B.W. Schermer & J.J. Oerlemans[1]

AI, strafrecht en het recht op een eerlijk proces

Computerrecht 2020/3

Data-analyse wordt steeds belangrijker binnen het strafrecht. In de afgelopen jaren heeft de politie onder andere door inbeslagname van servers van versleutelde communicatiediensten een schat aan gegevens verzameld over criminelen. Met behulp van geavanceerde data-analyse technieken wordt de politie wegwijs in deze berg gegevens. De verdediging beschikt niet noodzakelijkerwijs over dezelfde middelen hetgeen het recht op een eerlijk proces mogelijk in gevaar brengt. In deze bijdrage bespreken wij deze problematiek aan de hand van de 'Ennetcom'-zaak. Naast data-analyse technieken is ook algoritmische besluitvorming binnen het strafrecht aan een opmars bezig. Het voornaamste vraagstuk is hier of de juistheid en legitimiteit van dergelijke besluitvorming te controleren valt. Ook dit vormt een risico voor het recht op een eerlijk proces. In dit artikel staat de vraag centraal in hoeverre geavanceerde data-analyse en algoritmische besluitvorming raakt aan het recht op een eerlijk proces als beschreven in artikel 6 EVRM.

1. Inleiding

Verdachten worden in strafzaken steeds vaker geconfronteerd met de uitkomst van een data-analyse op basis van een grote hoeveelheid gegevens. Deze gegevens zijn bijvoorbeeld afkomstig van een inbeslaggenomen server met daarop de administratie van klantgegevens of transactiegegevens. Met behulp van data-analyse kunnen gegevens worden geselecteerd die mogelijk bewijsmateriaal in veel verschillende strafzaken opleveren. Het is ook denkbaar dat een algoritme het bewijs van een delict aanlevert en zelfs dat daar een geautomatiseerd besluit op wordt genomen. In dat geval is sprake van een toepassing van kunstmatige intelligentie en geautomatiseerde besluitvorming.

In dit artikel staat de vraag centraal in hoeverre de data-analyse van grote hoeveelheden gegevens en de inzet van kunstmatige intelligentie bij strafvorderlijke beslissingen raakt aan het recht op een eerlijk proces. Het artikel is verkennend van aard. Het vormt mogelijk het begin van een antwoord welke rechten de verdediging heeft of zal moeten krijgen in moderne strafzaken waarin data-analyse en kunstmatige intelligentie een grote rol spelen. Met deze kennis kunnen advocaten mogelijk beter verweer voeren in strafzaken. Ook zal het Openbaar Ministerie haar verantwoordelijkheid moeten nemen en inspanningen moeten leveren om verantwoord en rechtmatig om te gaan met deze nieuwe technieken in strafzaken.

Paragraaf 2 gaat in op de verhouding tussen grootschalige data-analyses en het recht op een eerlijk proces. Paragraaf 3 bespreekt algoritmische besluitvorming in relatie tot een eerlijk proces. Het artikel sluit af met een conclusie in paragraaf 4, waarin de auteurs pleiten voor de versterking van het recht op een eerlijk proces bij geautomatiseerde data-analyse en kunstmatige intelligentie.

2. Grootschalige data-analyse en het recht op een eerlijk proces

Deze paragraaf gaat nader in op grootschalige data-analyse en het recht op een eerlijk proces in strafzaken. Steeds vaker voelen verdachten en hun advocaten zich geconfronteerd met een grote hoeveelheid van belastend bewijs, afkomstig als resultaat van een data-analyse van een grote hoeveelheid gegevens. Advocaten vragen zich af of zij voldoende instrumenten hebben hun cliënten te verdedigen.[2] Dit raakt aan het recht op een eerlijk proces, zoals geformuleerd in artikel 6 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM).

In deze paragraaf wordt eerst de 'Ennetcom'-casus besproken om concreet te maken waarmee verdachten worden geconfronteerd. Daarna wordt het recht op een proces in artikel 6 EVRM in deze context besproken. Ten slotte wordt nagegaan hoe het recht op eerlijk proces beter kan worden geborgd.

2.1 *De Ennetcom-casus*

In 2016 heeft het Nederlandse Team High Tech Crime een grote hoeveelheid gegevens (7 Terabyte[3]) in beslag genomen van 'Ennetcom', een bedrijf dat werd verdacht van witwassen.[4] Het Nederlandse bedrijf Ennetcom leverde diensten op het gebied van versleutelde communicatie. Tijdens een doorzoeking bij het bedrijf zijn 3,6 miljoen versleutelde berichten in beslag genomen die zijn verstuurd via zo'n 40.000 smartphones van naar schatting 19.000 klanten.[5] Klanten konden met speciale BlackBerry-telefoons, voorzien van specifieke software, versleutelde tekstberichten

1 Bart Schermer is universitair hoofddocent bij het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden en partner bij juridisch adviesbureau Considerati. Jan-Jaap Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht en verbonden aan het Montaigne Centrum voor Rechtsstaat en Rechtspleging en het Willem Pompe Instituut voor Strafrechtwetenschappen.

2 D.N. de Jonge, 'Verdedigen in tijden van digitale bewijsvoering. Een onderzoek naar de mogelijkheden van toegang tot niet van het procesdossier uitmakende, maar mogelijk wel relevante, (digitale/technische) gegevens', p. 125-154, in: P.P.J. van der Meij e.a. (*red.*), *Aan de slag*, Liber amicorum Gerard Hamer: Sdu 2018 (hierna: de Jonge 2018).

3 Om een idee te geven van de omvang: één foto van goede kwaliteit is ongeveer twee megabyte. Duizend megabyte is één gigabyte. Duizend gigabyte is één terabyte.

4 De gedachte is dat de verdachte moet hebben geweten dat hij zijn speciaal geprepareerde telefoons vooral verkocht aan criminelen en zich daarmee schuldig maakte aan witwassen.

5 Zie, o.a., Tom Kreling, 'Justitie heeft toegang tot 3,6 miljoen versleutelde berichten van criminelen', *De Volkskrant*, 9 maart 2017.

en notities versturen.[6] De encryptiesleutels waren opgeslagen op de Blackberry Enterprise Servers van Ennetcom. Deze servers bevonden zich in Toronto, Canada. Na een rechtshulpverzoek van Nederland en een machtiging van een rechter-commissaris aan de Canadese autoriteiten zijn op 19 april 2016 de encryptiesleutels op de servers veiliggesteld zodat daarmee de berichten konden worden ontsleuteld door de Nederlandse opsporingsautoriteiten.[7]

Het Nederlands Forensisch Instituut (NFI) heeft software ontwikkeld waarmee zeer grote hoeveelheden gegevens snel en diepgaand geanalyseerd kunnen worden. Datasets zijn snel te doorzoeken om zo verbanden te leggen tussen verschillende attributen, zoals gebruikersnamen, bijnamen, telefoonnummers en e-mailadressen. Hierdoor kunnen rechercheurs en analisten vele malen sneller en effectiever werken in een opsporingsonderzoek.[8] De software, genaamd 'Hansken', is ook ingezet voor de analyse van de Ennetcom-data.[9] Het gaat dan bijvoorbeeld om zaken, waarbij de PGP-telefoon van de verdachte in een andere strafzaak in beslag is genomen en de telefoon en/of gegevens op de telefoon gematched worden met gegevens in de Ennetcom-dataset. In vonnissen is te lezen dat uit deze gegevens blijkt dat de verdachten hebben gecorrespondeerd over ernstige misdrijven, zoals het doden van een persoon. In de vonnissen worden delen uit de berichten geciteerd en deze berichten tellen mee als bewijs, onder andere om het vereiste 'voorbedachte rade' bij het delict moord te kunnen bewijzen. In de uitspraak van de rechtbank Gelderland is bijvoorbeeld te lezen:

> *"Berichten op 7 november 2015 na het tijdstip van overlijden van [slachtoffer]*
> Tussen 01.58 uur en 02.06 uur tussen [naam 1] en [naam 11]
> [naam 11] aan [naam 1]: *"gefixt"*
> [naam 1] aan [naam 11]: *"Is ie dood?"*
> [naam 11] aan [naam 1]: *"Broer ik heb me 9 op hemm geleegd [bijnaam 2] rende achter me aan met kalash".*
> (…)
>
> Tussen 04.52 en 06.14 uur berichtenwisseling tussen [naam 11] en [naam 2].
>
> [naam 2] aan [naam 11]: "*Bro kijk nu.nl hij is dooodddddd gappppp".*
> [naam 2] aan [naam 11]: "*Wolllahhhhh kan je foto accepteren".*
> [naam 11] aan [naam 2]: *"ja".*
> [naam 11] aan [naam 2]: "*Wis alle kanker berichten van je pgp af zo snel mogelijk als je dit leest".*
> [naam 2] aan [naam 11]: "*Heb gestuurd is laden hij Is net eropp gegooiddd half5".*
>
> Publicatie datum artikel nu.nl over doodgeschoten slachtoffer in Krommenie; 7.11.15 om 04.23 uur.
>
> Om 06.15. uur bericht [naam 11] aan [naam 2]: *"Jaaaa man ik heb gelezen kanker gruwelijk brol We hebben naam gemaakt bij die fucking orga het gaat goed komen [bijnaam 2] we gaan kapot maken ee wis die gesprken alles alles oke".*
>
> *Concluderend*
> Op grond van de hiervoor genoemde bewijsmiddelen is naar het oordeel van de rechtbank komen vast te staan dat [naam 2] en de inmiddels overleden [naam 11] de schutters zijn van de aanslag op [slachtoffer]. Daarbij is het dodelijke schot afkomstig uit het geweer waarmee door [naam 2] is geschoten."[10]

Kortom, het belang van de inbeslagname van de Ennetcom-data en de analyse daarvan door middel van onder andere Hansken kan niet worden onderschat. Het vormt in diverse onderzoeken naar zware drugscriminaliteit en liquidaties in Nederland een belangrijk deel van het bewijs.[11] In het bijzonder speelde de Ennetcom-data een sleutelrol in de veroordeling van crimineel Naoufal 'Noffel' F die werd verdacht van het aansturen van een liquidatie.[12]

2.2 *Toegang tot de dataset voor de verdediging*

De verdediging voerde in de zaak tegen Naoufal F. een interessant verweer, namelijk dat de verdediging onvoldoende mogelijkheden heeft gehad voor een "contra-expertise" op de Ennetcom-dataset.

In de uitspraak van de rechtbank Amsterdam van 19 april 2018 is in detail te lezen op welke wijze gebruik is gemaakt van de data-analyse op de Ennetcom-dataset met Hansken.[13] De Ennetcom-dataset is vervolgens onderzocht aan de hand van:

1. de e-mailadressen, IMEI-nummers en PIN-nummers die aan de verdachten in het onderzoek Tandem zijn gerelateerd;

6 De software maakte gebruik van het programma Pretty Good Privacy (PGP) om communicatieverkeer te versleutelen.

7 Zie Rb. Amsterdam 7 december 2018, ECLI:NL:RBAMS:2018:8713. In deze noot wordt verder niet ingegaan op de rechtmatigheid van de vordering van de sleutels via een rechtshulpverzoek aan Canada. Het verdient daarbij wel opmerking dat de bevoegdheid in art. 126ng lid 2 Sv slechts onder de strengste voorwaarden kan worden toegepast en met een vordering van een rechter-commissaris.

8 Zie voor meer technische details ook: H.M.A. van Beek e.a., 'Digital forensics as a service: Game on', *Digital Investigation* 2015, p. 20-38.

9 Na een zoekslag op rechtspraak.nl met sleutelwoorden als 'Ennet' of 'Hansken' zijn de volgende uitspraken geïdentificeerd: Hof Amsterdam 30 januari 2018, ECLI:NL:GHAMS:2018:240; Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504; Hof Amsterdam 4 mei 2018, ECLI:NL:GHAMS:2018:1550; Rb. Amsterdam 7 december 2018, ECLI:NL:RBAMS:2018:8713; Rb. Amsterdam 14 februari 2019, ECLI:NL:RBAMS:2019:971; Rb. Amsterdam 18 juli 2019, ECLI:NL:RBAMS:2019:5135; Rb. Den Haag 18 maart 2019, ECLI:NL:RBDHA:2019:2603; Rb. Amsterdam 18 juli 2019, ECLI:NL:RBAMS:2019:5135 en Rb. Gelderland 26 juli 2019, ECLI:NL:RBGEL:2019:2833.

10 Rb. Gelderland 26 juli 2019, ECLI:NL:RBGEL:2019:2833.

11 Zie o.a., Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504; Hof Amsterdam 4 mei 2018, ECLI:NL:GHAMS:2018:1550 en ECLI:NL:GHAMS:2018:1551 en Rb. Amsterdam 7 december 2018, ECLI:NL:RBAMS:2018:8713.

12 Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504.

13 Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504.

2. e-mailaccounts die voorkomen in de berichten van e-mailadressen en de contactpersonen van telefoontoestellen; en
3. (bij)namen van de verdachten in het onderzoek Tandem.

In Nederland is het zo dat op grond van artikel 149a Sv de officier van justitie verantwoordelijk is voor de samenstelling van de processtukken. Op grond van het 'relevantiecriterium' moet worden beoordeeld wat tot de processtukken dient te worden gerekend.[14] Het criterium betekent dat processtukken die stukken zijn die redelijkerwijs van belang kunnen zijn voor enige door de rechtbank in de zaak tegen de verdachte te nemen beslissing, zowel in ontlastende als in belastende zin.[15]

In deze zaak heeft het Openbaar Ministerie daaraan als volgt invulling gegeven. Op verschillende momenten in de periode van 9 februari 2017 tot en met 10 juli 2017 is aan de hand van zoektermen een specifieke dataset voor de zaak samengesteld, de zogenaamde "Tandem-dataset". De Tandem-dataset bevat drie categorieën berichten. In de eerste plaats zijn er berichten die door het Openbaar Ministerie als relevant voor de zaak *Tandem* zijn beoordeeld (categorie 1). Die berichten zijn in het dossier gevoegd. Een tweede categorie berichten heeft betrekking op berichten die volgens het Openbaar Ministerie niet relevant zijn voor het onderzoek Tandem, en ook niet voor andere opsporingsonderzoeken (categorie 2). Tot slot is er een categorie berichten die volgens het Openbaar Ministerie niet relevant zijn voor het onderzoek Tandem, maar waar zwaarwegende opsporingsbelangen in andere opsporingsonderzoeken aan inzage door de verdediging in de weg staan (categorie 3).

2.3 *Oordeel van de rechtbank*

De rechtbank Amsterdam stelt in haar vonnis voorop dat met betrekking tot het gebruik van Hansken geen sprake is van een deskundigenonderzoek en dat in die zin dus ook geen sprake kan zijn van een recht op tegenonderzoek/contra-expertise. De rechtbank geeft verder aan dat de verdediging de mogelijkheid heeft gekregen kennis te nemen van de berichten uit de bovengenoemde categorie 1 en 2. In berichten uit categorie 3 kreeg de verdediging geen inzage, omdat hier berichten in stonden die van belang waren voor andere opsporingsonderzoeken.

De rechtbank Amsterdam overweegt in meer detail dat de verdediging twee bezoeken heeft gebracht aan het NFI met een eigen, niet-geregistreerde, deskundige. Tijdens het eerste bezoek aan het NFI is aan de verdediging dezelfde presentatie gegeven die aan de rechercheurs die met Hansken werken wordt gegeven. Daarbij is de verdediging in de gelegenheid gesteld om vragen te stellen. De verdediging kon die dag – zeer kort – vrij en met behulp van Hansken in de Tandem-dataset zoeken. Daarbij had de verdediging toegang tot de berichten uit categorie 1 (gevoegd in het dossier) en categorie 2 (volgens het Openbaar Ministerie niet-relevante berichten). De berichten waarvan de inzage aan de verdediging is onthouden (categorie 3) waren niet toegankelijk voor de verdediging. Tijdens het tweede bezoek aan het NFI heeft de verdediging op beperkte wijze, zoals toegestaan door de rechter-commissaris, de samenstelling van de Tandem-dataset vanuit de Ennetcom-data kunnen controleren. Deze controle hield in dat de rechter-commissaris met behulp van een NFI-medewerker twaalf zoektermen in de Ennetcom-data heeft ingevoerd. In het bijzijn van de verdediging zijn die resultaten vergeleken met de resultaten in de dataset.

Samenvattend is duidelijk dat de rechters in deze zaak overtuigd zijn van de betrouwbaarheid van de data-analyse met Hansken en geen recht op contra-expertise op het systeem toewijzen. Daarbij overweegt de rechtbank uitvoerig waarom de verdediging voldoende mogelijkheden heeft gehad zelf zoekslagen uit te voeren in een set van geselecteerde gegevens die volgens de rechtbank relevante gegevens voor het proces bevatten. De verstrekte cd-rom met relevante gegevens zouden volgens de rechtbank verder voldoende leesbaar moeten zijn en de verdediging heeft in totaal 110 schriftelijke vragen aan het NFI kunnen stellen. Nadat die vragen zijn beantwoord, heeft de rechter-commissaris de deskundige nog gehoord, waarbij de verdediging in de gelegenheid is gesteld om vragen te stellen.

2.4 *Verhouding met het recht op een eerlijk proces*

De toegang tot het bewijs dat in een strafzaak tegen een verdachte wordt gebruikt, raakt het recht op een eerlijk proces in artikel 6 EVRM. In de Ennetcom-zaken betwist de verdediging dat zij in voldoende mate de toegang hebben gekregen tot het bewijsmateriaal. In dit kader is het deelrecht de 'equality of arms' uit artikel 6 EVRM het meest relevant. Het recht houdt in dat partijen in gelijke mate en voldoende in staat worden gesteld om het voor de zaak relevante materiaal te bestuderen en te betwisten.[16] Het Europees Hof van de Rechten voor de Mens (EHRM) heeft in jurisprudentie duidelijk gemaakt dat uit het beginsel is af te leiden dat de verdediging het recht heeft tot belastend én mogelijk ontlastend materiaal die de vervolgende autoriteiten als bewijsmateriaal in een strafzaak gebruiken.[17] De verdachte en

14 Op grond van art. 34 Sv kan de verdachte verzoeken specifieke stukken die van belang zijn bij de beoordeling van de zaak bij de processtukken te voegen. Echter, De Jong wijst erop dat een officier van justitie dergelijk onderzoek kan weigeren, omdat deze al heeft geoordeeld dat de gegevens geen processtukken zijn (oftewel: niet aan het relevantiecriterium voldoen) (De Jong 2018, p. 137). Zie uitgebreid over deze regeling R.H. Hermans, 'Nieuwe regels voor de kennisneming van processtukken', *Delikt en Delinkwent* 2012/27.

15 Zie hierover HR 7 mei 1996, *NJ* 1996/687, ECLI:NL:HR:1996:AB9820, m.nt. T.M. Schalken. Zie HR 22 januari 2008, *NJ* 2008/406, ECLI:NL:HR:2008:BA7648, m.nt. Borgers. Zie voor overwegingen hieromtrent met betrekking tot Ennetcom-data Rb. Gelderland 26 juli 2019, ECLI:NL:RBGEL:2019:2833.

16 Zie ook in de context van grootschalige data-analyes en algoritmen, M. Vetzo, J. Gerards & R. Nehmelman, *Algoritmes & grondrechten*, Boom Juridische Uitgevers 2018, p. 81 (hierna: Vetzo, Gerards & Nehmelman 2018). Zie ook, uitgebreider maar meer algemeen over dit deelrecht, F.P. Ölçer, *Recht op een eerlijk proces en bijzondere opsporing*, diss. Leiden, Nijmegen: Wolf Legal Publishers 2006, p. 123 e.v.

17 Zie o.a., EHRM 28 augustus 1991, nrs. 1170/84, 12876/87, 13468/87, ECLI:CE:ECHR:1991:0828JUD001117084, par. 67 (*Brandstetter/Oostenrijk*); EHRM 22 juli 2004, nrs. 39647/98 en 40461/98, ECLI:CE:ECHR:2004:1027JUD003964798, par. 46 (*Edwards en Lewis/Verenigd Koninkrijk*) en EHRM 18 maart 2014, nr. 40107/04, ECLI:CE:ECHR:2014:0318JUD004010704, par. 69-70 (*Beraru/Roemenië*).

verdediging moeten de mogelijkheid hebben het beschikbare materiaal te bestuderen en daarop te reageren. Daarvoor moeten zij voldoende tijd krijgen.[18]

Tegelijkertijd maakt het EHRM duidelijk dat het recht op transparantie en toegang tot het bewijsmateriaal niet oneindig is.[19] In de zaak *Doorson* laat het EHRM zelf ruimte bepaalde opsporingsmethoden geheim te houden, omdat anders de opsporingsbepaling te veel schade wordt toegebracht in verhouding tot het recht van de verdediging.[20] Ook kan van de verdediging onder omstandigheden worden verwacht dat zij aanvoeren voor welke reden zij toegang willen krijgen tot bewijsmateriaal.[21] Beperkingen tot toegang tot bewijsmateriaal moeten proportioneel zijn en met waarborgen zijn omgeven.[22] Het is echter nog onduidelijk welke beperkingen van toegang tot een dataset als bewijsmateriaal, als afgeleide van een grotere set aan gegevens, redelijk zijn. Het EHRM heeft zich nog niet over dit soort *big data*-vraagstukken uitgelaten.

2.5 *Toegang tot gegevens onderliggende aan de data-analyse*

Uit het bovenstaande blijkt dat toegang tot het materiaal in belastende en ontlastende zin jegens de verdachte een deelrecht is, dat wordt afgeleid uit een recht op een eerlijk proces in artikel 6 EVRM. De verdediging moet daarbij de mogelijkheid hebben de gegevens met betrekking tot de verdachte te bestuderen en te betwisten.

In de aangehaalde *Ennetcom*-zaak heeft de verdediging deze mogelijkheden in bepaalde mate gekregen (zie paragraaf 2.3). Het Openbaar Ministerie én de rechtbank Amsterdam lijken ervan uit te gaan dat de betrokken advocaat voldoende kennis zou moeten hebben om kennis te kunnen nemen van een grote hoeveelheid geselecteerde gegevens op een cd-rom als resultaat van de selectie die is gemaakt van een grotere dataset. Maar de vraag is of het leggen van die verantwoordelijkheid wel volledig bij de verdediging kan worden gelegd.[23] De verdediging gaf aan niet voldoende expertise en tijd te hebben de gegevens op de cd-rom te bestuderen. Wel kreeg de verdediging twee keer de mogelijkheid een beperkt aantal zoektermen in het Hanskensysteem te voeren. Zonder dossierkennis kunnen wij niet oordelen of dit voldoende is geweest om aan het deelrecht van de equality of arms te voldoen, maar het (onder voorwaarden) toegang verschaffen tot het Hansken-systeem voor zoekslagen van de verdediging is een belangrijke stap in de goede richting.

In het kader van de equality of arms heeft volgens ons het Openbaar Ministerie ook tot op zekere hoogte de verantwoordelijkheid om de mogelijkheid aan de verdediging te bieden de gegevens te analyseren die tegen de verdachte worden gebruikt, zonder te grote kosten voor het inhuren van bijzondere expertise. Om dat mogelijk te maken, kan bijvoorbeeld worden gedacht aan de inrichting van een *data room* waar de verdediging een dataset relatief eenvoudig kan bevragen.[24] Het gaat daarbij niet alleen om gegevens die het Openbaar Ministerie zelf voor een strafzaak heeft geselecteerd, maar ook om andere gegevens die gerelateerd zijn aan de verdachte en zijn vergaard als potentieel bewijsmateriaal jegens de verdachte, maar niet relevant werden geacht voor de strafzaak. Verzoeken waarbij *alle* beschikbare gegevens worden opgevraagd (ook van andere verdachten) of het opvragen van de broncode van de software die wordt gebruikt voor de data-analyse, lijken ons weinig kansrijk. Wel moet uiteraard aan de verdediging een uitleg worden geboden hoe de selectie uit een veel grotere set van gegevens tot stand is gekomen (zie ook uitgebreid paragraaf 3).

Het is zeker dat verdachten in de toekomst vaker te maken zullen krijgen met het resultaat van een selectie uit een grootschalige dataset dat in beslag genomen is in een andere stafzaak.[25] Daarbij kan gedacht worden aan de servers met transactiegegevens en communicatie van een *darknet market*[26], de transactiegegevens van een *bitcoin mixing service*[27] en andere gegevens uit versleutelde communicatiediensten.[28]

Een *silver bullet* als oplossing voor de kennisname en mogelijkheid tot betwisten van het resultaat van grote data-analyses kunnen wij niet geven. Het verdient echter aanbeveling dat het Openbaar Ministerie, met de Minister van Justitie en Veiligheid als eindverantwoordelijke, in samenspraak met de advocatuur tot bruikbare oplossingen komt.

18 Zij bijvoorbeeld EHRM 4 juli 2017, nr. 2742/12, ECLI:CE:ECHR:2017:0404JUD000274212, par. 151-152 (*Matanović/Kroatië*).

19 Vetzo & Gerards 2018, p. 120-121. Zie ook Hof Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4620. Art. 6 EVRM biedt geen ongeclausuleerd recht op kennisneming van stukken.

20 EHRM 26 maart 1996, 20524/92, ECLI:CE:ECHR:1996:0326JUD002052492, par. 70 (*Doorson/Nederland*) en EHRM 4 juli 2017, nr. 2742/12, ECLI:CE:ECHR:2017:0404JUD000274212, par. 152 (*Matanović/Kroatië*).

21 EHRM 4 juli 2017, nr. 2742/12, ECLI:CE:ECHR:2017:0404JUD000274212, par. 157 (*Matanović/Kroatië*).

22 Zie o.a. EHRM 16 februari 2000, nr. 27052/95, ECLI:CE:ECHR:2000:0216JUD002705295, par. 43 (*Jasper/Verenigd Koninkrijk*); EHRM 16 februari 2000, nr. 28901/95, ECLI:CE:ECHR:2000:0216JUD002890195, par. 54 (*Rowe en Davis/Verenigd Koninkrijk*)enEHRM24 juni2003,ECLI:CE:ECHR:2003:0624JUD003948298, par. 40-41 (*Dowsett/Verenigd Koninkrijk*).

23 Zie in dit kader ook de column van Arthur van der Biezen, 'Ennetcom-server als uitlokkingsmiddel', op Crimesite.nl van 24 juli 2019.

24 Zie ook, echter binnen de context van art. 30 Sv in plaats van 149a Sv, de toelichting op het artikel bij het Besluit procestukken in strafzaken, *Stb.* 2011, 602. Zie hierover ook in het ondernemingsrecht: J.H. de Wildt, 'Een blik over de grenzen: Vertrouwelijkheid, data rooms en confidentiality rings', *Tijdschrift voor Sanctierecht & Onderneming* 2017/1 en J.J.H. Joosten & J.C. Tijink, 'Gedagvaard in de VS: discovery', *Tijdschrift Ondernemingsrechtpraktijk* 2017/3.

25 Zie over de mogelijkheden van het combineren van gegevens en gebruiken van gegevens uit andere opsporingsonderzoeken ook: B.W. Schermer, 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht en handhaving* 2017(4).

26 Zie bijvoorbeeld Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, m.nt. J.J. Oerlemans.

27 Zie 'FIOD en OM halen witwasmachine voor cryptovaluta offline', Fiod.nl, 22 mei 2019.

28 Zie 'Doorbraak in onderscheppen cryptocommunicatie', 8 november 2018, Politie.nl, over de ontsleuteling van 258.000 berichten die zijn verstuurd via de app 'Ironchat'.

Die gaan volgens ons verder dan de verstrekking van de ruwe gegevens op een cd-rom. De inrichting van een *data room* waar de verdediging een dataset relatief eenvoudig kan bevragen is mogelijk een stap in de goede richting.

3. Geautomatiseerde besluitvorming binnen het strafvorderlijk proces

In het eerste deel van het artikel hebben wij beschreven hoe de politie geavanceerde data-analyse inzet om wijs te worden uit enorme hoeveelheden data. Naast geavanceerde data-analyse of 'data mining' kan ook kunstmatige intelligentie worden toegepast in het kader van de opsporing en vervolging. Zo zijn er onder de noemer *predictive policing* tal van experimenten binnen de politie die erop gericht zijn om met behulp van kunstmatige intelligentie crimineel gedrag te voorspellen.[29] Daarnaast kan kunstmatige intelligentie worden ingezet voor het nemen of ondersteunen van strafvorderlijke beslissingen door de officier van justitie, rechter-commissaris en rechter.

Het gebruik van kunstmatige intelligentie in diverse aspecten van het strafvorderlijk proces roept tal van juridische vragen op. In deze paragraaf richten wij ons op de vraag in hoeverre de inzet van kunstmatige intelligentie voor het geautomatiseerd nemen van strafvorderlijke beslissingen raakt aan de beginselen van een eerlijk proces. Meer specifiek richten wij ons op de vraag of de keuzes die een kunstmatige intelligentie maakt in het kader van de strafvordering transparant en uitlegbaar zijn. Hoe komt een kunstmatige intelligentie in de toekomst bijvoorbeeld tot het oordeel dat een individu verdacht is, dat voorlopige hechtenis noodzakelijk is, of dat een verdachte schuldig is?

3.1 *Motivering van beslissingen als voorwaarde voor een eerlijk proces*

Een cruciaal onderdeel van het recht op een eerlijk proces is dat het vonnis van de rechter deugdelijk gemotiveerd is.[30] Deze eis ligt besloten in artikel 121 Grondwet. Het moet voor de procespartijen en een hogere rechter te begrijpen zijn waarom een rechter tot zijn beslissing is gekomen.[31] In het kader van het strafrecht betekent dit dat de rechter de antwoorden op de vragen van artikel 348 Sv en in het bijzonder artikel 350 Sv moet onderbouwen.[32]

Naast het belang van een deugdelijke motivering tijdens het onderzoek ter terechtzitting is het ook van belang dat beslissingen in het vooronderzoek deugdelijk gemotiveerd zijn. Hier geldt wel dat in veel gevallen in dit stadium de motiveringsvereisten niet altijd expliciet zijn. De noodzaak tot onderbouwing van strafvorderlijk relevante beslissingen begint al bij de verdenking van een strafbaar feit. Dit moment is relevant, omdat de verdenking (artikel 27 Sv) het moment markeert waarop dwangmiddelen en opsporingsbevoegdheden kunnen worden ingezet tegen de betrokkene in een opsporingsonderzoek. Een opsporingsambtenaar moet in het proces-verbaal beschrijven op welke feiten en omstandigheden het vermoeden van schuld berust.[33] Wanneer een vermoeden van schuld 'redelijk' is, is echter niet scherp omlijnd.[34] Het vermoeden van schuld mag in ieder geval niet enkel subjectief zijn. Het vermoeden van schuld is nog niet redelijk als het enkel in de ogen van de opsporingsambtenaar bestaat: het oordeel moet op zichzelf redelijk zijn.[35] Zonder een dergelijke eis van objectiviteit zou het vermoeden oncontroleerbaar worden.[36]

Beslissingen gemaakt door de officier van justitie en de rechter-commissaris moeten ook onderbouwd, of op zijn minst controleerbaar zijn. Zo moet een rechter-commissaris bijvoorbeeld een bevel tot voorlopige hechtenis deugdelijk motiveren.[37] Voor beslissingen van de officier van justitie in relatie tot de inzet van dwangmiddelen en (bijzondere) opsporingsbevoegdheden geldt dat deze controleerbaar moeten zijn. Hoewel er doorgaans geen expliciete motiveringseis is, moet de zittingsrechter uiteindelijk wel de rechtmatigheid van het bewijs en de genomen beslissingen kunnen toetsen.[38]

3.2 *Algoritmische besluitvorming en het motiveringsvereiste*

Transparantie en legitimering van besluitvorming in alle facetten van de strafvordering is van groot belang. Het vereiste van deugdelijke motivering van besluitvorming geldt niet alleen voor mensen, maar strekt zich ook tot de middelen die zij gebruiken om tot beslissingen te komen. Zo oordeelde de bestuursrechter in 2017 bijvoorbeeld dat een bestuursorgaan een door een computersysteem genomen besluit deugdelijk moet motiveren:

> "Ter voorkoming van deze ongelijkwaardige procespositie rust in dit geval op genoemde ministers en de staatssecretaris de verplichting om de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit

29 Een voorbeeld in Nederland is het Criminaliteits Anticipatie Systeem (CAS).

30 Zie o.a. EHRM (GK) 29 november 2016, nr. 34238/09, ECLI:CE:ECHR:2016:1129 (*Lhermitte/België*), *EHRC* 2017/52, m.nt. K. Lemmens.

31 Vetzo, Gerards & Nehmelman 2018.

32 De artt. 348 tot en met 350 Sv vormen het 'beslismodel' voor de rechter ter terechtzitting. Art. 348 Sv stelt dat de rechter moet bepalen of de tenlastelegging geldig is, hij bevoegd is van het feit kennis te nemen, of de officier van justitie ontvankelijk is en of schorsing moet volgen. Art. 350 Sv stelt dat op basis van de tenlastelegging en het onderzoek ter terechtzitting bepaald moet worden of de feiten bewezen zijn en zo ja, welk strafbaar feit dit oplevert. Verder moet de rechter bepalen of de verdachte strafbaar is, en zo ja, welke straf of maatregel de verdachte wordt opgelegd.

33 J. Naeyé, hoofdstuk 5.3.1, in: *Handboek Strafzaken* 2005, par. 5.3.

34 J. Naeyé, hoofdstuk 5.3.1, in: *Handboek Strafzaken* 2005, par. 5.3. Zie ook uitgebreid in de context van algoritmen: R.A. Hoving, 'Verdacht door een algoritme. Kan predictive policing leiden tot een redelijke verdenking?', *Delikt en Delinkwent* 2019/41.

35 *Kamerstukken II* 2013/14, 286, nr. 3, p. 39.

36 A.L. Melai & M.S. Groenhuijsen e.a., 'Feiten of omstandigheden (art. 27 lid 1)', *Wetboek van Strafvordering* 2013.

37 Zie in dit kader: College voor de Rechten van de Mens (2017), Samenvatting Tekst en Uitleg, *Onderzoek naar de motivering van voorlopige hechtenis.*

38 Zie o.a. EHRM 12 mei 2000, nr. 35394/97, ECLI:CE:ECHR:2000:0512JUD003539497 (*Khan/Verenigd Koninkrijk*) en EHRM (GK) 10 maart 2009, nr. 4378/02, ECLI:CE:ECHR:2009:0310JUD000437802, (*Bykov/Rusland*).

> eigen beweging openbaar te maken op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn. Deze volledige, tijdige en adequate beschikbaarstelling moet het mogelijk maken de gemaakte keuzes en de gebruikte gegevens en aannames te beoordelen of te laten beoordelen en zo nodig gemotiveerd te betwisten, zodat reële rechtsbescherming tegen besluiten die op deze keuzes, gegevens en aannames zijn gebaseerd mogelijk is, waarbij de rechter aan de hand hiervan in staat is de rechtmatigheid van deze besluiten te toetsen."[39]

De eis dat de besluitvorming door de kunstmatige intelligentie transparant is geeft invulling aan het beginsel van eerlijk proces in het algemeen en dat van de equality of arms uit artikel 6 EVRM in het bijzonder.[40]

De Wet politiegegevens, die een belangrijke rol speelt bij dataverwerking in het kader van de opsporing, verbiedt geautomatiseerde besluitvorming zonder menselijke tussenkomst, wanneer dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft (artikel 7a Wpg).[41] Slechts wanneer er sprake is van voorafgaande menselijke tussenkomst (als in voor de definitieve beslissing wordt genomen) en duidelijke informatievoorziening aan de betrokkene is geautomatiseerde besluitvorming zonder menselijke tussenkomst toegestaan. Deze bepaling gaat evenwel niet in op de motiveringsvereisten voor geautomatiseerde besluiten. De in het artikel genoemde verplichte informatievoorziening is primair gericht tot de betrokkene, en bedoeld om deze in staat te stellen zijn standpunt kenbaar te maken of uitleg over het na een dergelijke beoordeling genomen besluit te krijgen en om op te komen tegen het besluit.[42] Gesteld zou kunnen worden dat deze informatievoorziening ook de zittingsrechter in staat zou moeten kunnen stellen om de rechtmatigheid van het besluit te toetsen. Om deze eis van uitlegbaarheid beter tot uiting te laten komen lijkt een meer expliciet motiveringsvereiste in wetgeving wenselijk.

In het kader van het moderniseringstraject Wetboek van strafvordering adviseerde de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops) om de uitlegbaarheid van geautomatiseerde data-analyse beter te verankeren in het nieuwe Wetboek van Strafvordering:

> "De wetgever dient aandacht te besteden aan geautomatiseerde data-analyse in het moderniseringstraject in brede zin, en daarbij de mogelijkheid te overwegen in het Wetboek van Strafvordering de momenteel impliciete eis van uitlegbaarheid van strafvorderlijke beslissingen te expliciteren indien deze beslissingen (mede) op geautomatiseerde data-analyse worden gebaseerd."[43]

Het kabinet ten slotte is ook de mening toegedaan dat transparantie en uitlegbaarheid van algoritmes van belang is. Op 8 oktober 2019 stuurde de Minister van Rechtsbescherming een brief naar de Tweede Kamer met een analyse van de waarborgen tegen risico's van data-analyse door de overheid.[44] Het kabinet hecht eraan dat geautomatiseerde data-analyses door de overheid zo transparant mogelijk zijn en ziet transparantie van algoritmes als een mechanisme dat van groot belang is voor een effectieve rechtsbescherming van de burger.[45]

3.3 *Motivering in de praktijk*

Uit het voorgaande mogen we concluderen dat het motiveringsvereiste zich ook uitstrekt tot algoritmische besluitvorming ingezet ten behoeve van de strafvordering, ook al is dat vaak niet al te expliciet. Het belang hiervan wordt ook door het kabinet ondersteund. Hoe deugdelijk de motivering van algoritmische besluitvorming in de praktijk moet zijn, is echter nog onduidelijk.[46] Grofweg zijn er in de context van het strafrecht twee problemen met betrekking tot een voor deugdelijke motivering noodzakelijke transparantie van algoritmes, te weten 1) complexiteit, en 2) de angst voor manipulatie/misbruik.

3.3.1 *Complexiteit*

Het eerste probleem met betrekking tot de transparantie is inherent aan het gebruik van complexe algoritmes: naarmate algoritmes complexer worden zijn zij moeilijker te bevatten voor mensen. Bij de meest complexe algoritmes (zoals bijvoorbeeld *deep learning* algoritmes) zijn de resulterende modellen dusdanig complex dat zij letterlijk onbegrijpelijk zijn voor mensen.[47] Met transparantie van het gebruikte besluitvormingsmodel is de strafvorderlijke beslissing dus nog niet deugdelijk gemotiveerd, want deze is onbegrijpelijk. Met andere woorden: transparantie staat niet gelijk aan begrijpelijkheid.

39 ABRvS 17 mei 2017, *Computerrecht* 2017/256, m.nt. B.M.A. van Eck.
40 ABRvS 17 mei 2017, *Computerrecht* 2017/256, m.nt. B.M.A. van Eck, p. 395.
41 Dit zal in een strafproces natuurlijk al snel het geval zijn.
42 MvT bij het Wijzigingsvoorstel Wet politiegegevens, *Kamerstukken II* 2017/18, 34889, nr. 3, p. 68.
43 Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018), Regulering van opsporingsbevoegdheden in een digitale omgeving (Commissie Koops), s. l., juni 2018, p. 28.
44 Ministerie van Justitie en Veiligheid (2019), *Waarborgen tegen risico's van data-analyses door de overheid*, 8 oktober 2019, kenmerk 2717062.
45 Ministerie van Justitie en Veiligheid (2019), *Waarborgen tegen risico's van data-analyses door de overheid*, 8 oktober 2019, kenmerk 2717062, p. 7.
46 Het gebruik van kunstmatige intelligentie binnen de strafvordering is overigens geenszins nieuw. Met een wat cynische blik zou je kunnen stellen dat wat vroeger juridische kennissystemen werd genoemd nu '*gerebrand*' is als *machine learning*. Het belangrijkste verschil met vroeger is wel dat de ontwikkelingen veel sneller gaan en de complexiteit van de gebruikte modellen veel groter is. Hierdoor ontstaan met name problemen op het gebied van de transparantie en uitlegbaarheid van geautomatiseerde beslissingen.
47 In feite is 'transparantie van algoritmes' geen accurate weergave van de problematiek. In veel gevallen zijn de gebruikte algoritmes namelijk openbaar en transparant. Het gaat veeleer om de transparantie/uitlegbaarheid van het model dat is gebouwd met behulp van de algoritmes en de beschikbare (trainings)data. In *machine learning* is een model een mathematische benadering van de werkelijkheid op basis van de beschikbare data. Een algoritme leert van de data en komt op basis daarvan tot een wiskundig model dat in staat is om nieuwe input data te vertalen naar een output.

Het is voor de discussie over transparantie van algoritmes van belang om een duidelijk onderscheid te maken tussen transparantie en begrijpelijkheid. Transparantie is een noodzakelijke voorwaarde voor begrijpelijkheid, maar staat daar niet aan gelijk. Kim *et al.* geven de volgende definitie van begrijpelijkheid (*interpretability*):

> "the degree to which a human can consistently predict the model's result."[48]

Met andere woorden, op basis van de *input* kun je altijd bepalen wat de *output* is. Zo lang er een volledig begrip is van de werking van het model (je kan op basis van de *input* en je begrip van het model altijd voorspellen wat de uitkomst is) spreken we van 'globaal interpretabele modellen'.[49] Transparantie is alleen een volwaardig alternatief voor deugdelijke motivering bij dergelijke globaal interpretabele modellen. De meeste complexe modellen (waar nu ook de meeste successen mee worden geboekt) zijn echter niet interpretabel. Vaak wordt voor dit type modellen de term *black box* model gehanteerd, maar dit is eigenlijk wat misleidend. Het probleem is namelijk niet dat je het systeem niet kunt bekijken, dat kan wel degelijk, je kunt het alleen niet bevatten.[50]

Uitgangspunt van het kabinet is dat overheidsorganisaties géén algoritmes mogen hanteren die te complex zijn om redelijkerwijs te kunnen worden uitgelegd.[51] Deze 'harde lijn' van het kabinet betekent echter niet dat elk gebruik van complexe algoritmes in de strafrechtketen daarmee onmogelijk is geworden. Wanneer een model niet globaal interpretabel is, moet gekeken worden in hoeverre een individuele beslissing *ex post* verklaard kan worden. Er is dan geen sprake van *global interpretability* maar van *local interpretability*. Het systeem als geheel is dus niet begrijpelijk, maar een individuele beslissing kan wel uitgelegd/verklaard worden. Een voorbeeld van een dergelijke oplossing is LIME (*Locally Interpretable Model-agnostic Explanations*).[52] LIME geeft een overzicht van de relevante attributen (*features*) uit de input data en hun geschatte weging in de uiteindelijke beslissing.[53] Zo zou LIME bijvoorbeeld gebruikt kunnen worden om te kijken welke attributen hebben bijgedragen aan het besluit van het model om een bepaalde persoon als verdachte aan te merken.

Onder de noemer *Explainable AI (xAI)* wordt momenteel veel onderzoek gedaan naar methoden zoals LIME om de begrijpelijkheid van AI systemen te vergroten.[54] Uitlegbaarheid zou daarmee het vertrouwen in AI systemen moeten vergroten.[55] Vanuit het perspectief van het recht op een eerlijk proces is hierbij overigens nog in het bijzonder relevant dat enkel de uitleg waarom een beslissing is genomen nog niet noodzakelijkerwijs de genomen beslissing legitimeert. Hiervoor is het noodzakelijk dat het handelen in lijn is met de formele eisen die het Wetboek van Strafvordering aan dat handelen stelt. Idealiter vallen uitleg en legitimering samen en is er dus sprake van een deugdelijke motivering van een legitieme beslissing.

3.4 *Manipulatie*

Het tweede probleem is meer van bestuurlijke aard. Het idee leeft dat wanneer een algoritme (lees: een besluitvormingsproces) transparant is, kwaadwillenden het systeem gaan manipuleren of beïnvloeden om tot voor hen gunstige uitkomsten te komen ('*gaming the system*'). Inzicht in algoritmische besluitvorming kan daarmee de effectiviteit van de opsporing ondermijnen.

Een gerelateerd risico – dat reeds in het eerste deel is besproken is – is dat dan ook de onderzoeksgegevens integraal openbaar moeten worden gemaakt, hetgeen voor (bedreigde) getuigen, slachtoffers et cetera een risico vormt. De effectiviteit van de opsporing is dus niet noodzakelijkerwijs gebaat bij transparantie. Sterker nog, het kabinet lijkt in haar Kamerbrief het gebruik van algoritmes in de opsporing uit te zonderen van het transparantiebeginsel door hen in een aparte categorie te plaatsen:

> "Categorie 5. Waar de uitlegbaarheid/transparantie niet wenselijk is om de werkzaamheid te behouden en ontwijkende/calculerend gedrag te voorkomen. Dit geldt bijvoorbeeld bij algoritmes die ten behoeve van opsporing en cybersecurity worden ingezet."[56]

Dit uitgangspunt van het kabinet staat op gespannen voet met artikel 6 EVRM en de (impliciete) eisen in het Wetboek van Strafvordering tot deugdelijke motivering van opsporings- en strafvorderlijke beslissingen. Van der Sloot en van Schendel wijzen in dit kader op het risico van een Kafkaëske situatie waarbij de burger berecht kan worden op basis

48 B. Kim, R. Khanna & O. Koyejo, 'Examples are not enough, learn to criticize! criticism for interpretability', in: *Advances in Neural Information Processing Systems* 2016.

49 Zie M. Ribeiro, T. Singh & C. Guestrin, '*Why should i trust you?: Explaining the predictions of any classifier*', in: 'Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining', *ACM* 2016, pp. 1135-1144 (hierna: Ribeiro e.a. 2016); C. Molnar, *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable* 2019; A. Adadi & M. Berrada, 'Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence' (XAI). *IEEE Access* 2018, Volume 6, pp. 52138-52160 (hierna: Adadi & Berrada 2018).

50 Zie in dit kader: D. Card, *The "black box" metaphor in machine learning*, 2017. Beschikbaar op: https://towardsdatascience.com/the-black-box-metaphor-in-machine-learning-4e57a3a1d2b0.

51 Ministerie van Justitie en Veiligheid (2019), *Waarborgen tegen risico's van data-analyses door de overheid*, 8 oktober 2019, kenmerk 2717062.

52 Ribeiro e.a. 2016.

53 L. Hulstaert, 'Understanding model predictions with LIME', 2018. Beschikbaar op: https://towardsdatascience.com/understanding-model-predictions-with-lime-a582fdff3a3b.

54 Zie Adadi & Berrada 2018.

55 A. Holzinger, C. Biemann, C. Pattichis & D. Kell, 'What do we need to build explainable AI systems for the medical domain?', arXiv preprint 2018 arXiv:1712.09923; D. Doran, S. Schulz & T.R. Besold, 'What Does Explainable AI Really Mean? A New Conceptualization of Perspectives', arXiv preprint 2017 arXiv:1710.00794.

56 Ministerie van Justitie en Veiligheid (2019), *Waarborgen tegen risico's van data-analyses door de overheid*, 8 oktober 2019, Bijlage 1: Richtlijnen voor het toepassen van algoritmes door overheden, p. 8.

van informatie waar hij of zij zelf geen toegang tot heeft.[57] Het standpunt van het kabinet laat zich ook moeilijk rijmen met de eerdere harde lijn dat onuitlegbare algoritmes geen plaats hebben binnen de overheid. Juist op een plek waar het overheidshandelen zo diep kan ingrijpen in het leven van burgers is het noodzakelijk dat de geautomatiseerde besluitvorming zo transparant en begrijpelijk mogelijk is.

Een mogelijke middenweg om dit probleem op te lossen is selectieve openbaarmaking van informatie en inzicht in de algoritmes, data en modellen. Zo hoeft een model dat wordt gebruikt in de opsporing niet openbaar te worden gemaakt, maar kan het in het kader van een concrete strafzaak mogelijk wel getoetst worden door de rechter en de verdediging, al dan niet via een externe deskundige.[58]

4. Conclusie

De toepassing van kunstmatige intelligentie ten behoeve van de strafvordering kan op gespannen voet staan met het recht op een eerlijk proces.

Na grootschalige data-analyses kunnen verdachten geconfronteerd worden met het resultaat van de data-analyse, in belastende zin. Uit het recht op een eerlijk proces in artikel 6 EVRM kan het deelrecht worden afgeleid dat de verdachte toegang moet hebben tot gegevens die tegen hem worden gebruikt in belastende en ontlastende zin. De verdediging moet daarbij de mogelijkheid hebben de gegevens met betrekking tot de verdachte te bestuderen en te betwisten. Het Openbaar Ministerie heeft tot op zekere hoogte ook zelf een verantwoordelijkheid de technische mogelijkheden aan de verdediging te bieden om de gegevens in een strafproces te bestuderen en te betwisten. In de toekomst zullen nog veel zaken volgen waarbij verdachten geconfronteerd worden met het resultaat van een grootschalige data-analyse die zijn veiliggesteld in andere strafzaken.

Bij verdergaande toepassingen van kunstmatige intelligentie binnen de strafrechtketen, meer specifiek geautomatiseerde besluitvorming, is het van belang dat de motivering van de besluitvorming deugdelijk is. Dit betekent dat de gekozen toepassingen transparant, uitlegbaar en controleerbaar zijn. De complexiteit van algoritmische besluitvorming en het voornemen van het kabinet om algoritmische besluitvorming in de opsporing *niet* te onderwerpen aan de eisen van transparantie en uitlegbaarheid zijn in dat kader zorgelijk, omdat zij een bedreiging vormen voor de equality of arms en het recht op een eerlijk proces.

57 B. van der Sloot & S. van Schendel, 'De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving', *WODC* 2019, p. 143.

58 Hierbij past wel de waarschuwing gegeven door Vetzo, Gerards en Nehmelman dat er een risico bestaat dat computer experts hierdoor mogelijk een (te) prominente rol in het strafproces gaan spelen, hetgeen ook kan leiden tot een *inequality of arms*. Zie: Vetzo, Gerards & Nehmelman 2018, p. 118.