Artikel

De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding

Mr. dr. M. (Maša) Galič*

1. Inleiding

Big data analytics, machine learning en *artificial intelligence* ('algorithmische systemen') vinden steeds meer hun weg naar het strafrecht. In deze context wijzen juristen en andere wetenschappers erop dat de automatisering die dergelijke algorithmische systemen meebrengen, ons uitdaagt om fundamentele strafrechtelijke kwesties te heroverwegen.¹ Daarbij gaat het onder meer om de begrijpelijkheid en transparantie van de rechterlijke besluitvorming, de rechten van de verdediging en het beginsel van *equality of arms*. Deze kwesties doen zich niet alleen voor in technologisch zeer complexe en controversiële zaken (zoals bij het gebruik van *machine learning*-algoritmes voor de beoordeling van vluchtrisico en recidive in procedures voor borgtocht of voorwaardelijke vrijlating in de Verenigde Staten²), maar ook met

betrekking tot 'meer eenvoudige'³ algorithmische systemen en schijnbaar onschuldige toepassingen. Een goed actueel voorbeeld van het laatste is het gebruik van geavanceerde zoekmachines in strafprocedures die efficiënt onderzoek van omvangrijke digitale datasets mogelijk maken. Denk hierbij bijvoorbeeld aan de zoekmachine Hansken en de gehackte berichtendiensten Ennetcom, Encrochat en SkyECC.⁴ In dit artikel onderzoek ik de vraag hoe het beginsel van *equality of arms* moet worden geïnterpreteerd om toegang tot omvangrijke datasets voor de verdediging mogelijk te maken en om het toetsen van de betrouwbaarheid van het bewijsvergaringproces te faciliteren.

De structuur van het artikel is als volgt. Allereerst beschrijf ik de actuele ontwikkelingen rondom digitaal bewijs. Vervolgens bespreek ik het *equality of arms*-beginsel en de in dat kader relevante jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM). Daarbij richt ik mij in het bijzonder op de bestaande rechten van de verdediging met betrekking tot de toegang tot omvangrijke datasets en geavanceerde zoekinstrumenten. Aan de hand van deze jurisprudentie

41

* Maša Galič is universitair docent straf(proces)recht bij de Vrije Universiteit Amsterdam.

1. Zie bijv. B.W. Schermer en J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht*, 2020/3; A. Završnik, 'Criminal Justice, Artificial Intelligence Systems, and Human Rights', *ERA Forum*, 2020/20, 567-583; U. Pagallo en S. Quattrocolo, 'The Impact of AI on Criminal Law, and Its Twofold Procedures', in W. Barfield en U. Pagallo (Eds.), *Research Handbook on the Law of Artificial Intelligence*, Londen: Routledge, 2018.

2. Zie bijvoorbeeld R.F. Lowden (2018), 'Risk Assessment Algorithms: The Answer to an Inequitable Bail System?' *North Carolina Journal of Law & Technology* 2018/19(221).

3. Deze 'meer eenvoudige' algorithmische systemen kunnen rule-based zijn, waarbij de stappen, methodologieën en resultaten kunnen worden herleid tot voorgeprogrammeerde instructies die door een mens worden ingevoerd, en over het algemeen bestaande regels of theorieën vertegenwoordigen. Ze kunnen echter zeer geavanceerd zijn, met honderden of zelfs duizenden stappen, zodat ze toch moeilijk uit te leggen zijn; M. Veale, *Algorithms in the Criminal Justice System*, Londen: The Law Society of England and Wales, 2019, p. 10-11.

4. Zie bijvoorbeeld C. Driessen en J. Meeus, 'Advocaten strijden tegen informatie uit "cryptophones"', *NRC*, 15 maart 2021.

onderzoek ik vervolgens de noodzaak van ruimere en aanvullende waarborgen, zowel met betrekking tot de toegang tot datasets, als met betrekking tot de kwestie van de betrouwbaarheid van digitaal bewijsmateriaal dat afkomstig is uit zoekinstrumenten voor omvangrijke gegevens. Tot slot reflecteer ik op de vraag hoe de Nederlandse strafrechtspraktijk zich verhoudt tot de jurisprudentie van het EHRM.

2. De opkomst van het digitaal bewijs

Terwijl in het verleden getuigenverklaringen en fysiek bewijs centraal stonden in het strafproces, draait het tegenwoordig steeds meer om digitaal bewijs en omvangrijke digitale datasets, die tot stand komen door het gebruik van verschillende soorten opsporingsbevoegdheden zoals telecommunicatiebewaking en de inbeslagname van computers, smartphones of servers. De rechten van de verdediging ten aanzien van getuigenverklaringen en fysiek bewijsmateriaal zijn in de loop der tijd grondig uitgewerkt, met name in het kader van het recht op een eerlijk proces in de zin van artikel 6 EVRM. Een dergelijke uitwerking heeft echter nog niet plaatsgevonden met betrekking tot grote datasets en de geavanceerde manieren om daaruit informatie (en bewijsmateriaal) te extraheren.

In het licht van deze opmerkelijke verschuiving ten aanzien van de bewijsvoering in het strafrecht hebben advocaten en wetenschappers aangevoerd dat geavanceerde technologische zoekinstrumenten de positie van het Openbaar Ministerie (OM) aanzienlijk versterken ten koste van de verdediging. De verdediging heeft over het algemeen geen toegang tot deze instrumenten en de volledige dataset die in het opsporingsonderzoek is verzameld,⁵ en zij heeft slechts beperkte toegang tot bepaalde delen van de secundaire dataset die door het OM zijn geselecteerd (op basis van de eerste zoekacties en door vastgestelde zoektermen) als potentieel relevant materiaal voor de zaak. De verdediging heeft over het algemeen ook geen toegang tot het geavanceerde zoekinstrument (ook wel *e-discovery* genoemd),⁶ dat het überhaupt mogelijk maakt om effectief te zoeken binnen zeer

grote hoeveelheden gegevens. Dit heeft tot gevolg dat de verdediging weinig invloed heeft op wat in een strafzaak als relevante informatie geldt en nauwelijks mogelijkheden heeft om ontlastend bewijs te vinden. Dit leidt vervolgens tot een aanzienlijke machts- en kennisasymmetrie.

Bovendien heeft de exponentiële groei van (verschillende soorten) gegevens de traditionele methoden voor het zoeken in databanken naar relevante informatie ontoereikend gemaakt, zodat nieuwe, complexere zoektechnieken moesten worden ontwikkeld.⁷ Deze zoektechnieken maken het onder andere mogelijk de analyse van ongestructureerde gegevens te automatiseren en patronen en verbanden tussen grote hoeveelheden gegevens te ontdekken (*datamining*). De werking van dergelijke nieuwe technieken is echter ondoorzichtig en moeilijk uit te leggen. Dit leidt tot een afgeschermd proces van bewijsverzameling dat de betrouwbaarheid van dit bewijs kan ondermijnen. Al deze kwesties speelden onlangs in Nederland naar aanleiding van de inbeslagname van de servers van Ennetcom, Encrochat en Sky ECC, en de vervolgingen die plaatsvonden op basis van gegevens die uit de servers werden gehaald door het gebruik van 'Hansken', een geavanceerde forensische zoekmachine.⁸

De opkomst van het digitaal bewijs bemoeilijkt de positie van de verdediging. De vraag is of nog gesproken kan worden van *equality of arms* tussen het OM en de verdediging. Om te bepalen welke rechten de verdediging op basis van dit fundamentele beginsel zouden moeten toekomen als het gaat om omvangrijke datasets en geavanceerde zoekinstrumenten, is het van belang te onderzoeken hoe het beginsel door het EHRM is uitgelegd.

3. Zoeken naar omvangrijke datasets met geavanceerde zoekinstrumenten en *equality of arms* in de jurisprudentie van het EVRM

3.1 Het doel en de reikwijdte van *equality of arms* in strafzaken

Het beginsel van *equality of arms* is een centraal element van het recht op een eerlijk proces, zoals neergelegd in art. 6 EVRM. In het algemeen heeft het beginsel tot doel ervoor te zorgen dat de partijen in strafzaken gelijke procedurele kansen krijgen om de zaak voor te bereiden, om hun argumenten voor te leggen aan de rechter en om proactief deel te nemen aan de gehele

5. Zie bijvoorbeeld M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en grondrechten*, Den Haag: Boom Juridisch, 2018; Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press, 2016; G.J. Zwenne en W.A.M. Steenbruggen, 'Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning', in *Big data in de zorg: Preadvies uitgebracht voor de Vereniging voor Gezondheidsrecht*, jaarvergadering 31 maart 2017. Preadvies / Vereniging voor Gezondheidsrecht no. 2017, Den Haag: Sdu Uitgevers, p. 73-99; D. de Jonge, 'Verdedigen in tijden van digitale bewijsvoering' in P. Meij e.a. (red.), *Aan de slag: Liber amicorum Gerard Hamer*, Den Haag: Sdu Uitgevers, 2018; M. Simonato, 'Defence rights and the use of information technology in criminal procedure', *International Review of Penal Law* (2014) 85, p. 261.

6. J. Henseler, *E-Discovery: op zoek naar de digitale waarheid*, HvA publicaties, Amsterdam: Amsterdam University Press, 2010.

7. Henseler 2010, p. 29.

8. Zie bijvoorbeeld EDRI, 'Dutch digital investigation: Pushing the boundaries of legality' (blog), 2017, verkregen op 2 oktober 2020 van <https://edri.org/our-work/dutch-digital-investigation/>.

procedure.⁹ Als zodanig speelt het beginsel een sleutelrol in de uitwerking van de rechten van de verdediging.¹⁰

Uiteraard is het nauwelijks mogelijk om de partijen in het strafproces geheel gelijke ‘wapens’ te geven. Vanaf het begin van het strafproces bevinden het OM en de verdediging zich in zeer verschillende posities. Het OM heeft duidelijk de overhand, omdat het de beschikking heeft over opsporingsdiensten en steeds complexere digitale technologie (bijvoorbeeld het gebruik van malware bij hackbevoegdheden). De verdediging heeft geen van deze middelen. Gelijke ‘wapens’ in het strafprocesrecht – met name in gematigd inquisitoire rechtssystemen – kan dan ook alleen maar worden opgevat als een bepaalde gelijkwaardigheid (*certain equivalence*),¹¹ of als een eerlijk evenwicht (*fair balance*).¹² *Equality of arms* houdt volgens het EHRM in dat ‘iedere partij een redelijke kans moet krijgen om haar zaak te presenteren onder voorwaarden die haar niet benadelen *vis-à-vis* haar tegenstander’.¹³ Het gebruik van de term ‘redelijk’ toont aan dat *equality of arms* vereist dat de procedurele rechten die de procespartijen toekomen worden gerespecteerd, ten minste voorzover de verschillende rollen van de partijen dat toelaten. Het doel is te zorgen voor een ‘redelijk symmetrisch evenwicht om een gelijke behandeling gedurende de gehele procedure te waarborgen’.¹⁴ De kern van *equality of arms* bestaat echter uit een *effectieve* en niet louter *theoretische* kans om bij te dragen aan de verdediging en om het door het OM aangedragen bewijs te betwisten.¹⁵

In de rechtspraak van het EHRM wordt het beginsel van *equality of arms* doorgaans in één zin genoemd met het recht op een adversaire proces.¹⁶ Er is inderdaad sprake van een aanzienlijke overlap en onderlinge samenhang tussen de begrippen, maar *equality of arms* wordt over het algemeen gezien als een ruimer beginsel dan het adversaire proces. Terwijl het recht op een adversair proces zich toespitst op kwesties van openbaarheid (het recht op toegang tot het dossier) en de mogelijkheid om het bewijsmateriaal aan te vechten en de argumenten van de tegenpartij te betwisten (impliciet in art. 6, lid 1 EVRM), strekt *equality of arms* zich uit tot een ruimere lijst van procedurele voorwaarden in strafprocedures (art. 6, lid 3 EVRM), waaronder het recht

om ontlastend bewijsmateriaal te verzamelen.¹⁷ Bovendien zijn de specifieke waarborgen in artikel 6, leden 2 en 3 EVRM niet uitputtend; het proces kan dus oneerlijk zijn, ondanks de naleving van de specifiek genoemde waarborgen.¹⁸ Deze openheid en flexibiliteit maken dat *equality of arms* bij uitstek een geschikte basis biedt voor een meer extensieve interpretatie van bestaande of de ontwikkeling van nieuwe rechten voor de verdediging die bij de opkomst van digitale bewijsmiddelen nodig zijn.

3.2 Toegang tot omvangrijke digitale datasets

Gezien het feit dat bewijskwesties in strafzaken tegenwoordig steeds meer betrekking hebben op digitaal bewijs dat afkomstig is uit omvangrijke datasets, is toegang tot deze datasets van groot belang voor de verdediging, zowel om te reageren op het standpunt van het OM als om zelf ontlastend bewijs te verzamelen.

In dit verband moet een onderscheid worden gemaakt tussen verschillende datasets en soorten gegevens. Ten eerste moet een onderscheid worden gemaakt tussen de ‘volledige dataset’ die bestaat uit alle gegevens die in een bepaald onderzoek zijn verzameld en de ‘secundaire dataset’ die het resultaat is van de eerste zoekacties van de volledige dataset door het OM. Dit onderscheid kan goed worden geïllustreerd aan de hand van de Ennetcom-Tandem-zaak uit 2018 voor de Rechtbank Amsterdam.¹⁹ In de Ennetcom-Tandem-zaak vormde alle gegevens (3,5 miljoen datapunten van 19.000 personen)²⁰ op de in beslag genomen Ennetcom-server de volledige dataset. Het OM heeft in de zaak vervolgens drie zoekopdrachten uitgevoerd in deze dataset met behulp van specifieke zoektermen, zoals trefwoorden (bijvoorbeeld bijnamen van verdachten of termen die vaak worden gebruikt om een moord of drugs aan te duiden), e-mailadressen en PIN-nummers.²¹ Deze zoekactiviteiten hebben geleid tot de samenstelling van de Tandem-dataset, een secundaire dataset, die het OM vervolgens vrijelijk verder kon doorzoeken om bewijs in de zaak te vinden.

Ten tweede moet een onderscheid worden gemaakt tussen de gegevens die door het OM relevant worden geacht en de gegevens die niet relevant worden geacht. Van de gegevens die relevant worden geacht, zal een nog kleinere selectie daadwerkelijk als bewijs worden beschouwd en deel uitmaken van het dossier (dat als een ‘tertiaire dataset’ kan worden beschouwd). Zo werd de Tandem-dataset verder onderverdeeld in drie categorieën van gegevens: (1) gegevens die door het OM relevant werden geacht voor de zaak en die aan het dossier werden toegevoegd; (2) gegevens die door het OM irrelevant werden geacht voor de zaak (en andere onderzoeken); en (3) gegevens die door het OM irrelevant

9. O. Sidhu, *The concept of equality of arms in criminal proceedings under article 6 of the European Convention on Human Rights*, Morsel: Intersentia, 2017, p. 4; S. Trechsel, *Human Rights in Criminal Proceedings*, Oxford: Oxford University Press, 2005, p. 104.

10. Trechsel 2005, p. 84.

11. Trechsel 2005, p. 96.

12. B. Rainey, E. Wicks en C. Ovey, *The European Convention on Human Rights*, Oxford: Oxford University Press, 2017, p. 291.

13. EHRM 22 februari 1996, nr. 17358/90, 59/1994/506/588 (*Bulut v. Oostenrijk*).

14. Sidhu 2017, p. 95.

15. Pagallo en Quattrocchio 2018, p. 396.

16. Zie bijvoorbeeld EHRM 28 augustus 1991, ECLI:CE:ECHR:1991:0828JUD001117084 (*Brandstetter t. Oostenrijk*); EHRM 16 februari 2000, ECLI:CE:ECHR:2000:0216JUD002705295 (*Jasper t. VK*); EHRM 25 september 2001, ECLI:CE:ECHR:2001:0925JUD004478798 (*P.G. en J.H. t. VK*).

17. Trechsel 2005, p. 95; Sidhu 2017, p. 97-98.

18. Zie bijvoorbeeld EHRM 27 februari 1980, ECLI:CE:ECHR:1980:0227JUD000690375 (*Deweert t. België*).

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

20. Rb. Gelderland, 26 juni 2019, ECLI:NL:RBGEL:2019:2833, p. 6.

21. Rb. Amsterdam 19 april 2018, a.w., 6.4.2, p. 8-9.

werden geacht voor deze zaak, maar die relevant zouden kunnen zijn voor andere onderzoeken.²²

Hoewel de jurisprudentie van het EHRM duidelijk maakt dat in beginsel volledige openbaarheid van het dossier vereist is, is het voorts nog onduidelijk in hoeverre en op welke manier de verdediging op grond van artikel 6 EVRM toegang moet krijgen tot de volledige en secundaire dataset. Het vervolg van deze paragraaf heeft daarom betrekking op de toegang van de verdediging tot de volledige en de secundaire dataset.

3.2.1 Indirecte toegang tot de volledige dataset

In 2019 deed het EHRM voor het eerst een specifieke uitspraak over de toegang tot de volledige dataset voor de verdediging. In *Sigurður Einarsson e.a. tegen IJsland* (Einarsson), een zaak tegen voormalige managers van Kaupping Bank, oordeelde het Hof dat de verdediging een legitiem belang heeft om toegang tot de volledige dataset – met hierin alle gegevens die in een bepaald onderzoek zijn verzameld – te krijgen. Het EHRM wijst hierbij op het *equality of arms*-beginsel, op basis waarvan de verdediging niet alleen passieve verdedigingsrechten heeft (de kennis van het materiaal tegen haar), maar ook actieve verdedigingsrechten, zoals de mogelijkheid om nieuw bewijsmateriaal te verzamelen om zichzelf vrij te pleiten of de straf te verminderen.²³ Volgens het Hof volgt uit artikel 6, lid 3, onder b EVRM dat de inhoudelijke activiteiten van de verdediging (*substantive defence activity*) alles kunnen omvatten wat ‘noodzakelijk’ is om de inhoudelijke zitting van het hoofdproces voor te bereiden.²⁴ De verdachte moet dus de mogelijkheid hebben om zijn verdediging ‘op passende wijze en zonder beperkingen te organiseren om zo in staat te zijn alle relevante verweren aan de rechter voor te leggen en aldus de uitkomst van het strafproces te beïnvloeden’.²⁵ Wat de toegang tot de volledige dataset betreft, heeft het Hof in Einarsson bevestigd dat het belangrijk is om te waarborgen dat de verdediging kan meepraten over criteria aan de hand waarvan wordt vastgesteld welke informatie in de dataset relevant is.²⁶ Volgens het Hof zou dit in de praktijk kunnen betekenen dat de verdediging wordt betrokken bij de vaststelling van specifieke trefwoorden of verbanden, die vervolgens in een geavanceerd zoekinstrument worden ingevoerd om de voor de zaak relevante documenten te zoeken.²⁷ Dit is zo ondanks het feit dat de ‘volledige verzameling van gegevens’ onvermijdelijk een grote hoeveelheid gegevens omvat, die op het eerste gezicht irrelevant is

voor de zaak.²⁸ Dit betekent dat de verdediging niet noodzakelijkerwijs recht heeft op *directe* toegang tot de volledige dataset, maar wel op *indirecte* toegang door deel te nemen aan het bepalen van de zoekwoorden of verbanden.

Het Hof lijkt dit standpunt ook te hebben ingenomen in de zaak *Rook tegen Duitsland* (Rook).²⁹ In deze zaak, tegen een directeur van een grote detailhandelaar in consumentenelektronica in Duitsland, waren ongeveer 80.000 telecommunicatiebewakingsgegevens geproduceerd en 14 miljoen elektronische bestanden in beslag genomen. Het Hof merkte in Rook op dat het recht op een adversair proces – nog los van het recht op toegang tot het dossier – vereist dat het OM ‘alle materiële bewijsstukken die in zijn bezit zijn voor of tegen de verdachte’ aan de verdediging bekendmaakt.³⁰ De term ‘materieel bewijs’ dient ruim te worden opgevat en kan niet beperkt worden tot bewijs dat door het OM als relevant wordt beschouwd. In plaats daarvan omvat de term ‘al het materiaal dat in het bezit is van de autoriteiten en dat mogelijk relevant is, ook als het *niet allemaal in aanmerking wordt genomen, of als het niet relevant wordt beschouwd*’.³¹ Dergelijk materiaal kan namelijk gegevens bevatten die de verdachte in staat zouden kunnen stellen zichzelf vrij te pleiten of zijn straf te laten verminderen. Indien dergelijk materiaal niet aan de verdediging wordt bekendgemaakt, zou dat neerkomen op het weigeren van faciliteiten die nodig zijn voor de voorbereiding van de verdediging (art. 6, lid 3, onder b EVRM).³²

Om *fishing expeditions* te voorkomen, kan de verdediging echter door de rechter worden verplicht om ‘specifieke redenen’ voor dit verzoek op te geven en te wijzen op specifieke kwesties die door middel van verdere zoekopdrachten kunnen worden opgehelderd in de volledige dataset.³³ Wanneer de verdediging onvoldoende specifiek redenen voor het verzoek opgeeft, stelde het Hof in Einarsson dat ‘[i]n dat opzicht de betrokken gegevens meer verwant [zijn] aan elk ander bewijs dat mogelijkerwijs het kunnen bestaan maar door het OM niet was verzameld, tegenover bewijs waarvan het OM kennis had, maar dat het weigerde aan de verdediging mede te delen’.³⁴ Aangezien het OM (net als de verdediging) in Einarsson niet op de hoogte was van de volledige inhoud van de grote hoeveelheid gegevens, en omdat de verdediging onvoldoende specifieke redenen op gaf om de volledige dataset verder te doorzoeken, concludeerde het Hof dat het OM in dat opzicht geen voordeel had ten opzichte van de verdediging in deze zaak. Met andere woorden: er was geen sprake van het achterhouden van bewijs of van geheimhouding (*non-disclosure*) in de

22. Rb. Amsterdam 19 april 2018, a.w., 6.4.2.

23. Simonato 2014, p. 287.

24. EHRM 4 juni 2019, ECLI:CE:ECHR:2019:0604JUD003975715 (*Sigurður Einarsson e.a. t. IJsland*), para. 86; zie ook EHRM 31 maart 2009, ECLI:CE:ECHR:2009:0331JUD002102204 (*Natunen t. Finland*), para. 42.

25. Zie bijvoorbeeld EHRM 31 maart 2009, (*Natunen t. Finland*), a.w., para. 42; EHRM 9 oktober 2008, nr. 62936/00, ECLI:CE:ECHR:2008:1009JUD006293600 (*Moiseyev t. Rusland*).

26. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 90 (nadruk van de auteur).

27. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 16, 24.

28. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 90.

29. EHRM 25 juli 2019, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook t. Duitsland*).

30. EHRM 25 juli 2019 (*Rook t. Duitsland*) a.w., para. 45.

31. EHRM 25 juli 2019 (*Rook t. Duitsland*) a.w., para. 58 (nadruk van de auteur).

32. *ibid.*

33. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 90; EHRM 25 juli 2019 (*Rook t. Duitsland*) a.w., para. 59.

34. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 90.

klassieke zin van het woord.³⁵ Als zodanig zorgt deze beperking in principe voor een redelijk symmetrisch evenwicht tussen de tegengestelde partijen (beide partijen hebben immers een beperkte toegang), waarbij ook mogelijke andere tegengestelde belangen worden bewaard.

Uit het voorgaande blijkt dat de verdediging dus het recht heeft om, ten minste op indirecte wijze, toegang te krijgen tot de volledige dataset door deel te nemen aan de vaststelling van de criteria waarmee wordt vastgesteld welke informatie voor de zaak relevant is (bijvoorbeeld door het verstrekken van aanvullende trefwoorden). Daarbij kan zij worden verplicht om specifieke redenen voor deze aanvullende zoekactiviteit op te geven.

3.2.2 *Directe of indirecte toegang tot de secundaire dataset en de zoekmachine*

Het EHRM heeft een iets steviger standpunt ingenomen ten aanzien van toegang tot de secundaire dataset die het resultaat is van de eerste zoekacties van de volledige dataset. Volgens het Hof in Einarsson is de situatie in dit geval anders dan met betrekking tot de volledige dataset, aangezien het OM *in feite* alle gegevens in de secundaire dataset heeft onderzocht – hetzij met de hand, hetzij met behulp van een geavanceerde zoekmachine – om te bepalen welk materiaal later in het dossier moet worden opgenomen.³⁶ Bovendien overwoog het Hof dat zelfs met betrekking tot het materiaal in deze dataset, dat a priori niet relevant is voor de zaak, de selectie niet door het OM alleen kan worden gemaakt zonder dat de verdediging erbij betrokken is *en* zonder enig rechterlijk toezicht op het proces.³⁷ Het Hof concludeerde dat ‘het passend zou zijn geweest als de verdediging de mogelijkheid had gekregen *om een zoekopdracht uit te voeren – of te hebben uitgevoerd – naar mogelijk ontlastend bewijs*’.³⁸ In tegenstelling tot de volledige dataset heeft het Hof hier niet geëist dat het verweer een motivering moet bevatten aan de hand waarvan kan worden bepaald welke gegevens voor de zaak relevant zijn. Het Hof heeft toch in aanmerking genomen of de verdediging een specificatie had verstrekt van het soort bewijs dat zij zoekt. En alhoewel het Hof dit niet beschouwt als een specifieke voorwaarde, wordt dit wel gezamenlijk met andere factoren meegenomen bij het beoordelen van de algehele eerlijkheid van het proces (zie paragraaf 3.2.3 over ‘eerlijkheid van het proces als geheel’).³⁹

Bovendien merkte het Hof in Einarsson op dat nadere zoekopdrachten in de secundaire dataset ‘technisch gezien vrij eenvoudig’ zouden zijn geweest, zodat er weinig reden is om de verdediging deze mogelijkheid niet te geven.⁴⁰ Hoewel het Hof hier niet nader op

inging, kon de gekozen formulering (d.w.z. ‘technisch gezien vrij eenvoudig’) worden geacht te impliceren dat verdere zoekopdrachten in de secundaire dataset – althans wanneer deze door de verdediging zelf worden uitgevoerd – toegang tot de geavanceerde zoekmachine omvatten. Als deze redenering klopt, zou dit een belangrijke aanvullende waarborg inhouden met betrekking tot de vraag wat als adequate faciliteiten moeten worden beschouwd (in art. 6, lid 3, onder b EVRM), aangezien toegang tot een grote hoeveelheid gegevens zonder dat er ook toegang is tot een geavanceerd zoekinstrument, niet neerkomt op een *effectieve* mogelijkheid om relevante informatie te vinden (dit wordt verder besproken in paragraaf 4.1). Bovendien, wat betreft de kwestie van voldoende tijd in artikel 6, lid 3, onder b EVRM, vond het EHRM in Rook dat het voldoende was om drie en een halve maand de tijd te hebben om 14 miljoen elektronische bestanden te doorzoeken *met toegang* tot een geavanceerd zoekmachine.⁴¹

Hoewel de toegang tot de secundaire dataset kan worden beperkt met het oog op concurrerende belangen (bijvoorbeeld de privacy van anderen), moeten eventuele beperkingen ‘strikt noodzakelijk’ zijn met het oog op de centrale rol van *equality of arms* in het recht op een eerlijk proces. Het Hof erkende de mogelijkheid van beperkingen op grond van concurrerende privacybelangen van anderen, maar stelde in Einarsson dat het ‘niet van mening is dat er in dat opzicht onoverkomelijke obstakels bestaan’.⁴² Hoewel het EHRM zelf over deze kwestie niet verder uitweidt, zijn er niettemin verschillende praktische en technische mogelijkheden te bedenken om aan de concurrerende belangen tegemoet te komen en tegelijkertijd in principe toegang te verlenen tot de volledige secundaire dataset (dit wordt verder besproken in paragraaf 3.1).

Op basis van Einarsson en Rook zou de verdediging direct of indirect toegang moeten krijgen tot de (volledige) secundaire dataset om naar ontlastend bewijsmateriaal te kunnen zoeken. Voor het geval deze zoekactie door de verdediging zelf zou worden uitgevoerd, lijkt het Hof zich op het standpunt te stellen dat de toegang tot de dataset ook toegang tot de geavanceerde zoekinstrumenten mag omvatten, met name gelet op het vereiste van voldoende tijd en faciliteiten. De verdediging lijkt ook niet verplicht te zijn om te specificeren welk soort bewijs zij verlangt wanneer zij om toegang tot de secundaire dataset verzoekt.

3.2.3 *Eerlijkheid van het ‘proces als geheel’ en andere beperkingen*

Het beginsel van *equality of arms* is niet absoluut en vereist dat de verdachte een ‘nadeel’ heeft ondervonden om van een inbreuk te kunnen spreken. Volgens de jurisprudentie van het EHRM wordt ‘nadeel’ gewoonlijk gelijkgesteld met feitelijk nadeel.⁴³ Er is sprake van benadeling als de procedurele ongelijkheid (*procedural inequality*) daadwerkelijk een negatief en materieel effect

35. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w.

36. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 91.

37. Het gebruik van ‘en’ impliceert een cumulatief verband; EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w.

38. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w. (nadruk van de auteur).

39. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 92.

40. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 91 (nadruk van de auteur).

41. EHRM 25 juli 2019 (*Rook t. Duitsland*) a.w., para. 72.

42. EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. IJsland*) a.w., para. 92.

43. Sidhu 2017, p. 103.

heeft gehad op het verweer en daarmee de betrouwbaarheid van de uitkomst van de strafzaak heeft beïnvloed. Een door de ongelijkheid veroorzaakt nadeel kan echter worden gecompenseerd door andere procedurele waarborgen, waardoor de procedure toch als eerlijk kan worden beschouwd. Dit is een gevolg van de aanpak die gericht is op de eerlijkheid van het 'proces als geheel', waarbij wordt bepaald of de waarborg al dan niet is nagekomen in het licht van de algemene context van de procedure.⁴⁴ Dit biedt lidstaten de mogelijkheid om het effect van procedurele ongelijkheden te compenseren met aanvullende waarborgen voordat het definitieve oordeel wordt geveld.

De verdediging moet overigens bewijzen dat sprake is van een daadwerkelijk nadeel als gevolg van de beperking van een procedurele waarborg. Hoewel het EHRM deze kwestie in bovengenoemde zaken niet heeft besproken, is het voorstelbaar dat het voor de verdachte zeer moeilijk kan zijn om dit te bewijzen als de lat voor de onderbouwing van dat nadeel te hoog wordt gelegd. Immers, als de verdachte niet kan weten welke potentieel ontlastende informatie kan worden gevonden in een omvangrijke dataset die mogelijk afkomstig is van duizenden andere personen, kan hij nauwelijks bewijzen dat hij daadwerkelijk nadeel ondervindt als hij geen toegang krijgt tot deze dataset (dit wordt verder besproken in paragraaf 3.1). Om vergelijkbare redenen wordt de benadering van het recht op een eerlijk proces in zijn geheel door academici als *unfortunate* bestempeld en bekritiseerd omdat het leidt tot een zeer laag niveau van procedurele gelijkheid.⁴⁵

4. De behoefte aan uitgebreidere of aanvullende rechten en mogelijkheden voor het Nederlandse strafprocesrecht

Hoewel de twee besproken arresten van het EHRM een waardevolle aanvulling en verduidelijking bieden ten aanzien van de waarborgen voor toegang tot zowel de volledige als de secundaire dataset, blijft er genoeg te wensen over wil men kunnen spreken van een redelijk symmetrisch evenwicht tussen het OM en de verdediging. Daarom beschouw ik de arresten als een opstapje om verder na te denken over uitgebreidere procedurele waarborgen in deze nieuwe datagedreven context. In het laatste deel van dit artikel bespreek ik de behoefte aan directe toegang tot de secundaire dataset en de zoekmachine alsook de behoefte aan aanvullende waarborgen met betrekking tot de betrouwbaarheid van digitaal bewijs. Tot slot ga ik kort in op de omvang van der-

gelijke waarborgen, door het prisma van het huidige Nederlandse strafprocesrecht.

4.1 Directe toegang tot de secundaire datasets en toegang tot de zoekmachine

Gezien de beperkte indirecte toegang tot de volledige dataset voor de verdediging (een beperking die in beginsel een redelijk symmetrisch evenwicht tussen de partijen waarborgt), stel ik voor dat de verdediging in principe directe toegang tot de secundaire dataset moet hebben. Dat wil zeggen dat de verdediging zelf moet kunnen zoeken naar mogelijk ontlastend bewijs. Het is voor de verdediging namelijk nauwelijks mogelijk om van tevoren precies te weten waar ze naar op zoek is in de omvangrijke datasets, die bestaan uit grote hoeveelheden van onderling verbonden hoeveelheden gegevens. Bij het zoeken in een enorme dataset met potentieel miljoenen datapunten weet men over het algemeen niet wat men zoekt totdat men het daadwerkelijk vindt (of ten minste iets heeft gevonden wat ermee verbonden is). En men kan dit in feite ook niet weten.⁴⁶ Denk aan de Ennetcom-server, die gegevens bevat van ongeveer 19.000 gebruikers (waarvan sommige op een of andere manier gerelateerd kunnen zijn aan de verdachte), zodat de verdediging geen goed idee kan hebben van wat daar als ontlastend bewijsmateriaal gevonden kan worden. Net als het OM moet de verdediging dus de mogelijkheid hebben om de gegevens herhaaldelijk te doorzoeken en de zoektermen te verfijnen die haar in staat kunnen stellen om te vinden wat ze zoekt. Aangezien dit niet kan worden bereikt door eenvoudigweg een lijst van te zoeken trefwoorden op te stellen (zonder inzicht in het soort resultaten dat deze opleveren, wat een verdere verfijning mogelijk zou maken), dient in beginsel directe toegang tot de secundaire dataset te worden geboden.

Bovendien, om de verdediging in staat te stellen de secundaire dataset *effectief* te doorzoeken, moet zij toegang hebben tot de geavanceerde zoekmachine. Deze directe toegang tot de secundaire dataset en de zoekmachine hoeft echter niet onbeperkt te zijn, vooral met het oog op concurrerende belangen (bijvoorbeeld informatie die relevant is voor een ander onderzoek).⁴⁷ Een andere technische mogelijkheid zou zijn dat het OM potentieel gevoelige gegevens zou *taggen*, zodat deze gegevens niet in de onmiddellijke zoekresultaten van de verdediging

44. Sidhu 2017, p. 84.

45. Zie b.v. Trechsel 2005, p. 226.

46. Rechter Pavli verwoordde het goed in zijn deels afwijkende mening in de Einarsson-zaak: om van de verdediging te eisen dat zij specificeert wat zij precies wil zoeken in de context van 'miljoenen documenten' is hetzelfde als eisen dat zij de precieze locatie van een naald in een hooiberg specificeert; EHRM 4 juni 2019, (*Sigurður Einarsson e.a. t. Ísland*) a.w., para. 8.

47. Zo hebben Schermer en Oerlemans (2020) al voorgesteld om toegang te verlenen via een *dataroom*, waar de verdediging gemakkelijk, doch in een gecontroleerde omgeving, de dataset met Hansken zou kunnen doorzoeken. Zij wijzen ook op suggesties met betrekking tot dataruimtes in het ondernemingsrecht: J.H. de Wildt, 'Een blik over de grenzen: Vertrouwelijkheid, data rooms en confidentiality rings', *Tijdschrift voor Sanctierecht & Onderneming* 2017/1, J.J.H. Joosten en J.C. Tijink, 'Gedagvaard in de VS: discovery', *Tijdschrift Ondernemingsrechtpraktijk* 2017/3.

zouden voorkomen.⁴⁸ De rechter-commissaris (RC) kan dan beslissen of het beperken van de toegang van de verdediging tot een specifiek gegeven in de specifieke context strikt noodzakelijk is. In plaats van een groot deel van de gegevens op voorhand uit te sluiten van de secundaire dataset, zou dit leiden tot een meer contextuele beoordeling van uitsluiting, waardoor een meer genuanceerde benadering van het behoud van concurrerende belangen mogelijk wordt.

Om vergelijkbare redenen moet de eis van het EHRM om ‘daadwerkelijk nadeel’ aan te tonen bij het bepalen of een weigering van toegang tot de secundaire dataset heeft geleid tot een schending van artikel 6 EVRM, niet een te hoge standaard opleveren voor de verdediging. Aangezien de verdachte niet weet wat er in zo’n omvangrijke dataset zou kunnen zitten, mag van hem ook niet worden verwacht dat hij in de zaak een concreet nadeel kan aantonen wanneer het recht op toegang niet zou worden verleend. Net als bij het bewijs van negatieve feiten is ook het bewijs van feitelijke vooroordelen over onbekende feiten *probatio diabolica*.

Bij toepassing van deze discussie op het Nederlandse strafrecht lijkt momenteel, bij gebrek aan meer specifieke bepalingen, het indienen van een verzoek bij de RC om bepaalde aanvullende opsporingshandelingen te verrichten op basis van artikel 182 Sv, de beste route voor de verdediging. Deze algemene bepaling is in principe ruim genoeg geformuleerd om de verdediging in staat te stellen toegang te vragen tot de secundaire dataset (inclusief het zoekinstrument) om naar ontlastend bewijs te zoeken. Dit verzoek dient wel te worden gemotiveerd (art. 182 lid 3 Sv). En hoewel de wet zelf niet aangeeft hoe nauwkeurig de motivering van de verdediging moet zijn, moet de RC dergelijke verzoeken inwilligen tenzij ze ‘niet relevant’ zijn, aldus de wetsgeschiedenis.⁴⁹ In de Ennetcom-Tandem-zaak heeft de RC slechts twee bezoeken aan het Nederlands Forensisch Instituut (‘NFI’) toegestaan, ondanks herhaalde verzoeken van de verdediging om de secundaire datasets met Hansken te mogen doorzoeken. De verdediging had hierdoor een *zeer beperkte* mogelijkheid om de dataset te doorzoeken tijdens een van de kortdurende bezoeken, zoals door de rechtbank is erkend.⁵⁰ En hoewel de verdediging iets meer dan een maand voor de uitspraak een cd-rom met de secundaire dataset heeft ontvangen,⁵¹ kreeg zij niet de gelegenheid om deze gegevens met Hansken te doorzoeken. Gezien de praktische onmogelijkheid om in iets meer dan een maand en zonder zoekmachine een grote hoeveelheid gegevens te doorzoeken, is het de vraag of in de Ennetcom-Tandem-zaak is voldaan aan de eis van voldoende voorbereiding ex artikel 6

lid 3 sub b EVRM. Op basis van de huidige jurisprudentie lijkt de toepassing van het Nederlandse strafrecht in zulke zaken⁵² dus een te beperkt niveau van toegang tot de secundaire dataset en de zoekmachine te bieden.

4.2 Testen van de betrouwbaarheid van het bewijsmateriaal: *logging* en contra-expertise

Een ander belangrijk recht waarover de verdediging zou moeten beschikken in de context van digitale datasets en geavanceerde zoekmachines, is het recht om de betrouwbaarheid van het verzamelde digitale bewijsmateriaal te testen. De betrouwbaarheid van digitaal bewijs hangt namelijk af van de betrouwbaarheid van de technologische middelen die worden gebruikt om het bewijsmateriaal te produceren en van het vermogen van de verdediging om het te authenticeren.⁵³

Bij relatief eenvoudige en verklaarbare algoritmische systemen, met name systemen die specifiek voor het forensische proces zijn ontworpen zoals de klassieke *e-discovery* instrumenten,⁵⁴ heeft het recht om de betrouwbaarheid van het bewijsmateriaal te toetsen hoofdzakelijk betrekking op de transparantie. Met andere woorden, de verdediging moet de mogelijkheid hebben om na te gaan hoe het OM tot een bepaalde (secundaire of tertiaire) dataset is gekomen. Een eenvoudige waarborg in dit verband is *logging*, dat al is gebruikt met betrekking tot het doorzoeken van smartphones bij arrestaties,⁵⁵ en ook is gereguleerd op basis van het Europese recht inzake bescherming van persoonsgegevens.⁵⁶ Met name met betrekking tot de volledige dataset, waartoe de verdediging in het algemeen slechts indirect toegang heeft, moeten logboeken met de activiteiten – dat wil zeggen alle ingevoegde zoektermen en de resultaten – beschikbaar zijn voor de verdediging. Zonder toegang tot deze logboeken zou het OM namelijk de mogelijkheid hebben om informatie te produceren zonder de relevante context.⁵⁷ Door logboeken van alle activiteiten in de zoekactiviteit beschikbaar te stellen aan de verdediging, kan het risico op uitsluiting van ontlastend materiaal of context worden vermindert. Hansken voorziet bijvoorbeeld al in de mogelijkheid van automatische *logging*,⁵⁸ dus het vaststellen van een dergelijk recht zou vanuit technisch oogpunt vrij eenvoudig kunnen zijn.

48. Gegevens met betrekking tot het juridisch beroepsgeheim zijn bijvoorbeeld al als zodanig gemarkeerd en uitgesloten wanneer het OM de dataset met Hansken doorzoekt; zie H.M.A. van Beek e.a., ‘Digital Forensics as a Service: Game On’, *Digital Investigation* 2015/15, p. 20.

49. *Kamerstukken II* 2009/10, 32 177, nr. 6, p. 23.

50. Rb. Amsterdam 19 april 2018, a.w., 7.3, p. 11.

51. Met uitzondering van een groot deel van de gegevens die het OM voor deze zaak irrelevant achtte, maar die relevant waren voor andere onderzoeken.

52. Zie Driessen en Meeus 2021 over de Encrochat- en PGP-safe-zaken.

53. Pagallo en Quattrocchio 2018, p. 394; K. Strutin, ‘Databases, e-Discovery and Criminal Law’, *Richmond Journal of Law & Technology* 2003/15, 1, p. 12.

54. Als zodanig zijn ze ontworpen met bepaalde waarden in het achterhoofd, zoals privacy, veiligheid en transparantie; zie bijvoorbeeld Van Beek e.a. 2015.

55. In ieder geval in Canada; zie B.C. Newell en B.J. Koops, ‘From horseback to the moon and back: Comparative limits on police searches of smartphones upon arrest’, *Hastings Law Journal* 2020/72, p. 66 e.v.

56. Zie art. 25 Richtlijn politie- en justitiegegevens (Richtlijn (EU) 2016/680); zie ook art. 32a Wet politiegegevens (artikel nog niet in werking).

57. Zie bijvoorbeeld D.B. Garrie en D.K. Gelb, ‘E-Discovery in criminal cases: A need for specific rules’, *Suffolk University Law Review*, 2010/43, p. 101; S. Gless, ‘AI in the courtroom: A comparative analysis of machine evidence in criminal trials’, *Georgetown Journal of International Law*, 2020/51, p. 195.

58. Van Beek e.a. 2015.

Voor de meer complexe (vooral autonome) algoritmische systemen is transparantie echter niet genoeg, omdat de resultaten van dergelijke systemen moeilijk uit te leggen zijn. Wetenschappers hebben toch enkele oplossingen geopperd om de betrouwbaarheid van deze systemen te kunnen toetsen. Eén idee is om toegang te geven tot de code, dat betekent de logica achter de beslissingen van het algoritmische systeem.⁵⁹ Echter de onderliggende code van dergelijke systemen is vaak niet publiekelijk beschikbaar (om geldige redenen), wat ook geldt voor de meeste algoritmen die in Hansken worden gebruikt. Zelfs als toegang tot de code zou worden verleend, zouden de resultaten nog steeds zeer moeilijk te verklaren zijn. Dat is met name zo in verband met autonome systemen die gebruikmaken van *deep learning*-technieken (die ook gepland zijn om te worden gebruikt bij de ontwikkeling van Hansken).⁶⁰

Mogelijk is het dus beter om in dit verband een specifiek recht op contra-expertise vast te leggen. Gezien het feit dat leken niet goed begrijpen hoe algoritmische systemen zoals Hansken functioneren – en dat zelfs deskundigen die het systeem zelf hebben gebouwd steeds meer moeite hebben om te begrijpen hoe het functioneert – moeten het OM, de verdediging en de rechter allemaal een groot vertrouwen hebben in het algoritmische systeem. In feite ontstaat hier geen ongelijke situatie zoals in het geval van DNA of andere soorten deskundig bewijs. Dit is erkend door Nederlandse forensische deskundigen die verbonden zijn aan het NFI zelf, die hebben verklaard dat ‘deze technologische revolutie in de forensische wetenschap kan leiden tot een paradigmaverschuiving waarbij een nieuwe rol van de forensische expert zal ontstaan als ontwikkelaar van bewijsanalyses’.⁶¹ Het zou dus zinvol zijn om het algoritmisch systeem zelf als deskundig bewijs te beschouwen, waardoor de verdediging het recht krijgt om contra-expertise te verrichten. Met deze erkenning kan bovendien een tegenwicht worden geboden aan de situatie – die zich met name in inquisitore systemen heeft ontwikkeld – waarbinnen digitaal bewijs min of meer verondersteld wordt correct te zijn en zelfs bij complexe technologische systemen wordt aangenomen dat de methode neutraal is. Met als gevolg dat elke mogelijkheid tot tegenspraak wordt ontmoedigd.⁶²

Dat die aannames ook worden gedaan in het Nederlandse systeem blijkt uit de rechtspraak. In 2019 oordeelde de Rechtbank Gelderland bijvoorbeeld in een zeer beknopte motivering dat de onvolledigheid van de resultaten als gevolg van een update van Hansken geen invloed had op de integriteit van de resultaten en dat de verdediging er niet in is geslaagd het tegendeel te bewij-

zen (en dat zonder toegang tot Hansken).⁶³ Sterker nog, de Rechtbank Amsterdam oordeelde in de Ennetcom-Tandem-zaak dat er met betrekking tot het gebruik van Hansken geen sprake kan zijn van expertise en dat de verdediging dus geen recht heeft op contra-expertise.⁶⁴ Om de betrouwbaarheid van digitaal bewijs op een hoog niveau te behouden zou de Nederlandse rechter zijn standpunt in dit opzicht moeten wijzigen. En in het verlengde hiervan zou de wetgever de nodige wijzigingen in het Wetboek van Strafvordering zelf moeten aanbren- gen, gelet op het grote belang van deze kwestie en de vroeger genoemde kwesties voor de *equality of arms* in strafzaken. Dit is zeker een ontwikkeling die aandacht verdient in het kader van de modernisering van het Nederlandse strafrecht.

5. Conclusie

In dit artikel heb ik besproken hoe de opkomst van digitaal bewijs en omvangrijke datasets in strafzaken de positie van de verdediging bemoeilijken. De vraag of er nog gesproken kan worden van *equality of arms* tussen het OM en de verdediging staat hier centraal. In deze context onderzocht ik hoe *equality of arms* moet worden geïnterpreteerd in het licht van het krijgen van toegang tot enorme datasets, en vanuit het recht om de betrouwbaarheid van digitaal bewijs te testen. Mijn bespreking, inclusief een analyse van twee EHRM-zaken uit 2019, biedt nieuwe inzichten voor de nodige regulering van deze opkomende problematiek.

Centraal in mijn analyse staat het punt dat de verdediging een geldig belang heeft om toegang te krijgen tot zowel de volledige als de secundaire dataset die in een strafzaak worden vergaard. De verdediging moet immers de mogelijkheid hebben om mee te bepalen wat in haar zaak als relevante informatie geldt. Verder nog, ze moet de mogelijkheid hebben om zelf te zoeken naar ontlastend bewijsmateriaal. Met betrekking tot de volledige dataset moet de verdediging ten minste de gelegenheid hebben om betrokken te worden bij de vaststelling van de zoektermen waarmee een dataset zal worden doorzocht. Om naar ontlastend bewijs te kunnen zoeken, dient de verdediging in principe volledige en directe toegang tot de secundaire dataset te krijgen. Dit is ook door het EHRM bevestigd in de Einarsson- en Rook-zaken.

Mijn andere centrale punt is dat de waarde van digitaal bewijs afhankelijk is van de betrouwbaarheid van de gebruikte technologische middelen en het vermogen van de verdediging om deze te authenticeren. Helaas heeft het EHRM zich hier nog niet over uitgesproken. Ik stel voor om nieuwe rechten van de verdediging in te voeren, zoals het recht op transparantie (bijvoorbeeld toegang tot de logboeken) en betrouwbaarheid. Met name met betrekking tot het gebruik van complexe algoritmische

59. Zie b.v. Pagallo en Quattrocchio 2018; M.A. Prins, ‘Een koelkast als getuige: Over de (toekomstige) rol van de internet of things in de opsporing’, *Delikt en Delinkwent* 2017/31.

60. A. Kloosterman e.a., ‘The interface between forensic science and technology: How technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system’, *Philosophical Transactions of the Royal Society*, 2015/370, p. B 5.

61. Kloosterman e.a. 2015, 2.

62. Zie bijvoorbeeld Pagallo en Quattrocchio 2018, p. 398; Simonato 2014, p. 267-268; Gless 2020.

63. Rb. Gelderland, 26 juni 2019 a.w., p. 9.

64. Rb. Amsterdam 19 april 2018, a.w., 7.3, p. 11.

sche systemen, waarvan de gehele werking moeilijk te begrijpen is voor alle betrokken partijen, zou het algoritmische systeem als deskundig bewijs kunnen worden beschouwd. Hierdoor krijgt de verdediging het recht om contra-expertise te verrichten.

Ten slotte: gezien het toenemende aantal in beslag genomen servers en gehackte berichtendiensten in Nederland (onlangs nog in de zaak SkyECC), verdienen deze punten veel aandacht in het kader van de modernisering van het Nederlandse strafrecht. Voor op de korte termijn stel ik voor dat rechters rekening houden met de voortschrijdende jurisprudentie van het EHRM, en een minder strenge aanpak hanteren bij het verlenen van toegang tot datasets, en zelfs tot de zoekmachine, aan de verdediging. Ook moeten zij kritischer kijken naar de betrouwbaarheid van digitaal bewijs dat door geavanceerde zoekmachines zoals Hansken wordt geproduceerd en moeten zij de verdediging in staat stellen dit adequaat te toetsen. Op wat langere termijn en gelet op het grote belang van al deze kwesties voor *equality of arms* in strafzaken, zou de wetgever concrete waarborgen voor de toegang tot en toetsing van datasets in het Wetboek van Strafvordering zelf kunnen aanbrenge(n). Een bredere vraag die ook door de wetgever nog moet worden beantwoord, is of het Wetboek van Strafvordering een toereikende wettelijke grondslag bevat voor het in beslag nemen van en zoeken in grote datasets. Helaas is de aandacht hiervoor lang niet groot genoeg; zelfs in het moderniseringsproces.