van persoonsgegevens (paragraaf 3.4).

3.2 De rechtspraak inzake artikel 8 EVRM

Er bestaat geen EHRM-jurisprudentie die specifiek betrekking heeft op preventief optreden op basis van datakoppeling. Jurisprudentie over *surveillance* en het gebruik van (digitale) technologieën door de politie is er echter wel. Deze rechtspraak kan waardevolle inzichten bieden over de grenzen van preventief optreden in het licht van artikel 8 EVRM.

De eerste vraag is of, en zo ja in welke gevallen, preventief optreden in strijd is met het recht op bescherming van de persoonlijke levenssfeer. Het EHRM legt dit recht ruim uit en voor deze casus is van belang dat het begrip persoonlijke levenssfeer de bescherming omvat van gegevens die betrekking hebben op iemands privéleven ('privégegevens'). Onder privégegevens kunnen ook gegevens vallen die worden verzameld in de openbare ruimte (of het publieke domein in het algemeen), zonder dat daarvoor indringende of geheime methoden worden gebruikt.[25] Een belangrijke factor in de toets van het EHRM is voorts wat er met de privégegevens wordt gedaan. Van een inbreuk is al snel sprake als privégegevens van een individu worden vastgelegd, opgeslagen of op een andere manier worden verwerkt (bijvoorbeeld via datakoppeling).[26] Zo kan het vastleggen van de bewegingen van een persoon in het centrum van een stad – zonder dat dit individu op andere wijze werd gehinderd – al tot een inbreuk op het privéleven leiden.[27]

Als sprake is van een inbreuk, is vervolgens de vraag of deze gerechtvaardigd is. In dat verband moet er niet alleen een legitiem belang zijn voor de inbreuk, maar dient er ook een wettelijke basis te zijn die aan bepaalde kwaliteitseisen voldoet. Achtergrond daarvoor is dat de wettelijke basis voor preventief optreden een waarborg moet bieden tegen willekeurig (overheids)optreden. Dat betekent dat de wet voldoende duidelijke toepassingsvoorwaarden moet bevatten.[28] Zo biedt bijvoorbeeld een 'stop-and-search-bevoegdheid', die inhoudt dat een politieagent een voetganger kan staande houden en fouilleren indien hij 'deze actie opportuun acht ter preventie van terrorisme', onvoldoende bescherming tegen willekeurige inmenging in het privéleven.[29] Een soortgelijke lijn van beoordeling kan worden gevonden in *mass surveillance*-zaken van het EHRM, waar brede en ongedifferentieerde *surveillance*-bevoegdheden niet in overeenstemming met de wet werden geacht.[30] Deze rechtspraak lijkt kortom erop te wijzen dat een zeer algemene wettelijke grondslag voor preventief politieoptreden zonder concrete toepassingsvoorwaarden (bijvoorbeeld een (bepaald) verdenkingscriterium), niet voldoet aan de vereisten voor een gerechtvaardigde inbreuk op het recht op privacy zoals neergelegd in artikel 8 EVRM.

Uit het voorgaande kan worden afgeleid dat het EHRM bij de beantwoording van de vraag naar de inbreuk op artikel 8 EVRM in de eerste plaats geen hoge lat plaatst bij het bepalen van wat privégegevens zijn. In de tweede plaats is interessant dat het Hof niet alleen het vergaren maar ook (juist) het (verder) verwerken van data – in Nederland gescheiden normeringssystemen[31] – bepalend laat zijn bij de vraag naar de inbreuk. Dit alles suggereert dat een wettelijke grondslag voor preventief optreden op basis van datakoppeling moet voldoen aan de eisen van artikel 8 EVRM en dus voldoende specifiek moet zijn. Het punt is echter dat de waarborgen die voortvloeien uit artikel 8 EVRM eerst dan van toepassing zijn als het gaat om privégegevens die betrekking hebben op een *individu*.[32] In het Sensingproject wordt echter pas een individu *geïdentificeerd* als iemand die in een risico-auto zit wordt staande gehouden. Voordien hebben de meeste van de gebruikte gegevens – de kleur van de auto, de route van de auto – niet direct betrekking op een individu. Ook bij het EHRM is aldus sprake van een op het individu gericht privacybegrip, zoals we ook in paragraaf 2.2 opmerkten ten aanzien van artikel 3 Pw en artikel 8 Wpg. Preventief optreden in het Sensingproject is echter gericht op het lokaliseren van een risicogroep die door algoritmen wordt gecreëerd en in eerste instantie niet op het individu. Op de vraag waarom dat individu als onderdeel van een groep wel beschermd zou moeten worden gaan we in de volgende

25. Zie bijv. EHRM [2001], app. no. 44787/98 (*P.G. en J.H. t. VK*); EHRM [2003], app. no. 44647/98 (*Peck t. VK*); EHRM [2004], app. no. 59320/00 (*Von Hannover t. Duitsland*); EHRM [2016], app. no. 61838/10 (*Vukota-Bojić t. Zwitserland*).
26. Zie bijv. EHRM [2000], app. no. 27798/95 (*Amman t. Zwitserland*); EHRM [2000], app. no. 28341/95 (Rotaru t. Roemenië); EHRM [1987], app. no. 9248/81 (*Leander t. Zweden*); P.G. en J.H. t. VK. Voor een nadere analyse van artikel 8 in de context van surveillance in de openbare ruimte zie M. Galič, *Surveillance and privacy in smart cities and living labs: conceptualising privacy for public space* (diss. Tilburg), Rotterdam: Optima Grafische Communicatie 2019, p. 268-322 te vinden via https://research.tilburguniversity.edu/en/publications/surveillance-and-privacy-in-smart-cities-and-living-labs-conceptu.
27. Vukota-Bojić t. Zwitserland.
28. Zie bijv. P.G. en J.H. t. VK; EHRM [2010], app. no. 4158/05 (*Gillan en Quinton t. VK*); EHRM [2008], app. no. 58243/00 (*Liberty en anderen t. VK*).
29. Gillan en Quinton t. VK, par. 80-87. Bovendien erkende het Hof in Gillan en Quinton de risico's van discriminerend gebruik van dergelijke bevoegdheden tegen zwarte en Aziatische personen, op basis van statistieken die aantonen dat zwarte en Aziatische personen onevenredig zwaar worden getroffen door de politiebevoegdheden in het Verenigd Koninkrijk.
30. Bijv. Liberty en anderen t. VK; zie ook P. De Hert & H. Lammerant, 'Predictive profiling and its legal limits: effectiveness gone forever?', in: B. van der Sloot e.a. (red.), *Exploring the boundaries of big data*, Amsterdam: Amsterdam University Press/WRR 2016.
31. Althans, vanuit strafvorderlijk perspectief. In het dataprotectierecht wordt alles wat met gegevens wordt gedaan beschouwd als 'verwerken'.
32. Zie over deze factor P. De Hert & S. Gutwirth, 'Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action', in: Y. Poullet e.a. (red.), *Reinventing data protection?*, Dordrecht: Springer 2009, p. 26.

doi: 10.5553/TBSenH/229567002021007004002

paragraaf in aan de hand van de theorievorming over *group privacy*.

3.3 Group privacy

Hedendaagse datakoppeling-technologieën verwerken gegevens op basis van patronen en groepsprofielen.[33] *Group-privacy*wetenschappers hebben erop gewezen dat bij dergelijke handelingen niet langer gegevens worden verzameld over één specifiek individu of over een kleine groep mensen, maar over grote en ongedefinieerde groepen op basis van patronen en groepsprofielen. Meestal gaat het dan om 'geaggregeerde' gegevens die in samenhang veel meer zeggen dan op zichzelf genomen.[34] Daarbij dienen de soorten gegevens die in het Sensingproject worden verzameld in gedachten te worden genomen: de kleur van een auto, de richting van de route en het land van registratie van de auto op basis van het kenteken.[35] Uitgaande van een correlatie tussen een groep van personen die in kleine witte auto's vanuit Duitsland naar de Roermondse Outlet rijdt en het plegen van diefstal, worden individuen beoordeeld op basis van genoemde groepskenmerken die zijn 'ontdekt' met behulp van datakoppeling.[36] Volgens group-privacy-wetenschappers, komen in dergelijke gevallen van groepsprofilering de privacyrisico's niet zozeer voort uit de toegang tot de losse gegevens (die op zichzelf niet per se erg privé zijn en soms niet eens betrekking hebben op een individu), maar vooral uit de mogelijkheid voor de overheid (of bedrijven) conclusies te trekken – en beslissingen te nemen – over mensen op groepsniveau op basis van correlaties. Met andere woorden: '*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*.'[37] Dat het hier niet louter gaat om theoretische bezwaren heeft de Toeslagenaffaire bij de Belastingdienst pijnlijk duidelijk gemaakt.

Het probleem met een inbreuk op de privacy als gevolg van datakoppeling ten behoeve van preventief optreden doet zich kortom niet pas voor op het moment dat een individu wordt geïdentificeerd en aangesproken (dat gebeurt ook lang niet bij elk individu dat deel uitmaakt van een profiel) maar al eerder, op het moment dat hij in zo'n groep wordt geplaatst. De theorievorming inzake *group privacy* laat zien dat in het huidige technologische landschap de bestaande mensenrechtelijke privacybescherming moet worden heroverwogen, althans moet worden uitgebreid naar situaties waarin het individu nog niet geïdentificeerd is, maar wel via het combineren van allerhande (op zichzelf soms niet eens persoonlijke) gegevens binnen een – veelzeggend – profiel wordt geplaatst.

3.4 (Europese) regelgeving inzake verwerken van persoonsgegevens

Een ander aspect van het recht op privacy betreft het recht op bescherming van persoonsgegevens. Dit is niet een tak van sport die een strafrechtjurist als vanzelfsprekend ook bestudeert, al was het maar omdat het niet bepaald gemakkelijk is om de regelgeving te doorgronden. Over de vraag wat precies persoonsgegevens zijn en zouden moeten zijn, bestaat een levendige discussie.[38] Voor de analyse van deze casus geven wij de discussie inzake het recht op bescherming van persoonsgegevens niet volledig en inclusief alle nuances en onduidelijkheden weer, maar leggen wij vooral de focus op onze interpretatie van de casus Roermond als het gaat om de vraag wat persoonsgegevens zijn.

33. Zie over profileren M. Hildebrandt & S. Gutwirth, *Profiling the European citizen: cross-disciplinary perspectives*, Dordrecht: Springer 2008.
34. L. Taylor, L. Floridi & B. van der Sloot, 'Introduction', in: L. Taylor e.a. (red.), *Group privacy: new challenges of data technologies*, Dordrecht: Springer 2016, p. 5. Geaggregeerde gegevens of data zijn data die van individuele data (bijv. geboortedatum) worden omgezet in meer algemene data (bijv. geboortejaar of zelfs decennium), en die via technologie worden gecombineerd met soortgelijke geaggregeerde data. Het doel is het vinden van correlaties, ofwel het vinden van een bepaald profiel (mensen uit dit decennium hebben een huis dat in deze prijsklasse valt), waarmee vervolgens weer andere mensen kunnen worden gevonden die binnen het profiel passen (en die ook weer helpen om dat profiel te verrijken), en op grond waarvan bepaalde acties kunnen worden uitgevoerd of beslissingen kunnen worden genomen (reclame-algoritmen werken zo, maar ook de statistische analyses van het CBS). Overigens lijkt het aggregatieniveau in Roermond uiteindelijk niet erg hoog te hebben gelegen.
35. Met uitzondering van kentekenplaten, die duidelijk betrekking hebben op een specifieke persoon, althans wanneer de bestuurder de eigenaar of huurder van de auto is.
36. Deze correlaties duiden echter alleen op een relatie tussen gegevens, zonder oorzaken of redenen daarvoor vast te stellen. Ze geven dus een soort voorspelling op basis van gedrag (bijv. uit statistieken) in het verleden, wat duidt op een kans dat het in de toekomst hetzelfde zal aflopen. Bovendien zijn er twee typen van groepsprofielen: distributieve en niet-distributieve. In een distributief profiel delen alle leden van de groep alle kenmerken van het groepsprofiel (bijv. in het groepsprofiel van 'vrijgezellen' zijn alle mannen niet getrouwd). In het Roermondse geval hebben we echter te maken met een niet-verdelend profiel, waarbij niet alle leden alle attributen van het profiel delen. Dit betekent dat personen die in dit groepsprofiel vallen al dan niet al deze kenmerken kunnen bezitten. Zo gaan bijvoorbeeld niet alle groepen personen die in kleine witte auto's van Duitsland naar de vestiging in Roermond rijden daarheen om diefstallen te plegen. Zie bijv. M. Hildebrandt, 'Defining profiling: a new type of knowledge?', in: M. Hildebrandt & S. Gutwirth (red.), *Profiling the European citizen: cross-disciplinary perspectives*, Dordrecht: Springer 2008; B. Schermer, 'The limits of privacy in automated profiling and data mining', *Computer Law & Security Review* 21(1) 2011.
37. Dit is een beroemd citaat van belangrijke privacywetenschappers uit de VS. Zie S. Barocas & 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.
38. Zie hierover bijv. M. Galič & R. Gellert, 'Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab', *Computer Law & Security Review* 40 (2021), in het bijzonder p. 7-11.

Kort gezegd zijn persoonsgegevens gegevens die individuen direct of indirect (kunnen) identificeren.[39] Kentekens en gegevens uit politiedatabanken met betrekking tot een bepaald voertuig (bijvoorbeeld een voertuig dat is gesignaleerd als gestolen of betrokken bij een eerder strafbaar feit) zijn duidelijk persoonsgegevens, omdat een individu door het gebruik van die gegevens direct kan worden geïdentificeerd. Voor wat betreft de Roermondse casus is derhalve relevant dat dergelijke kentekengegevens worden verzameld waardoor de casus onder de werking van de Wpg en Europese dataprotectiewetgeving valt.[40] Ook andere niet direct identificerende gegevens kunnen echter, als zij worden gecombineerd met andere persoonsgegevens, personen identificeren en in die zin als persoonsgegevens worden aangeduid.[41] In Roermond kunnen derhalve het type, de leeftijd en de kleur van een voertuig en zijn bewegingspatronen, als identificerend worden beschouwd indien ze worden gekoppeld aan andere (persoons)gegevens en als zodanig worden verwerkt. De technologie die gebruikt wordt voor het combineren van gegevens, en vooral hoe geavanceerd deze is, kan een rol spelen bij het waarderen van gegevens als persoonsgegevens. Voor het Sensingproject is echter vooral ook van belang dat het *doel* van het verzamelen en combineren van de gegevens is gelegen in het identificeren van auto's met daarin individuen, en in het staande houden van die individuen in de auto, en dat het staande houden eenvoudig tot het identificeren van personen leidt (nu immers doorgaans naar identificerende documenten zal worden gevraagd). De conclusie is kortom, dat de politie in het Sensingproject een scala van persoonsgegevens verwerkt.[42] Ook is relevant te constateren dat het begrip persoonsgegevens in potentie een bredere bescherming biedt dan het recht op bescherming van privégegevens zoals erkend door het EHRM.

Welke waarborgen bieden de Wpg en de Europese Richtlijn politie- en justitiegegevens (hierna: Richtlijn)?[43] De hoeksteen van de wetgeving inzake gegevensbescherming wordt gevormd door de beginselen van eerlijke verwerking (*fair processing principles*), zoals specificatie- en minimalisatie-beginselen.[44] Volgens deze beginselen moeten persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt. De gegevens moeten ook toereikend, ter zake dienend en niet bovenmatig zijn ten opzichte van de doeleinden waarvoor zij worden verwerkt.[45] Op basis van deze beginselen van eerlijke verwerking heeft de betrokkene ook verschillende rechten, waaronder het recht om informatie te ontvangen over de verwerking met betrekking tot zijn gegevens, om toegang te krijgen tot de gegevens die over hem zijn verzameld en om correctie of verwijdering te eisen van gegevens die betrekking hierop hebben.[46]

Ten aanzien van een effectieve waarborging en het toezicht op de naleving van de Wpg bestaan meerdere knelpunten. Het eerste knelpunt heeft te maken met de naleving of naleefbaarheid van de beginselen van eerlijke verwerking. Deze beginselen zijn immers open normen die niet goed aansluiten op de opsporingspraktijk en moeilijk te operationaliseren zijn.[47] Een tweede knelpunt houdt verband met de mogelijkheid tot beperking van de rechten van de betrokkene in de context van de rechtshandhaving. Het recht op toegang tot informatie kan in die context immers geheel of gedeeltelijk worden beperkt om te voorkomen 'dat afbreuk wordt gedaan aan het voorkomen, onderzoeken of opsporen van strafbare feiten, en in het geval dat deze beperking een noodzakelijke en evenredige maatregel vormt met inachtneming van de grondrechten en de gerechtvaardigde belangen van de betrokkene'.[48] Het is waarschijnlijk dat de politie deze beperkingen gerechtvaardigd acht zodra sprake is van criminaliteitsbestrijding en het risico bestaat dat toegang tot informatie opsporingsmethodes kan blootleggen. Een derde knelpunt ten slotte, hangt samen met de mogelijke genoemde beperkingen in combinatie met het feit dat een aanzienlijk deel van de verantwoordelijkheid voor de rechtmatige verwerking van persoonsgegevens in handen van het individu zelf ligt. Volgens de Richtlijn en de Wpg is de Autoriteit Persoonsgegevens (AP) het primaire toezichthoudende orgaan.[49] Een betrokkene kan een klacht indienen bij de AP, indien hij van mening is dat de verwerking van zijn persoonsgegevens volgens de Wpg niet rechtmatig of

39. Persoonsgegevens worden gedefinieerd als 'alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'; zie artikel 3 lid 1 Europese Richtlijn politie- en justitiegegevens (2016/680); artikel 1 lid b Wpg. Artikel 3 lid 1 stelt verder: 'als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiemiddel zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.'
40. De Wpg is van toepassing, wanneer de politie persoonsgegevens verwerkt in het kader van de uitvoering van de politietaak – wat in de Wpg 'politiegegevens' wordt genoemd. Hierin volgt de Wpg niet de Europese Richtlijn politie- en justitiegegevens (2016/680), die van toepassing is op 'voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid'. Dit onderscheid leidt tot verwarring over de werkingssfeer van de wetgeving inzake gegevensbescherming in de praktijk; zie H. Winter e.a., *De verwerking van politiegegevens in vijf Europese landen: samenvatting*, Den Haag: WODC 2020.
41. Zie bijv. N. Purtova, 'The law of everything: broad concept of personal data and future of EU data protection law', *Law, Innovation and Technology* 10(1) 2018.
42. Als de politie hier gegevens over etniciteit verzamelt – bijv. als de personen in het voertuig tot de Roma behoren (zoals aangemeld in het Amnesty International rapport) – dan verwerken ze ook bijzondere categorieën politiegegevens (*sensitive personal data*). Verwerking van dit soort gegevens is echter alleen toegestaan wanneer dit onvermijdelijk is voor het doel van de verwerking.
43. Richtlijn 2016/680.
44. Artikel 4 Richtlijn 2016/680.
45. Artikel 4 Richtlijn 2016/680; evenzo artikel 3, lid 1, en artikel 2 Wpg.
46. Artikelen 24a en b en 25 Wpg.
47. Winter e.a. 2020, p. 3.
48. Artikel 27, lid 1, onder b) Wpg; artikelen 13 t/m 16 Richtlijn 2016/680.
49. Artikel 35 e.v. Wpg.

doi: 10.5553/TBSenH/229567002021007004002

rechtvaardig is.[50] De betrokkene kan verder tegen de beslissing van de AP in beroep gaan bij een rechtbank in een bestuursrechtelijke procedure.[51] In het geval dat de betrokkene echter onvoldoende toegang heeft tot informatie over het soort gegevensverwerking dat op hem betrekking heeft, kan hij moeilijk vaststellen of de verwerking rechtmatig en eerlijk is geweest (bijvoorbeeld wat voor persoonsgegevens werden verwerkt en of dat echt nodig was voor de uitvoering van de politietaak). Dat betekent dat de controle op de naleving van het dataprotectierecht in belangrijke mate afhankelijk is van eventuele proactieve uitoefening van toezichtsbevoegdheden door de AP. De AP heeft echter onder de Richtlijn (en de Wpg) veel minder corrigerende, toezichthoudende en raadgevende bevoegdheden dan onder de AVG.[52] De AP heeft bijvoorbeeld geen bevoegdheid om verwerkingen stil te leggen of onrechtmatig verwerkte gegevens zelf te verwijderen.[53] Dat leidt tot de vraag of de AP wel een geschikt orgaan is om toezicht te houden op de verwerking van persoonsgegevens voor rechtshandhavingsdoeleinden.

4. Is het Sensingproject Roermond opsporing en wat betekent dat voor de reguleringsvraag?

4.1 Opsporing

In het licht van de zoektocht naar een nieuw of hernieuwd normeringssysteem voor preventief optreden op basis van datakoppeling dringt zich ook de vraag op of in een project als Sensing Roermond sprake is van opsporing, en zo ja, wat dat voor implicaties heeft. Want, hoewel in het juridisch document van de politie het Sensingproject vooral wordt geplaatst binnen de context van de algemene politietaak – en de vraag of sprake is van opsporing niet wordt geadresseerd althans in het midden wordt gelaten – en bovendien de nadruk van de regulering ligt op het verwerken van gegevens, lijkt het doel strafvorderlijk te zijn, namelijk 'de voorkoming, opsporing en vervolging van strafbare feiten die samenhangen met mobiel banditisme'.[54] Ook speelt blijkens de juridische nota de officier van justitie een centrale rol bij de uitvoering van het project.[55] Dat alles wijst erop dat hier reeds volgens de definitie van artikel 132a Sv sprake is van opsporing (namelijk 'het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen'). Dat is relevant omdat met dit doel – zoals ook uit de voorgaande paragraaf al bleek – het optreden in potentie veel meer impact heeft dan wanneer alleen gegevens worden verwerkt. Het impliceert bovendien vanwege die impact dat een strafvorderlijke grondslag met strafvorderlijke waarborgen in de rede ligt.

Dat preventief optreden moet worden gezien als opsporing is vanuit de historie van het Wetboek van Strafvordering niet vanzelfsprekend. De meest klassieke vorm van opsporing is die waar op grond van een redelijke verdenking dat een strafbaar feit is gepleegd, onderzoek wordt gedaan naar dat feit en de verdachte, met als doel de verdachte te berechten en te bestraffen als zijn daderschap wordt bewezen.[56] Dat lijkt ver af te staan van wat in het Sensingproject Roermond wordt gedaan en beoogd. De opsporingspraktijk beweegt zich echter al jaren 'naar voren',[57] hetgeen wil zeggen dat het strafrecht steeds vaker ingrijpt, en wil ingrijpen, in de voorfase van het strafbare feit c.q. niet-voltooide delicten.[58] Dat wordt wettelijk enerzijds mogelijk gemaakt en genormeerd door bepalingen in het materiële strafrecht – de omschrijving van wat een strafbaar feit verschuift naar de voorfase of wordt ruim gedefinieerd[59] – en anderzijds door bepalingen in het strafprocesrecht die het mogelijk maken op te treden als het beeld van een strafbaar feit nog niet erg scherp is. Zo gelden er ruime opsporingsmogelijkheden in geval van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd (artikel 126o Sv e.v.), kan opsporing naar terroristische misdrijven reeds aanvangen in geval van 'aanwijzingen' (artikel 126zf Sv e.v.), en kent de Wet op de economische delicten (WED) eveneens opsporingsbevoegdheden die 'in het belang van de opsporing' en zonder redelijk vermoeden kunnen worden ingezet.[60] Het Wetboek van Strafvordering kent daarnaast de bevoegdheid van het 'verkennend onderzoek' (126gg Sv), die het bundelen van gegevens

50. Artikel 31a Wpg.
51. Artikel 31b Wpg.
52. In plaats van zes corrigerende, tien toezichthoudende en tien raadgevende bevoegdheden in de AVG, staan in de Richtlijn alleen twee toezichthoudende, twee raadgevende en drie corrigerende bevoegdheden. De lidstaten kunnen in hun nationale wetgeving uiteraard meer bevoegdheden voorschrijven, maar in de Wpg is dat niet gebeurd. Zie P. De Hert & J. Sajfert, 'The role of data protection authorities in supervising police and criminal justice authorities processing personal data', in: C. Brière & A. Weyembergh (red.), *The needed balances in EU Criminal Law: past, present and future*, London: Hart 2018, p. 251-2.
53. Artikel 47 Richtlijn en artikel 35c Wpg; zie ook Winter e.a. 2020, p. 5.
54. Politiedocument (083) 'Nota rechtmatigheid OPTR en GPV', 15 augustus 2018, p. 3.
55. Politiedocument (083) 'Nota rechtmatigheid OPTR en GPV', 15 augustus 2018, p. 3, 4 en 5.
56. Zie B.F. Keulen & G. Knigge, *Strafprocesrecht*, Deventer: Kluwer 2016, p. 273 e.v. en M.J. Borgers, 'Het opsporingsbegrip anno 2009', in: M.J. Borgers e.a. (red.), *Politie in beeld* (bundel Naeyé), Nijmegen: Wolf Legal Publishers 2009, p. 27-64.
57. Vgl. M.F.H. Hirsch Ballin, *Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States* (diss. Utrecht), Den Haag: T.M.C. Asser Press 2012, p. 3-4.
58. Denk bijvoorbeeld aan de strafbaarstelling van voorbereiding (art. 46b Sr); Zie ook Hirsch Ballin 2012, p. 3-4.
59. De poging en de voorbereiding zijn daarvan voorbeelden, maar ook het in het leven roepen van bijvoorbeeld terroristische delicten zoals de samenspanning tot het plegen van een terroristisch misdrijf, deelname aan training voor terrorisme en lidmaatschap van een terroristische organisatie.
60. Bijvoorbeeld voorwerpen in beslag nemen, gegevens vorderen of zich toegang verschaffen tot elke plaats voor zover dat redelijkerwijs voor de vervulling van hun taak nodig is (zie artikelen 17 e.v. WED). Zie hierover Corstens/Borgers & Kooijmans 2018, p. 303-304.

doi: 10.5553/TBSenH/229567002021007004002

door opsporingsambtenaren behelst met als doel het al dan niet uitvoeren van (verder) onderzoek naar een wellicht gepleegd strafbaar feit (het betreft misdrijven die bedreigd worden met een gevangenisstraf van minimaal vier jaar en een ernstige inbreuk op de rechtsorde opleveren).[61] Ten slotte is in de jurisprudentie de inzet van repressieve controlebevoegdheden onder opsporing geschaard: controlebevoegdheden mogen worden ingezet als het doel daarvan (tevens) is het onderzoek in verband met strafbare feiten.[62] Daarbij moet gedacht worden aan het uitvoeren van verkeerscontroles op basis van de Wegenverkeerswet 1994, maar bijvoorbeeld ook aan de algemene controlebevoegdheden van de Algemene wet bestuursrecht (Awb), die van artikel 45 Wet wapens en munitie (WWM) en artikel 8j Opiumwet (Opw), of de taakstellende bepalingen van de politie (artikel 3 Pw jo. 11 Pw en 12 Pw).[63]

Kortom, het totaalbeeld laat zien dat opsporing een breed spectrum beslaat van onderzoek 'in verband met strafbare feiten', waarbij het zicht op het strafbare feit meer of minder concreet kan zijn. Doorslaggevend is het strafvorderlijke doel van het onderzoek – in combinatie met het daarbij horende gezag van de officier van justitie: het nemen van een strafvorderlijke beslissing. Een strafvorderlijke beslissing is ook al het niet verder verrichten van onderzoek (wanneer onderzoek naar mogelijke begane strafbare feiten geen redelijke verdenking oplevert, of de beslissing dat strafbare feiten worden gestopt).[64] Oftewel: als het onderzoek in verband met strafbare feiten plaatsvindt, is het doel van het nemen van strafvorderlijke beslissingen er in wezen ook altijd. Vanuit de opsporingsvraag, en als wordt gekeken naar het doel, verschilt de Roermondse casus naar ons idee dan ook niet van die uit het Tilburgse Veelplegerarrest, waarin een veelpleger door de politie op grond van artikel 2 (nu 3) Pw vrij intensief werd geobserveerd teneinde de veelpleger te betrappen bij het plegen van nieuwe winkeldiefstallen dan wel nieuwe winkeldiefstallen te voorkomen.[65] Het maakt naar ons idee bovendien geen verschil of de datakoppeling leidt tot de staandehouding van verdachte auto's of verdachten, of dat de datakoppeling geen hits oplevert. Mede gelet op het doel van de toepassing, het tegengaan van mobiel banditisme in het Outletcentrum Roermond, gaat het immers ook dan om onderzoek in verband met strafbare feiten.

4.2 Wettelijke basis

Wat nu zijn de consequentie van de constatering dat een project zoals Sensing Roermond moet worden gezien als opsporing? De eerste betreft de noodzaak voor een wettelijke basis. Maar in welke wet dient dan die basis te liggen? Nu de gehele methode – vergaren van informatie, verwerken informatie door koppeling, en het besluit tot staande houden van bepaalde auto's/groepen/individuen – zich beweegt op het snijvlak van bestaande wetten (Pw, Wpg, Sv) is op die vraag geen voor de hand liggend antwoord te vinden. Vanuit het oogpunt van voorzienbaarheid van de regeling, en (daarmee) de helderheid en werkbaarheid voor de praktijk, ligt het naar ons idee niettemin wel voor de hand dat zou worden gekozen voor een overkoepelende normering voor het volledige plaatje in één wet en niet voor een splitsing van de grondslagen. Het Wetboek van Strafvordering is in dat kader wellicht minder geschikt. De in het wetboek geboden normering voor de inzet van bevoegdheden is immers – ondanks de hier geschetste beweging naar voren – nog steeds (en dat is in het nieuwe wetboek niet anders) sterk toegesneden op de aanwezigheid van een redelijk vermoeden dat een strafbaar feit is gepleegd, en daarbij sterk geënt op de normering van vergaringsbevoegdheden in relatie tot een concreet individu, meestal de verdachte. Bevoegdheden voor preventief optreden op basis van niet op een concreet individu gerichte informatie passen kortom niet zo goed binnen die systematiek. Denkbaar is wel dat de nieuw te ontwerpen wet die de huidige Wpg en Wjsg moet gaan vervangen en die ook beter zou moeten aansluiten bij de Richtlijn, hiervoor geschikt zou kunnen worden gemaakt. Dat lijkt, blijkens een eerste aanzet van de uitgangspunten voor deze nieuwe wet, ook door de minister te worden beoogd.[66]

Bij het creëren van een dergelijke grondslag zien wij reeds in ieder geval twee aandachtspunten. Als eerste is van belang dat de officier van justitie een rol krijgt bij het toezicht op de uitvoering van de bevoegdheden. Dat volgt reeds uit het feit dat het hier gaat om opsporing, zoals we in de vorige paragraaf betoogden. Uit de juridische nota inzake het Sensingproject blijkt overigens dat in Roermond de officier van justitie ook als waarborg werd gezien. Daarbij is het ons niet duidelijk geworden hoe de officier van justitie zijn toezichthoudende rol vormgaf. Wat ons betreft is dat evenwel een toezicht dat is gebaseerd op de in de volgende paragraaf uiteen te zetten strafvorderlijke basisbeginselen. Aandachtspunt is nog wel de verhouding tussen de officier van justitie en de Autoriteit Persoonsgegevens. In paragraaf 3.4 wierpen wij de vraag op of de AP wel als een geschikt orgaan kan worden gezien om toezicht te houden op de verwerking van persoonsgegevens voor rechtshandhavingsdoeleinden. Nagedacht zou kunnen worden over

61. Deze bevoegdheid werd overigens door de wetgever destijds niet als opsporing gezien maar als voorbereiding van opsporing. Deze opvatting wordt heden ten dage als onjuist gezien. Zie Corstens/Borgers & Kooijmans 2018, p. 302, Keulen & Knigge 2016, p. 279, en zie ook de memorie van toelichting bij het wetsvoorstel tot vaststelling van het Nieuwe Wetboek van Strafvordering (ambtelijke versie juli 2020), p. 47.
62. Zie bijv. HR 30 juni 2020, ECLI:NL:HR:2020:1155 en HR 1 november 2016, ECLI:NL:HR:2016:2454, *NJ* 2017/84. De inzet mag dus niet uitsluitend opsporing zijn als de bevoegdheid een concreet controledoel heeft.
63. Zie het Tilburgse Veelplegersarrest, HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013/413.
64. Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (ambtelijke versie juli 2020), p. 46-47.
65. Het is ons overigens niet geheel duidelijk of in Roermond een hit een redelijk vermoeden oplevert of dat een redelijke verdenking pas kan ontstaan na een staandehouding en nader onderzoek. Wij vermoeden dat laatste.
66. *Kamerstukken II* 2020/21, 32761, nr. 173.

doi: 10.5553/TBSenH/229567002021007004002

een gedifferentieerd toezicht door bijvoorbeeld de officier van justitie en de AP, of dat een oplossing kan worden gevonden in een ander orgaan dat beschikt over speciale expertise (en bevoegdheden) in het kader van rechtshandhaving (zoals bijvoorbeeld in België).[67]

Een volgend aandachtspunt betreft de aansluiting van de normering van datakoppeling met het oog op preventief optreden op bevoegdheden zoals die in het Wetboek van Strafvordering zijn neergelegd. Het preventieve optreden op grond van datakoppeling zoals dat in Roermond gebeurde, kan maar hoeft niet gericht te zijn op een individu en is gebaseerd op algemene statistieken. Of sprake was van een redelijke verdenking in het geval een auto werd stil gehouden (en dus een verdachte staande wordt gehouden op grond van artikel 52 Sv) of dat het doen stilhouden van de auto plaatsvond op grond van artikel 160 Wegenverkeerswet 1994 is ons niet duidelijk. Bevoegdheden uit het Wetboek van Strafvordering hebben als toepassingsdrempel een individu dat wordt aangewezen op basis van objectiveerbare en op dat individu gerichte feiten en omstandigheden. De vraag is aldus of de informatie die voortkomt uit de datakoppeling ook tot het individu gerichte feiten en omstandigheden oplevert en, bovendien, of dit voldoende is voor het voor staandehouding vereiste 'redelijk vermoeden'. Het is denkbaar dat bepaald preventief optreden[68] op grond van datakoppeling kan geschieden op minder concreet op het individu gerichte informatie of anders gezegd: als nog geen sprake is van een redelijke verdenking zoals bedoeld in artikel 27 van het Wetboek van Strafvordering. Daarbij zal dan wel goed moeten worden nagedacht over welke bevoegdheden (variërend in ingrijpendheid) in welke wet en op basis van welke informatie kunnen worden ingezet, en hoe die bevoegdheden zich tot elkaar verhouden. Van belang is daarbij bovendien dat het (of in ieder geval een) doel van het optreden in het Sensingproject maakt dat sprake is van opsporing. Wanneer er uitsluitend sprake is van een strafvorderlijk doel (en dus opsporing), kunnen controlebevoegdheden voor dat doel niet worden ingezet.[69] Een oplossing zou kunnen worden gevonden in een wettelijke grondslag voor preventief optreden in vervolg op de datakoppeling die in ieder geval ook recht doet aan het opsporingskarakter van het optreden. De strafvorderlijke basisbeginselen die we in de volgende paragraaf bespreken kunnen ook voor die grondslag behulpzaam zijn.

4.3 Strafvorderlijke basisbeginselen

De tweede consequentie van de constatering dat het gaat om opsporing is dat de strafvorderlijke basisbeginselen een plek moeten krijgen in de normering van preventief optreden op grond van datakoppeling. Wij denken daarbij in de eerste plaats aan de onschuldpresumptie, en meer in het bijzonder: de behandelingsdimensie van de onschuldpresumptie.[70] In onze casus houdt deze kort gezegd in dat de met het gebruik van de Roermondse methode beoogde doelen (voorkomen van mobiel banditisme) en de afweging van die doelen tegen de belangen van het betrokken individu, niet mogen getuigen van een schuldoordeel – of anders gezegd: de schuld van de (nog niet) verdachte als een gegeven beschouwen.[71] Dat houdt in dat een wettelijke grondslag die de voorwaarden voor bepaald ingrijpen creëert zal moeten voorzien in een objectiveerbare koppeling aan strafbaar gedrag, ofwel, in het geval van Roermond, in een bepaalde mate van verdenking van winkeldiefstal op basis van objectieve factoren en ten aanzien van aanwijsbare individuen of auto's tegen wie verdere strafvorderlijke bevoegdheidsuitoefening kan plaatsvinden. Een dergelijke eis van objectiveerbaarheid kan tegelijkertijd op toepassingsniveau een waarborg bieden tegen etnisch profileren of discriminatie. In het Roermondse project zou bijvoorbeeld afdoende moeten worden onderbouwd waarom het gerechtvaardigd is om juist auto's met een Duits of Roemeens kenteken te volgen en staande te houden, en onder ogen moeten worden gezien of hier niet sprake is van een ongerechtvaardigd (indirect) onderscheid op basis van nationaliteit.[72] In dat licht is de betrouwbaarheid van de gebruikte data een niet te verwaarlozen onderdeel van de eis van objectiveerbaarheid. Reeds eerder hebben wetenschappers gewezen op het gevaar van gebruik van vervuilde data bij voorspellende algoritmen.[73] Dat dit moet worden voorkomen is evident; het *hoe* is vele malen ingewikkelder.

Uit het vereiste van de objectiveerbaarheid en betrouwbaarheid vloeit direct het volgende strafvorderlijke basisbeginsel voort, namelijk dat van de transparantie door middel van verbalisering. Binnen de context van een strafproces, maar ook in het kader van toezichthoudende mechanismen dient verantwoording te worden afgelegd over de keuzes die op basis van een wettelijke regeling zijn gemaakt. Die verbaliseringsplicht zal zich

67. WODC-rapport (2021), samenvatting, p. 7.
68. Dat kan staande houden zijn zoals in deze casus. Maar het kan bijvoorbeeld ook gaan om optreden dat gedrag van groepen beïnvloedt (het wegleiden van een risicogroep feestvierders van een bepaalde plek), of juist om meer ingrijpende bevoegdheden zoals preventief fouilleren.
69. Vgl. HR 30 juni 2020, ECLI:NL:HR:2020:1155.
70. J.H.B. Bemelmans, *Totdat het tegendeel is bewezen. De onschuldpresumptie in rechtshistorisch, theoretisch, internationaalrechtelijk en Nederlands strafprocesrechtelijk perspectief* (diss. Nijmegen), Deventer: Wolters Kluwer 2018, p. 135 e.v., in het bijzonder p. 146-148.
71. Bemelmans 2018, p. 412.
72. Vergelijk HR 9 oktober 2018, *NJ* 2019/24, m.nt. Reijntjes. Uit interne mailwisseling van de politieorganisatie blijkt dat bij deze vraag bij de juridische voorbereiding van het Roermondse project is afgewogen en negatief is beantwoord. Zie politiedocument 099. Overigens is niet inzichtelijk op basis van welke argumenten deze conclusie is getrokken
73. A. Das & M. Schuilenburg, '"Garbage in, garbage out." Over predictive policing en vuile data', *Beleid en Maatschappij* 2020 (47) 3, p. 254-268.

doi: 10.5553/TBSenH/229567002021007004002

ook moeten uitstrekken tot de input: welke data zijn op welke wijze gebruikt?[74]

Van eminent belang zijn voorts de (opsporings)beginselen van proportionaliteit en subsidiariteit. Niet voor elk strafbaar feit of voor elk type criminaliteit is het in het licht van die beginselen te legitimeren dat een ingrijpende methode ter preventie wordt ingezet. Naar ons idee wringt het in Roermond ook omdat de grootscheepse datakoppeling en het daarop gebaseerde optreden niet direct in redelijke verhouding lijken te staan tot het misdrijf dat moet worden voorkomen: winkeldiefstal. Daar zou tegenin kunnen worden gebracht dat het gaat om grootschalige en overlastgevende criminaliteit die ook nog eens heel moeilijk aan te pakken is. De vraag of legitimatie voor inzet van (bepaald) preventief optreden op basis van (een bepaalde wijze van) datakoppeling moet worden gezien in bepaalde vormen van criminaliteit zou niettemin op wetgevingsniveau moeten worden bediscussieerd en beantwoord. Is het een proportioneel middel voor overlastgevende criminaliteit, en zou het beperkt moeten worden tot bepaalde gebieden of plekken (die dan bijvoorbeeld bij AMvB aangewezen zouden kunnen worden)?

Ten slotte vestigen wij hier graag nog de aandacht op het strafvorderlijke stelselmatigheidscriterium. Dit criterium wordt in het gemoderniseerde wetboek gebruikt bij de vormgeving van enkele digitale opsporingsbevoegdheden.[75] Op grond van het criterium kan worden bepaald hoe groot de inbreuk op de privacy van een betrokkene is, vervolgens wordt het waarborgniveau bepaald: hoe groter de inbreuk hoe groter de waarborgen.[76] Indien een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan', is er in de huidige interpretatie sprake van stelselmatigheid. Op grond van deze interpretatie is het criterium weinig bruikbaar voor de hier door ons behandelde casus. In het Sensingproject ontstaat immers maar een zeer beperkt en weinig gevoelig beeld van iemands privéleven. Het probleem met het criterium is hier wederom dat het uitgaat van een individu dat moet worden beschermd terwijl datakoppeling zich grotendeels niet richt op individuen. Het stelselmatigheidscriterium is echter nadrukkelijk geïntroduceerd als een toekomstbestendig criterium en is daarmee een open criterium dat kan meebewegen met nieuwe technologieën en opvattingen in de maatschappij.[77] In dat licht denken wij dat het stelselmatigheidscriterium ook bruikbaar zou moeten kunnen zijn voor de normering van privacy-inbreuken als gevolg van preventief optreden op basis van datakoppeling. Het criterium kan zowel inzichten uit het EHRM als inzichten uit het persoonsgegevensrecht incorporeren en worden gekoppeld aan het concept van *group privacy*. Op die manier zou stelselmatigheid een criterium kunnen worden dat ook bescherming biedt tegen het soort privacy-inbreuken dat plaatsvindt bij preventief optreden op grond van datakoppelingsbevoegdheden.

5. Ten slotte: de contouren voor regulering van preventief optreden door datakoppeling

In deze bijdrage hebben wij onderzoek gedaan naar de vraag hoe preventief politieoptreden op basis van datakoppeling zou kunnen en moeten worden genormeerd. Het concrete voorbeeld waar wij onze analyse op hebben gebaseerd is het – inmiddels (voorlopig) gestopte – Sensingproject Outlet Roermond. Onze vraag en onze antwoorden gelden echter veel breder dan dit project. Het is realistisch te verwachten dat het Sensingproject pas het begin markeert van de inzet van vergelijkbare politieprojecten dan wel projecten met meer geavanceerde algoritmen, waarin dankbaar gebruik wordt gemaakt van alle data die tegenwoordig beschikbaar zijn, en van alle technologie die deze data kan combineren en verrijken.

Centraal in onze analyse staat het punt dat bestaande wetgeving onvoldoende in staat is de privacy van burgers te beschermen als die burgers ten behoeve van preventief politieoptreden in een algoritmische risicogroep worden geplaatst (en overigens ook niet in staat is discriminatie en etnisch profileren te voorkomen). Niet het 'geïdentificeerde individu' moet worden beschermd, maar het 'nog niet zichtbare individu' als onderdeel van zo'n risicogroep. Die bescherming moet van kracht worden op het moment dat de technologie het individu onderdeel maakt van zo'n groep. Een nieuwe grondslag voor preventief politieoptreden op basis van datakoppeling zal dan ook moeten worden vormgegeven vanuit dit besef. Het in dit stuk besproken concept van *group pri-*

74. Dat raakt ook aan de niet makkelijk te beantwoorden vraag hoe ingewikkelde algoritmen transparant moeten worden gemaakt voor diegenen in de strafrechtsketen die op grond van de uitkomsten een beslissing moeten nemen en de beslissing moeten kunnen toetsen. Zie hierover bijvoorbeeld A. Deeks, 'The Judicial Demand for explainable Artificial Intelligence', *Virginia Public Law and Legal Theory Research Paper No. 2019-51 (last revised 2 Feb 2020)*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440723; S. Gless, 'AI in the Courtroom: a comparative analysis of machine evidence in criminal trials', *Georgetown Journal of International Law, Vol. 51, No. 2, 2020*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3602038#.

75. Artikel 2.7.39 (onderzoek aan digitale-gegevensdragers en geautomatiseerde werken), artikel 2.7.41 (netwerkzoeking), en artikel 8.2.2 (stelselmatig overnemen persoonsgegevens uit publiek toegankelijke bronnen) van het wetsvoorstel Wetboek van Strafvordering (ambtelijke versie juli 2020), te vinden via www.rijksoverheid.nl/onderwerpen/nieuwe-wetboek-van-strafvordering.

76. Die gedifferentieerde waarborg ligt nu enkel in de bevoegde autoriteit: opsporingsambtenaar, officier van justitie of rechter-commissaris. Dat betekent echter niet dat zou kunnen worden nagedacht over een ruimer systeem van getrapte waarborgen (denk aan toepassingsvoorwaarden).

77. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, 2018 (Commissie-Koops), p. 41 en memorie van toelichting bij het wetsvoorstel Wetboek van Strafvordering (ambtelijke versie juli 2020), p. 410.

doi: 10.5553/TBSenH/229567002021007004002

vacy kan daarbij behulpzaam zijn. In tegenstelling tot het Wetboek van Strafvordering en het EVRM is de gedachte van bescherming van *group privacy* overigens wel reeds te herkennen in de regelgeving inzake bescherming van persoonsgegevens. Strafrechtjuristen zouden dan ook goed eraan doen zich meer te verdiepen in dit rechtsgebied.

Het andere centrale punt dat wij maken is dat het in een project zoals dat van Roermond gaat om preventief optreden in de zin van opsporing. Die constatering heeft belangrijke implicaties. Een wettelijke grondslag zal recht moeten doen aan strafvorderlijke basisbeginselen. En, hoewel zo'n grondslag wellicht niet het beste zal passen in het Wetboek van Strafvordering – dat immers traditioneel sterk gericht is op het strafproces terwijl dat in geval van preventief optreden in de regel niet aan de orde zal zijn – dient die wettelijke grondslag wel logisch aan te sluiten op het Wetboek van Strafvordering en bovendien ook aan zekere strafvorderlijke voorwaarden te voldoen. Toezicht op het preventieve optreden zal bijvoorbeeld moeten worden uitgevoerd door de officier van justitie, in combinatie met toezicht op de naleving van het dataprotectierecht door de AP of een ander onafhankelijk orgaan. Ook is van belang dat (toepassing van) bevoegdheden dien(t)(en) te voldoen aan de strafvorderlijke basisbeginselen. Wij doelen dan in ieder geval op de onschuldpresumptie, die concreet uitwerking krijgt in de eis van objectiveerbaarheid en betrouwbaarheid van de aanleiding tot optreden (en dus ook uitwerking heeft op de input van data). Daarnaast noemden wij de verbaliseringsplicht, de beginselen van proportionaliteit en subsidiariteit, en het stelselmatigheidscriterium.

Ten slotte: deze bijdrage doet op geen enkele manier recht aan de enorme complexiteit van het vraagstuk van preventief politieoptreden op grond van datakoppeling. Op vele punten gaan wij hoog over. Wij hopen niettemin wel dat we deze problematiek inzichtelijk hebben gemaakt en hebben laten zien voor welke uitdaging de strafrechtelijke wetenschap staat. De problematiek die het Sensingproject laat zien is wat ons betreft nog te weinig in zicht bij strafrechtjuristen, en het experimenteren met algoritmen te veel een aangelegenheid van enthousiaste praktijkbeoefenaars en technologen. Normering van dergelijke projecten vereist een samenwerking tussen technologen, strafrechtjuristen, dataprotectiejuristen, en de praktijk. Dat is, zeggen wij met enig gevoel voor understatement, niet bepaald makkelijk. Wat ons betreft is dat echter geen reden om niet eraan te beginnen. Het moment is nu, of eigenlijk, gisteren al.

doi: 10.5553/TBSenH/229567002021007004002