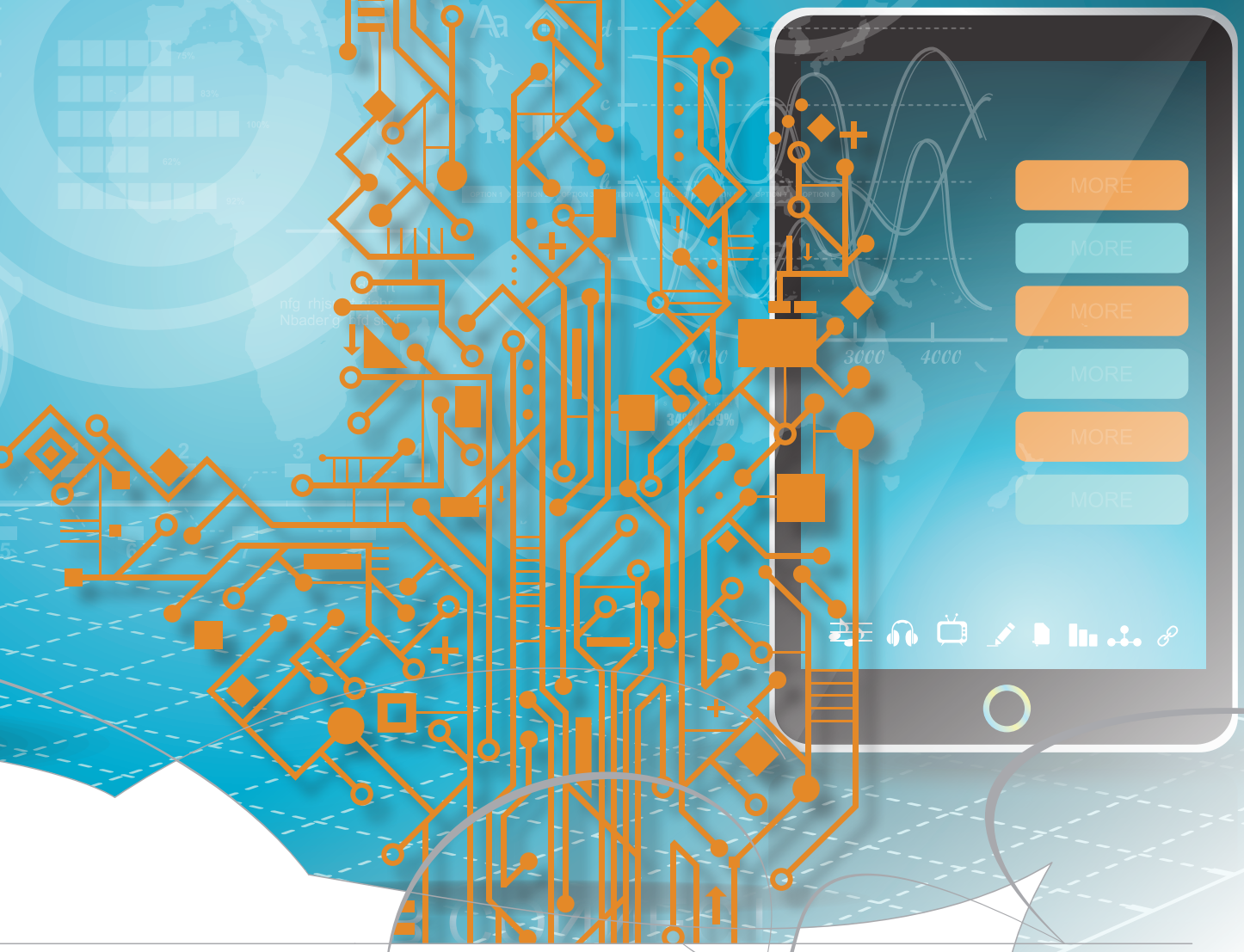
Beginselen digitaal

Digitalisering en de beginselen van de strafrechtspleging

Rapport van een verkennend onderzoek in opdracht van het WODC

Marloes Dijkstra
Stef Joosten
Evert Stamhuis
Mark Visser



Open Universiteit
www.ou.nl

Productie
Open Universiteit, Heerlen
Omslag
Open Universiteit, afd. Visuele communicatie
Bureauredactie en opmaak
John Dohmen

Druk- en bindwerk
Grafisch centrum OUNL, Heerlen

Inhoudsopgave

Samenvatting

De digitalisering heeft in de strafrechtspleging al behoorlijk grote veranderingen gebracht en dat zal in de toekomst eerder meer dan minder ingrijpend worden. In het strafrecht gelden echter fundamentele juridische waarden, veelal aangeduid met de term grondbeginselen, die bij het handelen en beslissen geëerbiedigd moeten worden. De vraag moet gesteld worden of en hoe dat gaat lukken: een digitalisering van de strafrechtspleging met respect voor de juridische grondbeginselen van de strafrechtspleging. Voor het uitvoeren van deze studie is de volgende vraag centraal gesteld:

Door welke informatietechnologische ontwikkelingen kan het handelen/beslissen van actoren in de Nederlandse strafrechtspleging veranderen? Welke positieve en negatieve aspecten brengen deze ontwikkelingen met zich mee ten aanzien van de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging?

De volgende deelvragen zijn onderscheiden.

1 Welke beginselen van strafrechtspleging zijn in verband te brengen met IT-ontwikkelingen?
2 Welke veranderingen in de Nederlandse strafrechtsketen zijn er in de afgelopen vijf jaar het gevolg van de ontwikkelingen in de IT?
3 Op welke punten ondersteunen de reeds zichtbare veranderingen de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging, dan wel leveren deze veranderingen spanning op met deze beginselen?
4 Welke voor de Nederlandse strafrechtsketen relevante IT-ontwikkelingen zijn in de komende tien jaren te verwachten?
5 Op welke punten zullen de te verwachten veranderingen steun geven aan de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging, c.q. zullen de veranderingen spanning met deze beginselen betekenen?

In deze studie wordt de conclusie getrokken, dat in het kader van digitalisering de grondbeginselen van de huidige strafrechtspleging overeind gehouden kunnen worden. In hoofdstuk 2 worden de relevante grondbeginselen beschreven, gevolgd door de beginselen die gelden voor de ontwikkeling van informatiesystemen. In de confrontatie van deze beide wordt de conclusie getrokken, dat de beginselen voor informatiesystemen niet van nature strijdig zijn met de juridische grondbeginselen. In hoofdstuk 3 wordt de recente overgang van papieren naar digitale dossiers in strafzaken beschreven. Deze operatie is vervolgens onderzocht met de vraag of er spanningen met de juridische grondbeginselen gebleken is. Er is spanning in deze zin waargenomen, maar die is niet toe te schrijven aan de informatietechnologie als zodanig. Een mogelijk toekomstscenario voor veranderingen door digitalisering wordt in hoofdstuk 4 ingepast in het kader van de juridische grondbeginselen. Dat leidt tot de conclusie dat schending van deze beginselen niet onvermijdelijk is. Digitalisering kan ondersteunend zijn of minst genomen neutraal ten opzichte van de grondbeginselen.

Dat er knelpunten zijn en zich zullen blijven voordoen, dat staat als een paal boven water. Die zijn echter niet toe te schrijven aan digitalisering op zichzelf,

maar hebben eerder te maken met gebreken in de regie, in kennis en in nabijheid en afstemming tussen de professionals uit de verschillende disciplines die in de digitalisering van dit complexe systeem betrokken zijn. Voor de knelpunten vormen de informatietechnische ontwikkelingen tot nu toe en in de toekomst in zichzelf niet de oorzaak en evenmin de oplossing.

In de toekomstige gedigitaliseerde strafrechtspleging zal de relatie tussen de IT-specialisten en de juridische professionals niet als producent-consument bestempeld kunnen worden. Beide zullen zich op de andere discipline moeten richten en de genoemde rollen met elkaar moeten gaan combineren tot de 'conducenten' van de digitale afdoening van strafzaken. De veranderingen in het handelen en beslissen zullen vast en zeker tot nieuwe vormen van realisatie van de grondbeginselen leiden, maar als beide disciplines vanuit hun principiële basis aan dit proces leiding geven, kan deze nieuwe toestand net zo verenigbaar zijn met het juridisch-normatieve kader als de huidige situatie en zijn er zelfs verbeteringen mogelijk.

Hoofdstuk 1

Vraagstelling en aanpak

1.1 Inleiding

De introductie van informatie- en communicatietechnologie (hierna IT) in de strafrechtspleging is niet van vandaag of gisteren. Tekstverwerkers en mailprogramma's worden al decennialang in de praktijk van het strafrecht benut. Elektronische aangifte bestaat al jaren (art. 163 lid 3 Sv) en ook het elektronisch proces-verbaal is in de wet opgenomen (art. 153 lid 2 Wetboek van Strafvordering). Toch is de strafrechtspleging nog sterk op papier georiënteerd. Wat er ook aan digitale voorgeschiedenis in een zaak voorhanden is, uiteindelijk slaat het allemaal neer in een papieren zaaksdossier, dat bij de overgang van de procesfasen van hand tot hand gaat. Niet verwonderlijk is het daarom, dat de strafrechtsketen (de *supply chain*) veelal uitgedrukt wordt in het per schakel verrichten van handelingen die blijken uit toevoegingen en bewerkingen in het dossier. Werkprocessen zijn op die leest geschoeid.

Voor de versterking van de prestaties in de strafrechtsketen wordt het een en ander verwacht van een vergrote inzet van IT in de gedingvoering. Het beleidsinitiatief *Versterking Prestaties Strafrechtsketen* (VPS) steunt op de gedachte dat IT ingezet kan worden voor verkorting van doorlooptijden, verbetering van de kwaliteit en van de samenwerking tussen de ketenpartners en verbetering van de werkprocessen en procedures. Het deelprogramma *Digitaal Werken in de Strafrechtsketen* (DWS) werkt dat verder uit in de invoering van de digitale ondersteuning in de procesgang met het digitale dossier als verbindende factor.[1]

In navolging van de beleidsdocumenten wordt steeds het woord 'strafrechtsketen' gebruikt. Dat is een gangbare manier om een belangrijk kenmerk van de strafrechtspleging te omschrijven: het is een aaneenschakeling van bewerkingen van een zaak. Gemeengoed geworden in de jaren '90 is deze benadering benut om ordening en stroomlijning aan te brengen in de werkprocessen van de opeenvolgende personen of organisaties die bij de afhandeling van een strafzaak betrokken zijn. Het ketendenken in de strafrechtspleging is niet bedoeld om een juridische benadering van de strafrechtspleging te vervangen. De normen voor een goede ketensamenwerking vallen niet samen met de juridische normen voor een goede strafrechtspleging. Die juridische normering is van een andere orde en kan in een keten volledig gerespecteerd worden (en evengoed onder spanning staan). De juridische normering van de strafrechtspleging komt voort uit gezaghebbende documenten en bestaat in een systeem van bepalingen in verdragen, wetten en richtlijnen. Naast deze geschreven normen vervult ongeschreven recht onmiskenbaar een rol bij de normering van de strafrechtspleging. Deze gezamenlijkheid van normen wordt in de doctrine beschouwd als een uitdrukking van wezenlijke juridische waarden of grondbeginselen. Sommige hiervan zijn tamelijk concreet omschreven in een verdrag of in onze Grondwet, andere worden gevonden als abstracties van de concrete bepalingen.

1. Zie *Kamerstukken II*, 29 279, nr. 178, p. 3-5.

Of het nu gaat om de invoering van een ketenbenadering enige decennia geleden, of om de digitalisering die nu aan de orde is, de wezenlijke juridische normering dient nog steeds gerespecteerd te worden in de afhandeling van strafzaken. Een vernieuwing van de werkwijze neemt immers het bindend gezag van deze normering niet weg. Om die reden moet de vraag gesteld worden of en hoe dat gaat lukken: een digitalisering van de strafrechtspleging met respect voor de juridische grondbeginselen van de strafrechtspleging. Daarbij is het logisch eerst te verkennen welke veranderingen er in het kader van de digitalisering al zijn gepasseerd en welke er mogelijkerwijs nog zullen komen. Vervolgens ligt er dan de taak om te onderzoeken welke gevolgen dat gehad heeft of zou kunnen hebben voor het respecteren van de juridische normering. Deels is dat het onderzoeken van het recente verleden en het heden, deels het theoretiseren over de toekomst. Het maken van een inventaris van juridische grondbeginselen kan natuurlijk niet ontbreken, waarbij de blik vooral gericht zal moeten zijn op die grondbeginselen, waarvan de doorwerking beïnvloed kan worden door de digitalisering.

De vraag moet gesteld worden waarop de verwachting berust, dat er inderdaad gevolgen zullen zijn. Als antwoord op die vraag past een aantal opmerkingen. Op de eerste plaats is dat nu juist wat we willen weten: is er een impact op het respect voor de beginselen te verwachten? Een uitkomst van deze verkennende studie zou kunnen zijn dat de digitalisering juridisch neutraal zal zijn, ook al klinkt dat juristen wellicht niet erg waarschijnlijk in de oren. Wetenschappelijk uitgedrukt: we hebben nog geen op de situatie toegesneden hypothese en een eerste verkennend onderzoek zal aan hypothesevorming bijdragen. Deze studie wordt evenwel in de eerste plaats uitgevoerd ten behoeve van de beleidsontwikkeling. Ten tweede wijzen we erop dat er juist over deze kwestie waarschuwende stemmen vanuit de rechtspraktijk te beluisteren zijn[2], waarop vanuit beleidsvorming en -uitvoering een respons gegeven moet worden. Ter ondersteuning van die respons verrichten wij deze studie. Ten slotte valt te wijzen op de gangbare theorie over dynamische systemen.[3] In die theorie uit de fysica, maar ook toegepast op het menselijke brein en op organisaties, wordt onder meer gepostuleerd, dat onderling verbonden fenomenen altijd zullen reageren op veranderingen in één van de fenomenen, waarbij er in interactie een nieuw evenwicht bereikt wordt. Deze theorie – hier gesimplificeerd weergegeven – voorziet in onderzoeksvragen over de veranderingen zelf, over de interactie en over het nieuwe evenwicht. Enkelvoudig toegepast op de strafrechtspleging: de werkwijze in de strafrechtspleging is verbonden met naleving van de juridische normering, dus als de werkwijze drastisch zou veranderen, heeft dat altijd effect voor het respecteren van de juridische normering en ontstaat een nieuw evenwicht, waarbij dat evenwicht niet gelijk is aan de 'oude' toestand. Onze taak is dan om te verkennen of en hoe deze nieuwe toestand verenigbaar zal kunnen zijn met de juridische grondbeginselen.

1.2 Scope

Een onderzoek naar de strafrechtspleging kan heel breed uitwaaieren: van strafwetgeving en handhavingsbeleid tot en met tenuitvoerlegging van opgelegde

2. Zie M. Slaghekke, *Column: Digitalisering en kennisneming van het procesdossier: 1-0 voor het OM*, op www.bijzonderstrafrecht.nl/2015/column-digitalisering-en-kennisneming-van-het-procesdossier-1-0-voor-het-OM/ inmiddels dode link (17 okt. 2016).
3. Zie J.B.J. van der Leij, 'Ontwikkelingen in het strafrecht-een aperitief', in: *Systeem in ontwikkeling: liber amicorum G. Knigge*. Nijmegen: Wolf Legal Publishers, 2005, p. 371-376, met verdere verwijzingen.

straffen. Een zinvolle beperking zou kunnen zijn dat in de strafrechtspleging gezocht wordt naar waar de meest spectaculaire ontwikkelingen op het gebied van IT vermoed worden. Niet onwaarschijnlijk is het dat we dan bij de opsporing uitkomen. Daar wordt al veel onderzoek naar gedaan en er zijn ook veel research resultaten beschikbaar. We hebben om verschillende redenen de scope beperkt door de opsporingsfase niet afzonderlijk te behandelen. Ten eerste zou bij de focus op de opsporing één fase in de strafrechtspleging alle aandacht opslokken. Daardoor zou voor het praktijkonderzoek het ketenkarakter uit het beeld verdwijnen, terwijl juist in het beleid van de afgelopen jaren op de ketenwerking de aandacht gericht was. Ten tweede, een combinatie van onderzoek van de opsporing en van de verdere schakels in de keten is eenvoudigweg te omvangrijk. Het in beeld brengen met welke IT-instrumenten op de verschillende plaatsen, nationaal en internationaal, door opsporingsinstanties geëxperimenteerd wordt, is een afzonderlijk onderzoek waard, waarin bijvoorbeeld een enorme variatie van handelen en specifieke normering aan de orde is.[4] Omdat nog weinig onderzoek zich richt op vervolgstappen in de strafrechtsketen, hebben wij ons hierop gericht. Op de momenten dat de uitkomsten van een opsporingsonderzoek verder de strafrechtsketen doorgaan, komen IT-ontwikkelingen natuurlijk wel weer in beeld in dit rapport.

Een tweede opmerking in verband met de scope is dat een onderzoek naar de gevolgen voor de juridische normering om een breder perspectief vraagt dan de *supply chain*. [5] Het staat voor iedereen vast dat de rechtsgrondslagen betekenis hebben voor personen of organisaties die geen schakel in de keten vormen en die soms wel, soms niet als ketenpartner bestempeld worden. Men denke alleen maar aan de verdachte en zijn advocaat, toch cruciale actoren in de strafrechtspleging. Onze invalshoek is dus een ruimere dan de keten. Dat neemt niet weg dat we veel aandacht besteden aan de keten, omdat zoals hierboven al bleek, het aangrijpingspunt voor het digitaliseringsbeleid op dit moment de strafrechtsketen is. Wanneer we dus het woord 'keten' gebruiken, is de aaneenschakeling van autoriteiten bedoeld, die achtereenvolgens bewerkingen verrichten gericht op de afdoening van een strafzaak. Het woord 'strafrechtspleging' wordt gebruikt wanneer de ruimere scope bedoeld is, dus wanneer ook de interactie met actoren buiten de keten in beeld is. De subvragen laten dat wisselende perspectief ook zien.

In de beleidsdiscussie van dit moment neemt het digitaal werken in de fase van de vervolging en berechting een grote plaats in, doordat daarop vanuit de autoriteiten stevig ingezet is. Dat bracht ons ertoe, dat we voor het onderzoek van de praktijk ons hebben geconcentreerd op de recente grote operatie, waarin men voor het strafdossier de omschakeling van papier naar elektronisch programmatisch aangepakt heeft. Daarmee zal de keten als verbindend element dus in het blikveld komen. De transitie van papier naar elektronisch kan als etiket ook wel op eerdere invoering van digitale technologie geplakt worden, maar het elektronisch strafdossier staat de laatste jaren als doelstelling toch wel op eenzame hoogte. Om die reden is de concentratie op de fase van vervolging en berechting voor dit moment geboden.

4. Vgl. B-J. Koops, C. Konings en F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht*, preadvies NVVS 2016, Oisterwijk: Wolf Legal Publishers 2016.
5. De Blok c.s. kijken juist vanuit die kant. Zie C. de Blok e.a., *Digitalisering in strafrechtsketens. Ervaringen in Denemarken, Engeland, Oostenrijk en Estland vanuit een supply chain perspectief,* RuG/WODC 2015.

De scope van deze studie is als volgt samen te vatten. We bestudeerden de inhoud en de realisatie van de juridische grondbeginselen, die in de fase van de vervolging en berechting gelding hebben. De IT-ontwikkelingen die in de praktijk in die fasen van de strafrechtspleging zichtbaar zijn of in de toekomst van betekenis zullen kunnen worden, werden onderzocht en besproken, waarbij het ketenperspectief wel aan de orde was maar niet leidend. De beginselen waarop naar de huidige stand van zaken de digitalisering invloed heeft of zal hebben, komen aan de orde.

1.3 Onderzoeksvragen en methoden

Voor het uitvoeren van deze studie is de volgende vraag centraal gesteld:

Door welke informatietechnologische ontwikkelingen kan het handelen/beslissen van actoren in de Nederlandse strafrechtspleging veranderen? Welke positieve en negatieve aspecten brengen deze ontwikkelingen met zich ten aanzien van de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging?

In deze vraagstelling onderscheiden wij de volgende deelvragen.

1 Welke beginselen van strafrechtspleging zijn in verband te brengen met IT-ontwikkelingen?
2 Welke veranderingen in de Nederlandse strafrechtsketen zijn er in de afgelopen vijf jaar het gevolg van de ontwikkelingen in de IT?
3 Op welke punten ondersteunen de reeds zichtbare veranderingen de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging, dan wel leveren deze veranderingen spanning op met deze beginselen?
4 Welke voor de Nederlandse strafrechtsketen relevante IT-ontwikkelingen zijn in de komende vijf jaren te verwachten?
5 Op welke punten zullen de te verwachten veranderingen steun geven aan de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging, c.q. zullen de veranderingen spanning met deze beginselen betekenen?

Methodisch bestond het onderzoek uit het bestuderen van schriftelijke bronnen, het interviewen van personen en het organiseren van een expertmeeting. De schriftelijke bronnen werden allereerst bestudeerd om daaruit de relevante ontwikkelingen af te leiden. Daartoe boden beleidsdocumenten, (digitale) nieuwsbrieven, webpublicaties en andere schriftelijke bronnen de informatie. Tevens werd de lijst met relevante grondbeginselen van de strafrechtspleging opgesteld op basis van bestudering van schriftelijke bronnen, in het bijzonder handboeken voor het strafprocesrecht en wetenschappelijke publicaties die specifiek dit onderwerp behandelden. De interviews dienden allereerst als aanvulling op de schriftelijke bronnen als het erom gaat de actuele IT-ontwikkelingen in de strafrechtspleging in beeld te krijgen. Tevens werd in de interviews aandacht besteed aan ervaringen met de gevolgen daarvan voor het respecteren van juridische grondbeginselen. De interviews waren partieel gestructureerd en de selectie van de te interviewen personen geschiedde op basis van aangetoonde ervaring met of een gebleken belang in digitaliseringsprojecten in de Nederlandse (straf) rechtspleging. Een lijst met geïnterviewde personen en de aanduiding van het belang vormt een bijlage bij dit rapport. De expertmeeting werd als middel ingezet om de voorlopige bevindingen, d.w.z. de voorlopige uitkomst van de beschreven beginselenstudie en de samengevatte impressies van de actuele

ontwikkelingen, te valideren en om vanuit het onderlinge gesprek tussen bij de praktijk van de digitalisering betrokken personen de verwachtingen aan te scherpen ten aanzien van de mogelijke knelpunten. De kring van personen was wijder getrokken dan de te interviewen betrokkenen. Een lijst met namen en functies/affiliaties is in een bijlage bij het rapport opgenomen. De expertmeeting was voorbereid door bij de uitnodiging een lijst met stellingen toe te voegen, waarop een reactie gevraagd werd. Deze peiling was slechts gericht op het ontdekken van zinvolle punten voor het debat. De stellingen formuleerden we door de uit het onderzoek tot dan toe gebleken spanningen of verwachtingen in een prikkelende positie te vertalen. De lijst bevindt zich bij de bijlagen. Tijdens de meeting werden de stellingen waaromtrent de meeste controverse leek te bestaan plenair besproken, samen met een korte presentatie van de voorlopige uitkomsten. Deze meeting leverde op een aantal punten hulp bij de voltooiing van het onderzoek: nadere onderbouwing van de scope; kritische reflectie op de mogelijke oplossingen wanneer zich spanningen zouden voordoen; aanvulling op de impressies uit de interviews ten aanzien van de projecten die recent in de keten uitgevoerd zijn.

Een laatste opmerking ten aanzien van de methode betreft het kader voor de analyse, het inzicht geven in wat tijdens ons onderzoek als relevante beginselen of ontwikkelingen beschouwd werd. Ten aanzien van de grondbeginselen voor de strafrechtspleging werden als relevant aangemerkt die beginselen die in de fase van de vervolging en berechting gelden en ten aanzien waarvan in de ontwikkeling van de digitalisering naar de huidige stand van de theorie spanning te verwachten is of juist ondersteuning in de realisatie van het beginsel in de praktijk. Daartoe hebben wij eigen wetenschap, schriftelijke bronnen en de interviews gebruikt om die verwachtingen te bepalen en te valideren. Wat de ontwikkelingen betreft waaraan we aandacht besteden, hebben we ons gericht op de recente veranderingsprocessen in het kader van de overgang van papier naar elektronisch, zoals daarover gerapporteerd is door het OM en de zittende magistratuur. Voor het hoofdstuk over de toekomst, hoofdstuk 4, zijn vooral die ontwikkelingen verwerkt, die in de periode tussen nu en vijf jaren zo ver gevorderd zijn dat impact op de strafrechtspleging realistisch is, al is het maar in de vorm van eerste pilots voor de toepassing.

1.4 Leeswijzer

Het voorliggende rapport heeft na deze inleiding nog vier hoofdstukken. In hoofdstuk 2 worden twee perspectieven op de digitale strafrechtspleging ontwikkeld: het juridische en het informatiekundige perspectief. Er wordt een inventarisatie gepresenteerd van de relevante grondbeginselen van de strafrechtspleging en we ontwikkelen beginselen voor informatiesystemen. In de vorm van een matrix laten we zien wat een combinatie van deze perspectieven oplevert voor de beantwoording van onze onderzoeksvraag. In dat hoofdstuk worden deelvraag 1 en gedeeltelijk deelvragen 4 en 5 beantwoord. Hoofdstuk 3 beschrijft de recente ontwikkelingen in de strafrechtsketen, in het bijzonder de experimenten om de documentenstroom digitaal te maken. Deelvragen 2 en 3 worden daarin beantwoord. In hoofdstuk 4 wordt de toekomst verkend en wordt op de deelvragen 4 en 5 verder ingegaan. Een samenvattende conclusie uit de bevindingen is in hoofdstuk 5 opgenomen. Daarnaast snijden we daar punten voor discussie en verder onderzoek aan.

Hoofdstuk 2

Het kader voor een digitale strafrechtspleging

2.1 Inleiding

De digitalisering van de strafrechtspleging is al lang aan de gang[6] in die zin dat informatiesystemen en -toepassingen al vele jaren ingezet worden in organisaties in de strafrechtsketen. Iedereen gebruikt al jarenlang computers voor tekstverwerking en berichtenverkeer, gegevensopslag en registratie van handelingen en gebeurtenissen. Dat daarmee niets veranderd is in de werkwijzen, valt moeilijk vol te houden. Toch is het al die tijd mogelijk gebleken om in het juridische kader aan de overgang naar informatiesystemen slechts zeer beperkt gevolg te geven, waardoor het vermoeden rijst dat de systemen en applicaties nog niet veel meer doen dan het ondersteunen van de reeds lang gebruikelijke, wettelijk verankerde werkwijzen. Als die aanname juist is, valt daaraan de veronderstelling te koppelen, dat ook de fundamentele kenmerken en beginselen van de strafrechtspleging tot nu toe fier overeind konden blijven staan . Of dat het geval zal blijven, is de centrale vraag voor dit onderzoeksrapport.

Om de betekenis van de ontwikkelingen te verhelderen is een Engelstalig onderscheid behulpzaam, dat tussen *digitalization* enerzijds en *digitization* anderzijds. Onder *digitalization* verstaan we het inzetten van informatietechnologie om het proces van strafrechtspleging te vernieuwen. Onder *digitization* verstaan we het omzetten van papieren gegevensdragers naar elektronische gegevensdragers, zonder wezenlijke veranderingen in de werkwijze. *Digitization* is bijvoorbeeld aan de orde in de Wijziging van het Wetboek van Strafvordering en de Wet op de economische delicten in verband met het gebruik van elektronische processtukken.[7] Over de verhouding tussen beide fenomenen kan het volgende opgemerkt worden. Wanneer men ten aanzien van bestaande analoge informatie digitaal processen wil uitvoeren, zal de analoge informatie eerst digitaal gemaakt moeten worden. Papier moet tot digitale dataconfiguratie omgeturnd worden. In die situatie veronderstelt *digitalization* de voorafgaande *digitization*, maar dat is omgekeerd niet het geval. *Digitization* kan immers ook ter ondersteuning van de bestaande (analoge) werkwijzen plaatsvinden en dat gebeurt ook allerwege. Daarnaast kan gezegd worden dat de *digitization* voor de *digitalization* niet nodig is als er een nieuw digitaal werkproces in gebruik genomen wordt ten aanzien van informatie die (ook) digitaal beschikbaar is.

Het zoeken naar een goede Nederlandse versie van het begrippenpaar heeft nog geen bruikbaar resultaat opgeleverd. Het onderscheid zelf is niettemin nuttig, ook al zal het beeld in de praktijk wellicht niet al te scherp in zwart-wit getekend kunnen worden. De introductie van een wordprocessing systeem, het digitaal maken van een kaartenbak, het toepassen van een evenementenregistratiesysteem, het betekent niet zonder meer dat de rechtens relevante handelingen en beslissingen geheel of gedeeltelijk door informatiesystemen uitgevoerd

6. De regering gaat uit van een startpunt in de jaren zestig: *Kamerstukken II* 2015/16, 29279, 298, p. 1.
7. *Kamerstukken II* 2014/15, 34090, 3, p. 49-50.

worden. Men kan zich afvragen of tot nu toe alleen maar pure ondersteuning geleverd wordt, maar we zien vaak dat men dat wel voor ogen heeft.

Een mooi voorbeeld van de veelkleurige praktijk levert de invoering destijds van het bos/polaris systeem, dat inmiddels niet meer in gebruik is.[8] Met behulp van een geautomatiseerd systeem, waarin allerlei kenmerken van de af te handelen zaak ingevoerd moesten worden, kreeg de officier van justitie door de computer een eerste indicatie voor de strafeis aangereikt. Een deel van de besluitvorming werd door de computer overgenomen, zo zouden we nu kunnen stellen. Illustratief is echter, dat in het zojuist aangehaalde bericht van januari 2003 benadrukt werd dat dit systeem niet de voorbode is van 'de computer als officier en rechter'. Men bedoelde zo te zien vooral *digitization* en niet *digitalization*. De aanwezige, uitgebreide strafvorderingsrichtlijn werd slechts in de computer ingevoerd. Toch betekende het gebruik van het systeem in de praktijk dat bos/polaris een geautomatiseerde gestandaardiseerde onderlinge weging van diverse zaakskenmerken uitvoerde, waarvan de uitkomst van grote betekenis was voor het requisitoir van de officier van justitie ter zitting.[9] Dat is meer geweest dan alleen de richtlijnen van analoog naar digitaal omzetten.

Dit hoofdstuk bespreekt de kaders voor de strafrechtspleging. De inzet van IT in de strafrechtspleging brengt ons midden in een veld, waarin wij twee dimensies onderscheiden: de dimensie van de fundamentele grondslagen en beginselen van het strafrecht in ruime zin en de dimensie van de ontwikkeling van informatiesystemen. De strafvorderlijke beginselen en de ontwikkelingen van informatiesystemen hebben in dit onderzoek zowel een normatieve als een feitelijke betekenis.[10] Met die kanttekening is het onderscheid in dimensies bruikbaar om houvast te bieden bij de beantwoording van de onderzoeksvragen die betrekking hebben op een duiding/waardering van de ontwikkelingen tot nu toe en op het doortrekken van lijnen naar de toekomst.

Hierna volgt een paragraaf, waarin een beredeneerde keuze wordt gemaakt voor de beginselen van de strafrechtspleging die in het onderzoek betrokken zijn. Daar zal, in navolging van wat in hoofdstuk 1 al betoogd werd, blijken dat de onderzoeksvraag een zekere selectieve aanpak rechtvaardigt. Vervolgens komen principes en fundamentele aspecten van de IT-ontwikkeling aan de orde, ontleend aan de informatiekunde. Natuurlijk zal dan onmiddellijk opvallen hoe verschillend juristen en IT-deskundigen naar de digitalisering kijken, maar aangezien beide disciplines van invloed zullen zijn op de toekomst, hebben we beide nodig. Met een matrix in paragraaf 2.4.1 ondernemen we een eerste theo-

8. De bos/polaris richtlijnen zijn begin 2015 verlaten door het OM. Zie: P.M. Schuyt, 'Nieuwe strafvorderingsrichtlijnen voor het openbaar ministerie', *Sancties* 2015, 10; J.P. Balkema, 'Het strafrechtelijk sanctiestelsel. Een terugblik op vijfentwintig jaar', *Sancties* 2016, 2. Nader over bos/polaris zelf zie bijv. een OM-bericht van 21 januari 2003, nog te vinden op https://www.om.nl/vaste-onderdelen/zoeken/@53989/bepaalt-officier/ (laatst geraadpleegd 5 aug. 2016). Zie voor het afscheid van bos/polaris: Aanwijzing Kader voor strafvordering en OM afdoeningen (2015A001), te vinden op https://www.om.nl/organisatie/beleidsregels/@88217/aanwijzing-kader-0/ (laatst geraadpleegd 15 okt. 2016).
9. Afwijking van de bos/polaris richtlijnen leidde soms tot niet-ontvankelijkheid van het OM. Zie bijv. Rb. Amsterdam 2 december 2014, gepubliceerd in *NBSTRAF* 2015/122. Afwijking van de richtlijnen werd slechts toegestaan bij een goede motivering: Hof Den Haag 20 februari 2012, gepubliceerd in *NBSTRAF* 2012/277.
10. Hoe verleidelijk ook, we zullen het onderscheid niet karakteriseren als norm versus feit; de juridische grondslagen en beginselen als normatief kwalificeren en de ontwikkeling van informatiesystemen als feitelijk. Het zou aan de aard van de beide dimensies geen recht doen.

retische poging beide dimensies op elkaar te betrekken. In de daarop volgende paragrafen gaan we in op een aantal verbanden.

2.2 Strafvorderlijke beginselen

'Aan het Nederlandse strafprocesrecht liggen, zoals aan elk stelsel van strafprocesrecht, bepaalde uitgangspunten ten grondslag. […] In het (juridisch) spraakgebruik plegen deze verschillende uitgangspunten alle met de term beginsel te worden aangeduid.'[11]

2.2.1 DE DOCTRINE

Er is in de Nederlandse juridische literatuur geen eenduidige, gezaghebbende vaststelling van de funderende uitgangspunten en kenmerken van de strafrechtspleging aanwezig. Dat heeft er onder meer mee te maken dat onze rechtsvormende autoriteiten, de wetgever en de Hoge Raad, over het algemeen weinig conceptueel te werk gingen en vooral pragmatisch concrete regelingen of oplossingen formuleerden. De resultaten daarvan worden ook nog niet door iedereen als consistent met elkaar geapprecieerd. Dientengevolge circuleren er verschillende lijstjes en kan men de her en der spraakverwarring beluisteren, bijvoorbeeld in de bewering, dat iets wel een stelselmatige grondslag is, maar in de rechtspraktijk niet wordt toegepast. Een voorbeeld om de meerduidigheid van principes te illustreren biedt het zgn. materiële onmiddellijkheidsbeginsel. Volgens sommigen was en is het een principe van het – thans nog geldende – wettelijk stelsel van 1926, dat alle bewijs onmiddellijk ten overstaan van de beslissende rechter gepresenteerd dient te worden en dat om die reden de rechter zich bij de beslissing moet richten op mondeling ter zitting afgelegde verklaringen van getuigen, niet op de verhoorverslagen van de politie of de rechter-commissaris. Of dit klopt of niet, de Hoge Raad heeft de huidige procesvoering, die het tegenovergestelde van onmiddellijk is en zwaar leunt op schriftelijke verslagen, mogelijk gemaakt in de rechtspraak die begon met het befaamde De-auditu arrest van 1926. De wetgever maakte kennelijk geen dwingende keuze voor een beginsel en de rechtspraak van de Hoge Raad gaf de ruimte voor een zodanige wijze van procederen, dat velen nu stellen dat dit beginsel, ook wel het best-evidencebeginsel genoemd, helemaal niet een fundamenteel kenmerk van de Nederlandse strafrechtspleging is. Anderen daarentegen pleiten voor terugkeer naar de oorspronkelijke keuze van de wetgever, zich mede beroepend op rechtspraak van het Europese Hof voor de Rechten van de Mens. Dezen stellen dus dat het beginsel wél gelding heeft en dat de praktijk daarmee strijdig is. [12] Hiermee wordt geïllustreerd dat, om zicht te krijgen op beginselen in de zin van fundamentele kenmerken, een bestudering van de regelgeving en de praktijk nodig is. Dat gebeurt in de strafrechtelijke literatuur, de doctrine, en daarom moeten we nu ons voor dit rapport tot die doctrine wenden.

Keulen/Knigge onderscheiden allereerst de beginselen van een goede procesorde: het verbod van willekeur, het vertrouwensbeginsel, het gelijkheidsbeginsel, het beginsel van zuiverheid van oogmerk (détournement de pouvoir) en het beginsel van behoorlijke en billijke belangenafweging.[13] Daarnaast onderscheiden zij het rechtszekerheidsbeginsel, het legaliteitsbeginsel, de onschuldpresumptie, het in-dubio-pro-reobeginsel, het nemo-teneturbeginsel en het fairtrialbeginsel.

11. G.J.M. Corstens, *Het Nederlands strafprocesrecht,* bewerkt door M.J. Borgers, Deventer: Kluwer, 2014, p. 41.
12. Zie Corstens/Borgers, a.w. p. 50 en 782-785.
13. B.F. Keulen & G. Knigge, *Strafprocesrecht*, Deventer: Kluwer 2016, p. 21-22.

Corstens/Borgers noemen de rechterlijke onafhankelijkheid en onpartijdigheid, het legaliteitsbeginsel, het onschuldbeginsel, het recht op rechtsbijstand, vertaling en vertolking, het zwijgrecht, het recht op interne en externe openbaarheid, de motiveringsplicht en de beginselen van een behoorlijke procesorde zoals ook door Keulen/Knigge op de reeds aangehaalde plaats gesignaleerd. Brants, Mevis, Prakken en Reijntjes tot slot noemen als grondslagen de volgende beginselen: legaliteit, openbaarheid, onafhankelijkheid van de rechter en in hoge mate ook van de vervolgingsautoriteit, berechting op basis van materiële waarheidsvinding en erkenning van de verdachte als rechtssubject.[14]

Verschillende auteurs komen dus tot verschillende lijstjes met strafvorderlijke beginselen in de zin van de systematische grondslagen. Een overeenkomst tussen allen is wel dat ze de beginselen zowel ontlenen aan het Nederlandse recht als het internationale recht, waarbij vooral art. 6 van het EVRM in beeld komt. Daarmee is terecht erkend dat de regelgeving voor onze strafrechtspleging niet alleen in de nationale wetten terug te vinden is, maar dat het verdragsrecht eveneens bron van regeling is en daarom ook geraadpleegd moet worden voor het opsporen van funderende principes. De beginselen, afgeleid uit de tekst van art. 6 EVRM, zijn achtereenvolgens: het recht op een eerlijke behandeling, recht op een openbare behandeling, behandeling van de zaak binnen een redelijke termijn, rechterlijke onafhankelijkheid en onpartijdigheid, toegang tot een bij wet ingestelde rechter, de onschuldpresumptie, het recht op vertaling en vertolking, het recht op *adequate facilities*, het recht op rechtsbijstand en het ondervragingsrecht.

Een inventarisatie van beginselen kan op deze manier zomaar resulteren in een lijst van meer dan twintig items. Dat roept de vraag op of deze alle een plek in dit rapport moeten krijgen. Het antwoord op die vraag is nee. Het relatief beperkte karakter van dit onderzoek brengt mee dat keuzes gemaakt dienden te worden ten aanzien van de te behandelen beginselen, aansluitend bij de vraagstelling. Het leidende perspectief bij het maken van die keuze is geweest de vraag welke beginselen in potentie (het meest) kunnen of zullen worden beïnvloed door (de in dit rapport behandelde) IT-ontwikkelingen. Bij de bespreking van de inhoud van de geselecteerde beginselen zal die relevantie met betrekking tot de in dit rapport behandelde IT-ontwikkelingen nader aan de orde komen.

Om te bepalen welke beginselen dit zijn, is gebruik gemaakt van een tweetal ijkpunten, gewogen met gebruik van de expertise en ervaring in de onderzoeksgroep. Als startpunt is gebruik gemaakt van de door Van den Hoogen in zijn proefschrift, *E-justice, beginselen van behoorlijke elektronische rechtspraak*, gesignaleerde beginselen. De reden hiervoor is gelegen in het feit dat deze beginselen dicht in de buurt liggen bij de scope van ons onderzoek. Deze auteur is, weliswaar met een andere vraagstelling, eveneens bezig geweest met grondslagen voor rechtspleging in een digitale context. Een tweede ijkpunt werd gevonden bij de beginselen die door verschillende auteurs in de voor dit rapport bestudeerde bronnen in verband zijn gebracht met digitalisering in de strafrechtsketen.[15] De voorlopig lijst is vervolgens bij de interviews gevalideerd. De vraagstellingen waren mede toegespitst op de aldus geselecteerde beginselen. Tijdens de interviews is vervolgens gevraagd of er eventueel andere beginselen relevant

14. C.H. Brants, P.A.M. Mevis, E. Prakken en J.M. Reijntjes, 'Op zoek naar grondslagen', in C.H. Brants e.a. (red.) *Op zoek naar grondslagen. Strafvordering 2001 ter discussie,* Den Haag: Boom Juridische uitgevers 2003, p. 9.
15. De onderbouwing van deze keuze is in essentie verweven met het gehele rapport en de bijbehorende literatuurlijst. Opsomming daarvan op deze plaats is om redenen van efficiëntie en overzichtelijkheid achterwege gelaten.

zouden kunnen zijn in de ogen van de geïnterviewde persoon. Een uitbreiding van de reeds opgestelde lijst bleek niet nodig te zijn.

Zoals gezegd is het proefschrift van Van den Hoogen mede als startpunt gebruikt. Van den Hoogen onderscheidt een vijftal beginselen waarbij hij zich heeft laten leiden en inspireren door art. 6 EVRM.[16] Zijn vijf beginselen zijn: toegankelijkheid van rechtspraak, openbaarheid van rechtspraak, berechting binnen redelijke termijn, onafhankelijkheid en onpartijdigheid en een eerlijke behandeling. Bij deze opsomming is een tweetal kanttekeningen gepast. Voor wat betreft de onpartijdigheid van de rechter geldt dat het zeker een fundamenteel beginsel voor e-justice zal zijn. Het valt echter niet in te zien hoe onpartijdigheid beïnvloed wordt door digitalisering *an sich.* Om die reden beperken we dit aspect voor ons onderzoek tot slechts de rechterlijke onafhankelijkheid.

In de bestudeerde bronnen zijn de hierna genoemde beginselen naar voren gekomen, waarop de digitalisering een of andere vorm van invloed zal kunnen uitoefenen. Er zijn nog vele andere beginselen van belang voor de strafrechtspleging van nu en de toekomst, maar die krijgen in de beschouwing geen nadere aandacht, omdat met de thans beschikbare kennis niet te bevroeden valt of ze als gevolg van de digitalisering beter of minder goed uit zullen komen. Hierbij moet worden toegegeven dat volstrekte conceptuele zuiverheid en onderlinge begrenzing, met afwezigheid van overlapping in de kenmerken en beginselen, ons ook niet haalbaar gebleken is. We zullen dat verderop zoveel mogelijk tonen en onderbouwen wat de opsomming uiteindelijk bepaald heeft.

We bespreken achtereenvolgens:

- het legaliteitsbeginsel
- het principe van toegang tot de onafhankelijke rechter
- het beginsel van equality of arms; waarin mede begrepen de interne openbaarheid en de passende middelen voor de verdediging
- het openbaarheidsbeginsel
- het beginsel van betrouwbaarheid
- het tijdigheidsprincipe.

Voordat we deze beginselen zullen bespreken, verdient de onschuldpresumptie aparte aandacht. Het gebruik van bijvoorbeeld datamining om criminaliteitspatronen op te sporen en te beslissen wie van de burgers daadwerkelijk stelselmatig aandacht ‘verdienen’, is iets waarvan we aannemen dat het reeds (op grote schaal) gebeurt. Deze verwerking van gegevens vindt in eerste instantie plaats ten aanzien van personen (en instanties) waartegen geen verdenking van het begaan van een concreet strafbaar feit bestaat.[17] In de literatuur worden in verband daarmee vraagtekens gezet ten aanzien van de onschuldpresumptie.[18]

Het valt op dat de onschuldpresumptie nu vooral in het geding lijkt te zijn bij de opsporing. Aangezien de vruchten van het vooronderzoek wel doorwerken in de opvolgende schakels van de strafrechtsketen, is dit beginsel niet onbelangrijk. We hebben echter in hoofdstuk 1 de bewegingen binnen het territoir van de

16. Zie nader: R.H. Van den Hoogen, *E-justice, beginselen van behoorlijke elektronische rechtspraak*, Den Haag: Sdu 2007, hoofdstuk. 2.
17. S. Brinkhoff, ‘Big data datamining door de politie’, *NJB* 2016, p. 994.
18. M. Hildebrandt, ‘Data-gestuurde intelligentie in het strafrecht’, in: *Homo Digitalis* (Handelingen Nederlandse Juristen-Vereniging 2016-I), Deventer: Kluwer 2016, p. 188-196.

opsporing buiten het bestek geplaatst, om welke reden we op het belang van de onschuldpresumptie in de opsporing als zodanig hier niet verder zullen doorgaan. Wel heeft het handelen van de opsporingsautoriteiten met behulp van IT betekenis voor het beginsel van betrouwbaarheid, uitgewerkt in de richting van redelijke en billijke belangenafweging en het motiveringsbeginsel. Deze beginselen veronderstellen dat aan de beslissingen in de keten juiste gegevens ten grondslag liggen, en dat handelingen of beslissingen met feiten worden onderbouwd. Langs die weg komt de normerende werking van de onschuldspresumptie terug in ons blikveld. We behandelen dit uitgangspunt verderop bij het beginsel van betrouwbaarheid dat in de strafrechtspleging principieel op basis van feiten geoordeeld wordt. Daarin ligt besloten dat alleen beslist wordt op basis van aannames die voldoende feitelijke grond hebben.

Hoe zit het dan met de verdenking, zo kan men vragen. Dat is toch vaak de basis voor een handeling of beslissing en toch géén feit waarvan de juistheid wordt vastgesteld. Deze constatering klopt, maar neemt niet weg dat in de strafrechtspleging het principe geldt dat de juistheid van feiten ten grondslag ligt aan de handeling. De verdenking is inderdaad (nog) geen vaststelling van de materiële waarheid, maar een vermoeden, dat op feiten gebaseerd is. Zo definieert de wet het zelf in art. 27 lid 1 Sv: een uit feiten en omstandigheden voortvloeiend redelijk vermoeden van schuld. Een voorbeeld ter verduidelijking: een aangifte van het slachtoffer levert de verdenking op ten aanzien van een persoon die in de aangifte genoemd wordt. We gaan er dan van uit dat de aangifte daadwerkelijk gedaan is met de bewoordingen of strekking zoals in de informatiedrager vastgelegd is. Dat is de feitelijke juistheid waarop de verdenking gebaseerd is. Dat neemt niet weg dat de als dader aangewezen persoon voor onschuldig gehouden moet worden tot zijn schuld vastgesteld is volgens de regels van de wet.

Een tweede kwestie, die voor de bespreking van de beginselen aandacht verdient, is de bescherming van de persoonlijke levenssfeer. Een studie over digitalisering schrijven zonder aandacht aan de bescherming van de persoonlijke levenssfeer en – daarvan afgeleid – dataprotectie te besteden, lijkt een onmogelijkheid, gelet op de zorgen en bezwaren die vanuit aandacht voor de privacy naar voren gebracht kunnen worden. [19] Het is echter niet vol te houden dat privacyprotectie zelfstandig een juridisch grondbeginsel van de strafrechtspleging genoemd kan worden. Hoe geven we aan dit onderwerp dan toch een juiste plaats, zo is de vraag. Voor de oplossing hiervan hebben we ons wederom tot de doctrine gewend en dan valt op dat diverse auteurs de bescherming van de persoonlijke levenssfeer (in de zin van art. 10 GW en art. 8 EVRM) behandelen bij de legaliteit.[20] Art. 8 EVRM biedt daartoe ook een aanknopingspunt, omdat voor de inbreuken op het in lid 1 gegarandeerde recht op bescherming van de persoonlijke levenssfeer de eis geldt dat deze voorzien moeten zijn in de wet. Die wet moet bovendien aan bepaalde kwaliteitseisen voldoen. Deze stand van zaken heeft ons doen besluiten aandacht aan dit belangrijke onderwerp te besteden als we het legaliteitsbeginsel aan de orde stellen. Daarmee willen we niet suggereren dat in het strafrechtelijke legaliteitsbeginsel alle beginselen van

19. Vergelijk J. Kohnstamm, *Het spiegelkabinet van de argwaan*, speech 8 april 2005, te vinden op https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/artikelen/art_jko_2005_speech_njcm.pdf (laatst geraadpleegd 17 okt. 2016)

20 M.S. Groenhuijsen & G. Knigge, 'Afronding en verantwoording. Algemeen deel', in M.S. Groenhuijsen & G. Knigge (red.), *Afronding en verantwoording. Eindrapport Strafvordering 2001*, Deventer: Kluwer 2004, p. 25-29. A.M. Berkhout-van Poelgeest, 'Enkele vragen over de legaliteit in het strafproces (artikel 1 Sv)', in: C. Brants, P.A.M. Mevis en E. Prakken (red.), *Legitieme strafvordering. Rechten van de mens als inspiratie in de 21ste eeuw,* Antwerpen-Groningen: Intersentia Rechtswetenschappen, 2001, p. 29-31.

privacybescherming opgenomen zijn, integendeel. Een rechtmatige, en dus door regels beperkte omgang met inbreuken op de persoonlijke levenssfeer, is een principe voor al het overheidshandelen. Die beperkende regels, uit nationale en supranationale bronnen, binden de strafrechtelijke autoriteiten evenzeer als andere instanties. De binding aan de wettelijke regels – privacybeschermende en andere regels – is verankerd in het strafrechtelijke grondbeginsel van de legaliteit.

2.2.2 HET LEGALITEITSBEGINSEL

Als de wetgever voor het strafrecht ergens een principiële keuze heeft gemaakt, dan is dat wel in de artikelen 1 Wetboek van Strafrecht (een reprise van art. 16 van de Grondwet, tevens opgenomen in art. 7 EVRM) en 1 Wetboek van Strafvordering. De wet dient het uitgangspunt te zijn. Hoe ruim of beperkt vervolgens de legaliteit is, vormt voorwerp van vele doctrinaire beschouwingen in zowel het materiële als het formele recht. Voor dit onderzoek is echter slechts het formele deel van het legaliteitsbeginsel van belang dat is gecodificeerd in art. 1 Sv dat bepaalt *'Strafvordering heeft alleen plaats op de wijze bij de wet voorzien'*. Dit gedeelte ziet op de opsporing, vervolging en berechting van strafbare feiten. Dit artikel richt zich in de eerste plaats tot de overheid (wetgever) met de opdracht om strafvordering bij wet te regelen. Deze opdracht omvat zowel het toedelen van bevoegdheden (opsporing, vervolging, berechting) als de uitwerking daarvan. Daarnaast richt het artikel zich ook tot alle autoriteiten in het strafproces, waaronder opsporingsambtenaren (politie), openbaar ministerie (OM), de rechter-commissaris (R-C) en de zittingsrechter. Deze actoren dienen zich bij de opsporing c.q. vervolging c.q. berechting te houden aan de grenzen van de wet. Tot slot heeft het legaliteitsbeginsel een waarborgfunctie ten opzichte van de verdachte. Deze is beschermd tegen de (eventuele) willekeur van overheidswege. Het legaliteitsbeginsel eist dus dat strafrechtelijke uitspraken geschieden op basis van de wet en dat het strafrechtelijk handelen zich conform de wet voltrekt. In de literatuur wordt doorgaans het standpunt ingenomen dat het legaliteitsbeginsel geen keurslijf van regels dient te geven. Het dient om een structuur te bieden waarbinnen de procespartijen zinvol en doelgericht kunnen opereren en vormt een waarborg voor een behoorlijke taakuitoefening of rolvervulling door de procesactoren.[21]

De wetgever tracht met het oog op de legaliteit zoveel mogelijk de geschreven regeling bij de ontwikkeling van de tijd te houden. Ook de digitalisering in de strafrechtsketen tot nu toe is gepaard gegaan met een bijbehorend wetgevingsproces. De wetgever heeft de digitale processtukken in de wettelijke regeling een plaats gegeven, nadat eerst alleen de digitale aangifte geregeld was. [22]

Een bevoegdheid mag slechts worden gebruikt ten behoeve van het doel waarvoor ze is gegeven. Omdat schending van het beginsel van *détournement de pouvoir* samenhangt met de vraag welke grenzen de regelgeving stelt, wordt dit beginsel behandeld als subonderdeel van het legaliteitbeginsel. In de literatuur wordt gewezen op het mogelijke probleem dat met informatiesystemen vaak

21. Zie onder meer: Groenhuijsen & Knigge 2004, p. 8-9.
22. Zie bijv.: Wet digitale processtukken Strafvordering, 17 februari 2016, *Stb*. 2016, 90 en Besluit houdende regels betreffende het gebruik van elektronische stukken (Besluit digitale stukken Strafvordering, *Stb*. 2016, 359). Van Wees waarschuwt niettemin: *'Ten slotte moet steeds worden bewaakt dat de techniek niet op de loop gaat met de wet en de normen van de rechtsstaat.'* M.E. van Wees, 'Modernisering en digitalisering van het strafproces', *DD* 2015, 72, p. 812.

meer *kan* dan (volgens de regelgeving) *mag*.[23] Dat maakt dit aspect van legaliteit van belang voor het voorliggende rapport.

Een andere consequentie van respect voor de wet is de instandhouding c.q. bewaking van de wettelijke taakverdeling. Met de taakverdeling in de strafrechtspleging is niet zozeer een procesgang handig verkaveld, er is een bepaalde garantie beoogd.[24] Het OM staat in vergelijking met de politie meer op afstand van een onderzoek, zodat het in zijn taakuitoefening (leiding en toezicht op de opsporing, beslissen tot vervolging) een bepaalde mate van magistratelijkheid aan de dag kan leggen. De rechterlijke macht staat nog meer op afstand en is bovendien omgeven met extra waarborgen van persoonlijke en institutionele onafhankelijkheid ten opzichte van de overige staatsmachten. De meest verstrekkende beslissingen worden dan ook aan de rechter toevertrouwd[25], evenals het toezicht op de meest ingrijpende onderzoeksmethoden. Wanneer de digitalisering dwingt tot een hoge mate van afstemming en afhankelijkheid tussen ketenpartners ter zake van de technologische keuzes en de te implementeren werkprocessen, rijst de vraag of de zelfstandigheid van de instanties niet in het geding is. Die zelfstandigheid heeft een waarborgfunctie, welke onder druk zou komen als er te veel onderlinge betrokkenheid komt of wellicht zelfs dominantie van een actor die in het wettelijk systeem niet zou mogen domineren. Als voorbeeld kan de overdracht van dossiers aan de zittende magistratuur genoemd worden. Het Openbaar Ministerie, dat verantwoordelijk is voor de samenstelling van het procesdossier, zou door zijn IT-keuzes in verregaande mate kunnen bepalen wat de speelruimte voor het werk van de strafrechter is. Voor iets vergelijkbaars wordt wel gevreesd in de relatie OM-politie.[26]

In het kader van de civielrechtelijke implementatie van het programma KEI hebben de kantonrechters in Amsterdam er met een in het NJB gepubliceerde brief[27] op gewezen dat de voorgenomen digitalisering bepaalde risico's meebrengt. Zij beargumenteren dat digitalisering ook standaardisering meebrengt. Dit laatste zou ertoe kunnen leiden dat rechters minder maatwerk kunnen leveren[28] en op het niveau van een individuele zaak aan beslissingsmogelijkheden moeten inboeten en daarmee in hun autonomie worden beperkt. Uit het NRC van 19 maart 2016 komt het volgende illustratieve citaat:

> *'De kwaliteit van de strafdossiers die de politie instuurt, […] is matig, zegt Pennink. In ongeveer dertig procent van de dossiers zit geen wettig bewijs. Of ze zijn zó summier dat onduidelijk is wat er nu precies is waargenomen. Het hele proces van vervolging bij justitie is geautomatiseerd. Bij het parket „kijkt daar vrijwel niemand meer inhoudelijk naar", zegt Pennink. De burger die bij de kantonrechter dan bezwaar komt maken, heeft snel het voordeel van de twijfel. Ook bij de officier trouwens – die eist soms zelf al vrijspraak, vermin-*

23. Zie bijv.: M. Roessingh, 'iColumbo kan meer dan hij mag', *Trouw*, 2 november 2013 en A. Das, 'Waarom de rechtspraak fishing expeditions niet moet faciliteren', *NJB* 2016, p. 1180.
24. Zie onder meer: Corstens/Borgers 2014, p. 42.
25. Art. 113 lid 3 GW: 'Een straf van vrijheidsontneming kan uitsluitend door de rechterlijke macht worden opgelegd.'
26. Verderop in dit rapport (par 3.3 en 3.5) zal blijken dat de eigenstandigheid van de actoren gevolgen gehad heeft, ook al heeft dat diversiteit in technisch opzicht tot gevolg.
27. A.W.J. Ros, 'KEI: Kans of keurslijf', *NJB* 2016, 5, p. 339-341.
28. Het leveren van maatwerk is opgenomen in het interne beleidsdocument; Professionele standaarden strafrecht' Vindplaats: https://www.rechtspraak.nl/SiteCollectionDocuments/20160220-professionele-standaarden.pdf. p. 8 (laatst geraadpleegd op 15 okt. 2016).

dert boetes of vraagt om voorwaardelijke straffen. De strafzittingen lijken zo net een publieke archiefopruiming van justitie.'[29]

Met name de opmerking over automatisering van het proces van vervolging roept de vraag op of 'de computer' de persoon daarachter voldoende ruimte laat om zelfstandig en onafhankelijk tot een inhoudelijke beslissing te komen en of dat in alle gevallen door de wet geëist wordt. In dat kader moet de recente uitspraak van de Hoge Raad vermeld worden over de boetepraktijk in bepaalde WAHV-zaken.[30] In een vordering tot cassatie in het belang der wet had de Advocaat-Generaal bij de Hoge Raad aan het hoogste rechtscollege een vraag voorgelegd inzake de automatische sanctieoplegging, zonder tussenkomst van een persoon, ter zake van niet naleving van de APK-plicht. De Hoge Raad oordeelde dat de werkwijze van de betrokken instanties (RDW en CJIB) niet in strijd is met het legaliteitsbeginsel. De tekst en de strekking van de bepaling, art. 3 WAHV, verzetten zich er niet tegen, dat na automatische systeemvergelijking volledig geautomatiseerd een bestand met overtredingen gegenereerd en aan het CJIB overgedragen wordt, waaraan het CJIB automatisch de sanctiebeschikkingen koppelt. Blijkens de wetsgeschiedenis was deze werkwijze voorzien. De ambtenaar had voor de productie van het bestand met overtredingen het systeem met generieke instructies gevoed. De HR neemt daarop het feitelijk oordeel van het Hof over dat de sancties door die ambtenaar opgelegd waren. In aanvulling op deze vaststelling is niet vereist dat per geval een ambtenaar persoonlijk de eventuele bijzondere omstandigheden onderzoekt en in de beoordeling betrekt. Aldus blijft de onderhavige boetepraktijk binnen de grenzen die de wet stelt.[31]

Niet alleen de strafrechtspleging, maar alle overheidshandelen is onderhevig aan het principe dat de persoonlijke levenssfeer gerespecteerd wordt en inbreuken daarop alleen rechtmatig zijn als zij door de wet veroorloofd en gereguleerd zijn. Art. 8 EVRM waarborgt het recht van eenieder op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Brinkhoff zegt terecht dat *'Anno 2016 veel (gevoelige) informatie van en over burgers digitaal beschikbaar is. Deze informatie is bijvoorbeeld opgeslagen in de talrijke digitale databases van zowel private ondernemingen als overheidsinstanties. Het internet biedt eveneens een steeds groter wordende hoeveelheid (vrij toegankelijke) persoonsgegevens.'*[32] Het is evident dat het merendeel van deze gegevens betrekking heeft op onschuldige (of in ieder geval niet verdachte) burgers. Het doorzoeken van die gegevens zal dan ook in potentie de privacy van burgers in bepaalde mate schenden. De vraag die daarbij opkomt is of en zo ja, hoe de privacy van met name de onschuldige, maar in mindere mate ook de wel verdachte[33] burgers is gereguleerd en beschermd.[34]

29. NRC 19 maart 2016. Vindplaats: https://www.nrc.nl/handelsblad/2016/03/19/bij-de-gewonemensenrechter-1600515 (laatst geraadpleegd op 15 okt. 2016).
30. HR 16 febr. 2016, ECLI:NL:HR:2016:240, *NJ* 2016/404.
31. Zie ook Wetenschappelijke Raad voor het Regeringsbeleid (WRR), *Big Data in een vrije en veilige samenleving*, Amsterdam University Press, 2016, in welk rapport een stevig verbod op automatische besluitvorming in het geval van Big Data processen wordt aanbevolen; p. 142.
32. Brinkhoff 2016; WRR 2016, p. 66-67.
33. Zo reguleert de Wbg en de Wpg wel de verzameling en verwerking van persoonsgegevens, maar kan de privacy van verdachten makkelijker opzij worden gezet (doelbindingsbeginsel) dan die van niet verdachte burgers.
34. En dat die bescherming serieus genomen dient te worden blijkt gevoeglijk uit de uitspraak van het Hof Justitie eind 2014 waarbij de omstreden 'dataretentierichtlijn' in zijn geheel werd vernietigd, onder meer wegens een te grote schending van de privacy van burgers die onvoldoende proportioneel bleek. Zie: HvJ EU 8 april 2014, C293/12 en C594/12 *(Digital rights Ireland en Seitlinger)*. Nader over

Het is een gegeven dat digitaal opgeslagen data gevoelig zijn voor onwettige beschikbaarheid of verwerking. Dat kan gebeuren door inbraak van buitenaf, maar ook door fouten van binnenuit. Zo lekten door een fout van een ambtenaar bij de gemeente Rotterdam eerder dit jaar persoonsgevoelige gegevens van 15.000 burgers uit.[35] Het valt aan te nemen dat deze en andere problemen zich binnen de strafrechtsketen eveneens kunnen voordoen. De eis van conformiteit aan de wet heeft natuurlijk gevolgen voor de beveiliging van data, zoals de stukken in het digitale dossier.[36] Problemen met, of lekken in de beveiliging alsmede menselijke fouten in de omgang met de informatietechniek kunnen (en zullen) leiden tot problemen die mede hun impact zullen hebben op de privacy van betrokkenen. De relevantie van de privacy voor dit onderzoek is hiermee nog eens extra onderbouwd.[37]

2.2.3 TOEGANG TOT DE RECHTER

Het respecteren van de wet betekent ook dat de procespartijen toegang hebben tot de rechter die de wet toegekend heeft. Dit principiële uitgangspunt wordt zelfstandig genoemd, bijvoorbeeld in art. 17 van de Grondwet. Een rubricering onder het legaliteitsbeginsel zou evengoed te rechtvaardigen zijn. Het valt echter op dat in de doctrinaire lijst de toegang tot het recht/de rechter afzonderlijk naar voren komt en daarom volgen wij hier die keuze. In de uitwerking zal wellicht met legaliteit enige overlap niet te vermijden zijn en dat geldt evenzeer voor de zo dadelijk te noemen *adequate facilities*. Dat bleek indirect al toen wij hierboven de waarborgen van de onafhankelijkheid van de rechter in par. 2.2.2 bespraken. De toegang tot de rechter is gefundeerd in de bijzonderheid dat deze institutie omgeven is met garanties voor onafhankelijkheid en onpartijdigheid. Die hadden dus evengoed hier genoemd kunnen worden, maar er is meer.

Het opwerpen van digitale drempels, of juist het verlagen van drempels door digitalisering voor de procesactoren, is allereerst te beschouwen vanuit het perspectief van het recht voor de verdediging op voldoende voorzieningen, maar te hoge drempels komen binnen de werking van het beginsel van toegang tot de rechter. [38] Bij de digitalisering in de vreemdelingenketen en het burgerlijk proces is in dat verband een vraag gesteld over het verplichte karakter van digitaal procederen. Om de toegang tot de rechter niet ongeoorloofd te blokkeren is de verplichting in het burgerlijk proces nu alleen afgekondigd voor professionele

deze uitspraak zie bijv. H. Hijmans, 'De ongeldigverklaring van de Dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof van Justitie', in: *NtEr* 2014, 7. Voor een meer algemene kritische noot zie de reeds aangehaalde preadviezen van de NJV vergadering 2016.

35. Zie nader: http://nos.nl/artikel/2091635-privegegevens-rotterdammers-op-straat-door-fout-ambtenaar.html (laatst geraadpleegd op 15 okt. 2016).
36. Een relatie die ook het CBP niet is ontgaan getuige zijn advies bij het wetsvoorstel digitale processtukken, p. 3 (bijlage bij: *Kamerstukken II* 2014/15, 34090, 3).
37. Koops c.s. 2016, p. 129-130 inventariseren de materie op een andere wijze. Zij noemen de rechtsgoederen: vertrouwelijkheid van gegevens, integriteit van gegevens en beschikbaarheid van gegevens.
38. Van den Hoogen 2007, p. 33.

partijen.[39] Ter zake van het strafrecht zal in de toekomst in ieder geval ook gerekend moeten worden met digitaal minder geverseerde justitiabelen.[40]

2.2.4 EQUALITY OF ARMS / INTERNE OPENBAARHEID / ADEQUATE FACILITIES

Equality of arms, ofwel het beginsel van gelijkheid van wapenen, vloeit voort uit het meeromvattende recht op een eerlijk proces zoals gewaarborgd in art. 6 EVRM. *Equality of arms* houdt, kort gezegd, in dat in een procedure tegenover elkaar staande partijen over gelijke kansen en mogelijkheden dienen te beschikken. Het EHRM verwoordt de inhoud van *equality of arms* als volgt:

> *'equality of arms implies that each party must be afforded a reasonable opportunity to present his case – including his evidence – under conditions that do not place him at a substantial disadvantage vis-à-vis his opponent'*.[41]

Voor het doel van dit onderzoek onderscheiden we binnen de *equality of arms* twee nadere, elkaar deels overlappende, deelonderwerpen: interne openbaarheid en de adequate faciliteiten voor de verdediging.

Voor dit onderzoek is allereerst van belang dat voor alle procespartijen tijdens het onderzoek ter terechtzitting alle processtukken waarop de rechter zijn beslissing kan funderen bekend zijn. De rechter mag niet over meer of andere informatie beschikken dan de procespartijen. Het recht op kennisneming van processtukken kan worden gezien als uitwerking van het beginsel van interne openbaarheid[42] en is in Nederland geregeld in art. 30 e.v. Sv. Art. 6 lid 3 onder b EVRM geeft de verdachte het recht te beschikken over de tijd en faciliteiten (*adequate facilities*) die nodig zijn voor de voorbereiding van zijn verdediging. Tot die faciliteiten behoort in ieder geval het recht van te voren kennis te nemen van de gedingstukken.[43] Het beginsel van *equality of arms* brengt verder mee dat partijen, over en weer, in de gelegenheid dienen te worden gesteld om elkaars stukken op adequate wijze te bestuderen en daarop commentaar te leveren.[44] Verdediging, OM en rechter dienen dus over dezelfde informatie te beschikken, in die zin dat wat door het OM aan de rechter voorgelegd wordt, ook ter beschikking van de verdediging moet staan. Het is niet zo dat in alle stadia van de zaak allen over dezelfde stukken moeten beschikken. Het OM stelt het dossier voor de rechter samen en kan binnen zekere grenzen stukken weglaten.[45] Alles wat aan

39. Zie bijv. Rechtspraak Nieuwsbrief 14 juli 2016, https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Wetten-digitaal-procederen-aangenomen.aspx. Zie nader: E. Bauw, 'KEI, een gamechanger voor de civiele en bestuursrechtspraak?', in: *RMThemis* 2016, 2, p. 56; C.M. Aarde & J.E.J. Prins, 'Digitalisering binnen de rechtspraak: van KEI naar Big Data', in: *RMThemis* 2016, 2, p. 63.
40. Deze vraag is ten aanzien van KEI civiel en bestuur ook opgeworpen in een recent artikel in het NRC. Zie: https://www.nrc.nl/handelsblad/2016/03/19/bij-de-gewonemensenrechter-1600515. Op rechtspraak.nl verscheen al snel een tegenreactie. Zie: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Toegang-tot-kantonrechter-blijft-gewaarborgd.aspx (beide links laatst geraadpleegd op 15 okt. 2016).
41. EHRM 27 oktober 1993, nr. 14448/88, *NJ* 1994, 534, m.nt. H.J. Snijders & E.J. Dommering, *(Dombo/Nederland),* r.o. 33.
42. Corstens/Borgers 2014, p. 48. Keulen/Knigge 2016, p. 229; zie ook bijv. EHRM 16 februari 2000, nr. 28901/95, *(Rowe en Davis/Verenigd Koninkrijk).*
43. Keulen/Knigge 2016, p. 228; Hildebrandt 2016, p. 189. Zie voor jurisprudentie inzake de inzage in het procesdossier bijv. EHRM 24 juni 1993, nr. 14518/89 *(Schuler-Zgraggen/Zwitserland).*
44. EHRM 18 maart 1997, nr. 21497/93, *NJ* 1998, 278, m.nt. H.J. Snijders *(Mantovanelli/Frankrijk).*
45. Zie hierover nader: Reijntjes 2009, p. 54-58.

de rechter voorgelegd wordt, behoort de verdachte (en zijn advocaat) te kunnen krijgen. Ten slotte geldt dat de verdediging, op gelijke voet als het OM, ook stukken aan het procesdossier moet kunnen toevoegen.
In het algemeen wordt aangenomen dat digitaal procederen, op basis van digitale stukken, het mogelijk maakt om stukken sneller en eerder aan alle betrokken actoren ter beschikking te stellen.[46]

> *'Ja, alles […] wordt gedeeld met alle partijen. Het kan natuurlijk wel zo zijn dat er op het laatste moment nog iets wordt toegevoegd aan het dossier. Maar het grote voordeel van digitaal procederen is dat alle partijen over dezelfde stukken kunnen beschikken. Je "mist" geen fax van vlak voor de zitting.'*[47]

In het kader van digitaal procederen kan naast het voorgaande nog worden gewezen op de verschillende mogelijkheden die een digitaal dossier biedt voor verschillende groepen gebruikers. Voor het inzien en (met name) doorzoeken en bevragen van zo'n dossier zijn aanvullende voorzieningen in de zin van software nodig. Zou het dan problematisch zijn, dat de ene partij over voorzieningen beschikt die het mogelijk maakt zaken uit een dossier te halen (verbanden, kleine details in een zeer groot dossier) die voor anderen vrijwel onmogelijk te achterhalen zijn, zo kan men vragen. In het kader van de *equality of arms* zal de vraag aan de orde moeten komen tot welke hoogte het verschil in deze secundaire faciliteiten principieel problematisch is.[48] Daarbij moet een onderscheid in het oog gehouden worden tussen de beschikbaarheid van het digitale dossier en de aanvullende applicaties voor bewerking of verwerking. Het niet beschikbaar stellen van de dossier*inhoud* is in ieder geval ongeoorloofd. Als die inhoud vervolgens met diverse applicaties te verwerken is en er zijn geen onredelijke kosten aan verbonden, komt het onderhavige beginsel niet onder spanning te staan. In het bijzonder de leden van de advocatuur zouden het zelfs wel verkieselijk kunnen vinden om hun eigen bewerkingapplicatie te hanteren. Dat ondersteunt hun onafhankelijkheid ten opzichte van de vervolgings- en berechtingsautoriteiten.

Interne openbaarheid gaat niet helemaal op in de equality of arms tussen vervolging en verdediging. Ook voor het slachtoffer heeft de interne openbaarheid gevolgen. Deze heeft recht op (gedeeltelijke) inzage in stukken.

Uit de jurisprudentie van het EHRM halen we nog een interessant aspect van interne openbaarheid naar voren. Het Straatsburgse Hof legt een verbinding met de toegang tot de behandeling van de zaak ter terechtzitting. Onderstaand citaat uit een uitspraak verwijst naar het recht om van de voor hem relevante informatie direct kennis te nemen.

> *'In the interests of a fair and just criminal process it is of capital importance that the accused should appear at his trial, both because of his right to a hearing and because of the need to verify the accuracy of his statements and compare them with those of the victim – whose interests need to be protected – and of the witnesses […] Article 6, read as a whole, guarantees the right of an accused to*

46. Het advies van de reclassering bij het wetsvoorstel digitale processtukken stelt zelfs onomwonden *'dat men op die manier sneller over de juiste informatie kan beschikken zodat er efficiënter gewerkt kan worden';* bijlage bij: *Kamerstukken II* 2014/15, 34090, 3, p. 1.
47. L. Hesselink, 'Ervaringen met digitaal procederen over asiel en bewaring. We moeten eraan', in: *A&MR* 2016, 2, p. 75.
48. Een vergelijkbaar risico werd ook door Van den Hoogen reeds onderkend. Zie: Van den Hoogen 2007, p. 111.

participate effectively in a criminal trial. In general this includes, inter alia, not only his right to be present, but also to hear and follow the proceedings.'[49]

In de zaak die tot deze uitspraak leidde, klaagde de verdachte dat hij niet fysiek, maar slechts bij wege van videoconference 'aanwezig' heeft kunnen zijn bij zijn terechtzitting. Dat in deze specifieke zaak uiteindelijk geen schending van art. 6 EVRM wordt aangenomen brengt geen verandering in de geldende uitgangspunten, doch geeft slechts aan dat deze niet absoluut zijn. De door de digitalisering gefaciliteerde mogelijkheden van *onlineconferencing* dienen zich in de verschillende fasen van de strafrechtspleging aan. Mits zorgvuldig toegepast zouden deze mogelijkheden gebruikt kunnen worden met respect voor de waarborgen van art. 6 EVRM.

Een praktische toepassing van het beginsel van interne openbaarheid kan, althans in theorie, worden gevonden in de mogelijkheid om (bewijs)stukken ter zitting inzichtelijk te maken, bijvoorbeeld op schermen, voor alle procespartijen. Het moge geen verrassing zijn dat de digitale mogelijkheden voor deze en verwante toepassingen reeds lange tijd bestaan. Hierin liggen derhalve mogelijkheden voor gebruik in de strafrechtsketen, die nu al benut worden.

2.2.5 OPENBAARHEID

Het beginsel van openbaarheid, hier bedoeld als de openbaarheid naar buiten, wordt omschreven als het principe dat het strafproces toegankelijk is voor de rechtsgenoten, dus voor hen die daarbij niet als procesdeelnemer direct zijn betrokken.[50] In de praktijk is de uitwerking hiervan dat zowel het onderzoek ter terechtzitting (art. 269 lid 1 Sv) als het uitspreken van het vonnis (art. 362 lid 1 Sv) in het openbaar plaatsvindt.[51] Het meest basale doel hiervan is het mogelijk maken van controle op de rechtspleging. Verder speelt ook een rol dat de openbare terechtzitting ten opzichte van de buitenwereld iets demonstreert. Er wordt op criminaliteit gereageerd met een door het recht ingekaderde reactie.

In de Nederlandse procescultuur vervult het schriftelijke dossier een spilfunctie. Dit schriftelijke dossier dat de basis vormt voor het onderzoek ter terechtzitting is echter niet openbaar. Van Lent constateert in haar dissertatie dat het zonder kennis van het dossier in de meeste gevallen moeilijk te volgen is wat er op een terechtzitting gebeurt, en voor een juridische leek vrijwel onmogelijk zich een gefundeerd oordeel over de strafzaak en de behandeling daarvan te vormen.[52] Nu de externe openbaarheid in Nederland beperkt lijkt tot de zitting en uitspraak[53] is de vraag wat de relevantie van dit beginsel is voor dit onderzoek. Allereerst kan worden gewezen op het gemak waarmee in de zittingszaal stukken van het dossier met de betrokken partijen, maar ook overige aanwezigen, gedeeld kunnen worden, simpelweg door deze te laten zien op bijvoorbeeld een groot scherm. Ook het direct afspelen van verschillende soorten media kan zonder al te veel problemen en voor eenieder toegankelijk gebeuren.[54] Voor het overige kan hier verwezen worden naar het onderzoek van De Blok e.a.

49. EHRM 5 oktober 2006, 45106/04 *(Marcello Viola/Italie).*
50. L. van Lent, *Externe openbaarheid in het strafproces* (diss.), Den Haag: Bju 2008, p. 1; Corstens/Borgers 2014, p. 49.
51. Zie in dit verband ook art. 6 lid 1 EVRM.
52. Van Lent 2008, p. 4.
53. Iets dat ook in de relevante internationale verdragen het uitgangspunt lijkt te zijn. Zie: Van Lent 2008, p. 2.
54. Dit voordeel voor de externe openbaarheid werd in de interviews meermaals genoemd.

die ten aanzien van één der onderzochte landen constateren: *'In Estland is het ontwerp van E-file gestoeld op het bereiken van transparantie, voor zowel partijen in de keten als voor de burger. Het publieke deel van E-file geeft burgers inzicht in de strafzaken waarbij zij betrokken zijn. Voor de slachtoffers geeft dit systeem daarmee inzicht in de vorderingen in de strafzaak en ook in de straf die de dader uiteindelijk opgelegd krijgt.'*[55] Hiermee wordt direct duidelijk dat wat ons betreft externe openbaarheid als beginsel meer behelst dan louter de 'open deur' tijdens zitting en uitspraak.[56] Ook informatieverstrekking aan media en publiek kan daar bijvoorbeeld onder worden geschaard. Wellicht biedt een gedeeltelijk publiek openbaar deel van de beschikbare informatie (naar Ests voorbeeld) daarvoor een aanknopingspunt. Voor het overige kan bij externe openbaarheid worden gedacht aan de publicatie van uitspraken via media als rechtspraak.nl.[57] Niet alleen de transparantie van de rechtspraak, maar ook de controleerbaarheid van beweringen/impressies daarover wordt ermee gediend.[58]

Zowel juridisch als informatietechnisch sluit externe openbaarheid aan bij de interne openbaarheid, maar de eerste brengt wel extra eisen met zich mee. Publiek delen van informatie impliceert bijvoorbeeld voorzieningen om informatie te anonimiseren en om gegevens te kunnen 'zwartlakken'. Dat vereist ook een systeem van check-and-doublecheck om te waarborgen dat er geen fouten mee gemaakt worden. Wat eenmaal uit handen is, valt immers niet meer terug te halen en de vermenigvuldiging en verspreiding gaat in de digitale wereld nog weer sneller dan in de papieren wereld.

2.2.6 BETROUWBAARHEID; BELANGENAFWEGING, WAARHEIDSVINDING EN MOTIVERING

Het beginsel van betrouwbaarheid van de strafrechtspleging stelt de norm, dat de handelingen en beslissingen – waarmee invloed uitgeoefend wordt op de levens van individuele burgers – gebaseerd zijn op de feiten, voortkomen uit een redelijke afweging van alle belangen en voorzien zijn van een toereikende onderbouwing. Het tegendeel zou men willekeur kunnen noemen, veelal de signatuur van een autoritaire en corrupte strafrechtspleging. Er behoort een zekere en navolgbare band met de vastgestelde feiten te bestaan en die vaststellingen zelf moeten ook verantwoord worden op een wijze die controleerbaar is.

Uit de literatuur komt naar voren dat digitalisering met zich meebrengt dat de gegevens, feiten en data die een systeem genereert niet altijd even makkelijk en

55. C. de Blok e.a., *Digitalisering in strafrechtsketens. Ervaringen in Denemarken, Engeland, Oostenrijk en Estland vanuit een supply chain perspectief*, WODC 2014, p. 13.
56. In vergelijkbare zin: Van Lent 2008.
57. Recent is een nieuwe zoekmachine geïntroduceerd waarmee ruim 4 miljoen nationale en Europese uitspraken voorzien van een European Case Law Identifier (ECLI) kunnen worden gevonden. De zoekmachine is te bereiken via: https://e-justice.europa.eu/content_ecli_search_engine-430-nl.do. Voor nadere informatie zie: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Miljoenen-uitspraken-uit-Europese-landen-nu-online-doorzoekbaar.aspx. Over de wenselijkheid van het publiceren van elke uitspraak zie: Van den Hoogen 2007, p. 11.
58. Zie voor een voorbeeld uit de arbeidsrechtelijke praktijk: Volkskrant 30 juni 2016, vindplaats: http://www.volkskrant.nl/economie/wet-asscher-werkt-averechts-personeel-ontslaan-alleen-maar-moeilijker~a4330296/. *"In het onderzoek zijn van vier rechtbanken […] alle uitspraken geanalyseerd, dus ook de rechterlijke beslissingen die niet openbaar zijn gemaakt. Dan blijkt dat het aantal keren dat de rechter het aangevraagde ontslag verbiedt meer dan verdubbeld is […] Opmerkelijk is dat dit onderzoek een heel ander beeld van de nieuwe ontslagpraktijk oplevert dan de rechterlijke uitspraken die tot dusver op internet zijn gepubliceerd. Op grond van alleen de gepubliceerde uitspraken lijkt er voor werkgevers nauwelijks iets veranderd."*

niet voor iedereen even makkelijk op juistheid te controleren zijn.[59] Een bewering kan echter systematisch correct en als zodanig te controleren zijn, maar afzonderlijk daarvan geldt dat een beoordeling van de feitelijke juistheid ook vereist is. Een 'behoorlijke' rechtspraak brengt immers mee dat deze slechts kan geschieden aan de hand van 'juiste' feiten. De Nederlandse strafrechter is daarbij gehouden actief aan waarheidsvinding te doen. Deze feiten vormen ook de basis voor het beginsel van behoorlijke en billijke belangenafweging en de motiveringsplicht, de verwezenlijking waarvan zich moeilijk laat denken zonder dat de betrouwbaarheid van de onderliggende gegevens in voldoende mate gewaarborgd is. De genoemde beginselen hebben als zodanig echter een voor dit rapport te grote reikwijdte zodat wij ertoe hebben besloten om betrouwbaarheid en behoorlijkheid, in de zin van uitspraak doen op basis van juiste gegevens, voor gebruik binnen dit rapport als strafvorderlijk beginsel te onderscheiden.[60] Daarbinnen zijn de subonderwerpen veiligheid (van digitale data) en de juistheid van de aan de beslissing ten grondslag liggende gegevens (integriteit) onderscheiden.

Veiligheid

Onmiskenbaar gaat het gebruik van digitale gegevens gepaard met nieuwe mogelijkheden om die gegevens te manipuleren.[61] Een oorspronkelijk juiste weergave van een feitelijke waarneming kan in de digitale vorm gemakkelijk inhoudelijk aangepast worden, en daarmee niet langer juist zijn. Het knippen en plakken in digitaal beeldmateriaal afkomstig van een beveiligingscamera is aan de orde van de dag, aangezien veelal maar een fragment van de opname relevant is en het technisch zeer eenvoudig uit te voeren is. Dat vraagt om een controlemechanisme om te kunnen vaststellen of niet door fragmenten weg te knippen de feitelijke boodschap van de opname bezijden de waarheid terechtgekomen is. In de praktijk vervult de meelopende tijdswaarneming die functie.

Het onderwerp dataveiligheid is te omvangrijk om op deze plaats volledig recht te doen. We volstaan daarom met een illustratie aan de hand van onderwerpen die tijdens de behandeling van het wetsvoorstel digitale processtukken aan bod gekomen zijn. Dit doen we aan de hand van een aantal citaten:

> *'Voor elektronische documenten is het niet mogelijk onderscheid te maken tussen een origineel en een kopie hiervan. Hier komt bij dat de inhoud van een elektronisch document eenvoudig is te wijzigen. De integriteit van elektronische documenten is lastiger vast te stellen dan de integriteit van papieren documenten. […] Daarom is het noodzakelijk informatie vast te leggen en te bewaren over de eigenschappen van elektronische documenten, de auteur(s) hiervan en de in de tijd daarin aangebrachte wijzigingen.'*[62]

> *'Een regeling als het onderhavige wetsvoorstel kan dan ook niet zonder de waarborg dat de gegevens beveiligd worden opgeslagen en dat daarmee zorgvuldig*

59. Lodder & Schuilenburg vragen in dat verband om bezinning ten aanzien van het vertrouwen dat kan worden gesteld in uitkomsten van analyses van gegevens zonder dat deze inzichtelijk zijn. Zie: A.R. Lodder & M.B. Schuilenburg, 'Politie-webcrawlers en predictive policing' in: *Computerrecht* 2016/81. Zie WRR 2016, p. 113-114.
60. Het is opvallend dat het principe van de materiële waarheid in diverse handboeken niet in de beginselencatalogus figureert. Keulen en Knigge noemen de materiële waarheid bij de rolbeschrijving van de rechter; Keulen/Knigge 2016, p. 42.
61. Wolters Ruckert & Van Sloten spreken in relatie tot het gebruik van Big Data over 'de mythe van beveiliging'. Zie: N. Wolters Ruckert & L. van Sloten, 'Big Data: Big privacy challenges', in: *Computerrecht* 2016/2.
62. *Kamerstukken II* 2014/15, 34090, 3. Daarin wordt de inhoudelijke overlap tussen betrouwbaarheid en juistheid direct duidelijk.

wordt omgegaan. Zij wordt dan ook, al dan niet middels een verwijzing naar een bij AMvB of richtlijn vast te leggen gedragscode voor alle procespartijen, in het wetsvoorstel node gemist.'[63]

'Het gebruik van elektronische processtukken heeft een zeker risico, met name waar het de integriteit van die stukken betreft. Net als dat er een risico bestaat dat een papieren handtekening wordt vervalst, papier zoek raakt, of een dossier 'op straat' belandt. De Raad onderschrijft op zichzelf het uitgangspunt van het Wetsvoorstel dat van een processtuk in elektronische vorm de integriteit kan worden nagegaan, doordat iedere wijziging daarvan kan worden vastgesteld. De Raad wijst er echter op dat het Wetsvoorstel op dit punt wel erg stellig uitgaat van de technische mogelijkheden om de integriteit van elektronische documenten ook in de toekomst vast te kunnen stellen.'[64]

'De aan het woord zijnde leden merken op dat bij het vaststellen van het betrouwbaarheidsniveau één van de overwegingen is de hoge eisen die gesteld mogen worden aan de betrouwbaarheid van de processtukken vanwege de aanzienlijke belangen die er spelen in een rechtszaak. […] Echter, de regering is niet van mening dat de hoogst mogelijke betrouwbaarheid van de authenticatie en daarop gebaseerde ondertekening van toepassing hoeven te zijn. De regering beargumenteert dit door te stellen dat een handgeschreven handtekening ook vervalst kan worden.'[65]

Het belang van veilig omgaan met informatie is dat de staat en zijn burgers erop mogen vertrouwen dat informatie niet terechtkomt op plaatsen en bij mensen waarvoor deze informatie niet is bedoeld.[66] Een gebruikelijke maatregel is het plaatsen van een digitaal hek om deze informatie. Dit is echter riskant. Een digitaal hek blokkeert niet alleen onbedoeld gebruik, maar ook bedoeld (of zelfs noodzakelijk) gebruik van informatie. In dat geval gaan mensen 'over het hek heen' en verliest de beveiliging zijn functie. Het veelvuldig gebruik van e-mail voor het versturen van vertrouwelijke gegevens illustreert dit punt. Wanneer de beveiliging op bijvoorbeeld een zaaksysteem te streng is, voelen mensen zich gedwongen om de informatie 'dan maar' over e-mail te versturen. Te sterke beveiliging werkt onveilig gedrag in de hand. Goede beveiliging maakt een precies onderscheid tussen bedoeld en onbedoeld gebruik van informatie.

Juistheid van de feiten

Bij het begrip juistheid ligt de focus op de toepassing van de, als alles loopt zoals bedoeld, veilige informatie. De overeenstemming met de materiële waarheid van de feitelijke vaststellingen die ten grondslag liggen aan de uiteindelijk genomen beslissing, is het uitgangspunt voor de rechtskracht.. Juist bij gebreke of uitputting van de mogelijkheid tot herstel klemt de noodzaak des te meer dat de feiten vanaf de aanvang kloppen. Bij het nemen van beslissingen kan voornamelijk worden gedacht aan de vervolgingsbeslissing van het OM en de uitspraak van de rechter. Hier ligt ook de link met het begrip behoorlijkheid

63. Advies NOvA bij wetsvoorstel digitale processtukken. Bijlage bij *Kamerstukken II* 2014/15, 34090, 3.
64. Advies RvdR bij wetsvoorstel digitale processtukken. Bijlage bij *Kamerstukken II* 2014/15, 34090, 3.
65. *Kamerstukken II,* 2014/15, 34090, 5, p. 8.
66. Hoe lastig dit is wordt treffend geïllustreerd in het advies van de NOvA bij het wetsvoorstel digitale processtukken waar op pagina 3 wordt gerefereerd aan een ontvangen stuk waarin onbedoeld de track-changes aangebracht door het ministerie van VenJ zijn blijven staan (bijlage bij: *Kamerstukken II* 2014/15, 34090, 3).

nu een verdachte ervan moet kunnen uitgaan dat OM en rechter 'behoorlijk' beslissen, dat wil zeggen op basis van juiste, veilige informatie (en uiteraard een deugdelijke belangenafweging enz.). Het lijkt evident dat wanneer de veiligheid onvoldoende kan worden gegarandeerd, dat gevolgen kan hebben voor de integriteit, juistheid en/of behoorlijkheid van de te nemen feitelijke beslissing. Verder roepen wij hier nog in herinnering dat een onjuistheid in een bepaalde fase meereist naar de volgende schakel van de strafrechtsketen, tenzij die daar gedetecteerd en gecorrigeerd wordt. We wezen daar al op bij de opmerkingen over de onschuldpresumptie. Ten aanzien van een specifiek gegeven – de identiteit van personen – heeft de wetgever voor elke schakel in de keten reeds voorgeschreven dat de juistheid gecheckt wordt.[67]

2.2.7 TIJDIGHEID

Het beginsel postuleert dat de over de uitkomst van vervolging en berechting binnen een redelijk tijdsbestek zekerheid en duidelijkheid gegeven wordt . Dat principe komt het duidelijkst tot uiting in het recht op behandeling (en afdoening) van een zaak binnen een redelijke termijn. Het heeft van alles te doen met simpelweg de snelheid waarmee een strafzaak door de keten beweegt en ten aanzien waarvan digitalisering een grote verandering zou gaan opleveren. Alleen al uit de beleidsstukken en voortgangsbrieven inzake het VPS programma die de minister van VenJ halfjaarlijks aan de Kamer doet toekomen blijkt, dat ten aanzien van deze snelheid bepaalde verwachtingen leven.[68] Exemplarisch is bijvoorbeeld de zinsnede:

> *'Digitalisering is een belangrijke voorwaarde om strafzaken sneller, slimmer, beter en transparanter af te wikkelen. Met behulp van digitale voorzieningen kunnen dossiers sneller beschikbaar worden gesteld, administratieve lasten sterk worden verminderd en zaakstromen beter worden gevolgd.'*[69]

Wanneer we het hebben over het begrip tijdigheid kunnen daarbinnen in het kader van de digitale stukkenstroom een tweetal zaken worden onderscheiden. Allereerst het verstrekken van informatie. Een digitaal dossier, zo is de gedachte, maakt het eenvoudiger om informatie uit te wisselen tussen partijen.[70] In de memorie van toelichting bij het wetsvoorstel digitale processtukken wordt de verwachting uitgesproken dat met behulp van digitale voorzieningen dossiers sneller ter beschikking (van partijen) kunnen worden gesteld.[71] In de gepubliceerde beleidsvisie is een en ander als volgt verwoord:

> *'Digitalisering maakt verplaatsing en vermenigvuldiging van informatie mogelijk op een veel grotere schaal, met een veel groter gemak en met een veel grotere snelheid dan in het papieren tijdperk.'*[72]

67. Wet identiteitsvaststelling van verdachten, veroordeelden en getuigen van 18 juli 2009, *Stb*. 2009, 317, in werking sinds 1 oktober 2010.
68. Zie de (voortgangs)brieven van het ministerie van VenJ aan de Tweede Kamer inzake het programma Versterking Prestaties Strafrechtsketen; bijv.: *Kamerstukken II* 2011/12, 29279, 165, p. 15; Voortgangsrapport Versterking Prestaties Strafrechtsketen juni 2014, bijlage bij *Kamerstukken I* 2013/14, 33750, VI, nr. AB, p. 8.
69. *Kamerstukken II,* 2012/13, 29279, 165, p. 5.
70. In vergelijkbare zin: Hesselink 2016.
71. *Kamerstukken II* 2014/15, 34090, 3, p. 2.
72. Naar digitaal werken in de strafrechtsketen, perspectief en richting, p. 25. Bijlage bij: *Kamerstukken II* 2015/16, 29279, 298.

Verder kan gewezen worden op de overdracht tussen de verschillende instanties die ten aanzien van de voortgang van de strafzaak een behandeling doen en de bewaking van de voortgang door middel track-and-trace van zaken. Fysieke aflevering van dossiers zou niet meer nodig zijn en ten aanzien van dreigende vertraging wordt het menselijk opletten ondersteund door een volgsysteem. In het volgsysteem kan een digitaal dossier automatisch geregistreerd worden, een papieren dossier moet eerst ingeboekt worden.

Ter afsluiting van deze paragraaf kan de volgende balans opgemaakt worden. Er zijn een aantal fundamentele principes van de strafrechtspleging, in het bijzonder de vervolging en berechting, die geraakt kunnen worden door de digitalisering. In welke mate en of dat als ondersteuning of ter ondermijning zal uitpakken, kan variëren. Deze laatste stelling laat zich nader beproeven door dieper te graven in wat bij IT-ontwikkelingen de uitgangspunten of beginselen zijn. Informatiesystemen worden gebouwd volgens bepaalde kenmerken/normen, eigen aan het vakgebied, en inzicht in de inhoud van die normen brengt ons verder in de beantwoording van de vraag of er steun dan wel bedreiging voor strafrechtelijke beginselen te verwachten is. In paragraaf 2.3 worden die normen ontwikkeld, in paragraaf 2.4 laten we dan de confrontatie tussen beide werelden zien.

2.3 Informatietechnische beginselen / desiderata

2.3.1 INLEIDING

Informatietechnische oplossingen in de strafrechtsketen krijgen concreet vorm in informatiesystemen. Deze verkenning verstaat onder ‘strafrechtelijk informatiesysteem’ elk computersysteem, dat in de strafrechtelijke afdoening gebruikte gegevens verwerkt om de strafrechtspleging te ondersteunen. Deze definitie is met opzet breed gekozen, zodat elke voorziening voor digitalisering in de strafrechtsketen onder de noemer ‘informatiesysteem’ kan worden besproken.

Informatiesystemen worden beschouwd, ontworpen en gebouwd volgens bepaalde principes. Wanneer we die principes als kenmerk beschouwen, kunnen we stellen dat ze een beschrijvende rol vervullen. De beginselen hebben echter ook een aspiratieve kant. Ze kunnen de rol van desideratum vervullen, van een richting waarin men wil werken. Ze zijn dan naast beschrijving een principieel programma van eisen, waarmee in een bepaald project de concrete vereisten/specificaties geformuleerd worden.

De vraag waar IT-beginselen vandaan komen is een lastige. De informatiekunde kent geen beginselenleer, zoals we die in de juridische wetenschap kennen. Een gebrek aan consensus maakt het moeilijk te verwijzen naar ‘algemeen gangbare’ principes. Om deze discussies te vermijden en toch een aantal beginselen te kunnen bespreken, hebben wij ons verstout om op eigen gezag een aantal beginselen te formuleren.[73]

Elke sectie in dit deel van hoofdstuk 2 bespreekt een informatietechnisch beginsel. We bespreken van elk beginsel welke eisen het stelt aan informatiesystemen in de strafrechtsketen. Ook bespreken we welke risico’s het niet-voldoen aan

73. Een lezer die moeite heeft met een door ons benoemd principe kan eenvoudig volstaan met de auteurs dezes te bekritiseren. Bij gebrek aan consensus in het vakgebied zullen we het hiermee moeten doen.

deze eisen oplevert voor het strafrecht. In paragraaf 2.4 werken we dan de dynamiek verder uit door verslag te doen van onze theoretische beschouwing met als vraag: wat betekent versterking van een bepaald IT-beginsel voor de grondbeginselen van de strafrechtspleging, die we in paragraaf 2.2 opgenomen hebben. De opbrengt van deze exercitie kan gebruikt worden om mede richting te geven aan de beleidsvorming voor digitalisering van de strafrechtpleging.

2.3.2 INTEGRITEIT VAN GEGEVENS

Onder integriteit wordt verstaan de juistheid, in de zin van correct en volledig, van gegevens[74]. Bij informatiesystemen voor het strafrecht wil een gebruiker kunnen rekenen op juiste registratie van feiten. Onder juistheid wordt in de praktijk verstaan dat een opgeslagen gegeven overeenkomt met de werkelijkheid[75] in de reële wereld.

Het risico van onjuiste gegevens bestaat in elk informatiesysteem. In sommige gevallen lukt het om dat risico te ondervangen. Zo is er bijvoorbeeld veel vertrouwen in de kwaliteit van gegevens in de strafdossiers bij Justid, hoewel ook daar soms (buiten de schuld van Justid om) onjuiste gegevens voorkomen. Soms is desondanks het vertrouwen nog niet 100%. In de burelen zal men nog geregeld een medewerker kunnen aantreffen die een (papieren) zaaksdossier raadpleegt om een feit uit 'het systeem' te verifiëren. Een informaticus kan dan constateren dat de medewerker kennelijk de waarheid van dat geregistreerde feit betwijfelt. Hij mag dat interpreteren als een teken van onvoldoende vertrouwen in de integriteit van gegevens in het informatiesysteem. Hij zal zich afvragen of het informatiesysteem wel voldoende garanties biedt ten aanzien van de integriteit van gegevens.

In theorie dient elk informatiesysteem in de strafrechtspleging de werkelijkheid weer te geven. Dit is een basale eis aan administratieve informatiesystemen in het algemeen.[76] De informaticus, die informatiesystemen ontwerpt en bouwt voor de strafrechtspleging, dient zich dan ook bewust te zijn van de complexiteit van het begrip 'waarheid'. Doelbewust laat hij het Cartesiaanse waarheidsbegrip links liggen, maar voegt zich naar het meer praktische (juridische) uitgangspunt dat een 'feit' door een waarnemer wordt vastgesteld en door een ander (bijvoorbeeld de rechter) voor waar of onwaar kan worden gehouden. De informaticus is zich bewust van de subjectieve en intersubjectieve aspecten van waarheid.

In systemen die redeneren met kennis dienen redeneerstappen valide te zijn. Voor de informaticus komen redeneerstappen overeen met waarheidsbehoudende transformaties op gegevens. Dat wil zeggen dat de uitkomst van de redenering (een nieuw gegeven) de gebruikte gegevens naar hun aard en inhoud niet veranderd heeft, maar juist aanvaard en verwerkt.

74. De gebruikte definitie is ontleend aan Van der Veen & Bokhorst, Normen IT-voorzieningen, e-Overheid, sept. 2010, te vinden op https://www.digitaleoverheid.nl/images/stories/nieuws_2010/normenit_noradossier_informatiebeveiliging.pdf (laatst geraadpleegd op 15 okt. 2016).
75. Epistemologisch is 'overeenkomend met de werkelijkheid' al meer dan een eeuw achterhaald. In de praktijk weet men echter wat er bedoeld wordt: een opgeslagen gegeven, bijvoorbeeld 'Piet is geboren op 12 april 1959', komt overeen met de werkelijke geboortedatum van Piet. Hiermee wordt óók bedoeld dat dit feit objectief vaststelbaar is, bijvoorbeeld door de rechter.
76. Dit informatietechnische beginsel is ook bekend als 'één werkelijkheid', en is als eis in menig aanbestedingsdocument terug te vinden.

Onjuiste gegevens en gegevens waarvan de waarheid niet (meer) kan worden vastgesteld, worden door een informaticus als gegevensvervuiling gezien. Er zijn twee soorten ontrouw aan de waarheid: een gegeven is verkeerd ingevoerd of een gegeven is later aangetast/gewijzigd. Een goede gegevensbeheerder dient te zorgen dat de vervuilingsgraad van een informatiesysteem laag blijft. In dit verband wordt soms gesproken van 'gegevenshygiëne' (of het gebrek daaraan). Een externe vervuilingsanalyse is een onderzoek waarin de integriteit van gegevens wordt onderzocht. Dit kan duidelijkheid geven over de betrouwbaarheid van gegevens in een informatiesysteem.

Met het voorgaande beogen wij duidelijk te maken dat de integriteit van gegevens allerminst vanzelfsprekend is. Innovaties in de strafrechtsketen worden echter gepresenteerd[77] met een impliciete aanname dat het met de integriteit van gegevens goed zit. Gesprekken met deskundigen in de praktijk van het strafrecht stellen ons echter niet gerust ten aanzien van de gegevenshygiëne en van de integriteit van bestaande gegevensverzamelingen in de strafrechtsketen.

2.3.3 CONSISTENTIE

De logica leert dat consistentie een noodzakelijke eigenschap is van elke gegevensverzameling. Vanuit dit perspectief kent elke informaticus een stellige, exacte definitie van consistentie: binnen één context mag geen enkel gegeven zowel waar als onwaar zijn. Een risico is dat opgeslagen inconsistenties leiden tot procedurefouten of erger. Als, bijvoorbeeld, een informatiesysteem zou weergeven dat op 12 april 2011 een verzoek tot wraking ex artikel 512 Sv in de strafzaak met zaaknummer 11-252 door de wrakingskamer van de Rechtbank Arnhem is behandeld, en tegelijk geeft het informatiesysteem weer dat dit verzoek *niet* behandeld is, dan zijn deze gegevens inconsistent. Ook voor de jurist, die een informatiesysteem gebruikt, is een consistente registratie van juridisch relevante feiten een absolute voorwaarde. Consistentie van een gegevensverzameling kan binnen een gegevensverzameling zelf bepaald worden en is los van de buitenwereld te toetsen.

Voor een informaticus is consistentie allerminst vanzelfsprekend. Dit laat zich aan een eenvoudig voorbeeld illustreren. Stel dat een informatiesysteem de volgende regel moet handhaven: 'In Nederland heeft elke persoon één geboortedatum'. Stel nu dat de verdachte in de strafzaak met zaaknummer 11-252 volgens het informatiesysteem 1 mei 1972 als geboortedatum heeft, maar tegelijk ook geregistreerd is met geboortedatum 19 augustus 1972. Dit levert een strijdigheid op met de regel, die we ook kennen als een overtreding. In die zin is elke overtreding van een regel een inconsistentie. Om deze inconsistentie op te heffen kent de informaticus verschillende keuzes. Hij kan bijvoorbeeld concluderen dat er sprake is van twee personen, die elk een andere geboortedatum hebben. Maar hij kan ook concluderen dat een van beide data incorrect is en dus geschrapt moet worden uit de gegevensverzameling. Een optie is ook om de genoemde regel ongeldig te verklaren. Nog weer een andere optie is om even niets te doen en een vraag uit te zetten naar iemand die deze inconsistentie wél kan oplossen. Het aantal opties om een inconsistentie op te lossen is in theorie oneindig groot.

77. Bijvoorbeeld de animaties wekken de indruk dat er op dit vlak niets gebeuren kan; https://www.rechtspraak.nl/Voor-advocaten-en-juristen/modernisering-rechtspraak/Paginas/Animatie-modernisering-rechtspraak.aspx en https://www.rechtspraak.nl/Voor-advocaten-en-juristen/modernisering-rechtspraak (beide links laatst geraadpleegd op 15 okt. 2016)

In een strafzaak is het normaal dat de officier van justitie en de raadsman van de verdachte elkaar soms tegenspreken. Dat is echter niet de tegenspraak die een inconsistentie oplevert. Enkele voorbeelden maken dat duidelijk. De volgende twee uitspraken zijn niet inconsistent: 'De officier van justitie heeft gezegd dat proces-verbaal met nummer 99023171 niet in het dossier zit.' en 'De Raadsman heeft gezegd dat proces-verbaal met nummer 99023171 wel in het dossier zit.'. Wel inconsistent zijn: 'Proces-verbaal met nummer 99023171 zit in het dossier.' en 'Proces-verbaal met nummer 99023171 zit niet in het dossier.'. Ook inconsistent zijn: 'De officier van justitie heeft gezegd dat proces-verbaal met nummer 99023171 niet in het dossier zit.' en 'De officier van justitie heeft gezegd dat proces-verbaal met nummer 99023171 wel in het dossier zit.'.

Een informaticus zal het informatiesysteem laten registreren van welke persoon een uitspraak afkomstig is. Zolang er geen regel is die zegt dat twee verschillende personen geen strijdige uitspraken mogen doen, is er van inconsistentie geen sprake.

Voor een jurist ligt dat anders. Als de officier van justitie en de raadsman elkaar tegenspreken, is het aan de rechter om te beslissen wie er gelijk heeft. Een jurist is gewend aan dit spel en verwacht van een informatiesysteem dat inconsistenties binnen een strafzaak op consistente wijze geregistreerd kunnen worden.

Zolang een informatiesysteem alleen feiten registreert en reproduceert blijft het risico van inconsistentie beperkt tot het onbruikbaar worden van de inconsistente gegevens. Dat neemt niet weg dat inconsistenties door het systeem bij voorkeur wel herkend worden. Als een informatiesysteem daarnaast ook redeneert, en nieuwe gegevens registreert die uit deze redeneringen zijn ontstaan, dan kan deze 'vervuiling' een veel groter deel van de gegevensverzameling infecteren.

Het consistentiebeginsel vereist dat een informatiesysteem kan voorkómen dat een regel overtreden wordt. Dat vereist ofwel een bewijs dat overtreding onmogelijk is, ofwel software die gegevens bewaakt in het geval dat er een kans op overtreding bestaat. Ofschoon informatiesystemen veel van dit soort regels bevatten, is er in de praktijk zelden sprake van dat elke regel ofwel bewezen is, ofwel bewaakt wordt. Maar weinig systemen kunnen inconsistenties op voorhand uitsluiten. Integendeel, de kans op inconsistenties is in vrijwel elke gegevensverzameling reëel aanwezig. Een interne vervuilingsanalyse kan daarover duidelijkheid verschaffen. De gesprekken met de geraadpleegde deskundigen laten niet zien dat ten aanzien van de consistentie van bestaande gegevensverzamelingen in de strafrechtsketen analyses plaatsvinden.

2.3.4 CONTEXTUALITEIT

Integriteit van gegevens en consistentie veronderstellen beide een waarheidsbegrip. Vanuit de logica is bekend dat waarheid alleen in context[78] bestaat. Een informaticus weet dat en heeft dus kennis van de context nodig om integere en consistente gegevensregistratie mogelijk te maken. Daartoe dient elk feit in de juiste context te worden geregistreerd. Ook juristen kunnen al vertrouwd zijn met de contextafhankelijkheid van waarheid. Er zijn vele materieelrechtelijke studies, mede naar aanleiding van rechtspraak, over de autonome invulling van

78. Onder context wordt hier verstaan de totale omgeving waarin iets zijn betekenis krijgt.

begrippen in de verschillende subdisciplines van het recht, zoals 'inkomen' of 'eigendom', maar ook in het hier meer relevante procesrecht kunnen juristen omgaan met verschillende versies van de waarheid.

In feite vormt elke juridische zaak een zelfstandige context. Dat verklaart de belangstelling voor zaaksystemen in de strafrechtsketen. Vanuit een informatietechnisch perspectief geldt binnen elke zaak één waarheid, in de verschillende stadia van het strafproces is eerder het tegendeel aan de orde. Actoren doen verschillende beweringen, die regelmatig diametraal tegenover elkaar staan. Daarvoor heeft de informaticus wel een oplossing. Hij zal alle feiten, die binnen die context worden geregistreerd, willen voorzien van de bron (de persoon die dat feit heeft beweerd) en een tijdstip van waarneming (wanneer die persoon het heeft beweerd). Dat stelt hem in staat om de informatietechnische waarheid weer te geven, zonder dat het systeem ertoe dwingt om discrepanties op te lossen. Dat is de waarheid in de context van het systeem, maar nog niet de waarheid in de context van het strafproces. Het is aan gebruikers zoals een rechter om tegenstrijdigheden in beweringen van verschillende personen op te lossen en die oplossing als een nieuwe bewering in het systeem op te nemen.

In de praktijk is het maken van zaaksystemen erg ingewikkeld gebleken. De geschiedenissen van vernieuwingen van GPS, BVO/BVH en REiS, wat alle drie zaaksystemen zijn, illustreren dat. Systemen die wel binnen de verwachte functionaliteit, tijd en budget zijn gerealiseerd, zoals CDD+ (Justid), zijn geen zaaksysteem. In een separaat onderzoek zou gekeken kunnen worden of het ontbreken van een goede theoretische basis voor zaaksystemen[79] een rol speelt bij het moeizame verloop van eerdergenoemde projecten.

2.3.5 AUTHENTICITEIT

Om feiten te kunnen vaststellen, worden in toenemende mate digitale bewijsmiddelen ingezet, zoals onderschept e-mailverkeer, bewijzen van zakelijke transacties, of materiaal dat via social media in de wereld is gekomen. Een risico daarbij is dat de authenticiteit van deze bewijsmiddelen steeds moeilijker is vast te stellen. Onder authenticiteit verstaan we de mate waarmee de identiteit van de opsteller en/of verzender ervan met zekerheid is vast te stellen.[80]

Omdat het beoordelen van authenticiteit van gegevens in het strafrecht tot de dagelijkse praktijk behoort, ligt het in de rede om dit ook naar eisen voor informatiesystemen te vertalen. Omdat het hier gaat om het vaststellen van de identiteit van opsteller en/of verzender, vertaalt zich dat naar eisen aan het systematisch metadateren van opgeslagen justitiële en strafvorderlijke gegevens. Metadateren is bekend uit de wereld van digitale documentvoorziening, waar metadata aan dossiers worden toegevoegd ten behoeve van archivering.[81] Om authenticiteit van gegevens in het strafrecht te kunnen beoordelen, is metadatering aan de bron echter een vereiste. Om de kwaliteit van metadatering te kunnen garanderen, is handmatige metadatering onvoldoende. Mensen maken

79. In de praktijk wordt de definitie van 'zaak' in veel zaakgerichte IT-projecten uitvoerig besproken. Dat is gebeurd bij GPS, BVO/BVH en REiS. Dat gebeurt binnen en buiten de strafrechtsketen, binnen en buiten Justitie, en binnen en buiten de overheid. Externe IT-ers, die veel organisaties hebben gezien, herkennen deze discussie en kennen de afloop. Met een bruikbare theorie zouden deze discussies niet gevoerd hoeven worden. Daaruit concluderen wij dat een bruikbare theorie over zaaksystemen ontbreekt.
80. M. van Stekelenburg, *De betere byte in de strijd om het gelijk*, dissertatie VU Amsterdam, Delft: Eburon 2010.
81. Eisen over metadatering van archiefbescheiden zijn vrij specifiek beschreven in het Archiefbesluit 1995.

immers fouten, ook als ze achter een beeldscherm zitten. Om de kwaliteit te garanderen in het strafrecht is maximaal geautomatiseerd metadateren aan de bron van zowel gestructureerde als documentaire gegevens gewenst.

De overheid heeft bij wet een aantal gegevens als 'authentiek' aangemerkt.[82] Zij worden door de overheid zelf ontsloten in zogenaamde basisregistraties. In de wet van elke basisregistratie ligt vast welke gegevens van die basisregistratie authentiek zijn. Ook kan een gegeven authentiek zijn doordat het via een algemene maatregel van bestuur (AMvB) als zodanig wordt aangemerkt. De authentieke gegevens in de basisregistraties zijn zonder nader onderzoek bij de uitvoering van publiekrechtelijke taken te gebruiken.

De authenticiteit van een gegeven is niet uitsluitend belangrijk in de strafrechtspleging. Toch is het wel vooral in het strafrecht dat zulke hoge eisen aan het systeem gesteld worden. Bij niet-juridische informatiesystemen zijn maatregelen om de authenticiteit van digitale gegevens te ondersteunen nog veel minder gemeengoed.[83]

2.3.6 DUURZAAMHEID

Onder duurzaamheid wordt verstaan dat feiten, die in het verleden zijn geregistreerd, op enig moment ongewijzigd kunnen worden getoond. Er bestaat een risico dat een gegeven uit het verleden niet meer bestaat, of dat het in de loop van de tijd veranderd is. Het kan zelfs zijn dat er door gewijzigde software aan een gegeven inmiddels op een andere manier betekenis wordt toegekend, waardoor de oorspronkelijke betekenis verloren gegaan is.

De informaticus is zich ervan bewust dat feiten tijdsafhankelijk kunnen zijn. Voor het registreren van feiten kiest de informaticus voor een duurzaam gegeven. Bijvoorbeeld, om te registreren dat Piet minderjarig is, slaat hij niet de leeftijd, maar de geboortedatum van Piet op in een personenbestand. De geboortedatum blijft met het verstrijken van de tijd immers hetzelfde, terwijl de leeftijd elk jaar spontaan verandert.

Duurzaamheid vereist ook dat de voorziening, waarin gegevens zijn opgeslagen, blijft bestaan. Hiervoor zijn back-up- en uitwijkmogelijkheden nodig. Ook moet er zekerheid tegen onbedoeld wissen van gegevens zijn.

Het ongewijzigd kunnen tonen vereist ook dat een gegeven of document niet is gewijzigd terwijl het opgeslagen was. Voor zulke garanties is het zetten van een digitale handtekening een optie, omdat met cryptografische technieken gegarandeerd kan worden dat een document sinds het zetten van die handtekening niet gewijzigd is.

Duurzaamheid impliceert ook dat een informatiesysteem onderscheid maakt tussen stukken die gecommuniceerd zijn en stukken die nog in ontwikkeling zijn. In een stuk in ontwikkeling kunnen wijzigingen plaatsvinden. Een stuk dat tussen partijen wordt gecommuniceerd wordt gewoonlijk opgeslagen om later

82. https://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties/stelselvoorzieningen/stelselcatalogus/authentieke-gegevens (laatst geraadpleegd op 15 okt. 2016).

83. Hier wordt gedoeld op technische voorzieningen om uitspraken te traceren naar de bron en het tijdstip van uitspreken. Hiervan is buiten de (straf-)rechtsketen minder vaak sprake.

te kunnen terughalen wat de zendende partij heeft opgeschreven. Het systeem moet zo'n stuk dus kunnen 'invriezen' en duurzaam opslaan. Ook bij het 'invriezen' is een digitale handtekening een geschikt hulpmiddel.

Duurzaamheid van gegevens is niet specifiek voor het strafrecht. In veel toepassingen buiten het strafrecht en buiten de overheid is duurzaamheid een wenselijke eigenschap. Wel specifiek voor het (straf)recht zijn de gevolgen van gebreken aan de duurzaamheid. Twijfel over de status van een bewijsmiddel kan voor het verloop van een zaak grote gevolgen hebben, zoals terzijdestelling door de rechter, met eventueel een andere uitkomst van de zaak als gevolg.

2.3.7 COMPLIANCE

De wettelijke kaders die voor de gebruikers van een systeem gelden zijn natuurlijk ook van toepassing op het ingeschakelde informatiesysteem. Onder compliance verstaan wij de overeenstemming tussen wet en systeem in die zin dat de mogelijkheden en beperkingen van een systeem corresponderen met de wettelijke mogelijkheden en beperkingen. Een systeem verricht niet meer handelingen dan met toepassing van de wettelijke regels toegelaten is en evenzeer: een systeem maakt mogelijk (al) wat de wet mogelijk maakt. Wanneer men moet zeggen: 'de wet staat iets toe, maar ons systeem kan dat niet aan', dan is volgens deze definitie dat systeem niet compliant.

Het risico dat een informatiesysteem onwettige dingen doet is niet denkbeeldig. Echter, omdat de gebruiker van informatiesystemen in de strafrechtsketen in principe juridisch bekwaam is, kan hij zelf op de eventuele gebreken inspelen. In die zin is het risico indirect. Het te verwachten gevolg is dus niet dat er wetten overtreden worden, maar wel dat er onnodig inspanning gevraagd wordt van medewerkers in de strafrechtsketen om het systeem aan te vullen. Dat verandert als het informatiesysteem eigenstandig eindproducten van een werkproces maakt. Dan wordt het risico van wetschending direct.

In ontwerpen van bepaalde informatiesystemen, die binnen het onderzoeksteam bekend zijn[84] zitten wisselende voorzieningen voor het ondersteunen van compliance. Zo kent INDIGO[85] een kennismotor (Eng.: 'knowledge engine' of 'rule engine') die is ingericht om de regels vanuit de Vreemdelingenwet 2000 te kunnen toepassen. Daarmee ondersteunt INDIGO zijn gebruikers met juridische kennis, bijvoorbeeld bij het nemen van beslissingen over verblijfsstatus. Wanneer de juridische regels dwingend zijn, kan de menselijke factor minder belangrijk worden. Als de wet echter discretionaire ruimte laat, ondersteunt het systeem het niet-discretionaire deel van het beslisproces en doet dat dan wetsconform.

Een risico van op regels gebaseerde technologie is dat richtlijnen de facto tot regel worden gemaakt. Hiervan levert het al eerder genoemde bos/polarissysteem een mooi voorbeeld. Dat systeem was bedoeld om uniformiteit van de afdoening van veel voorkomende lichte strafzaken te ondersteunen door de toepassing van de OM-richtlijnen te automatiseren. Op een zeker moment ontstond er ophef[86] over een (in de ogen van het publiek te lage) straf voor een 18-jarige

84. INDIGO, VIRO, REiS, GPS (deze systemen zitten niet allemaal in de strafrechtsketen, maar wel in het justitiële domein).

85. Het zaaksysteem van de Immigratie- en Naturalisatiedienst.

86. http://www.daardan.nl/2012/01/taakstraf-voor-agentbeuker-dankzij-softe-polaris-richtlijnen/ (laatst geraadpleegd op 15 okt. 2016).

hanggroepjongere die een agent sloeg. De reactie van de woordvoerder van het OM luidde: ‘Ik kan me voorstellen dat het niet aansluit bij de beleving van de burger, maar wij houden ons aan de richtlijnen.’ Dat voedde de beeldvorming dat bos/polaris het werk van de beslisser had overgenomen.

Om compliance van een systeem te ondersteunen ligt het voor de hand om juridische grondslagen in de vorm van referenties naar toegepaste wetsbepalingen mee te nemen in informatiesystemen. Voor strafrechtelijke beweringen (in bijv. uitspraken en pleitnota’s) zien we dat geregeld gebeuren. Voor in de vervolging en berechting gebruikte gegevens zien we dat veel minder. In de ons bekende ontwerpen zien we dat werkprocessen in kaart zijn gebracht op basis van workshops met ervaren gebruikers. Een verantwoording van procesbeschrijvingen in termen van procesrechtelijke regels (uit Strafvordering, maar ook uit beleidsregels en reglementen van de betrokken organen) ontbreekt veelal. In dat geval is overeenstemming met de wet in het ontwerp niet toetsbaar.

In verband met de toetsbaarheid van systemen willen we in verband met de compliance ten slotte nog een opmerking maken over auditeerbaarheid; een krom Nederlands woord dat de toegankelijkheid voor audits van een systeem uitdrukt. Een compliant systeem geeft goede toegang voor inspecties op de legaliteit van de uitkomsten.

2.4 Een theoretische confrontatie

2.4.1 EEN MATRIX

In paragraaf 2.2 is een lijst ontwikkeld van beginselen die bij de digitalisering van de strafrechtspleging relevant zijn. Daarna hebben we in paragraaf 2.3 gewezen op beginselen van informatiesystemen, die ook een wenselijkheid uitdrukken. In de nu volgende paragraaf doen we verslag van het theoretisch op elkaar betrekken van beide beginselen. We hebben onszelf de vraag gesteld wat dynamiek in de IT-beginselen zou kunnen betekenen voor strafvorderlijke beginselen uit de lijst. Bijvoorbeeld, voor welke beginselen zal een grotere consistentie van een informatiesysteem gevolgen hebben en wat is dan de aard van dat gevolg: een bedreiging of een kans? We tekenen hier de matrix en schrijven de relevante cellen in de volgende paragrafen uit. Een nummer in de cel wijst naar de paragraaf met dat nummer.

Diverse cellen zijn leeg. In de theoretische confrontatie van de juridische en informatiekundige expertise zijn de meest in het oog springende verbanden geïnventariseerd. De lege cellen in de matrix zouden we ook kunnen vullen met een korte beschouwing, want onze bewering met deze matrix is niet dat in lege cellen niets op te merken zal zijn. We kozen op basis van onze inschatting van pregnantie ten aanzien van onze vraagstelling voor de aangegeven verbanden.

	integer	*consistent*	*contextueel*	*authentiek*	*duurzaam*	*compliant*
legaliteit	2.4.2		2.4.3			2.4.4
toegang						
equality of arms	2.4.5		2.4.6			
openbaarheid	2.4.7		2.4.8			
betrouwbaarheid	2.4.9	2.4.9	2.4.9	2.4.9		
tijdigheid	2.4.10	2.4.10	2.4.10			

Deze oefening hebben wij uitgevoerd op basis van het bestaande perspectief van de transitie van digitaal naar elektronisch. De mogelijke toekomst met andere verderstrekkende IT-ontwikkelingen komt later terug. Gebleken is dat op het moment van ons verkennend onderzoek geen toetsbare hypothese opleverde voor de huidige praktijk. De aard van de digitalisering in de strafrechtspleging kan samengevat worden als transitie van papier naar digitaal. Daarin is de dynamiek, die wij in de horizontale as van de matrix veronderstellen, nog amper waarneembaar. Die beweging zal ongetwijfeld beter te zien zijn als de *digitilization* in de strafrechtspleging doorbreekt (zie par. 2.1). In paragraaf 3.6. hebben we de betekenis van de recente ontwikkelingen voor de beginselen van de strafrechtspleging naar aanleiding van het praktijkonderzoek beschreven.

2.4.2 'LEGALITEIT' EN 'INTEGER'

Waar de integriteit beter verzekerd is, neemt de kans op een verwerking of openbaarmaking tegen de regels van de privacybescherming af. Het is een indirecte causaliteit waaraan hier gedacht wordt, omdat de juistheid van een gegeven op zichzelf nog niet betekent, dat het verwerken of openbaar maken toegestaan is. Evenmin is een inbreuk op de beveiliging van een gegevensbestand met kans op vervuiling als gevolg op zichzelf meteen een gerealiseerde schending van iemands privacy. De kans daarop is echter wel vergroot. Die redenering mag ook omgedraaid worden: als integriteit in de zin van beveiliging van gegevens beter geworden is, wordt de kans op schendingen van de privacy verkleind.

2.4.3 'LEGALITEIT' EN 'CONTEXTUEEL'

Een contextueel informatiesysteem honoreert de bijzonderheden van het proces, de handeling of de beslissing waarvoor de applicatie bedoeld is. De bijzonderheden van de strafrechtelijke context zijn in hoge mate in de wettelijke bepalingen neergelegd, aangezien legaliteit zo een fundamentele waarde is. Wanneer voor het ontwerpen/bouwen van een informatiesysteem – zaaksgebonden of anderszins – beter gelet wordt op de specifieke strafrechtelijke context, zal aan de wettelijke regels beter vertaling gegeven worden. De aard van het juridische waarheidsbegrip zal bijvoorbeeld duidelijk worden en de regels van het systeem zullen daarnaar gevoegd kunnen worden. Met name bij ondersteuning van beslissingen (in welke schakel van de keten dan ook) wordt dan beter veiliggesteld dat de bevoegde autoriteit tot een beslissing komt op basis van de weging van standpunten. Concreter: het systeem slaat niet op tilt als er eens drie onderling verschillende beweringen ten aanzien van hetzelfde beslispunt in verwerkt worden: twee partijstandpunten en een beslissing. Net als hierboven geldt ook hier dat bij het ontwikkelen van een systeem de context ingebracht moet wor-

den door de juridisch deskundigen en (met veel geduld misschien) overeind gehouden in het proces van ontwerp en bouw van een systeem.

De positie van het slachtoffer c.q. de nabestaande lichten wij hier even uit, hoewel het strikt genomen niet nodig is. In de vorige alinea kan bij de term 'partij' immers tevens aan deze actor gedacht worden. Het slachtoffer is – dat behoeft hier geen nadere toelichting[87] – allang uit zijn bijrol in het strafproces geëmancipeerd en neemt een eigen plaats in de context van de strafrechtspleging in. Verwerking van zijn inbreng in een informatiesysteem gaat beter als die context beter vertaald is naar de regels van dat systeem. De huidige stand van de regeling dwingt er dus toe, dat in een systeem minimaal rekening gehouden wordt met het slachtoffer als actor. Contextualiteit betekent vervolgens ook dat in het systeem verwerkt wordt, dat de rechtspositie van het slachtoffer verre van gelijk is aan die van de verdachte. Het slachtoffer slechts als actor toevoegen kan dus verkeerd uitpakken, want dat zou meebrengen dat de context, het verschil in positie ten opzichte van de andere actoren, genegeerd wordt. .

2.4.4 'LEGALITEIT' EN 'COMPLIANT'

We hebben bij legaliteit gewezen op de wettelijke basis in verband met digitaal handelen en dat specifieker gemaakt door te benadrukken, dat een systeem niet meer en niet minder mag doen dan de wettelijke regeling opdraagt of toelaat. Dat heeft betrekking zowel op handelingen/beslissingen in de strafrechtsketen als op verwerking van gegevens en op de taakverdeling tussen de schakels in de keten. Als een systeem groeit in compliance, zal het daarmee beter voldoen aan het beginsel van legaliteit en geschikter zijn voor een stelsel van een kwaliteitsaudit op dit beginsel. De beginselen uit beide assen van de matrix werken hier dezelfde kant op. Zoals we zojuist al lieten doorschemeren, is daarvoor wel nodig dat een team van ontwerpers en bouwers van het systeem gemengd samengesteld is. Zonder kennis en inzicht in de wettelijke regelingen kan niet verwacht worden dat de juridische verantwoording van de procesbeschrijvingen op orde komt, als aanvulling op de werkproceskennis, die nu vaak al wel ingebracht wordt. Werkproceskennis alleen is echter te beperkt, omdat die in de strafrechtspleging alleen maar bemiddelt tussen de wettelijke regeling en het informatiesysteem en daarbij naar onze waarneming mede onderworpen is aan andere wetmatigheden, zoals efficiency, bedrijfscultuur en persoonlijke voorkeur.

In dit verband veroorloven wij ons nog een opmerking over wetgevingsbeleid, aangezien het plan is dat een herziening van het Wetboek van Strafvordering met digitalisering gelijk op zal gaan. Het is niet goed wanneer noodzakelijk bevonden wettelijke bepalingen niet ingevoerd worden omdat het informatiesysteem dat niet zou kunnen hanteren. In dat opzicht betrekken we de stelling: eerst de wet, dan het systeem. Het informatiesysteem is dienaar van de wet. Dat staat echter geenszins in de weg aan een interactief wetgevingsproces, waarbij de schrijvers van de conceptbepalingen voor de keuze van een arrangement het oor te luisteren leggen bij de IT-specialisten.[88] Met name in geval van een keuze tussen juridisch gelijkwaardige alternatieven achten wij het kiezen voor het IT-perspectief geen probleem. Het bouwen van een prototype, dat zowel de technische bouwbaarheid als de samenwerking tussen juristen en technici aantoont, levert daarbij extra kennis en inzicht op van uitvoeringdetails.

87. Zie Corstens/Borgers 2014, p. 63-64.

88. Dit werd al betoogd in I.Th.M. Snellen, J T. Schokker, *Wetgeving en systeemontwikkeling*, 's-Gravenhage 1993.

Een volledig compliant systeem (wellicht een droombeeld) bevat alle voorzieningen om te bereiken dat gegevens alleen opgeslagen, gedeeld en anderszins verwerkt worden in de gevallen en onder de voorwaarden die in de wet gegeven zijn. Een beweging in die richting bevordert dus ook in dat opzicht de legaliteit. Het is de opdracht voor alle beheerders van databestanden uit de meest recente EU-regeling voor dataprotectie[89], waarin *privacy by design* het trefwoord is. Als dat doel bereikt wordt, is een systeem compliant en ondersteunt het de wettelijke bescherming van de privacy. Wellicht overbodig, maar toch voor alle duidelijkheid zeggen we erbij, dat volledige compliance niet inhoudt dat er geen inbreuken op de privacy plaatsvinden. Het onderzoeken, vervolgen en berechten van strafbare feiten gaat altijd gepaard met inbreuken op dit grondrecht en nergens in enig gezaghebbend document wordt dit uitgesloten. Het gaat om transparantie en regulering ten aanzien van de gevallen waarin en de voorwaarden waaronder inbreuken geoorloofd zijn en ten aanzien van gebruik, opslag en bewaring van de verkregen privacyrelevante informatie.

2.4.5 'EQUALITY OF ARMS' EN 'INTEGER'

Equality of arms kan gediend worden met een verbetering van de integriteit van de gegevens. In het bijzonder gaat het dan om de interne openbaarheid. Eén van de grote drempels om gegevens in een systeem met de verdediging te delen is immers dat data, als ze eenmaal gedeeld zijn, uit handen van de autoriteiten zijn. De verantwoordelijkheid voor de juistheid ligt allereerst bij deze autoriteiten. Voor het risico dat onjuiste gegevens verspreid worden bestaat daarom veel aandacht. Wanneer het systeem beter garandeert dat er geen fouten in de data zijn, wordt de drempel verlaagd om de verdediging toegang te verschaffen. Juistheid heeft hier niet de betekenis: overeenkomstig de materiële waarheid. Het gaat erom dat de beweringen in het systeem kloppen. Men denke juist hier aan het volgende voorbeeld. Al wat als 'de processtukken in de zaak' voor de verdediging toegankelijk gemaakt wordt, moet ook werkelijk als processtukken aangemerkt zijn door de autoriteit die daar over gaat, in casu de officier van justitie; eventueel de zittingsrechter in een latere fase. Een integer systeem bewaakt goed dat de geautoriseerde persoon daarover een beslissing genomen heeft en dat dus de bewering van het systeem: 'dit zijn de processtukken' klopt.

Wij zien overigens niet over het hoofd dat er in de strafrechtelijke afdoening procesfasen zijn en evenmin dat het weerhouden van informatie in een bepaalde procesfase, met name het vooronderzoek, onder omstandigheden als goed beleid beschouwd kan worden. Dat staat echter los van het informatiesysteem, dat in die situatie moet faciliteren dat weerhouding als variant mogelijk is. Dat is eerder een voorbeeld van verbeterde contextualiteit dan van integriteit.

Op deze plaats kan net als hierboven een opmerking gemaakt worden over de behoefte aan informatie bij het slachtoffer of de nabestaanden. Mutatis mutandis geldt wat in de vorige alinea over de verdediging geschreven is ook voor het slachtoffer. De drempel om toegang tot informatie te verschaffen kan lager worden als de integriteit in het systeem toeneemt.

89. Richtlijn(EU) 2016/680. Pb EU L 119/89.

2.4.6 'EQUALITY OF ARMS' EN 'CONTEXTUEEL'

Een beter inspelen op de context van de strafrechtspleging kan ten voordele van het beginsel van *equality of arms* aangewend worden. Het toegang verschaffen tot gegevens wordt makkelijker omdat de eigen positie van de verdediging en de procesfase in het systeem geabsorbeerd wordt. Bijvoorbeeld hoeft een document geen eindproduct van het gehele proces te zijn om beschikbaar gesteld te worden voor kennisneming door de verdediging. Het standpunt van het OM, de aantijgingen van de aangifte in het proces-verbaal van de politie worden als zodanig opgevat en niet als materieel feit. Anders zou het systeem immers dienst weigeren.

Het uploaden van eigen data van de verdediging wordt eveneens gemakkelijker in een systeem dat de specifieke context beter honoreert. Het systeem heeft er immers ruimte voor dat in de ondersteuning van het strafgeding tegengestelde beweringen verwerkt worden. Op die tegengesteldheid wordt in het systeem geanticipeerd doordat tegengesteldheid in juridische zin niet tegengesteldheid is in informatiekundige zin.

2.4.7 'OPENBAARHEID' EN 'INTEGER'

Het drempelverlagend effect van een betere integriteit in een systeem voor de externe openbaarheid behoeft wellicht weinig toelichting. Een betere integriteit verlaagt de kans op een openbaarmaking van een onjuist feit tijdens het openbare onderzoek ter zitting. Dat is in de dagelijkse gang van het zittingsonderzoek met het analoge dossier geborgd doordat bijvoorbeeld de rechter alleen 'de originele foto's' toont. Bij een goede integriteit is gewaarborgd dat het digitale beeld ook 'de originele foto' weergeeft.

2.4.8 'OPENBAARHEID' EN 'CONTEXTUEEL'

Het effect van verbetering van contextualiteit in een systeem is voor de openbaarheid ook gunstig in die zin dat een openbaarmaking door de verdediging in het systeem ondersteund kan worden. Het op de zitting tijdens het pleidooi tonen van een geüpload bestand, bijvoorbeeld een videofragment, stuit niet af op de eis dat het systeem alleen maar de waarheid van het openbaar ministerie of de rechter mag verwerken, of alleen de geautoriseerde versie van het videofragment. Zo zit het strafgeding immers niet in elkaar. De versie van de verdediging heeft een plaats naast die van de vervolging en het is aan de rechter om uiteindelijk zijn versie centraal te stellen als het bewijsmiddel waarmee hij zijn oordeel onderbouwt. Dat het op zitting tonen van haar eigen versie voor de verdediging mogelijk zou zijn, had ook als voorbeeld onder 2.4.5 genoemd kunnen worden van een verbeterde *equality of arms*. Het geeft de verdediging een faciliteit in handen om desgewenst tegenwicht te bieden tegen beeldmateriaal van de vervolging, waar de indruk bestaat dat (video)beelden op zichzelf een stevige impact hebben in het zittingsonderzoek.

2.4.9 'BETROUWBAARHEID' EN 'INTEGER, CONSISTENT, CONTEXTUEEL EN AUTHENTIEK'

Dat verbetering van feitelijke betrouwbaarheid wint met een positieve ontwikkeling van integriteit, consistentie, contextualiteit en authenticiteit is geen verrassing. De IT-desiderata gaan immers alle vier over toenemend vertrouwen in wat het systeem verwerkt c.q genereert. De beginselen op de horizontale en verticale as vertonen hier zoveel overeenkomst, dat de vraag opkomt of er geen

sprake is van een vorm van *begging the question*. We houden toch staande dat een onderscheid juist het inzicht vergroot omdat de informatietechnische 'betrouwbaarheid' (bedoeld als samenvatting van de vier genoemde informatietechnische desiderata) conceptueel geheel los staat van de juridische betrouwbaarheid. Overweging 30 van de Richtlijn EU 2016, 680, verwoordt dit verschil heel fraai en helder: 'Het beginsel van juistheid van gegevens moet worden toegepast met inachtneming van de aard en het doel van de verwerking in kwestie. In het bijzonder bij gerechtelijke procedures zijn verklaringen die persoonsgegevens bevatten, gebaseerd op de subjectieve perceptie van natuurlijke personen en niet altijd te controleren. Het vereiste van juistheid dient derhalve geen betrekking te hebben op de juistheid van een verklaring, maar alleen op het feit dat een specifieke verklaring is afgelegd.'[90] Deze overwegingbetoogt in essentie dat de informatietechnische juistheid gaat over een objectief waarneembaar feit, en de juridische juistheid gaat over een (subjectief, rechterlijk) oordeel. De vaststelling op de verticale as komt uiteindelijk juridisch gezag toe, de concepten op de horizontale as niet. Het duidelijkste voorbeeld om het onderscheid tussen de horizontale en verticale as toe te lichten, is het rechterlijk bewijsoordeel, waarin het gaat om de materiële waarheid. Gegevens uit een informatiesysteem die ter onderbouwing in de bewijsredenering gebruikt worden, krijgen pas door het gebruik in de rechterlijke redenering het gezag van materiële juistheid en niet al eerder omdat ze in een consistent, duurzaam of authentiek systeem gegenereerd zijn.

2.4.10 'TIJDIGHEID' EN 'INTEGER, CONSISTENT EN CONTEXTUEEL'

Een positieve ontwikkeling ten aanzien van de integriteit, de consistentie en de contextualiteit heeft niet zonder meer gevolgen voor de tijdigheid. We wijzen niettemin op een effect, maar dan van indirecte aard. De versterking van de genoemde kenmerken betekent dat er in het systeem minder fouten voorkomen. Fouten zorgen voor *hiccups* in de voortbrenging en maken correctie noodzakelijk. Minder fouten maakt de logistiek van de ene naar de andere actor efficiënter, doordat er geen extra bewerkingen nodig zijn en doordat de overdracht in een keten meteen na de bewerking in de vorige schakel kan plaatsvinden. De volgende schakel kan als het ware meteen aan de slag. Dat zou niet het geval zijn als de foutkans niet geminimaliseerd wordt.

2.5 Afsluiting

De verschillende voorspellende waarnemingen hierboven overziende valt op dat het zonnetje lijkt te schijnen en er geen wolkje aan de lucht is. Dat is inderdaad ons betoog, wanneer we vanuit de grondbeginselen en desiderata theoretisch redeneren. Als de praktijk dus minder zonnig is, hoeft dat geen voeding te leveren voor de stelling dat strafrechtspleging en IT niet samen zouden kunnen optrekken in de goede richting. Samen in dezelfde richting werken kán wel, maar het gebeurt vaak niet, voor welke ervaring vele oorzaken zullen bestaan. Er zijn bovendien nog vele en vaak lange wegen af te leggen, gedurende welke tocht met halffabricaten en deelproducten gewerkt moet worden of zelfs af en toe een doodlopend spoor gevolgd wordt. Dan zullen naar redelijke verwachting de ervaringen minder positief zijn dan hier voorgeschoteld. Neem het voorbeeld om de *equality of arms* te bevorderen door laagdrempelig toegang te verschaffen tot een systeem dat door justitie ten behoeve van de zaak gebruikt is om een

90. Richtlijn (EU) 2016/680, Pb L 119/89.

zaaksdossier samen te stellen en over te dragen. De beveiliging blijft een hot issue en zal eerst in een pilot verder getest worden. Zolang dat nog gebeurt – en testen is een tijdrovende en dure fase in de ontwikkeling van een informatiesysteem – zal van een volledige toepassing van gelijke inzage geen sprake zijn en zal de advocatuur niet met hetzelfde systeem kunnen werken als de magistratuur en daarvan ook niet de gemakken ervaren. Voor die gemakken mag bovendien de financiële drempel niet onredelijk zijn in die zin dat de noodzaak tot investeringen in kantoorsoftware voor de advocatuur (en dan niet alleen de Zuidaskantoren) binnen de perken van het redelijke zal moeten blijven of misschien wel op nul gesteld moet worden. Voor de bouw van een systeem worden echter grote bedragen gespendeerd en wordt vaak software gebruikt waarop intellectuele eigendom rust. Dat bemoeilijkt voorlopig de vrije beschikbaarstelling van een systeem of een deel daarvan. Nu lopen we echter te veel op het betoog vooruit. Het volgende hoofdstuk pakt datgene wat we hier slechts even aanstippen opnieuw op, als we verslag doen van onze bevindingen rondom de recente initiatieven om het zaaksdossier te digitaliseren. De problemen en vragen die we net noemden, komen daarbij weer aan de orde.

Hoofdstuk 3

De digitale stukkenstroom in de strafrechtsketen

3.1 Inleiding

Veranderingen in de Nederlandse strafrechtsketen als gevolg van digitalisering concentreren zich rond het procesdossier. Om die reden richt de aandacht van dit hoofdstuk zich op de digitale stukkenstroom. Doel van dit hoofdstuk is om zicht te krijgen op de kansen en risico's van digitalisering in de strafrechtsketen ten aanzien van verdragsrechtelijke en (grond)wettelijke beginselen. Met het onderzoek van de recente praktijk willen we zicht krijgen op actuele stand van zaken en de effecten van daadwerkelijke overschakeling naar elektronisch procederen in strafzaken. In lijn met onze opmerkingen in de inleiding zij nogmaals opgemerkt, dat dit niet de eerste of enige vorm van digitalisering is. Wel is het de digitalisering die in de praktijk met veel beloften is omgeven en in de afgelopen tijd en nu nog veel aandacht krijgt. Daarmee beoogt dit hoofdstuk een antwoord te geven op onderzoeksvragen 2 en 3.
Het bureau-onderzoek is hier aangevuld met een klein aantal interviews van betrokkenen bij de proeftuinen. Daarmee bedoelen we personen die in een digitaliseringsproject de leiding hadden of in de uitvoering werkzaam waren. Een lijst met geïnterviewden met een korte beschrijving van de betrokkenheid is in bijlage 2 opgenomen. De semi-gestructureerdheid van de interviews heeft ertoe geleid dat voor een deel een vaste vragenlijst is gehanteerd. De vragenlijst is ten behoeve van verschillende interviews gedeeltelijk gepersonaliseerd en tot slot gedurende de serie interviews voortdurend op punten aangepast. Het opnemen van één specifieke vragenlijst is dus niet mogelijk. In de tekst over de proeftuinen is getracht een onderscheid aan te houden tussen de beschrijving van wat er feitelijk uitgeprobeerd is en wat de ervaringen/evaluaties waren van betrokkenen enerzijds en de reflectie op de projecten van de auteurs van dit rapport anderzijds. Op deze wijze uitgevoerd bieden de interviews uitsluitend impressionistische informatie.De interviews kwam derhalve ook in het rapport een bescheiden plaats toe. Ze hebben ons ondersteund in de kritische appreciatie van wat er aan geschreven informatie beschikbaar was. Her en der worden er impressies, maar ook niet meer dan dat, aan ontleend.

Dit hoofdstuk begint met een overzicht van de context. Ons betoog begint met een samenvatting van de kaders van digitalisering, waarna de geschiedenis rond COMPAS en GPS wordt samengevat. Vervolgens bespreken we de omzetting van papieren naar elektronische documenten. Voordat we toekomen aan een bespreking van beginselen, schetsen we de manier waarop het GPS-dossier door verschillende belanghebbenden wordt gebruikt.

3.2 Kader

In de inleiding van het vorige hoofdstuk is onderscheid gemaakt tussen 'digitilization' en 'digitization'. Digitalization betekent dat werkprocessen of delen daarvan door computers uitgevoerd worden. *Digitization* beperkt zich tot het digitaal produceren, opslaan en overdragen van informatie als vervanging voor

papier. In het programma Digitaal Werken in de Strafrechtsketen (DWS)[91] zijn ten aanzien van de *digitization* ambities geformuleerd en zijn verschillende pilotprojecten uitgevoerd, waarvoor de aanduiding 'proeftuinen' in zwang is.

> *'De wensenlijst is duidelijk. Geen dossiers doorschuiven en kopiëren, maar elkaar toegang geven tot informatie. [...] Met het onder substitutie scannen gaan gescande digitale stukken het papieren origineel vervangen. Dat lijkt een kleine stap, maar het is een megaklus, waarbij uiteindelijk duizenden mensen betrokken zijn.'*[92]

Het programma DWS valt niet los te zien van het rapport 'Prestaties in de strafrechtsketen' van de Algemene Rekenkamer uit 2012.[93] In dit rapport worden verschillende kritische noten gekraakt ten aanzien van het functioneren van de strafrechtsketen. Naar aanleiding hiervan is het programma Versterking Prestaties Strafrechtsketen (VPS)[94] gestart. Dit programma heeft de volgende prioriteiten: ongewenste uitstroom minimaliseren/kwaliteit verhogen, van het aangifteproces een hoogwaardig dienstverleningsproces maken, de in-, door- en uitstroom van zaken in de keten inzichtelijk en transparant maken, elektronische informatie-uitwisseling, doorlooptijden verkorten en tot slot de modernisering en herijking van het Wetboek van Strafvordering. Onderdeel van het programma VPS is het subprogramma DWS, waarin wordt gewerkt aan het coördineren van het digitaliseringsproces van de strafrechtsketen. DWS is opgezet met het doel om de digitalisering van de strafrechtsketen te coördineren.[95] Deze doelstelling bleek echter te ambitieus, met als gevolg dat DWS zich uiteindelijk effectief slechts bezig heeft gehouden (en bezighoudt) met het digitaliseren van het (straf)procesdossier en het digitaliseren van de stukkenstroom. In een door DWS zelf uitgegeven e-zine staan de taken als volgt beschreven:

> *'Binnen het programma DWS werken ketenpartners samen aan de digitalisering van werkprocessen.*[96] *Nieuwe werkprocessen, software en hardware worden getest in proeftuinen en bij projecten van politie, openbaar ministerie, rechterlijke macht en executiepartners. In de huidige eerste fase verdwijnt het papieren dossier op de meeste plekken en verschijnt het digitale dossier. […] De ketenpartners dragen, elk afzonderlijk, zorg voor de realisatie van hun projecten. Het programma biedt een platform voor afstemming, discussie en gezamenlijke besluitvorming in de keten. De opdracht is het (digitaal) verbinden van systemen én professionals. DWS maakt onderdeel uit van het programma Versterking Prestaties van de Strafrechtsketen (VPS) van het ministerie van Veiligheid en Justitie.'*[97]

91. Voor meer informatie over DWS zie: Digitaal werken in de strafrechtsketen, E-Zine van DWS, oktober 2015; Digitaal werken in de strafrechtsketen, E-Zine van DWS, maart 2016.
92. Digitaal werken in de strafrechtsketen, E-Zine van DWS, oktober 2015, 1, p. 3.
93. *Kamerstukken II* 2011/12, 33173, 1.
94. Voor meer informatie zie de website van de Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/versterking-prestaties-strafrechtsketen/inhoud/programma-s-verbetering-strafrechtsketen.
95. Zie: Brief aan Tweede Kamer van 12 november 2013 bij 33605 VI ek-B, GPS (Geïntegreerd processysteem strafrecht) in relatie tot VPS en KEI, p. 3, 5, *Kamerstukken II* 29 279, nr. 178.
96. Wij zagen vooral wat verderop in het citaat wordt aangegeven: het overzetten van de stukkenstroom. Digitale werkprocessen in andere zin zijn kennelijk wel voorgenomen.
97. Digitaal werken in de strafrechtsketen, E-Zine van DWS, oktober 2015, 1, p. 1.

De minister van justitie schrijft in 2013:

> *'De norm is dat in 2016 processtukken in de strafrechtsketen digitaal worden uitgewisseld. Concreet houdt dit in dat OM, rechtspraak en de partners in de executiefase (o.a. CJIB, 3RO) in 2016 processtukken digitaal uitwisselen. Om dit te realiseren is onlangs het deelprogramma Digitaal Werken in de Strafrechtsketen (DWS) van start gegaan. […] De politie is met volle kracht bezig de eigen informatievoorziening op orde te brengen. […] Behalve het verkeer binnen de keten is er ook de communicatie met de advocatuur en met de burger (verdachte, slachtoffer, getuige, aangever, benadeelde partij). […] Dat proces (naar digitaal werken in de strafrechtsketen) voltrekt zich onder de vlag van het programma VPS: het programma Digitaal werken in de strafrechtsketen (DWS) is ondergebracht binnen de structuur van het overkoepelende programma VPS.'*[98]

3.3 COMPAS en GPS

Het digitale strafdossier wordt, afhankelijk van het soort zaak, geregistreerd in ofwel GPS (Geïntegreerd Processysteem Strafrecht) ofwel COMPAS (Communicatie Openbaar Ministerie en Parket Administratie Systeem). GPS verwerkt de bulk aan zaken, de zogenaamde standaardzaken, terwijl COMPAS nog slechts wordt gebruikt voor de verwerking van de, in absolute aantallen minder belangrijke, maatwerkzaken. De nadruk in het navolgende zal liggen op GPS, maar voor de volledigheid volgen daarvoor enkele opmerkingen over COMPAS.

Het proces van digitalisering in de strafrechtspleging is al geruime tijd aan de gang.[99] Zo is het systeem COMPAS al in 1988 speciaal ontwikkeld voor het OM. COMPAS is een registratiesysteem dat tevens wordt gebruikt om zaken integraal te managen van proces-verbaal, via dagvaarding naar het vonnis. In 1999 is besloten om COMPAS te vervangen, omdat het technisch ouderwets werd bevonden en men vond dat updaten geen zin meer had.[100] In januari 2005 schrijft een leverancier in een offerte aan het OM: 'Het GPS-project gaat met de ontwikkeling van het increment Maatwerkzaken zijn laatste fase in. Met de pilot en volledige uitrol van Maatwerkzaken voor eind 2006, kan het bestaande COMPAS-systeem worden uitgefaseerd.' Op 9 juli 2009 schrijft de Minister aan de Tweede kamer[101] dat inmiddels ook verder gewerkt wordt aan de applicatie voor de maatwerkzaken en dat een gezamenlijke pilot van OM en de Rechtspraak wordt gestart. In 2013 rapporteert de Minister opnieuw aan de Kamer[102]. Recent was namelijk door middel van een proeftuin in Rotterdam ervaring opgedaan met het gebruik van GPS voor maatwerkzaken. Deze proef beoogde om meer complexe zaken (MK-loopzaken en zaken met preventieve hechtenis) in GPS voor te bereiden, stukken uit te wisselen in het proces en de zaak af te doen. In de Rotterdamse

98. Brief van 12 november 2013, GPS (Geïntegreerd processysteem strafrecht) in relatie tot VPS en KEI, p. 3.
99. J. Rademaker, De digitale strafrechtspleging. Strafrechtelijke informatisering in meervoudig perspectief, Zwolle, Tjeenk Willink, 1996.
100. Langbroek & Tjaden 2008, p. 3.
101. Tweede Kamer, vergaderjaar 2008-2009, 31 700 VI, nr. 155.
102. Brief van 12 november 2013, GPS (Geïntegreerd processysteem strafrecht) in relatie tot VPS en KEI, p. 3.

proeftuin is het gebruik van GPS tijdelijk gestaakt.[103, 104] Over de details daarvan is in de onderhavige verkenning geen duidelijkheid verkregen. Veranderingen in het IT-platform, in het bijzonder GPS, zouden noodzakelijk zijn om de Rotterdamse handelwijze in de rest van het land toe te passen. Anno 2016 wordt COMPAS nog altijd gebruikt, zowel binnen het OM als bij rechtbanken. Op de werkvloer is men weinig hoopvol over de implementatie van maatwerkzaken in GPS op de korte termijn. Het voorgenomen einde van COMPAS, ondanks de al zeventien jaar bestaande ambitie daartoe, is nog altijd niet in zicht. Toch blijkt uit de interviews dat de meeste respondenten ervan uitgaan dat GPS uiteindelijk wel gebruikt zal gaan worden voor maatwerkzaken.[105] Op dat systeem richten we nu verder de aandacht.

GPS is/wordt het middelpunt van het digitale dossier en is specifiek opgezet om het papier in de strafrechtsketen overbodig te maken. GPS functioneert als register met administratieve gegevens, maar tevens als opslag voor het gehele strafdossier dat vanuit GPS (online) ingezien en uitgelezen kan worden en waaraan stukken kunnen worden toegevoegd. Oorspronkelijk was het de bedoeling dat GPS voor de fase van vervolging en berechting zou worden gebruikt.[106] In 2007 geeft toenmalig P-G Van Brummen aan dat de rechtspraak niet onverdeeld positief is over de ontwikkeling en mogelijkheden van GPS, maar dat hij er desondanks van uitgaat dat de Rechtspraak bij de ontwikkeling van GPS betrokken zal blijven. Over het eventueel afhaken van de Rechtspraak zegt hij: '*Ik kan mij dat niet voorstellen. De strafrechtspleging behoort in een keten te blijven functioneren.'*[107] Samenwerking tussen OM en ZM bleek op dit gebied echter geen haalbare kaart.[108] De Rechtspraak haakt in 2009 af en het OM blijft als enige opdrachtgever over voor de ontwikkeling van GPS.[109]

Uit het voorgaande wordt in grote lijnen duidelijk hoe OM en ZM zich tot nu toe tot elkaar verhouden inzake de elektronische uitwisseling van stukken. In de zojuist geciteerde brief wordt ook in grote lijnen duidelijk wat de positie van GPS is:

> *'GPS is rond het jaar 2000 bedacht en in de loop der jaren ingehaald door nieuwe ontwikkelingen. […] In 2011 is het project GPS afgerond. Het systeem GPS is in bedrijf genomen en wordt sindsdien gebruikt voor alle standaardzaken; in april 2013 werd de miljoenste zaak door het OM in GPS vastgelegd. […] Wij werken nu toe naar volledig digitaal werken in de strafrechtsketen. […] GPS is een belangrijke mijlpaal in de ontwikkeling daarnaartoe. Maar […] de*

103. Digitaal werken in de strafrechtsketen, E-Zine van DWS, maart 2016, 1, p. 11: '*Recent is eind 2015 in Rotterdam echter de invoer van nieuwe zaken in GPS tijdelijk gestaakt. Voordat het project in de proeftuin kan worden gecontinueerd, moet een aantal bevindingen zijn opgelost. Hiertoe is een multidisciplinair team samengesteld dat werkt aan het wegnemen van de ondervonden problemen.'*
104. Voortgangsrapport Versterking Prestaties Strafrechtsketen december 2015, p. 6: *'De aanzienlijk complexere beproeving van maatwerkzaken in de proeftuin Rotterdam heeft inzichten opgeleverd voor aanpassingen in de systemen van het OM en de rechtspraak. Die aanpassingen worden nu gerealiseerd, waarna in 2016 de werkprocessen verder worden uitgewerkt. Daarna zal het resultaat opnieuw beproefd worden voordat landelijk wordt uitgerold.'*
105. Waarbij aangetekend, maar daarover later meer, dat niet alle respondenten even positief zijn over de geschiktheid van GPS voor de verwerking van standaardzaken.
106. Langbroek & Tjaden 2008, p. 4.
107. P. Vermaas, 'GPS wordt steeds beter. Interview met H. van Brummen', in: *Opportuun* 2007, 8, p. 9-11.
108. Langbroek & Tjaden waren sceptisch over de ketenbenadering en de haalbaarheid daarvan. Zie: Langbroek & Tjaden 2008, p. 6-7.
109. Van Wees 2015, p. 801; Brief van 12 november 2013, GPS (Geïntegreerd processysteem strafrecht) in relatie tot VPS en KEI, p. 2.

voornemens tot digitalisering van de strafrechtsketen zijn […] de oorspronkelijke ambities van GPS al voorbij.
In 2016 moeten voorzieningen zijn gerealiseerd ten behoeve van de digitale uitwisseling van processtukken door het OM en de Rechtspraak met de burger en de advocatuur. […] De advocatuur krijgt op afzienbare termijn de mogelijkheid om digitale dossiers via een goed beveiligd portaal op te halen. […] Landelijk is een proces ingericht om de papieren processen-verbaal van opsporingsambtenaren te scannen en vervolgens digitaal te verwerken in GPS. […] Het project GPS omvatte bij de start in 2000 drie elementen: het registreren van zaken die bij het OM binnenkomen, het ondersteunen van het werken met digitale strafdossiers door officieren van justitie én rechters en het besturen van de werkstroom (de stroom strafzaken) binnen de arrondissementsparketten. Het omvatte (en omvat) niet het hoger beroep.'[110]

In de interviews wordt het beeld bevestigd dat de ontwikkeling en het beheer van GPS volledig in handen is van het OM en de overige partijen daarmee in hoge mate afhankelijk van het OM zijn om stukken in GPS toe te kunnen voegen.

Alle wegen naar GPS lopen via het OM. Hierin schuilt in eerste instantie wel een zekere logica. Het is immers het OM dat verantwoordelijk is voor het opsporingsonderzoek en op grond van art. 149a lid 1 Sv ook voor de samenstelling van de processtukken waarin de resultaten van dat onderzoek hun neerslag vinden. Het moge echter duidelijk zijn dat het voorbereidend onderzoek de facto wordt uitgevoerd door de politie. Een mogelijkheid voor de politie om zelfstandig dossiers digitaal aan te leveren aan het OM door middel van het uploaden in GPS (of anderszins) ontbreekt echter tot op heden. Zoals Van Wees opmerkt: *'De politie is helaas nog niet in staat om dossiers ook digitaal aan te leveren aan het OM, zodat de papieren politiedossiers op de parketten worden ingescand.'*[111]

Eenzelfde soort beperking geldt ten aanzien van de verdediging, die niet in een digitaal zaaksdossier in GPS een document kan uploaden. Dat aan deze mogelijkheid geen hoge prioriteit gegeven zou zijn, is niet meteen onlogisch. Het toevoegen van stukken aan het dossier door de verdediging wordt in de praktijk veelal pas gewenst – als het al voorkomt – als de zaak al overgedragen is aan de rechter voor de zitting. . Bij een digitaal dossier in GPS zou het nochtans wenselijk zijn dat de verdediging ook in het vooronderzoek iets aan het dossier toevoegen kan, al was het alleen maar om te bevorderen dat de informatie bij de vervolgingsbeslissing betrokken wordt. Dat is praktisch bezien meer aangewezen bij maatwerkzaken dan bij standaardzaken, maar het is de bedoeling dat ook maatwerkzaken in GPS verwerkt zullen gaan worden. Of het nu in het vooronderzoek is of in de berechtingsfase, de verdediging heeft in het huidige systeem het OM nodig om stukken in het GPS-dossier te laten opnemen. Een document dat ter zitting overgelegd wordt, bijvoorbeeld een deskundigenrapport of een preliminair schriftelijk verzoek, kan dus niet vanzelf in het digitale GPS-dossier gevoegd worden. Als de rechter ter zitting beslist heeft dat het overgelegde document aan de stukken toegevoegd zal worden, zal het uploaden in een digitaal GPS-dossier in de regel wel gebeuren. Het huidige beeld is dat het OM dit dan moet uitvoeren.

110. Brief van 12 november 2013, GPS (Geïntegreerd processysteem strafrecht) in relatie tot VPS en KEI.
111. Van Wees 2015, p. 802.

Deze stand van zaken is door de ingebruikneming van het advocatenportaal niet veranderd. Dit portaal is in de tweede helft van 2015[112] in werking genomen. Het advocatenportaal bracht vooruitgang doordat advocaten strafdossiers, voor zover het GPS-standaardzaken betreft, kunnen downloaden. Uploaden blijft echter onmogelijk zodat daarvoor de weg via het OM bewandeld dient te worden. Op dit portaal komen we in paragraaf 3.4 terug.

Er komt echter een moment in de strafprocedure dat de zittingsrechter verantwoordelijk wordt voor de volledigheid en juistheid van het procesdossier. Van Wees legt daarbij nadrukkelijk de relatie met het onderwerp van dit rapport, te weten de strafvorderlijke beginselen:

> *'De rechter dient daarbij de naleving te verzekeren van een aantal rechtstatelijke waarborgen. De rechter moet immers bezien of het dossier compleet is met het oog op de beantwoording van de vragen van artikel 348 en 350 Sv. Bij het verstrekken van toegang tot het dossier aan procespartijen en -deelnemers dient te worden gehandeld overeenkomstig wet- en regelgeving, waaraan het beginsel van een eerlijk proces ten grondslag ligt.'*[113]

Het is de rechter die daarvoor in de fase van de berechting de verantwoordelijkheid draagt. Op deze plaats kan dus worden vastgesteld dat de verantwoordelijkheid van de rechter in de gedigitaliseerde zaken nu niet zodanig uitgewerkt is, dat deze op gelijke wijze als de officier van justitie daarvoor GPS kan gebruiken.

3.4 De omzetting van papier naar digitaal

Het strafproces is van oudsher op papier georiënteerd, net als alle andere vormen van stelselmatige verwerking van informatie in een bureaucratische omgeving. De overgang van lijvige dossiers die in voorkomende gevallen met karretjes naar de zittingszaal gereden worden naar het meenemen van een tablet of laptop waarop alle benodigde informatie voorhanden is, vergt naast fysiek werk ook een cultuuromslag. Daarop zal in een later stadium nader worden ingegaan, maar nu eerst een indruk van hoe de overgang van papier naar digitaal er op dit moment uitziet.

Het proces start bij de politie die een proces-verbaal (p.v.) digitaal opstelt in het eigen systeem. Als het p.v. af is wordt het geprint en ondertekend met een zogenaamde 'natte' handtekening. De verschillende delen van een strafdossier worden vervolgens naar het OM vervoerd. Het OM beoordeelt elke zaak om standaard- en maatwerkzaken te onderscheiden. Standaardzaken worden in GPS verwerkt en maatwerkzaken in COMPAS.[114] Alleen de stukken van de standaardzaken worden gedigitaliseerd voor gebruik in GPS. Nadat een zaak is gekwalificeerd als 'standaard' wordt deze naar het kantoor van de Justitiële Informatiedienst Justid in Almelo vervoerd. Daar worden de papieren dossiers centraal ingescand in een zogenoemde scanstraat. Als het scannen voltooid is worden deze door Justid digitaal aangeleverd in GPS en worden op deze manier digitaal beschikbaar voor het OM om verder in behandeling te worden genomen. Dit

112. De precieze datum is om wat voor reden dan ook in nevelen gehuld. De beleidsstukken en enkele artikelen noemen echter alleen data in de tweede helft van 2015.
113. Van Wees 2015, p. 808.
114. In de vorige paragraaf is al gemeld, dat de proeftuin Rotterdam waarin GPS werd getest voor de verwerking van maatwerkzaken op dit moment gestopt is.

scannen is de afgelopen tijd getest in de proeftuin Noord-Nederland en gaat als volgt in zijn werk:

> *'Op dit moment worden elke maandag, dinsdag en donderdag de processen-verbaal uit Arrondissementsparket Noord-Nederland richting Almelo gereden. De […] aktes van uitreiking van een dagvaarding worden […] door Justid gescand en zijn na het scannen direct beschikbaar in het digitale dossier.'*[115]

Deze digitale dossiers betreffen vooralsnog slechts stukken afkomstig van of binnengekomen via het OM, maar er wordt wel toegewerkt naar de mogelijkheid voor in ieder geval de politie om zelfstandig digitaal stukken te kunnen aanleveren:

> *'In Noord-Nederland is de zogenaamde indirecte methode beproefd, waarbij processen-verbaal (pv's) van de politie via het OM worden aangeleverd aan Justid ter digitalisering. Dit is de eerste te implementeren stap. Aanvullend hierop vindt een beproeving van de zogenaamde directe methode in Oost-Nederland plaats. In deze beproeving wordt vooral gekeken naar de toekomstige mogelijkheid voor rechtstreekse aanlevering van pv's door de politie aan Justid.'*[116]

Voor een gedetailleerde bespreking van de wet- en regelgeving die de invoering van en het werken met digitale dossiers omringt is hier geen plaats. In het kader van beveiliging, een typisch informatietechnisch onderwerp, zou bijvoorbeeld aandacht moeten worden besteed aan de regelgeving die daaromheen is opgetuigd (of in de steigers staat). Hier zal voor nu slechts aandacht worden besteed aan een tweetal vragen die zeer nauw verweven zijn met de overgang van papieren naar digitale dossiers. Allereerst komt de vraag aan de orde hoe het papieren dossier zich wettelijk verhoudt tot het digitale dossier en ten tweede wordt aandacht besteed aan de, deels zeer praktische, vraag naar hoe de opslag van digitale dossiers is geregeld.

In het huidige art. 153 lid 2 Sv wordt een digitaal p.v. in essentie gelijkgesteld met een ondertekend papieren exemplaar.[117] Met de inwerkingtreding van de Wet digitale processtukken Strafvordering[118] zal de tweede volzin van dit artikellid komen te vervallen en zal de regeling verplaatst worden naar het uitvoeringsbesluit. Het regelen van een deugdelijke wettelijke basis voor het zogenaamde 'scannen onder substitutie' (vervanging van het papieren voor een digitaal stuk) lijkt onderwijl wel van belang, nu in de proeftuin Noord-Nederland daarmee al volop is geëxperimenteerd. In het programma DWS blijkt deze procedure zelfs al geëvalueerd te zijn.[119]

Wat betreft het archiveren van digitale dossiers en de daarmee samenhangende vraag naar de bewijswaarde van gearchiveerde digitale dossiers ten opzichte

115. Digitaal werken in de strafrechtsketen, E-Zine van DWS, oktober 2015, 1, p. 4.

116. Digitaal werken in de strafrechtsketen, E-Zine van DWS, maart 2016, 1, p. 10.

117. Het College van Procureurs-Generaal merkt in zijn advies bij het wetsvoorstel digitale processtukken echter op dat een expliciete gelijkstelling ontbreekt. Bijlage bij: Kamerstukken II 2014/15, 34090, 3, p. 2.

118. Wet gepubliceerd in *Staatsblad* 2016, 90, 17 februari 2016.

119. Digitaal werken in de strafrechtsketen, E-Zine van DWS, maart 2016, 1, p. 10: '*In februari 2016 is de eindevaluatie (scannen onder vervanging voor interventiezaken) opgeleverd en het resultaat, de zogenaamde indirecte methode, is door de stuurgroep goedgekeurd.*'

van papieren versies kan men zich een controverse licht voorstellen.[120] De ene persoon ziet een paradijselijk visioen van een klein gebouw met servers waarin alle strafdossiers digitaal gearchiveerd zijn. Voor een ander is dat een nachtmerrie vanwege de kwetsbaarheid van die centrale digitale archivering, het risico van storing, misbruik en dergelijke. Dit vraagstuk is van grote betekenis voor een behoorlijke overheidsbureaucratie met bijbehorende veiligheid van gegevensopslag en archieven, maar de directe invloed daarvan op strafvorderlijke beginselen is voorlopig niet heel groot. Het volgende citaat is in dat opzicht veelzeggend.

> 'De angst voor een mega-archief is onterecht […] "We krijgen zeker niet een groot ketenarchief. De archieven voor het OM, ZM en de Politie blijven gescheiden." Zo bepaalt elke ketenpartner zelf de 'houdbaarheidsdatum' van zijn dossiers.'[121]

Zo bezien lijkt de praktijk erop neer te komen dat weliswaar niet één groot centraal 'mega-archief' wordt gecreëerd, maar dat de verschillende ketenpartners allemaal hun eigen (versie van de) dossiers gaan opslaan.

3.5 Het GPS-dossier gebruiken

Nu we gezien hebben dat in GPS een digitaal dossier gevormd is, bespreken we het gebruik ervan door ketenpartners en overige betrokkenen. Om toegang tot gegevens te krijgen zijn verschillende systemen beschikbaar voor verschillende actoren.

GPS beschikt sinds jaar en dag over een eigen viewer, simpelweg de GPS-viewer genoemd. Deze viewer is ontworpen voor de registratie en beoordeling van standaardzaken en wordt daar blijkens de ingewonnen informatie nog altijd voor gebruikt. Juist de beperkte functionaliteiten en de afwezigheid van allerhande, voor standaardzaken onnodige, opties worden, zo blijkt uit de interviews, als voordeel gezien voor het werken met dossiers die deze functionaliteiten niet vereisen.

Voor de meer complexe zaken is bij het OM de digitale dossier viewer (DDV) ontwikkeld. Ervaringen hiermee zijn opgedaan in de proeftuin Rotterdam. Deze viewer functioneert als een soort bril waarmee het dossier in GPS bekeken wordt. DDV bevat ten opzichte van de GPS-viewer enkele aanvullende functionaliteiten zoals de mogelijkheid meerdere documenten tegelijkertijd in te zien.

> *'In aanvulling op deze functionaliteit is er ook de optie 'werkdocument' in de viewer opgenomen. Dit is een Word-document waarbij een gebruiker op het linker scherm het PV opent en op het rechterscherm het werkdocument. Vervolgens kunnen in dit werkdocument aantekeningen gemaakt worden, die direct in het digitale dossier (en daarmee in GPS) worden opgeslagen.'*[122]

Toen de Rechtspraak zich in 2009 terugtrok uit de ontwikkeling van GPS, is een start gemaakt met de ontwikkeling van DIVOS ten behoeve van de zittende magistratuur. Een eerste versie daarvan, DIVOS I, is lokaal ontwikkeld in Rot-

120. Nader over dit onderwerp: Van Wees 2015, paragraaf 3.2.

121. Digitaal werken in de strafrechtsketen, E-Zine van DWS, oktober 2015, 1, p. 5.

122. Digitaal werken in de strafrechtsketen, E-Zine van DWS, oktober 2015, 1, p. 7.

terdam en vormt de basis voor het nu landelijk gebruikte DIVOS (in de wandelgangen ook wel DIVOS II genoemd). Een blik achter de schermen bij zowel het OM als de Rechtspraak leert, dat DDV en DIVOS in hoge mate overeenkomen. Dit werd in onze interviews bevestigd. Beide systemen zijn ontwikkeld als een soort bril om in GPS te kijken, de dossiers te kunnen doorzoeken, te ordenen en te bewerken.

Het advocaten- c.q. slachtofferportaal is een hybride vorm die zowel inzage biedt als transacties met GPS ondersteunt (reeds genoemd in par. 3.2).

> *'Advocaten hebben toegang tot het advocatenportaal. […] Daarna kan het aangevraagde dossier (geheel of gedeeltelijk) gedownload en/of bekeken worden. […] Via de eigen computer heeft de advocaat daardoor toegang tot alle stukken die door medewerkers van het OM en de Rechtspraak zijn klaargezet. Advocaten kunnen vervolgens zelf bepalen op welke wijze zij het strafdossier willen gebruiken (digitaal of printen op papier). Het is ook mogelijk om een document in het advocatenportaal […] direct te bekijken, zonder het eerst te hoeven downloaden. […] Hierdoor kunt u bijvoorbeeld snel vaststellen of het document wel of niet relevant is om te downloaden, of kunt u een nagekomen stuk dat vlak voor een zitting is verstrekt direct raadplegen vanaf een tablet of smartphone, zonder het eerst te hoeven downloaden.'*[123]

Voor zover wij hebben kunnen nagaan biedt het advocatenportaal op dit moment alleen mogelijkheden tot inzien en downloaden. Bewerken, doorzoeken en/of ordenen van het dossier wordt door de advocaat met behulp van eigen software gedaan[124]. De applicaties DDV en DIVOS zijn niet beschikbaar gesteld aan de advocatuur. De geïnterviewden uit het OM en de zittende magistratuur zien daartoe ook geen reden. Tijdens de expertmeeting werd de verwachting uitgesproken dat ook de advocatuur niet bijzonder gretig zal zijn om applicaties van justitie over te nemen, onder meer vanwege de afhankelijkheid die dat met zich mee zou kunnen brengen.

3.6 Kansen en risico's voor strafvorderlijke beginselen

3.6.1 INLEIDING

In de voorgaande paragrafen is de overgang van papieren stukken naar het digitale dossier vanuit verschillende invalshoeken beschreven. Daarbij zijn zowel organisatorische als informatietechnische onderwerpen aan bod gekomen. Deze paragraaf legt een verband tussen deze onderwerpen en de bijbehorende strafvorderlijke beginselen. Daarmee komen we toe aan een gedeeltelijke beantwoording van de vraagstelling van dit onderzoek, namelijk de deelvragen 2 en 3. Deze beantwoording geschiedt in termen van kansen en risico's. Praktische factoren, die de uitvoeringspraktijk compliceren maar met de beginselen weinig te maken hebben, zijn niet in deze analyse verwerkt. Om kansen en risico's voor de strafvorderlijke beginselen te illustreren met voorbeelden, fungeert GPS als *Leitmotiv* in deze sectie. Deze focus is mede ingegeven door de centrale positie die GPS in de digitalisering inneemt.

123. https://loket.rechtspraak.nl/Professionals/Advocatuur/45 (laatst geraadpleegd op 15 okt. 2016).

124. Zoals ontwikkeld binnen bijvoorbeeld het reeds genoemde samenwerkingsverband Silex; zie: http://www.mr-online.nl/juridisch-nieuws/31449-advocaten-slaan-handen-ineen-voor-digitaal-procederen. (laatst geraadpleegd op 15 okt. 2016).

In deze paragraaf wordt met de opsomming van beginselen uit hoofdstuk 2 als kapstok beschreven wat er tot nu toe boven water is gekomen aan kansen of risico's. In het digitaal maken van de stukkenstroom is vooruitgang geboekt en valt er dus van ervaringen te leren. Die zijn in de interviews en rapportages onderzocht. In aanvulling daarop reflecteren we ook zelf op mogelijke kansen en risico's, ons daarbij beperkend tot de elektronische stukkenstroom. Op overige digitaliseringsontwikkelingen gaan we in hoofdstuk 4 in.

3.6.2 LEGALITEIT

De overgang van papieren processtukken naar elektronische documenten, die samen in een GPS-dossier ondergebracht worden, heeft op zichzelf niet blootgelegd dat er een toename of afname is van misbruik van de aan ketenpartners toegekende bevoegdheden. Dat verbaast niet, want ondanks de grote inspanningen is het toch niet meer dan een administratieve verandering onder de ruim wapperende banier van de wettelijke taken voor verslaglegging en dossiersamenstelling. Het digitaal maken van de stukken maakt dat niet moeilijker of makkelijker. Als bijvoorbeeld een officier van justitie de overdracht van een dossier aan de rechter onrechtmatig zou willen uitstellen[125], dan kan dat in de papieren wereld net zo goed als in de digitale wereld. Zolang digitalisering beperkt blijft tot 'digitization' zien wij geen toename in het risico voor het beginsel van détournement de pouvoir.

De spanning tussen een efficiënt veranderproces enerzijds en de wettelijke verdeling van taken, bevoegdheden en verantwoordelijkheden anderzijds is in het DWS programma voelbaar[126]. Dat bleek bijvoorbeeld ook uit het afhaken door de Rechtspraak van het GPS-programma. Het waarborgen van de eigen onafhankelijke positie van een ketenpartner zet een kennelijke rem op samenwerking als het IT-voorzieningen betreft. Dat in dit voorbeeld de 'rem' uitging van de Rechtspraak is niet relevant, omdat het argument van autonomie mutatis mutandis op elke ketenpartner van toepassing is. Op het eerste gezicht lijkt het zelf beheren van gegevens een versterking van de eigen onafhankelijkheid op te leveren. De informatiekunde spreekt dit echter tegen. Gegevens die gedeeld worden, hoeven niet via technische voorzieningen te worden getransporteerd. Wijzigingen en herstelde fouten zijn in het geval van gedeelde gegevens direct voor alle deelnemers beschikbaar. Naar onze overtuiging is de onafhankelijkheid van ketenpartners beter gediend met correcte en actuele gegevens, dan met de wetenschap zelf verantwoordelijk te zijn voor de eigen gegevens, inclusief eventuele vervuiling.

Tussen OM en Rechtspraak bestaat geen overeenstemming over wie precies wanneer de eindverantwoordelijkheid draagt voor de compleetheid van het procesdossier.[127] Dit blijkt ook uit onze interviews. Sommige geïnterviewden geven aan dat er een 'informele' weg bestaat waarlangs eventuele problemen met bijvoorbeeld het (te) laat indienen van stukken worden opgelost. Wil bijvoor-

125. P.P.J. van der Meij, 'De laatste duit in het zakje. Over waarheidsvinding in strafzaken en de beperkingen van de verdediging', in: *Strafblad* december 2014; J. Boksem, 'Nader onderzoek geboden?', Pre-advies voor de jaarvergadering van de Nederlands-Vlaamse Vereniging voor Strafrecht 2015, p. 16-17.

126. Ibid.: '*Samenwerken binnen de strafrechtsketen is, ook gezien de verschillen in wettelijke taken en verantwoordelijkheden, niet vanzelfsprekend. De taken en verantwoordelijkheden van politie/OM/rechtspraak zijn duidelijk gescheiden.*'

127. De RvdR merkt in haar advies bij het wetsvoorstel digitale processtukken op dat in de nieuwe wet daarvoor geen oplossing wordt geboden; bijlage bij: Kamerstukken II 2014/15, 34090, 3, p. 2.

beeld het OM of de verdediging in een laat stadium nog stukken toevoegen aan het procesdossier dan kan dat in de papieren wereld alleen door deze stukken ter griffie aan te leveren. Deze voegt de stukken toe aan het dossier, waarna de verschillende overige betrokkenen een kopie ontvangen. Die oplossing werkt omdat de zittende magistratuur (ZM) de regie behoudt en eventueel het toevoegen kan weigeren. Als in de digitale wereld stukken zonder tussenkomst van de griffie direct in het digitale dossier worden gezet, verliest de zittende magistratuur deze regie. De digitale-dossiervoorziening dient dan ook aan de eis te voldoen dat partijen alleen via de griffie stukken kunnen toevoegen, net als in de papieren wereld. Dat lijkt echter inefficiënt en in essentie een voorbeeld van het handhaven van oude werkprocessen in een nieuw jasje. Een andere oplossing, voorgesteld door Van Wees,[128] is om te werken met een dossierindex die bepaalt welk stuk zichtbaar is en voor wie. Het wijzigen in de index staat gelijk aan zeggenschap over het dossier. Er dient dan wel overeenstemming te bestaan over het moment dat zeggenschap overgaat van OM naar ZM. Uit de interviews komt naar voren dat op dit moment gewerkt wordt met een informele, en daarmee niet afdwingbare, afspraak tussen OM en de Rechtspraak dat het dossier drie weken voor de zittingsdatum door het OM wordt overgedragen. Aangegeven wordt dat een meer bestendige oplossing technisch op dit moment niet haalbaar is. Waarom werd niet duidelijk.[129]

Tegenstellingen als hiervoor beschreven staan bij nadere beschouwing in verband met verschillende strafvorderlijke beginselen. In de overdracht van OM naar ZM doen zich problemen voor.[130] Zowel de Raad voor de Rechtspraak als de Raad van State[131] onderstrepen de behoefte aan regelgeving op dit punt. Kennelijk wordt het beginsel van legaliteit in deze adviezen zo ingevuld dat men de veranderende digitale praktijk graag geregeld ziet. De wetgever heeft echter gekozen voor een grotere afstand tussen wettelijke regeling en werkpraktijk. De flexibiliteit die zo aan het legaliteitsbeginsel toegekend wordt, verdient ondersteuning. Als de overdracht in de strafprocedure voldoende duidelijk in de wet gemarkeerd is, dwingt het legaliteitbeginsel niet tot nadere vastlegging in de wet van de wijze waarop dat in het werkproces geschiedt. i De situatie is nu zo dat besloten is tot gebruik van het systeem GPS. In principe impliceert dat de keuze voor gedeelde[132] opslag van documenten. Thans is de praktijk dat het OM het dossier in GPS beheert en op een bepaald moment ‘vrijgeeft’ aan de Rechtspraak en verdediging (via het advocatenportaal). Het systeem maakt het mogelijk om tussentijds stukken toe te voegen en op die manier het dossier stukje bij beetje te vullen en voor de advocaat om het gehele dossier of gedeelten te raadplegen en te downloaden. Blijkens de “Handleiding Advocatenportaal: Mijn Strafdossier” is in het uploaden van stukken nu niet voorzien. Welke keuze men uiteindelijk voor de inrichting kiest maakt ons vanuit beginselperspectief niet uit. Een gedeeld digitaal dossier kan een naadloze overgang van OM naar ZM realiseren,

128. M.E. van Wees, ‘Modernisering en digitalisering van het strafproces’, *DD* 2015, 72.

129. Voor informatiekundigen geldt de frase ‘technisch niet haalbaar’ als eufemisme voor ‘bestuurlijk niet haalbaar’. Puur taalkundig gezien is ‘technisch niet haalbaar’ onjuist, want de techniek kent dit soort beperkingen niet.

130. Task Force OM-ZM, Recht doen: Samenwerken loont, Openbaar Ministerie & Rechtspraak, Februari 2014

131. In zijn Advies Conceptwetsvoorstel digitale processtukken (bijlage bij: Kamerstukken II 2014/15, 34090, 3) zegt de RvdR het te betreuren dat op dit punt niet ‘van de gelegenheid gebruik is gemaakt om te voorzien in een regeling voor het (elektronisch) verkeer tussen het openbaar ministerie en de Rechtspraak’. Zie Raad van State in zijn advies bij het wetsvoorstel digitale processtukken. Door de wetgever is dit niet overgenomen. Zie: Kamerstukken II 2014/15, 34090, 4, p. 13-14 en Kamerstukken II 2014/15, 34090, 3, p. 44.

132. Wij spreken liever van ‘gedeelde’ dan van ‘gecentraliseerde’ opslag, om de aandacht naar samenwerking toe te leiden.

met respect voor de verdeling van taken en posities, waarbij fysieke verplaatsing van elektronische inhoud achterwege blijft.
Door kostenbesparingen te willen realiseren met gebrekkige IT-middelen, kan legaliteit wel in het geding komen. Al eerder kwam de quote voor over de automatisering van het proces in de vervolgingsfase.[133] Wat hier zichtbaar wordt, is een tamelijk praktisch gevolg van wat kan worden gezien als een neveneffect van digitalisering: kostenbesparing.[134] Verschillende gesprekspartners geven aan dat de verwachte kostenbesparing door toenemende efficiëntie in twijfel getrokken moet worden, in ieder geval de realisatie daarvan binnen de gestelde termijn. Het heeft er in de praktijk echter alle schijn van dat de politiek de spreekwoordelijke huid verkocht heeft voordat de beer geschoten is. Verschillende gesprekspartners geven aan dat een deel van de verwachte bezuinigingen reeds merkbaar is. Op de werkvloer is minder menskracht beschikbaar en zijn functionarissen vervangen door goedkopere, lager opgeleide werknemers; in de beleving van sommige gesprekspartners.[135] Capaciteitsproblemen die hierdoor kunnen ontstaan, kunnen indirect een risico voor onafhankelijke oordeelsvorming in de vervolging opleveren. Als deze werkdruk resulteert in het kritiekloos en onnadenkend gebruiken[136] van 'het systeem', dan legt dat ook een extra druk op informatietechnische eisen aan het applicatielandschap. Als deze problemen onbeheersbaar worden en naar buiten toe zichtbaar worden, verwachten wij dat de burger een toename van bureaucratie in de strafrechtsketen ervaart. De maatschappij als geheel wordt dan geconfronteerd met een toename van het aantal procedurefouten.

In verband met het voldoen aan de wettelijke bescherming van persoonsgegevens kunnen een aantal opmerkingen gemaakt worden. Het startpunt daarvan is de reeds bij de beschrijving van het begrip privacy in het tweede hoofdstuk gedane vaststelling dat opslag van gegevens inherent een risico voor de privacy van daarin genoemde personen met zich meebrengt. Dit gevaar wordt navenant groter naarmate meer gegevens worden opgeslagen en verwerkt. Nu de omvang van gegevensopslag in de digitale wereld in abstracto groter lijkt dan die in de papieren wereld, en tevens nieuwe wijzen van het verwerken van persoonlijke data aan de orde zijn, kan worden gesteld dat het belang van dataprotectie in de komende tijd zal toenemen.

Een eerste potentieel probleem is gelegen in de beveiliging van gegevens. Uit de interviews komt daaromtrent een diffuus beeld naar voren. Allereerst onderkent men dat beveiliging in de digitale wereld kwetsbaar is. Daarmee is digitalisering

133. NRC 19 maart 2016. Vindplaats: https://www.nrc.nl/handelsblad/2016/03/19/bij-de-gewonemensenrechter-1600515 (laatst geraadpleegd 15 okt. 2016): '*Het hele proces van vervolging bij justitie is geautomatiseerd. Bij het parket 'kijkt daar vrijwel niemand meer inhoudelijk naar."*

134. De memorie van toelichting bij het wetsvoorstel digitale processtukken, en de bestudeerde beleidsstukken inzake VPS ondersteunen soms wel, soms niet duidelijk de verwachting ten aanzien van de kostenreductie. Zie in vergelijkbare zin het advies van de Raad van State bij het wetsvoorstel digitale processtukken: Kamerstukken II 2014/14, 34090, 4, p. 6-8.

135. Het onderhavige onderzoek strekt zich niet uit tot de personele gevolgen. Zie voor de consequenties van KEI op dit vlak *Begroting Veiligheid en Justitie 2017* in NJB 2016/33, p. 2419. Naar ons is verteld is het eerste administratieve personeel reeds ontslagen en staat een volgende reorganisatieronde in de steigers. Daar staat tegenover dat recent 35 miljoen euro extra geld is vrijgemaakt voor de rechtspraak, onder meer voor de financiering van digitalisering van procedures. Zie nader: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Jaarlijks-35-miljoen-extra-voor-Rechtspraak.aspx (laatst geraadpleegd op 15 okt, 2016).

136. Dit verschijnsel wordt ook wel 'vervreemding door automatisering' genoemd. Zie ook https://www.rathenau.nl/nl/publicatie/het-gaat-niet-om-technologie-het-gaat-om-ons (laatst geraadpleegd op 16 okt. 2016).

in beginsel een risico voor de privacy. Daarentegen zien sommige geïnterviewden ook dat de digitale wereld andere en wellicht betere mogelijkheden voor beveiliging biedt dan de papieren wereld die beperkt is tot sloten en kluizen.[137] In zoverre wordt dus ook een kans gezien voor versterking van de privacybescherming, zoals in de versleuteling van gegevens.

Een tweede opmerking in dit verband is gelegen in de gebrekkige kennis bij de geïnterviewden ten aanzien van hoe de beveiliging nu feitelijk werkt (en of er überhaupt wel beveiligd wordt). Eerder bij de behandeling van het legaliteitsbeginsel is al opgemerkt dat de indruk bestaat dat bestaande wetgeving ten aanzien van beveiliging wordt vereenzelvigd met het bestaan van (adequate) beveiliging. Het moge duidelijk zijn dat de wet in dit kader niet meer kan doen dan het creëren van een inspanningsverplichting voor betrokkenen om adequate beveiliging te verzorgen, maar dat dit het bestaan daarvan op geen enkele wijze praktisch ondersteunt. Deze denkwijze in combinatie met een gebrek aan ter zake doende (IT-)kennis bij betrokkenen levert in onze optiek een risico op.

Tot slot zij verwezen naar het eerder genoemde praktische probleem dat het mogelijk is geworden voor het OM om tussentijds losse stukken aan het dossier in GPS en het advocatenportaal toe te voegen. Enkele geïnterviewden gaven aan dat er enige vrees bestaat dat daardoor het overzicht over het dossier als geheel vermindert en de kans op fouten, en daarmee gevaren voor de privacy van betrokkenen, toeneemt omdat privacygevoelige informatie toch in verkeerde handen kan komen.

3.6.3 TOEGANG TOT DE RECHTER

Tot nu toe valt niet waar te nemen dat er beperkingen ten aanzien van de gang naar de rechter opgeworpen zijn door de digitalisering van de stukkenstroom. Een plausibele verklaring is dat het initiatief voor een strafproces bij het OM ligt. Deze instantie is volop betrokken in de initiatieven om digitaal procederen te testen. Kijken we naar het beginsel van toegang tot de rechter, dan moeten we dus kijken naar die delen van de strafvordering waar de verdediging wél het initiatief heeft. Naast hoger beroep, cassatie en herziening betreft dit het klagen over het niet vervolgen (art. 12 Sv), het beklag tegen inbeslagneming of voortduring van het beslag en aanverwante beklagprocedures zoals over de teruggave van het rijbewijs (art. 552a Sv; art. 164 lid 8 WVW), verzoeken om schadevergoeding voor ondergaan voorarrest (art. 89 Sv), verzoeken om vergoeding van de kosten van de verdediging (art. 591 en 591a Sv) enzovoort. Er zijn ons in deze verkenning geen gegevens onder ogen gekomen over de mate waarin dit type procedures voorkomt in standaardzaken. Theoretisch valt echter niet vol te houden dat er alleen maar sprake van kan zijn in maatwerkzaken. Echter, van experimenten met digitalisering in deze categorie van procedures is ons niets gebleken. De vraag in hoeverre de toegang tot de rechter in het geding komt voor mensen met beperkte digitale vaardigheden verdient onzes inziens meer aandacht. Een verplichting om voor een beklag/bezwaar/verzoek digitale instrumenten te gebruiken, op straffe van bijvoorbeeld niet-ontvankelijkheid, schendt dit beginsel voor digibeten.

137. De RvdR stelt in zijn advies bij het wetsvoorstel digitale processtukken (p. 2-3) echter dat uit het wetsvoorstel een wel erg groot optimisme blijkt ten aanzien van de beveiligingsmogelijkheden.

Hoger beroep, cassatie en herziening betreffen weliswaar de reguliere afdoening van een strafzaak (standaard dan wel maatwerk), maar het zijn momenten waarop het initiatief slechts in een minderheid van de gevallen bij het OM ligt. Toegang tot de hogere rechter vertoont in dit opzicht verwantschap met de hiervoor genoemde procedures op initiatief van de verdachte. Hierbij vereist het beginsel van toegang tot de rechter evengoed dat digitalisering geen belemmeringen mag opwerpen.

Verband houdend met het aanwenden van rechtsmiddelen, maar op zichzelf daartoe niet beperkt, is de vraag voor wiens rekening het komt wanneer stukken, bijvoorbeeld ten aanzien van het aanwenden van een rechtsmiddel, de geadresseerde niet of niet tijdig bereiken ten gevolge van een technische storing.[138] Noch de wet, noch de aanhangige ontwerp-regelgeving bevatten een duidelijke regeling hieromtrent. Niet ondenkbaar is dat wanneer de gevolgen daarvan niet worden geregeld dit in concrete gevallen kan leiden tot het de facto gesloten zijn van de toegangspoort tot de rechter, waarbij de rechter geroepen zal zijn te bepalen in wiens risicosfeer die storing ligt. [139] Het ligt in de lijn der verwachting dat wanneer de techniek die bij de autoriteiten in gebruik is het laat afweten, de justitiabele daarvoor niet het risico zal dragen.[140]

3.6.4 EQUALITY OF ARMS

OM en rechtspraak hebben voor het inzien en doorzoeken van dossiers beiden een aparte viewer ontwikkeld, respectievelijk DDV en DIVOS. Wanneer bedacht wordt dat beide systemen niet beschikbaar zijn voor de verdediging (of het slachtoffer) moet de vraag gesteld worden of de equality of arms in gevaar komt. Zowel de dossieropslag als de viewers zijn door de overheid (OM en rechtspraak) zelf ontwikkeld. Het lijkt mogelijk dat deze partijen daardoor zichzelf meer mogelijkheden kunnen toebedelen dan voor de verdediging beschikbaar zijn. Hierin schuilt een gevaar voor de equality of arms, dat overigens door de geïnterviewden grotendeels niet wordt onderkend of gedeeld.[141] De compensatie zou gezocht kunnen worden in het beschikbaar stellen van de technologie om te lezen en te bewerken, vergelijkbaar met de beschikbaarstelling destijds van het geautomatiseerde bos/polarissysteem. In dezelfde lijn ligt het mogelijk verplicht maken van de digitale vorm om stukken in te dienen. Wanneer dat kan, zoals nu, met relatief geringe aanvulling van de wijdverbreide kantoorsoftware, is vooral gemak te verwachten. Noodzaak tot grote investering aan de kant van de advocatuur zou een onjuiste drempel voor het voeren van de verdediging betekenen.

Onder de adequate faciliteiten moeten we nog even terugkomen op de toegang tot hoger beroep, cassatie en herziening. In de situatie dat digitaal procederen in eerste aanleg mee gaat brengen, dat ook het instellen van bijvoorbeeld hoger beroep slechts met een digitaal instrument mogelijk zal worden, is het even opletten. Personen die wettelijk gerechtigd zijn tot het gebruik van een rechtsmiddel, moeten daartoe binnen redelijke grenzen steeds toegang hebben. De

138. In vergelijkbare zin, zie het advies van de RvdR bij het wetsvoorstel digitale processtukken, p. 2 (bijlage bij: *Kamerstukken II* 2014/15, 34090, 3).

139. Ook de Raad van State signaleert de afwezigheid van een regeling omtrent termijnoverschrijding ten gevolge van technische storingen en adviseert de regering daar alsnog aandacht aan te besteden.. Zie: *Kamerstukken II* 2014/15, 34090, 4, p. 11-13.

140. Zie HR (civiele kamer) 19-02-2016, ECLI:NL:HR:2016:296

141. In algemene zin is dit risico al in 2007 door Van den Hoogen onderkend. In zoverre bestaat hier dus een discrepantie tussen de literatuur, de visie van de onderzoekers en hetgeen de praktijk laat zien. Zie Van den Hoogen 2007, p. 111.

overheid mag aan het instellen van dat rechtsmiddel eisen stellen net als overigens nu al gebruikelijk is. In de praktijk moet voor de justitiabelen die moeite met die eisen hebben, ondersteuning mogelijk zijn zonder dat zij kosten zouden moeten maken. De toegang tot de hogere rechter moet niet slechts *de jure* maar ook *de facto* open zijn naar de mate waarin de wet dat geeft.[142]

Dit klemt vooral bij hoger beroep en bij herziening. Bij cassatie geldt nu al een verplichting zich van een advocaat te bedienen. Die dienen sowieso meegenomen te worden in de digitalisering. We wijzen ter vergelijking nogmaals op de situatie in de aanpalende rechtsplegingen, waar juist de professionele actoren de verplichting tot digitaal procederen opgelegd gekregen hebben.

3.6.5 OPENBAARHEID

Openbaarheid is voorgeschreven in de Grondwet (artikel 121), in de Wet op de Rechterlijke Organisatie (artikelen 4 en 5) en in het Wetboek van Strafvordering (artikelen 269 en 362). Ook artikel 6 lid 1 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) en artikel 14 van het Internationaal Verdrag inzake Burgerrechten en Politieke rechten (IVBPR) behelzen een verplichting tot een openbare terechtzitting en een openbare uitspraak. Van Lent[143] baseert haar definitie van externe openbaarheid op dit samenstel van bepalingen en vermeldt daarbij dat de externe openbaarheid geldt in de fase van berechting en niet tijdens het voorbereidend onderzoek. Interne openbaarheid in het strafrecht gaat vooral over de toegang van de verdachte (en diens raadsman) tot de processtukken. Een gedeelde opslag van documenten wordt door de geïnterviewden veelal gezien als een versterking of kans voor de interne openbaarheid en de equality of arms. Juist door te delen beschikken alle betrokkenen vrijwel gelijktijdig over dezelfde stukken in dezelfde versies. Dit maakt het ook minder makkelijk voor bijvoorbeeld het OM om nodeloos lang 'op de stukken te blijven zitten'.[144] Daardoor is een gedeeld dossier ook een aanwinst voor het beginsel van détournement de pouvoir.

De digitale vorm maakt het tonen van de inhoud van een stuk met de gangbare apparatuur eenvoudig. Uit de bronnen is niet gebleken dat men met het projecteren van informatie in de zittingszaal afzonderlijk geëxperimenteerd heeft. Vrijwel alle geïnterviewden zien het digitale dossier als een kans, en een reeds deels gerealiseerde kans ook, voor de externe openbaarheid. Als alle partijen over hetzelfde dossier in digitale vorm beschikken, is het gemakkelijk om tijdens de zitting stukken gezamenlijk te bekijken en ook te tonen aan de overige aanwezigen.[145] Er worden echter ook kansen gemist. Doordat GPS niet in staat is om andere dan tekstuele media te verwerken, kan binnen het systeem nog niet gewerkt worden met bijvoorbeeld audio en video. Het ter zitting tonen van dit soort media moet dus nog altijd met behulp van usb-sticks, dvd's enzovoort geschieden, met alle mogelijke problemen van dien. Door gesprekspartners van

142. Ook in de toekomst zal de Helpende hand-rechtspraak leidend moeten zijn in een wereld met alleen nog digitaal verkeer tussen gerechtelijke autoriteiten en burgers. Zie Corstens/Borgers, p. 945/6. Dat brengt met zich mee, dat de autoriteiten gehouden zullen zijn tot goede voorlichting en assistentie in gevallen van dreigende tekortkomingen bij de aanwending van het rechtsmiddel.
143. Van Lent 2008.
144. Mits het OM niet onnodig lang op stukken blijft zitten. Daarover wordt in de praktijk wel regelmatig geklaagd. Ook hier lijkt dus nog een cultuuromslag nodig. Zie bijv.: P.P.J. van der Meij, 'De laatste duit in het zakje. Over waarheidsvinding in strafzaken en de beperkingen van de verdediging', in: *Strafblad* december 2014.
145. In vergelijkbare zin: M.E. van Wees, 'Modernisering en digitalisering van het strafproces', in: *DD* 2015, 72.

het OM wordt dit als een aanzienlijke belemmering ervaren nu in veel (en steeds meer) zaken, zoals bijvoorbeeld geweldpleging in het uitgaansleven, overvallen enzovoort, videobeelden regelmatig een belangrijke rol spelen bij de bewijsvoering. Een aantal geïnterviewden geeft dan ook aan dat GPS op dit gebied slagen zou moeten maken, maar vraagt zich tegelijkertijd ook af of dat binnen dit systeem wel tot de mogelijkheden behoort.

3.6.6 BETROUWBAARHEID / BEHOORLIJKHEID

In hoofdstuk 2 hebben wij betrouwbaarheid en behoorlijkheid geformuleerd als beginsel, vanwege de juistheid van gegevens en dus de kwaliteit van de informatievoorziening die hier in zicht komt. Over de betrouwbaarheid van de systemen en de daarin staande gegevens wordt binnen alle lagen van de strafrechtsketen nagedacht. Een probleem waarover onze gesprekspartners niets lijken te weten is hoe die betrouwbaarheid in de praktijk aan de systemen wordt gegarandeerd. De wet biedt aanknopingspunten voor de beveiliging van stukken, bijvoorbeeld door (momenteel in transitie verkerende) regelgeving omtrent de elektronische handtekening, maar ook door de Baseline Informatiebeveiliging Rijksdienst (BIR:2012). Uit onze interviews is het beeld ontstaan dat men vertrouwt op regelgeving en er dan maar van uitgaat dat het met de technologie wel goed zal komen.[146] Echter, geen der gesprekspartners kon duidelijk maken waarop dat vertrouwen is gebaseerd. Tegelijk weten we van bestaande systemen dat documentatie niet altijd volledig is, dat er sprake is van gegevensvervuiling en dat er voortdurend kritiek is op sommige systemen. Dus is het zinvol ons af te vragen of zulke informatiesystemen het beginsel van betrouwbaarheid in gevaar brengen. Voor inhoudelijke informatie lijkt het risico beperkt, omdat dossierstukken uitsluitsel geven over de werkelijkheid. Als systemen foute informatie verschaffen, kunnen we terugvallen op (al dan niet digitale) dossierstukken. Voor procedurele kennis geldt dit in mindere mate, omdat de administratie van de processgang niet per definitie met bewijsstukken is gedocumenteerd. Foute registratie of interpretatie van procedurele gegevens kan leiden tot procedurefouten. Als die niet tijdig opgemerkt worden, is het onderhavige beginsel van betrouwbaarheid/behoorlijkheid in het geding

In de literatuur wordt veelal uitgegaan van ofwel enkelvoudige opslag met meervoudig gebruik ofwel meervoudige opslag van elektronische stukken. De praktijk laat zien dat er sprake is van een hybride vorm daarvan. Er is vanwege de centrale positie van GPS sprake van enkelvoudige opslag van het gehele dossier. Er is echter geen sprake van meervoudig gebruik. In de praktijk worden door OM en de Rechtspraak verschillende viewers (DDV resp. DIVOS) gebruikt, waarbinnen de partijen werkkopieën beheren. Daarop vinden ook bewerkingen plaats. Daarom is de facto sprake van meervoudige opslag. Als deze bewerkingen zich zouden beperken tot annotaties, zou dit geen probleem zijn. Als partijen echter geen zekerheid hebben, dat zij in dezelfde versie van een document werken, is er een probleem met de equality of arms. De facto komt de opslag van elektronische stukken dus neer op meervoudige opslag, meervoudig gebruik.[147] Deze versnippering zou wel kunnen leiden tot een verminderd overzicht over zaakstukken. Dit brengt uiteraard veiligheidsrisico's met zich mee,

146. Zie bijvoorbeeld: Advies van het College van Procureurs-Generaal bij het wetsvoorstel digitale processtukken p. 4 (bijlage bij: Kamerstukken II 2014/15, 34090, 3); M.E. van Wees, 'Modernisering en digitalisering van het strafproces', in: *DD* 2015, 72.

147. Zie in dit verband het advies van de NOvA bij het wetsvoorstel digitale processtukken, p. 5 (bijlage bij: Kamerstukken II 2014/15, 34090, 3).

het gevaar van verlies of (al dan niet digitale) diefstal neemt toe en bij een eventueel 'lekken' van dossiers kan ook de privacy van personen die daarin worden genoemd in het geding zijn.
Een praktisch probleem waar men in GPS tegenaan liep is, dat bij elke wijziging in een documentversie een nieuwe versie werd aangemaakt waardoor op termijn een documentenchaos ontstond. Dit is opgevangen door functionaliteit in te bouwen die ervoor zorgt dat de gebruiker van GPS nu nog slechts een definitief document te zien krijgt. Waar in de tussentijd de verschillende gewijzigde versies zijn gebleven, is ons onduidelijk zodat het maar de vraag is of de voornoemde beginselen inderdaad gewaarborgd zijn of dat slechts sprake is van een optisch effect.

Tot slot vestigen wij de aandacht op het beheer, het onderhoud en de doorontwikkeling van GPS. Vanwege het feit dat GPS een, in IT-termen zeker, tamelijk oud systeem is, blijken er in de praktijk maar weinig specialisten (meer) te zijn die daarmee overweg kunnen. Deze specialisten zitten bovendien allemaal bij een beperkt aantal commerciële partijen.[148] GPS is daarmee vergaand afhankelijk van de kennis van die commerciële partij. Dit roept de vraag op of de overheid het systeem zelf voldoende 'in de hand' heeft en kan controleren. Hoe wordt bijvoorbeeld de beveiliging van het systeem gecontroleerd wanneer niemand binnen de overheid daar iets zinnigs over kan zeggen? Wat gaat men doen wanneer het systeem plotseling inderdaad structureel overbelast raakt en de beheerder niet thuis geeft? En, veel banaler, wat als de nu nog beschikbare specialisten besluiten er de brui aan te geven of de monopolist opeens de absolute hoofdprijs gaat vragen voor het beheer van een systeem dat essentieel is voor het functioneren van ons strafrecht? De afhankelijkheid van één enkele (markt) partij is bekend onder de term *vendor lock-in*. Dit is een risico.

3.6.7 TIJDIGHEID

Over de tijdigheid of snelheid kunnen we relatief kort zijn. De meeste respondenten zien de in beleidsstukken genoemde effectiviteitswinst niet of slechts gedeeltelijk terug. Daar staat tegenover dat de meeste respondenten wel enige vooruitgang zien en ook verwachten dat er slagen in de effectiviteit gemaakt zullen gaan worden. De termijn waarop dit te verwachten zal zijn loopt sterk uiteen met schattingen tussen de vijf en enkele tientallen jaren. Opvallend is dat de respondenten veelal aangeven ketenbrede samenwerking, in lijn met de conclusies van De Blok et al., te zien als gunstige voorwaarde voor het slagen van digitaliseringsprojecten,[149] terwijl tegelijkertijd het gebrek aan mogelijkheden tot samenwerking ook een remmende factor is. Daarbij is het doorgaans de andere partij die niet wil samenwerken.

3.7 Beantwoording van onderzoeksvragen 2 en 3

In de Nederlandse strafrechtsketen zijn de ontwikkelingen als gevolg van de ontwikkelingen in de IT samen te vatten als 'digitization'; een transitie van papie-

148. Iets dat overigens niet alleen voor GPS geldt, maar ook voor bijvoorbeeld INDIGO (zaakssysteem van het IND) dat wordt beheerd en doorontwikkeld door Cap Gemini. Zie nader: https://www.computable.nl/artikel/nieuws/wie-gunt-wat/5084183/3152533/ind-kiest-capgemini-voor-beheer-indigo.html (laatst geraadpleegd op 15 okt. 2016).

149. In vergelijkbare zin op rechtspraak.nl. Zie: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/De-zachte-kant-van-digitalisering.aspx (laatst geraadpleegd op 15 okt. 2016). In zoverre lijkt de uitvoerende praktijk te botsen met de uitgangspunten op papier.

ren naar elektronische documenten. Deze ontwikkeling is moeizaam verlopen, maar de ontwikkelingen bieden vertrouwen dat deze transitie over een aantal jaren voltooid zal zijn.

Een gedeeld dossier ondersteunt strafvorderlijke beginselen als interne openbaarheid, equality of arms, en zelfs legaliteit (door het vermijden van fouten in de strafvordering). Voor het overige verwachten wij weinig gevolgen voor de beginselen, omdat 'digitization' zich beperkt tot de transitie van papieren naar elektronische documenten. Van 'digitalization' verwachten wij ingrijpender gevolgen, maar het valt te betwijfelen of wij de komende vier jaren ontwikkelingen zullen kunnen waarnemen die zich als 'digitalization laten kwalificeren.'

Hoofdstuk 4

De strafvorderlijke beginselen en trends in IT

4.1 Inleiding

Hoofdstuk 3.6 benoemt kansen en risico's voor de relevante strafrechtelijke beginselen en beantwoordt daarmee de tweede en derde onderzoeksvragen over de huidige praktijk van de vervolging en berechting. Dit hoofdstuk komt tot een beantwoording van de vierde en vijfde onderzoeksvraag: Welke ontwikkelingen staan ons te wachten en hoe beïnvloeden die de genoemde beginselen? Geen mens kan de toekomst kennen. Maar, we kunnen er wel over redeneren en beredeneerde verwachtingen uitspreken over ontwikkelingen in de digitalisering van de strafrechtspleging. Dat doen we in dit hoofdstuk. We bespreken eerst een aantal ontwikkelingen en gaan vervolgens vanuit het perspectief van deze ontwikkelingen in op de strafvorderlijke beginselen, ontwikkeld in hoofdstuk 2 en op de recente praktijk toegepast in hoofdstuk 3.6.

4.2 Trends

Voor te verwachten ontwikkelingen kan men te rade gaan bij *trendwatchers*. Wat zij presenteren, geeft zicht op wat er aan technologische toepassingen net uitgevonden of te verwachten is. Dat is nog niet hetzelfde als de maatschappelijke aanvaarding of duurzaamheid van die toepassing. Nieuwe technologie is met name relevant voor de beleidsontwikkeling als zij een zekere duurzaamheid en schaalbaarheid vertoont. We hebben geprobeerd daarmee rekening te houden bij de te beschrijven ontwikkelingen.

Voor digitalisering in de maatschappij in brede zin heeft onderzoeksbureau Gartner in 2016 tien ontwikkelingen benoemd.[150] Bij elk daarvan hebben wij een aantal voorbeelden uit de strafrechtsketen en daarbuiten verzameld.

1. *Een weefsel van apparaten (device mesh)*

   Mensen worden omgeven door een uitdijend arsenaal aan apparaten, die (veelal draadloos) met elkaar verbonden zijn, zoals smartphone en tablet, maar ook apparaatjes die het klimaat in huis regelen, energiegebruik monitoren en ons sportieve gedrag vastleggen. Deze apparaten zijn in netwerken met elkaar verbonden.
   In de strafrechtsketen kennen we daar voorbeelden van. Vooral in de opsporing wordt een arsenaal aan signalerings-, detectie-, en opsporingsapparatuur en -software ingezet. In het detentie- en reclasseringsdeel kennen we bewaking op afstand en de enkelband, bewakingsapparatuur, enz. Bij OM en ZM zien we vooral generieke apparaten zoals smartphones en tablets. Criminelen gebruiken bijvoorbeeld wegwerptelefoons en versleutelde

150. http://www.gartner.com/newsroom/id/3143521 (laatst geraadpleegd op 15 okt. 2016).

telefoons voor anoniem converseren, skimmingapparatuur, CCTV-tapping apparatuur voor observatiedoeleinden[151].

2. *Alomvattende gebruikservaring (Ambient User Experience)*

   Mensen worden ondergedompeld in nieuwe gebruikservaringen, bijvoorbeeld app-gebaseerd (bijv. Parkmobile, Google Maps), augmented reality (bijv. bij medische operaties, simulaties, head-up displays), virtual reality (bijv. training, gaming).
   In het strafrecht zien we vooral experimenten, zoals een Europees gefinancierde proef in Staffordshire (UK) om juryleden via virtual reality het plaats delict te laten bezoeken.[152] In Zürich hebben wetenschappers misdaden gereconstrueerd in virtual reality. In Nederland is sprake van virtual reality behandelingen voor zedendelinquenten.
   Ook voor criminelen kan bijvoorbeeld augmented reality (Google Glass) nuttig zijn voor het voorbereiden van een inbraak.

3. *Informatie over alles*

   De diversiteit van informatie, die mensen krijgen, en de mogelijkheden om die informatie te verrijken, ermee te redeneren en te combineren neemt in snel tempo toe. Nu al is het heel gewoon om combinaties van reis, verblijf en uitstapjes in één transactie te boeken. Terwijl we een maatwerkkeuken samenstellen, combineren we ongemerkt gegevens uit magazijnen met actuele gegevens van toeleveranciers. Datzelfde, maar complexer, gebeurt bijvoorbeeld in havenplanningssystemen, voorspellende remote-sensing-systemen en vele andere (zichtbare en minder zichtbare) toepassingen die anno 2016 onze maatschappij draaiend houden.
   Ook binnen de strafrechtsketen, en dan met name in de opsporing, zien we dit verschijnsel opkomen onder noemers als big data en data analytics. Uiteraard vindt dit niet plaats in de volle openbaarheid, maar wij gaan ervan uit dat de opsporing beschikt over geavanceerde middelen voor digitaal rechercheren. De vernieuwing op dit moment zit vooral in de mogelijkheden om meerdere gegevensverzamelingen te combineren.[153] Bijvoorbeeld kan het combineren van Facebook-gegevens met gegevens uit leerlingvolgsystemen in een kinderporno-onderzoek net het verschil maken om het slachtoffernetwerk in beeld te krijgen. De complexiteit van dit soort rechercheerwerk komt voort uit de diversiteit van bronnen. Om vast te kunnen stellen of de oogst daaruit juridisch bruikbare feiten bevat, gaat de opsporing behoefte krijgen aan wiskundig geschoolde gegevensanalisten.
   In het criminele circuit bestaan weinig ethische regels om de stortvloed van openbaar beschikbare informatie te combineren. Er mag dan ook verwacht worden dat criminelen de resultaten van data-analyse zullen gebruiken voor bijvoorbeeld het selecteren van overvaldoelen, het afpersen van mensen, en het rekruteren van leden.[154]

151. J. Verhoef, R. Hiemstra en A. Cachet, 'Politie, ICT en toekomstvisie', in: *Tijdschrift voor de Politie,* 75 (4), 2013, pp. 6-10, hebben het over het verlies van een voorsprong.
152. http://www.staffs.ac.uk/news/prestigious-grant-award-for-virtual-crime-scene-research-tcm4290882.jsp?utm_source=Homepage&utm_medium=Tabs&utm_campaign=Homepage%20Tabs (laatst bezocht 30-11-2016).
153. Zie voor een voorbeeld ten behoeve van politiesurveillance http://www.sciencemag.org/news/2016/09/can-predictive-policing-prevent-crime-it-happens (laatst geraadpleegd op 15 okt. 2016).
154. Rutger Leukfeldt, *Cybercriminal networks. Origin, growth and criminal capabilities*, diss. OU 2016, laat zien dat onlinecontacten

4. *Zelflerende technologie*

Om de explosie van gegevens en gegevensbronnen bij te houden, zijn meer gegevensanalisten nodig dan opleidingen kunnen leveren. Zelflerende machines bieden uitkomst. Onderzoek van gegevens wordt daarmee steeds meer geautomatiseerd. Neurale netwerken en genetische algoritmen zijn voorbeelden van zelflerende technologie, die worden ingezet om gegevens uit 'de wereld' te exploreren en analyseren. Het inzetten van 'the crowd'[155] wordt ook steeds vaker toegepast voor complexe en arbeidsintensieve vraagstukken, zowel voor gegevensverzameling als voor het in een netwerk uitvoeren van complexe databewerkingen (zie ook hierna onder 8). Zo heeft bijvoorbeeld de firma Niantic (eigendom van Google) opvallende locaties en ontmoetingspunten wereldwijd in kaart gebracht door spelers al wandelend op pad te sturen met het succesvolle (gratis) spel 'Ingress'. Daarmee heeft Google Maps de kaartinformatie voor wandelaars verkregen, wat nu (wederom door Niantic) in het spelletje 'Pokémon-Go' te gelde wordt gemaakt.
In de strafrechtsketen zien we ook een toenemende inzet van zelflerende technologie. Het Criminaliteits Anticipatie Systeem (CAS) gebruikt bijvoorbeeld neuralenetwerktechnologie voor predictive policing.[156,] Ook word 'the crowd' ingezet, bijvoorbeeld in Amber-alerts[157] en buurt-whatsapps.[158] In de rechtspraak zijn daarvan nog geen voorbeelden aangetroffen, ofschoon ook daar mogelijkheden liggen. Zo pleit bijvoorbeeld hoogleraar Marc Hertogh al enige tijd voor het inzetten van 'the crowd' in de rechtspraak om de betrokkenheid van het publiek bij de rechtspraak te verbeteren.[159]
Voor criminelen is deze technologie ook interessant. Zij kunnen er kwetsbaarheden mee opsporen en kansrijke doelwitten aanwijzen.

5. *Autonome technologie*

Robots, autonome voertuigen, een koelkast die zelf op tijd een vers pak melk bestelt; het zijn enkele van vele in het oog springende voorbeelden van autonome technologie. Ook softwareassistenten zoals Google Now, Microsoft's Cortana en Apple's Siri vallen hieronder. Van die laatste categorie verwacht Gartner in de nabije toekomst veel maatschappelijke verandering.
In de strafrechtsketen zijn ook voorbeelden te vinden van autonome technologie. Het opsporen van synthetische drugs, wat drugshonden niet lukt, kan wel met een 'autonome neus' (eNose).[160] In de rechtspraak wordt nog geen geloof gehecht aan een rechter op basis van autonome technologie.[161] Het dichtst bij autonome softwareassistenten in de strafrechtsketen komt de boetepraktijk rondom verkeersovertredingen, onverzekerd rijden en nietnaleving van de APK-plicht. Die hebben we genoemd in hoofdstuk 2 en daar

belangrijk zijn naast realliferelaties.

155. Mamykina et. al., 'Learning From the Crowd: Observational Learning in Crowdsourcing Communities', in: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ACM 2016, New York, NY, USA, pp. 2635-2644.
156. Dick Willems, 'Predictive Policing — wens of werkelijkheid?', in: *Tijdschrift voor de Politie,* jrg.76/nr.4/5/14, pp. 39-42. In iets genuanceerdere zin zie: A.R. Lodder & M.B. Schuilenburg, 'Politie web-crawling en predictive policing', in: *Computerrecht* 2016, 81.
157. http://www.amberalert.nl/ (laatst geraadpleegd op 16 okt. 2016).
158. http://wabp.nl/ (laatst geraadpleegd op 16 okt. 2016).
159. http://rechtennieuws.nl/42277 (laatst geraadpleegd op 16 okt. 2016).
160. https://beveiligingnieuws.nl/nieuws/politie-wil-drugshonden-robots-vervangen, 15 sept 2016 (laatst geraadpleegd op 15. okt. 2016).
161. Maarten Feteris, 'Komt het ooit tot robotrechters?', in: *Rechtspraak*, Magazine van de Raad voor de rechtspraak, juni 2016, p. 7.

hebben we laten zien, dat juridisch de autonomie (nog) niet aanvaard wordt. In de criminaliteit vinden autonome systemen evengoed hun toepassing. Drones om bendeoorlogen te beslechten, inbraakrobots, bewaking en besturing van hennepplantages zijn voor de hand liggende voorbeelden.

6. *Adaptieve veiligheid*

Mensen willen elke dag veilig zijn, terwijl de wereld snel verandert en dat strekt zich uit tot hun persoonlijke data. Het klassieke veiligheidsdenken gaat uit van het afsluiten van toegang tot gegevens en tot functionaliteiten. In zogenaamde 'security perimeters' wordt een 'digitaal hekwerk' om het te beveiligen object opgetrokken, zodat de toegang tot de inhoud kan worden gecontroleerd en beperkt tot mensen met de juiste autorisatie. Gartner stelt dat deze denkwijze niet langer voldoet, omdat het aantal en de diversiteit van de te beveiligen objecten het onmogelijk maken om alles met vooraf bedachte veiligheidsregels adequaat te organiseren. Veiligheidsmaatregelen moeten zich dynamisch aanpassen aan de situatie van het moment. Daarom hanteert Gartner de aanduiding 'adaptief'.
Voor de strafrechtsketen betekent deze ontwikkeling dat de aandacht in toenemende mate uitgaat naar preventieve veiligheid en dreigingsanalyse. Met het toenemend aantal datalekken[162] wordt duidelijk dat ook zelfbescherming en gedragsbeïnvloeding nodig zijn om informatie te beveiligen.
De toepassing van dezelfde veiligheidstechnologie in de criminaliteit ligt voor de hand vanwege het belang van criminelen om onzichtbaar te opereren.

7. *Geavanceerde systeemarchitectuur*

In de grote datacenters van tegenwoordig is rekenkracht en opslagcapaciteit vrijwel ongelimiteerd beschikbaar. Zelfs in consumentencomputers is het al tien jaar normaal om meerdere processoren op één chip aan te treffen. Nieuwe systeemarchitecturen laten computers meer werken zoals het menselijke brein. Dit maakt niet-algoritmische software mogelijk, zoals associerende en lerende systemen. Ook maakt het zelfs de kleinste apparatuur steeds slimmer.
Voor de strafrechtsketen biedt dit mogelijkheden, bijvoorbeeld om beslissingsondersteuning te faciliteren, maar het gebruik daarvan is in de onderhavige verkenning niet aangetroffen.

8. *Weefselarchitecturen (Mesh App and Service Architecture)*

De klassieke softwarearchitectuur bestaat uit drie lagen: een gegevenslaag, een applicatielaag en een businesslaag. Deze drielaagsarchitectuur diversifieert. Door virtualisatie van hardware kunnen op elk willekeurig moment computers en opslagstructuren worden bij- of afgeschakeld. Softwareagents, die autonoom hun werk verrichten, kunnen vrijelijk door het internet reizen en op willekeurige plekken hun werk doen. Door samen te werken in een zogenaamd 'botnet' leveren zulke agents rekenintensieve diensten, waarbij de performance op robuuste wijze kan worden gegarandeerd. Voor de uitvoering van omvangrijke bewerkingen doet de concrete beschikbaarheid van apparatuur op een bepaalde plaats er in beginsel niet meer toe.

162. Symantec, Internet Security Threat Report, vol. 21, april 2016.

Het slim op zoek gaan naar bewerkingscapaciteit elders is ingebouwd in het programma.
Voor het strafrecht kunnen dergelijke systemen een wapen zijn in de strijd tegen de georganiseerde misdaad.[163] Maar ook voor cybermisdaad en spionagedoeleinden bieden botnets volop kansen. Van dat laatste zijn voldoende voorbeelden voorhanden: afpersing met behulp van ransomware, DDOS-aanvallen die servers verlammen, trojaanse paarden om heimelijk gebruik te maken van andermans rekenkracht, enzovoort.
Om de kansen en bedreigingen, die van deze 'weefsels van agents' uitgaan, het hoofd te bieden is veel multidisciplinaire kennis vereist,[164] die het karakter van de strafrechtsketen blijvend gaat veranderen.
Criminele toepassingen zijn momenteel wijd verbreid. Ransomware en DDos-aanvallen zijn bekende voorbeelden van weefsels van agents.

9. *Internet-of-things (IoT-)platformen*

Apparaten zoals smartwatches, domotica, beveiligingsapparatuur, remote sensing worden pas echt waardevol als zij in groter verband samenwerken. IoT-applicaties zoals waterhoogtebewaking in de Rijn, het monitoren van toegang voor bewoners in een verpleeghuis, of het bijhouden van de actuele plaats en status van vrachtauto's zijn voorbeelden daarvan. Omdat het maken van dit soort applicaties sterk groeit, voorziet Gartner dat met name de platformen voor IoT-applicaties sterk groeien.
Voor de strafrechtsketen betekent dit dat het experimenteren, zoals met enkelbandbewaking, eenvoudiger en goedkoper wordt. Het maken van dit soort applicaties is specialistisch werk. Daarom ligt het voor de hand dat de effecten van deze trend via softwareleveranciers in de strafrechtsketen komen.
Met het kleiner en robuuster worden van internetverbonden toepassingen valt te verwachten dat IoT-platformen ook bij criminelen aftrek zullen vinden. Voor hen is nu al het hacken van auto's, waterkeringen en dergelijke 'going concern'.

In dit brede scala van ontwikkelingen is weinig structuur te ontwaren. Uiteraard is Gartner een gezaghebbende trendwatcher, maar de lijstjes van trends en ontwikkelingen van verschillende trendwatchers lopen nogal uiteen. Wij volstaan dan ook met de door Gartner ingegeven opsomming, waarvan wij overigens het fenomeen 3D printen in onze bespreking overgeslagen hebben. Criminele toepassingen daarvan zijn licht te bedenken, maar de relevantie voor de door ons bestudeerde fasen in de strafrechtspleging zien we op dit moment niet. We kunnen vaststellen dat zelfs het lijstje van Gartner omissies bevat. Het verschijnsel blockchain ontbreekt bijvoorbeeld in deze lijst[165]. Wel constateren wij dat de genoemde ontwikkelingen in de informatieverzameling (datacollectie met behulp van allerhande devices, datamining) zich het meest nadrukkelijk aandienen ten behoeve van de opsporingsfase en in de openbare veiligheid. Het is echter niet de opsporingsfase, waar deze verkenning over gaat.

163. M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht' Preadvies voor de Jaarvergadering van de Nederlandse Juristenvereniging, 10 juni 2016 te Haarlem, Handelingen NJV, 146e jaargang/2016-1, Deventer: Wolters Kluwer 2016, p. 137-240.
164. Kees Homan, 'Oorlogvoering in de digitale ruimte', in: *Internationale Spectator*, jrg. 66, pp. 84-87, febr. 2012.
165. Een blockchain is in essentie een veilige manier om transacties zonder tussenpersoon (zoals een bank of notaris) uit te voeren. Bitcoin is daarvan slechts één verschijningsvorm, maar blockchains worden bijvoorbeeld ook gebruikt in moderne versiemanagementsystemen en bij overdracht van eigendommen. Zie Anka Ernes, *Eigendom in de virtuele dimensie*, https://www.ou.nl/web/rechtswetenschappen/webcolumn-RW (laatst geraadpleegd 30-11-2016) met verdere verwijzingen.

De vierde onderzoeksvraag ziet op it-ontwikkelingen die relevant worden voor de strafvorderlijke beginselen in de komende vijf jaar. In elk van de volgende secties bespreken wij een strafvorderlijk beginsel, maar nu vanuit een toekomstperspectief.

4.3 De beginselen

4.3.1 LEGALITEIT

Zolang er sprake is van *digitization*, ofwel de overgang van papieren naar elektronische documenten, zijn de gevolgen voor het legaliteitsbeginsel beperkt. De structuur van het strafvorderlijke proces verandert immers niet wezenlijk. Die conclusie is in hoofdstuk 3.7 al getrokken. Van *digitalization* is sprake als het strafproces in procedurele zin verandert door de mogelijkheden van digitalisering te benutten[166]. In dat geval is legaliteit geenszins vanzelfsprekend. Zo biedt de toepassing van zaaksystemen en digitale meetinstrumenten nieuwe mogelijkheden voor herinrichting van het strafvorderlijk proces. Dit heeft in het verleden geleid tot versnellingsprojecten zoals 'Fast Lanes', 'Verkeerstoren plus', 'Snelrechtplus', 'Voorsorteren' en 'ZSMHoven'.

De door Gartner gesignaleerde trend van zelflerende en autonome technologie zien we terug in de strafrechtsketen. Er is een groeiende belangstelling voor regelbeheersing, kennistechnologie en kunstmatige intelligentie. Informatiesystemen worden steeds vaker op basis van juridische regels ontworpen, gemotiveerd vanuit het legaliteitsbeginsel. In lijn met wat in hoofdstuk 2 beschreven staat, valt dat toe te juichen. Echter, een gebrekkige en soms mislukkende realisatie bedreigt diezelfde legaliteit. De huidige software-praktijk biedt weinig geruststelling, omdat naleving van juridische regels niet in het ontwerp wordt gegarandeerd. De redenering dat het gebruik van regelsystemen leidt tot betere naleving bevat een klassieke redeneerfout: het verwart noodzakelijke met voldoende voorwaarden. De combinatie van een leverancier die een regelsysteem aanbiedt en zich laat voorstaan op legal compliance, en een afnemer die de deskundigheid mist om onder de motorkap te kijken, is eerder regel dan uitzondering. Daarom bepleiten wij een kritische houding over de toepassing van regelbeheersing, kennistechnologie en kunstmatige intelligentie. De moeilijkheden, die overheidsorganisaties (zoals IND, Belastingdienst, DUO) in de praktijk hebben ondervonden met regelbeheersing, onderstrepen dat hieraan niet licht getild mag worden.

Hoopvol voor de legaliteit zijn ontwikkelingen in het regelgebaseerd ontwerpen[167], waarbij juridische regels al in de ontwerpfase worden toegepast en de resulterende software toetsbaar aan deze regels voldoet. Regelgebaseerd ontwerpen kan gezien worden als automatisering van de automatisering. Door juridische regels op de juiste wijze te coderen kunnen zij fungeren als invoer voor geautomatiseerde softwaregeneratoren. Dat levert niet alleen correcte software op, maar ook ingebouwde naleving van de regels die zijn ingevoerd.

Hoopgevend is ook wat we kunnen zien bij organisaties die grootschalige IT zowel dynamisch veranderen als betrouwbaar in bedrijf houden. Voorbeelden daarvan zijn er legio, zoals Booking.com, Netflix, Bol.com en Amazon.com;

166. Verslag Conferentie 'Strafrechtsketen Versterkt en Versnelt', 13 december 2012, Utrecht.
167. S. Joosten, L. Wedemeijer en J. van der Woude: Rule Based Design, Open Universiteit, 2013. Zie ook http://portal.ou.nl/web/rule-based-design.

internationale internetbedrijven die alleen dankzij de hoge kwaliteit van hun IT kunnen bestaan. Wij verwachten dat de overheid in de nabije toekomst steeds vaker hun softwarekwaliteit, hun flexibiliteit en hun kostenstructuur als norm zal hanteren. Daarvoor is wel een inhaalslag nodig in het voortbrengingsproces van IT-vernieuwingen.

4.3.2 TOEGANG TOT DE ONAFHANKELIJKE RECHTER

Dit beginsel heeft een aspect van toegang en een aspect van onafhankelijkheid. In hoofdstuk 3.6 is betoogd dat het aspect van toegang vooral de afwezigheid van obstakels betreft. Digitalisering werpt op zichzelf al obstakels op voor personen die slecht meekomen in de informatiemaatschappij. Om de toegang te garanderen zal de strafrechtsketen oog moeten houden op niet-digitale toegang. Uit onze gesprekken is gebleken dat hier wel degelijk aandacht voor is. Echter, een strafrechtadvocaat vertelde ons ook dat de toegang tot het digitale strafdossier voor de verdachte zelf nog niet soepel verloopt. We hebben geen redenen gevonden om aan te nemen dat de digitalisering in de praktijk vrij is van obstakels die de toegang beperken.

Het aspect van onafhankelijkheid kan in het geding komen naarmate computers slimmere taken krijgen. Het voorbeeld uit hoofdstuk 2.1 van Bos/Polaris, waar een magistraat zich verschool achter een door de computer afgegeven richtlijn, illustreert dit risico. Een boeiende ontwikkeling in dit verband vormen de zogenaamde argument assistance systems[168] (AAS), die het juridisch redeneren ondersteunen. Dergelijke software ondersteunt juridische professionals bij het construeren van een redenering. Doel daarvan is te komen tot een deugdelijke belangenafweging en motivering op basis van de materiële waarheid. De ideeën hierover bestaan al sinds de vorige eeuw, maar het doorbreken van kunstmatige intelligentie en kennistechnologie op grote schaal maakt het waarschijnlijk dat argument assistance systems ook in het recht zullen doorbreken. In een optimistisch scenario leidt deze ontwikkeling tot een verbetering van de kwaliteit van pleitnota's en uitspraken. In een pessimistisch scenario kan het leiden tot het kritiekloos volgen van een computer en het bijbehorende bureaucratisch gedrag[169]. De verleiding om een advies van een computer kritiekloos te volgen, groeit onder hoge werkdruk. Die verleiding groeit ook naarmate computers meer en betere adviezen geven. Omdat deze ontwikkeling zowel positief als negatief kan uitpakken, is het verstandig om vanuit de strafrechtsketen proactief te zijn. Dit kan bijvoorbeeld door wetenschappelijk onderzoek naar argument assistance systems te initiëren of daaraan deel te nemen.

4.3.3 EQUALITY OF ARMS

In het licht van deze studie is het beginsel 'equality of arms' geïnterpreteerd in de richting van een gelijke informatiepositie. Niet alleen het verschaffen van dezelfde dossierstukken op hetzelfde moment, maar ook het beschikken over vergelijkbare functionaliteit en gelijkheid in kwalitatieve zin horen daarbij. Daarmee raakt equality of arms aan andere beginselen, zoals interne openbaarheid en adequate facilities. Tijdens ons onderzoek deed zich de vraag voor of een viewer op documenten, zoals DIVOS, niet ook aan de verdediging ter beschikking moet worden gesteld. Het antwoord van de gesprekspartners was negatief:

168. Bart Verheij, Automated Argument Assistance for Lawyers, proceedings ICAIL-99, Oslo, pp. 43-52.
169. Vergelijkbaar met wat in hoofdstuk 2 over Bos/Polaris werd gesignaleerd.

de verdediging kan best zorgen voor haar eigen voorzieningen om digitale documenten te bekijken.

Dit wordt echter anders wanneer digitalisering verder gaat dan de transformatie van papieren naar elektronische dossiers. Als het OM bijvoorbeeld een misdrijf reconstrueert in een kostbare virtual-reality (VR) techniek met grote psychologische overtuigingskracht, moet de rechter dan de verdediging faciliteren met vergelijkbare middelen of moet de verdediging zich maar behelpen met een schriftelijke redenering op geduldig papier? En kan de verdediging dan aanvoeren dat de VR-reconstructie niet toelaatbaar is, omdat de verdediging geen vergelijkbare faciliteiten voor haar contra-reconstructie kan betalen?

De hiervoor genoemde argument assistance systems (AAS) zijn een voorbeeld van een technologie die het gelijke speelveld kan beïnvloeden. De partij met de betere argument assistant heeft een voorsprong op de tegenpartij. Het is voorstelbaar dat AAS-technologie in de praktijk een groot kwaliteitsverschil in het juridisch redeneren zal maken. In dat geval mogen we verwachten dat een werkelijk onderscheidende juridische AAS alleen weggelegd is voor grote advocatenkantoren, die meer kunnen investeren in technologie, maar die in het huidige beeld niet het leeuwendeel van de strafzaken onder hun hoede hebben Als slechts één der partijen hierover beschikt, is het alsof een duel met sabel tegenover machinegeweer plaatsvindt. Dat levert een mogelijke bedreiging op van het beginsel van equality of arms.

Het onderhavige beginsel is ook van betekenis wanneer het generen van verdenking of bewijs plaatsvindt met behulp van Big Data toepassingen. In het bijzonder de navolgbaarheid van de algoritmes die de uitkomst van deze toepassingen zo sterk bepalen, kan opgeworpen worden als een eis vanuit de transparantie voor de verdediging. Die transparantie valt echter niet eenvoudig te realiseren wanneer die algoritmes zeer complex zijn en/of voorwerp van intellectuele eigendom. Een kritische blik door een deskundige van de verdediging mogelijk maken wordt dan in de praktijk lastig.

Voor het beginsel van equality of arms is onze conclusie dat ontwikkelingen in de IT wel degelijk consequenties kunnen hebben. Vanwege de diversiteit van IT-ontwikkelingen zal toekomstige jurisprudentie hierin richting moeten geven vanuit een regulatief kader in de strafvorderlijke regeling. Niet elke technologische nieuwigheid kan immers voorwerp worden van actie van de wetgever, maar de omschrijving en bewaking van (de doorwerking van) het onderhavige beginsel hoort ook in de wet onmiskenbaar te zijn vastgelegd. Nu hebben we een optelsom van concrete wettelijke bepalingen en een verdragsrechtelijke garantie uitgewerkt in rechtspraak. Het kan ook - in het kader van actualisatie - dat de actuele stand geabsorbeerd wordt in een speciale paragraaf over de verdediging, die een expliciete waarborg en uitwerkingen bevat. Wat de keuze moet zijn, hangt af van de gekozen legaliteitsopvatting, hetgeen verder buiten het bestek van dit rapport valt. In elke stand van de wetgeving zal de jurisprudentie in concrete gevallen moeten voorzien en daarmee het beginsel verder ontwikkelen.

4.3.4 OPENBAARHEID

De externe openbaarheid is momenteel ingevuld door het publiceren van de voornaamste uitspraken op rechtspraak.nl. In hoofdstuk 3 is opgemerkt dat de zaaksystemen van de rechtspraak nog geen voorzieningen voor audio en video hebben. Echter, de ontwikkeling van niet-tekstuele media, zoals audio, video,

virtual reality, augmented reality en dergelijke, dienen zich ook aan in de strafrechtsketen. Te verwachten is dat de externe openbaarheid grotendeels via het internet verder gestalte zal krijgen. Wanneer de behoefte aan andere dan tekstuele openbaarheid zich aandient, kan de strafrechtsketen langs digitale weg in die behoefte voorzien.

Ten aanzien van de procedurele gegevens[170] is de externe openbaarheid nog heel beperkt. Procesinformatie en -verantwoording beperken zich tot jaarverslagen, zittingsagenda's, rechtbankreglementen en wat dies meer zij. Maar van systematische openbaarmaking van de procesgang, zoals dat bij uitspraken wel het geval is, is nog geen sprake. Rechterlijke uitspraken zijn openbaar en worden vaak via internet beschikbaar gesteld. In welke fase een zaak zich bevindt voordat de openbare behandeling plaatsvindt of voordat de uitspraak onherroepelijk is, wordt niet publiek bekendgemaakt. Procedurele gegevens komen slechts naar buiten op basis van WOB-verzoeken. Omdat externe openbaarmaking gericht is op professioneel geïnteresseerden, is de vraag aan de orde welke professionals hieraan behoefte hebben. Of de Wet Openbaarheid Bestuur voldoende is om aan dit beginsel tegemoet te komen is door ons niet onderzocht. Maar aanwijzingen van het tegendeel zijn ook niet aangetroffen.

4.3.5 BETROUWBAARHEID / BEHOORLIJKHEID

In hoofdstuk 3 zagen we dat gegevens in de strafrechtsketen niet altijd gedeeld worden, maar dat ketenpartners zelf kopieën onderhouden van justitiële en strafvorderlijke gegevens. Dit levert een risico op dat partijen niet beschikken over dezelfde gegevens dan wel dezelfde versie van gegevens. Beoordelingsfouten, die het gevolg kunnen zijn van incorrecte gegevens, schaden de betrouwbaarheid en behoorlijkheid in de strafvordering. Over de omvang van dit fenomeen en de gevolgen ervan in de maatschappij is weinig bekend. Over de kwaliteit van gegevens in de strafrechtsketen bestaan wel twijfels, maar harde kennis hierover ontbreekt. Dit onderwerp, dat wij aanduiden als 'gegevenshygiëne', heeft niet de aandacht die noodzakelijk is voor een betrouwbare en behoorlijke strafvordering. Ontwikkelingen en trends, zoals bijvoorbeeld marktonderzoeker Gartner die meldt, gaan over nieuwe hardware- en softwarefunctionaliteit, maar niet over gegevenshygiëne. Vanuit de markt mogen we dan ook op afzienbare termijn geen oplossingen verwachten, die gericht zijn op het vergroten van de betrouwbaarheid en behoorlijkheid in de strafrechtsketen.

Naast gegevenshygiëne is er nog een bron van risico's voor het beginsel van een betrouwbare en behoorlijke strafrechtspleging. Voor het correct en tijdig naleven van regels wordt veelal naar zaaksystemen gekeken. Uitgerekend dit soort toepassingen kost veel geld en moeite om te implementeren. De thans in gebruik zijnde zaaksystemen (bijv. GPS, Compas, ReIS), beperken zich veelal tot registratieve functionaliteit, ofschoon de ambitie bij aanschaf van die systemen veel hoger lag. Een positief effect van deze systemen op efficiency en foutkansen is door ons niet waargenomen. Als de kwaliteit (zoals de betrouwbaarheid, integriteit, juistheid, authenticiteit) van gegevens in genoemde systemen wordt betwijfeld, is de betrouwbaarheid van de strafrechtspleging in het geding.

170. Onder procedurele gegevens wordt verstaan gegevens die ten behoeve van correcte uitvoering van een strafproces worden verwerkt. Het gaat hier dus niet om strafvorderlijke gegevens in de zin van de WJSG. Dat zijn persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg verwerkt (Art. 1 sub b WJSG).

Opmerkelijk is dit alles wel, omdat er veel technologie bestaat om dit op te lossen: NoSQL-databases voor grootschalige semantische gegevensopslag zijn bruikbaar om de kwaliteit van de gegevenshuishouding te verbeteren en toetsbaar te maken. Geautomatiseerde ontwikkelstraten voor beheersbare en snelle voortbrenging van software kunnen zorgen dat projecten kleiner worden en beheersbaar verlopen. Formele technieken kunnen correctheid ondersteunen en garanties voor naleving van wet- en regelgeving bieden. Een verklaring van het werken met kostbare, verouderde technologie kan wellicht gevonden worden in een kennisachterstand. Er is echter meer aan de hand. In onze gesprekken viel ook te beluisteren dat de wil tot samenwerken tussen ketenpartners niet altijd voldoende is om te komen tot effectieve ketenoplossing.

In het kader van betrouwbaarheid wijzen wij nogmaals op de kansen van argument assistance systems. Door de kwaliteit van het juridisch redeneren te vergroten, biedt dit soort technologie veel kansen voor betrouwbare strafrechtspleging en kan zij daarmee het grotere geheel van strafrechtelijke beginselen dienen. Niettemin is oplettendheid geboden, omdat dit type systemen een schijn van neutraliteit en gezag mee kunnen brengen die niet zonder meer aanvaard hoeft te worden. Wanneer bijvoorbeeld de huidige wijze van ondersteuning van de straftoemeting door rapportage over het toekomstig recidiverisico geautomatiseerd zou worden, moeten de kritische vragen die de rechter en de procespartijen bij zo een rapport kunnen hebben, nog steeds gesteld kunnen worden.[171]

4.3.6 TIJDIGHEID

Het verkorten van doorlooptijden in de strafrechtsketen is begin 2010 benoemd als een ketenomvattende prioriteit van het ministerie van Justitie. Deze doelstelling is vervolgens opgenomen in het programma Herontwerp Keten Strafrechtelijke Handhaving[172]. In hoofdstuk 3 hebben wij reeds vastgesteld dat onze gesprekspartners geen verbetering op dit gebied hebben ervaren. Desalniettemin blijft er hoop dat digitalisering dit doel kan realiseren. De genoemde studie geeft een aantal oorzaken.

- Er wordt gewezen op een gebrek aan aansluiting van de registratiesystemen van ketenpartners: ‘Sommige ketenpartners gebruiken in verschillende geografische gebieden verschillende registratiesystemen. Ook registreren verschillende ketenpartners op basis van andere registratie-eenheden (zaken, personen, delicten, enz.), of ontbreekt er een identificerend kenmerk op basis waarvan personen en/of zaken gevolgd kunnen worden door de keten.’
- In genoemd onderzoek is door ketenpartners gewezen op mogelijke problemen met de betrouwbaarheid van de data. Het kan hier gaan om ontbrekende parketnummers, waardoor de koppeling moeilijk tot stand te brengen is, of registratiefouten bij de invoer van datumvelden.
- Er wordt gewezen op procedurele oorzaken, zoals verplichte wachttijden, betaaltermijnen (voor transacties), en overdracht tussen verschillende organen in de strafrechtsketen.

Vanuit de logistieke theorie[173] is bekend dat de verhouding tussen doorlooptijd en bewerkingstijd per zaak overwegend uit wachttijd bestaat. Dat geldt niet

171. Zie over een geautomatiseerde risicorapportage in de V.S. https://www.propublica.org/article/machine-bias-risk-assessment-in-criminal-sentencing (laatst bezocht 1-11-2016).

172. A.M.G. Zuiderwijk et al., Doorlooptijden in de strafrechtsketen, Cahier 2012-1, WODC, Den Haag, 2012.

173. E.M. Goldratt, *The Goal*, uitg. Taylor & Francis Ltd, 1984.

alleen voor fabrieken, pakketbezorgers en vergunningverleners, maar net zo goed voor de actoren in de strafrechtsketen die de strafzaken behandelen. Logistieke verbetering komt voort uit het voorkomen van wachttijden, of het verkorten van wachttijden als het onvermijdbaar is. Informatiesystemen kunnen daar alleen indirect wat aan doen door de juiste informatie actueel en betrouwbaar correct te leveren. Actueel (real-time) beschikbare informatie is vanzelfsprekend behulpzaam daarbij. Correcte informatie voorkomt fouten en dus wachttijden. Het werken met gedeelde gegevensbronnen voorkomt ook wachttijden. In de praktijk blijken deze voordelen echter moeilijk realiseerbaar vanwege de organisatorische veranderingen (change management) die ermee gepaard gaan. Ten slotte kan ook een actoroverstijgend track-and-trace systeem de basis bieden voor een goede doorstroom en dus voor reductie van wachttijd.
Zo beschouwd raakt tijdigheid ook aan beginselen als betrouwbaarheid en behoorlijkheid. Ook hier bieden de trends, die Gartner heeft waargenomen, weinig zicht op oplossingen. Genoemde oorzaken vereisen een aanpak die de kwaliteit van gegevensregistratie en de logistieke inrichting van de strafrechtsketen raakt.

4.4 Beantwoording van onderzoeksvragen 4 en 5

Op grond van de waarneming dat partijen in de strafrechtsketen moeite hebben met vernieuwingsprojecten, verwachten wij dat veel IT-gerelateerde vernieuwingen in de nabije toekomst voorlopig aan de strafrechtsketen voorbij zullen gaan. De transitie van papier naar elektronische gegevensverwerking (digitization) wordt naar onze verwachting in de komende vijf jaar voltooid. Wel wordt de blik gericht op verdergaande digitalisering (digitalization), hetgeen de mogelijkheid biedt voor een inhaalslag. Wanneer ‘de strafrechtsketen’ ontdekt hoe bijvoorbeeld pakketbezorgers, sociale media en internetwinkels hun vermogen om te vernieuwen organiseren, kan het idee postvatten dat zulke kwaliteit ook in de strafrechtsketen de norm zou kunnen zijn. In onze waarneming vertoont de strafrechtsketen nu een zekere gewenning aan een achtergebleven vermogen tot vernieuwen. Een verschuiving van bestuurlijke aandacht naar het vernieuwingsvermogen kan dan ook verstrekkende gevolgen hebben voor de strafrechtsketen. Transities die in andere branches zijn gerealiseerd, laten zien dat er veel mogelijk is. Wel zien wij ten minste vier noodzakelijke voorwaarden:

1. Een extroverte, lerende IT-organisatie met kennis van moderne innovatie zorgt dat IT-vernieuwingen onder controle blijven en soepel verlopen. Het zichtbare resultaat ervan is dat organisatorische veranderingen niet meer gefrustreerd worden door tegenvallende en uitlopende IT-vernieuwingen. Deze voorwaarde sluit aan bij conclusies van de commissie Elias[174], namelijk dat het de rijksoverheid ontbreekt aan lerend vermogen op ICT-gebied, dat de ICT-kennis van de rijksoverheid tekortschiet en dat het ICT-projectmanagement zwak is.
2. Effectieve bestuurlijke keuzes zijn nodig om de richting te bepalen. Investeren in vernieuwingsvermogen heeft bijvoorbeeld effect op alle toekomstige vernieuwingen en is dus effectiever dan investeren in één vernieuwing. Reflectie op eigen bestuurlijke keuzes in de strafrechtsketen sluit aan op twee conclusies van de commissie Elias, namelijk dat de verantwoordings- en besluitvormingsstructuur bij ICT-projecten zeer gebrekkig is en dat de rijksoverheid haar ICT-projecten niet onder controle heeft.

174. Eindrapport Parlementair onderzoek naar ICT-projecten bij de overheid, Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 5.

3. Methoden, zoals ‘DevOps’ en ‘Agile Software Development’ in combinatie met automatisering van het automatiseren, zorgen dat IT-projecten beheersbaar worden. Het dagelijks in productie nemen van micro-innovaties, zonder verstoring of bedreiging van werkprocessen, is hiervan een direct waarneembaar gevolg.
4. Technologische ontwikkelingen uit de kunstmatige intelligentie en rule based design maken mogelijk dat correcte software wordt gemaakt, dat juiste gegevens worden geleverd, en dat ‘de IT beter snapt’ wat strafvordering betekent. Een significant meetbare afname van correctief werk in de keten en computers die ‘meedenken’ zijn hiervan een direct waarneembaar gevolg.

De veelomvattendheid van deze voorwaarden verklaart waarom quick-fixes niet werken. Maar het feit dat er in de maatschappij voldoende voorbeelden zijn van organisaties met goede logistiek geeft zicht op reële kansen voor de strafrechtsketen.

In de vorige paragraaf hebben we beredeneerd dat voor de beginselen van de strafrechtspleging de mogelijke ontwikkelingen in de toekomst zowel kansen als bedreigingen kunnen betekenen. Steun aan de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging verwachten wij van ontwikkelingen in de IT, die de informatievoorziening volwassen maken. De bedreigingen voor strafrechtelijke beginselen, vanwege gebrekkige informatievoorziening, stellen acute eisen aan het vermogen tot vernieuwen. Ontwikkelingen, die gericht zijn op vaardigheid in het toepassen van IT, groei van kennis, verdere professionalisering van het eigen personeel en technische kennis van software dragen daaraan direct bij.

Hoofdstuk 5

Conclusie en discussie

5.1 Algemeen

De digitalisering heeft in de strafrechtspleging al behoorlijk grote veranderingen gebracht en dat zal in de toekomst eerder meer dan minder ingrijpend worden. In deze studie komen wij tot de conclusie dat digitalisering er niet toe hoeft te leiden dat we bepaalde grondbeginselen van onze strafrechtspleging zullen moeten opgeven. We zien in de beginselen waarmee informatiesystemen ontwikkeld worden, geen onvermijdelijke bedreiging van de strafvorderlijke beginselen. Ook uit de ontwikkelingen van de laatste jaren en uit een voorzichtig toekomstscenario kunnen we niet anders concluderen dan dat de strafvorderlijke beginselen overeind gehouden kunnen worden. Dat gaat echter niet vanzelf. Digitalisering kan ondersteunend zijn, maar ook misbruikt worden. Dat er knelpunten zijn en zich zullen blijven voordoen, dat staat als een paal boven water. Die zijn echter naar ons oordeel niet toe te schrijven aan digitalisering op zichzelf, maar hebben eerder te maken met het gebruik en de besturing ervan. Voorbeelden zijn gebreken in de regie, de dominantie van het bezuinigingsperspectief, achterblijvende kennis en te weinig afstemming tussen de professionals uit de verschillende disciplines. In de toekomstige gedigitaliseerde strafrechtspleging zal de relatie tussen de IT-specialisten en de juridische professionals niet als producent-consument bestempeld kunnen worden. Beide zullen zich op de andere discipline moeten richten en de genoemde rollen met elkaar moeten gaan combineren tot de 'conducenten' van de digitale afdoening van strafzaken. De veranderingen in het handelen en beslissen zullen vast en zeker tot nieuwe vormen van realisatie van de grondbeginselen leiden, maar als beide disciplines vanuit hun principiële basis aan dit proces leiding geven, kan deze nieuwe toestand net zo verenigbaar zijn met het juridisch-normatieve kader als de huidige situatie en zijn er zelfs verbeteringen mogelijk. Dat betekent in ieder geval een georganiseerde dialoog en de monitoring van projecten vanuit beide disciplines.

In hoofdstuk 2 hebben wij als eerste gekeken naar strafvorderlijke beginselen. Ofschoon de informatica geen traditie kent rond beginselen, hebben wij toch gemeend daarnaast een aantal informatietechnische beginselen te moeten formuleren, om deze te kunnen confronteren met strafvorderlijke beginselen. Daaruit is een antwoord op de eerste onderzoeksvraag geformuleerd. In hoofdstuk 3 hebben wij vervolgens gekeken naar veranderingen in de praktijk in de strafrechtsketen in het licht van onderzoeksvragen 2 en 3. Daarin is onderzocht in hoeverre deze digitalisering kansen en risico's oplevert voor de strafvorderlijke beginselen. In hoofdstuk 4 is daar een toekomstperspectief aan toegevoegd en zijn de ontwikkelingen in de IT vanuit de beginselen geduid. Dat levert een antwoord op onderzoeksvraag 4 op. Onderzoeksvraag 5 wordt ook in dat hoofdstuk beantwoord.

Gezien het verkennende karakter van dit onderzoek pretenderen wij niet met nieuwe feitelijke observaties te komen. Door de confrontatie van ontwikkelingen met beginselen komen echter veel vragen naar voren, die soms een fundamenteel punt raken. Een poging om passende antwoorden te vinden, vereist diepgravender onderzoek. Voor deze verkenning is het voldoende om deze vra-

gen te stellen en daarop door te redeneren. Ons onderzoek heeft in ieder geval geen aanwijzingen opgeleverd dat de informatietechnische ontwikkelingen de oorzaak zijn van bepaalde druk op de grondbeginselen van de strafrechtspleging en evenmin dat voor eventuele druk nu en in de toekomst de techniek een panacee zal zijn.

Dit laatste hoofdstuk bestaat uit drie korte delen. Allereerst vatten wij de antwoorden op alle onderzoeksvragen samen. . Het tweede deel bevat discussiepunten die uit het onderzoek naar voren zijn gekomen. Wij sluiten af met vragen die buiten de scope van het onderhavige onderzoek vallen en naar de mening van het onderzoeksteam in de toekomst beantwoord zullen moeten worden.

5.2 Beantwoording van de onderzoeksvragen

5.2.1 WELKE BEGINSELEN VAN STRAFRECHTSPLEGING ZIJN IN VERBAND TE BRENGEN MET IT -ONTWIKKELINGEN?

Onder beginselen verstaan wij een catalogus van wezenlijke kenmerken en kernwaarden die door het nationale recht en verdragsrecht gearticuleerd zijn. We onderscheiden de volgende beginselen die in het licht van de IT-ontwikkelingen relevant zijn:

A het legaliteitsbeginsel, waarbij aandacht gegeven is aan de volgende deelaspecten: respect voor de wettelijke taakverdeling, respect voor de wettelijke begrenzing van bevoegdheden en respect voor de normen ter bescherming van persoonsgegevens;

B het principe van toegang tot de onafhankelijke rechter, waarbij aandacht besteed is aan mogelijke drempels voor justitiabelen;

C het beginsel van equality of arms, waarin mede begrepen is de kenbaarheid voor de verdediging van alle informatie die in de berechting gebruikt wordt en de beschikbaarheid van passende middelen voor de verdediging;

D het openbaarheidsbeginsel, waarmee de openbaarheid naar het publiek bedoeld wordt, de zgn. externe openbaarheid;

E het beginsel van betrouwbaarheid, waarin begrepen is de deugdelijke belangenafweging en beoordeling en onderbouwing op basis van de materiële waarheid;

F het tijdigheidsprincipe, dat vooral in beeld gekomen is door de doelstelling om met IT de efficiency te vergroten.

5.2.2 WELKE VERANDERINGEN IN DE NEDERLANDSE STRAFRECHTSKETEN ZIJN IN DE AFGELOPEN VIJF JAAR HET GEVOLG VAN DE ONTWIKKELINGEN IN DE IT?

De afgelopen vijf jaar hebben gestaan in het teken van de vervanging van papieren stukken door elektronische stukken. In de opsporing treffen we duidelijk meer aan dan ‘digitization’ alleen. De veranderingen in de gehele strafrechtsketen gaan langzamer dan de veranderingen in de maatschappij.

De uitgebreide beantwoording is vervat in hoofdstuk 3.

5.2.3 OP WELKE PUNTEN ONDERSTEUNEN DE VERANDERINGEN DE WERKING VAN VERDRAGSRECHTELIJKE EN (GROND)WETTELIJKE BEGINSELEN BINNEN DE STRAFRECHTSPLEGING DAN WEL LEVEREN DEZE VERANDERINGEN SPANNING OP MET DEZE BEGINSELEN?

Zolang er sprake is van transitie van papieren naar elektronische stukken, zijn strafvorderlijke beginselen nauwelijks in het geding. Ze hoeven niet bijzonder in de knel te komen en tegelijk zien we ook nog geen grote winst in de bevordering van het respect voor die beginselen. Kansen zijn er wel en die kunnen binnen afzienbare tijd met name de faciliteiten voor de verdediging verbeteren. Daar waar de computer taken uitvoert en waarde toevoegt aan de strafrechtsketen is per vernieuwing een kritische beschouwing ten aanzien van beginselen op haar plaats. De discussie rond big data is daarvan een voorbeeld.

Voor een uitgebreide beantwoording verwijzen wij naar hoofdstuk 3 en 4.

5.2.4 WELKE VOOR DE NEDERLANDSE STRAFRECHTSKETEN RELEVANTE IT-ONTWIKKELINGEN ZIJN IN DE KOMENDE VIJF JAAR TE VERWACHTEN?

De transitie van papier naar elektronische gegevensverwerking (digitization) wordt naar verwachting voltooid. De blik wordt gericht op verdergaande digitalisering (digitalization). Wij verwachten een inhaalslag, met verstrekkende gevolgen voor de strafrechtsketen. Wij zien ten minste vier noodzakelijke voorwaarden om de ontwikkelingen in de informatica in te zetten voor het versterken van beginselen van strafrecht en strafvordering:

1. Methoden, zoals “DevOps” en “Agile Software Development” in combinatie met automatisering van het automatiseren.
2. Technologische ontwikkelingen uit de kunstmatige intelligentie en rule based design.
3. Een extroverte, lerende IT-organisatie met kennis van moderne innovatie.
4. Effectieve bestuurlijke keuzes.

Voor een uitgebreide beantwoording verwijzen wij naar hoofdstuk 4.

5.2.5 OP WELKE PUNTEN ZULLEN DE TE VERWACHTEN VERANDERINGEN STEUN GEVEN AAN DE WERKING VAN VERDRAGSRECHTELIJKE EN (GROND)WETTELIJKE BEGINSELEN BINNEN DE STRAFRECHTSPLEGING C.Q. ZULLEN DE VERANDERINGEN SPANNING MET DEZE BEGINSELEN BETEKENEN?

Als de transitie naar elektronische gegevensverwerking voltooid kan worden, is het dat de geboekte efficiencywinst ingezet wordt voor de afwegingen die om meer tijd en aandacht van een mens vragen. Bedoeld zijn die handelingen/beslissingen die menselijke discretie vereisen. Dan wordt datgene wat wij onder het beginsel van betrouwbaarheid gerubriceerd hebben, bevorderd.

Ten aanzien van de legaliteit zal hoog op de agenda gezet moeten worden dat de nieuwe toepassingen wettelijk gereguleerd zijn. Dat dient ertoe dat de middelen voor die doelen aangewend worden waarvoor ze beschikbaar gesteld zijn en dat waarborgen van transparantie en controle in werking zijn. Ten aanzien van de rechtspositie van het individu, in het bijzonder het verdachte individu, zijn er wel zorgen. Wanneer de informatiegaring niet gebaseerd is op een geconstateerde misdaad, maar wel verwerkt wordt in allerlei platforms en systemen, kan het heel moeilijk worden om van de verdenking af te komen en van interventies van de zijde van de autoriteiten gevrijwaard te blijven. Men moet de

risico's onder ogen zien die informatiedeling tussen overheid en particulieren voor de reputatie van de eens als verdachte aangemerkte persoon en dus voor diens maatschappelijk functioneren met zich mee brengt. Het recht om weer vergeten te worden moet niet illusoir zijn en dat ook ten opzichte van anderen dan de overheid. Wat heb je aan het beginsel van *equality of arms* als de consequenties niet door de overheid maar door machtige private organisaties getrokken worden? Dat maakt de toegang tot een onafhankelijke rechter des te meer relevant. Dat beginsel is ook aan de orde bij de elektronische sanctionering door een intelligent systeem. Er zal laagdrempelige toegang moeten blijven tot een onafhankelijke beoordeling van bijzondere omstandigheden die tot opheffing van de sanctie kunnen leiden. De (on)mogelijkheden om daadwerkelijk kritisch te zijn ten aanzien van de complexe bewerkingen die in de toekomst de grondslag zijn voor de informatie, handeling of beslissing, moeten in het centrum van de belangstelling staan.

Verdere beantwoording van deze vraag vindt plaats in hoofdstuk 4.

5.3 Discussie

Uit hoofdstuk 3 komt naar voren dat de strafrechtsketen zich thans bezighoudt met 'digitization', ofwel de transitie van papier naar digitaal. Uit hoofdstuk 4 blijkt dat de maatschappij op tal van manieren bezig is met 'digitalization', ofwel verdergaande vernieuwing waarbij computers zelf taken uitvoeren. Dit is consistent met onze eigen waarneming en wat onze gesprekspartners vinden: de digitalisering in de maatschappij loopt voor op digitalisering in de strafrechtsketen. De vraag is of dit ernstig is. In het licht van strafvorderlijke beginselen ligt het in de lijn van dit onderzoek om deze discussie te voeren. In hoofdstuk 3 hebben wij betoogd dat hierdoor het beginsel van legaliteit in het geding kan komen. Wij hebben een gebrek aan technische kennis aangetroffen, die op zichzelf niet verrassend is. Wij hebben ook waargenomen dat aannames over de correcte werking van systemen vanuit informatietechnisch perspectief onjuist zijn. Dit brengt het risico met zich mee, dat de officier van justitie c.q. de rechter in hun beoordelingen kunnen komen tot een foutieve duiding van feiten. Het feit dat de strafrechter zelf ook tot waarheidsvinding geroepen is, maakt het risico te meer serieus. De tegenwerping, dat de rechter bij het beantwoorden van vragen over hoe feiten uit een informatiesysteem beoordeeld moeten worden, deskundigen mag raadplegen is hierbij onvoldoende. Deskundigen kunnen immers alleen helpen bij het duiden van expliciete vraagstukken. Als de rechter zich niet bewust is van een vraagstuk komt er ook geen deskundige op de proppen. Dan is er ook het aspect van procedurefouten als gevolg van gebrekkige IT. Als onderzoeksteam willen wij aan deze discussie het aspect van 'gebrekkige kennis van IT' bijdragen. In het programma KEI is dit feit ook onderkend, maar dat is op zichzelf niet voldoende.

Rond het thema van big data is de vraag aan de orde in hoeverre ongerichte verzameling van gegevens op gespannen voet staat met het beginsel van doelbinding, dat wij als belangrijk aspect van legaliteit naar voren gebracht hebben. Over deze vraag is ook in eerder onderzoek al het nodige geschreven. Maar daarmee is zij nog niet beantwoord. De vraag heeft niet alleen een juridisch, maar ook een ethisch aspect. In de juridische sfeer vragen wij ons af welke regels nodig zijn. In de ethische sfeer is het de vraag onder welke voorwaarden het geoorloofd is om big-data-onderzoek te gebruiken om strafrechtelijke overtredingen te signaleren. Als onderzoekers stellen wij ons op het standpunt dat een gericht onderzoeksdoel, getoetst op juridische en ethisch normen in een praktisch bruikbaar stelsel van checks en balances, een goede waarborg biedt

voor het beginsel van doelbinding. Het enkele feit dat een onderzoek gericht is op een doelgroep en niet op een individu doet daar niet aan af. Wel dient door goede regeling ondervangen te worden dat bestaande databases gebruikt worden voor doelen waarvoor ze nooit gecompileerd zijn. Het thema is dus nog volop in discussie en ons lijkt de richting voor het debat, die Moerel en Prins wijzen een verstandige. Laat het debat gaan over de uiteindelijke toepassing van de resultaten van de analyses.[175]

5.4 Buiten bestek

Het voorgaande roept vragen op die buiten het bestek van dit onderzoek vallen. Vragen, waarvan de beantwoording soms diepgravender onderzoek vergt dan een verkenning. In deze sectie benoemen we enkele vragen, waarvan wij als onderzoekers vinden dat beantwoording ervan noodzakelijk is om te kunnen komen tot verantwoorde beleidskeuzes. We hebben ons niet gewaagd aan een verklaring van de matige vooruitgang in de digitalisering van de strafrechtsketen. Dat deze digitalisering gepaard gaat met voorzichtigheid, juist vanwege het belang dat aan strafrechtelijke beginselen wordt gehecht, verdient waardering. Echter, zorgvuldigheid en vooruitgang zouden aan elkaar verbonden moeten kunnen worden. We wezen hierboven al op het kennisaspect en in het debat met de experts beluisterden wij ook dat ketenpartners misschien nog niet genoeg vertrouwen in elkaar hebben om op dit punt met behoud van eigen wettelijke verantwoordelijkheid samen te werken. Onze waarnemingen zijn op dit punt anekdotisch. Het verdient in de beleidsvoorbereiding apart onderzoek, of en in welke mate dat het geval is en waardoor dat in dit concrete geval veroorzaakt wordt.

Welke systeemarchitectuur voor een toekomstbestendige ondersteuning van vervolging en berechting aan te bevelen is, hebben we niet onderzocht. Op basis van onze studie kunnen we wel zeggen dat de juridische autonomie van een actor gefaciliteerd moet kunnen worden welke keuze men ook maakt. De basisuitgangspunten van systeemontwikkeling (hoofdstuk 2) bieden zicht op het respecteren van de onafhankelijkheid van de rechter en de autonomie van de verdediging. In welke mate bijvoorbeeld het werken met een gemeenschappelijke gegevensruimte daartoe in concreto mogelijkheden biedt, is een boeiende vraag. Bij de beantwoording daarvan moet onzes inziens betrokken worden dat de beweging in de vervolging en berechting niet beperkt is tot een eenrichting stroom van gegevens, van de ene naar de volgende strafrechtelijke autoriteit in de keten. Alleen al met de door ons aan in hoofdstuk 1 gesignaleerde ruimere kring van actoren in de strafrechtspleging is het beeld complexer.[176]

Met dat complexe beeld voor ogen veroorloven wij ons nog een laatste overweging. Wij hebben de strafrechtspleging benaderd als een systeem met ten minste twee dimensies, de juridische en de informatietechnische. Beide zijn niet statisch maar aan verandering onderhevig. Vanwege de onderlinge connectie zullen bewegingen niet beperkt blijven tot alleen het juridische of alleen het informatietechnische perspectief. Veranderingen door verdere digitalisering van werkprocessen in de afdoeningsketen zullen vroeg of laat een of andere impact op de juridisch gewaarborgde positie van actoren buiten de keten hebben. Bij

175. E.M.L. Moerel & J.E.J. Prins in *Homo Digitalis*, 2016, p. 53; idem WRR 2016, p. 11.

176. P. Wisse, *Interoperabiliteit voor informatieverkeer in publiek domein*, UvA PrimaVera Working Paper 2008-08, p. 18-19, onderscheidt ketenprocessen en meer complexe netwerkprocessen.

die ontwikkeling zullen om die reden bij voorbaat de gevolgen voor de actoren buiten de keten betrokken moeten zijn. Juridische grondbeginselen kunnen en moeten als beginselen recht overeind blijven staan en geven tegelijk ruimte voor nieuwe realisaties. Mocht er echter iemand zijn die meent, dat de dimensies los van elkaar functioneren, dan willen we dat beeld corrigeren. Dat is niet de dynamiek van het systeem van de strafrechtspleging, in elk geval niet voor de fasen van vervolging en berechting die wij bestudeerd hebben. Reden te meer om voor de 'conducenten'-benadering te pleiten, zoals hierboven gedaan is.

Summary

Digitalisation has already brought about considerable changes in the criminal justice administration. In the future such changes will only have a deeper impact. The legal values that rule in criminal justice, usually described as fundamental principles, have to be respected in acting and decision making. The question should be asked whether this can work: digitalisation of the criminal justice administration while respecting the legal fundamental principles of that administration. The following question was central in the study as reported here:

Which developments in information technology will possibly change the action/decision making by actors in the Dutch criminal justice administration? Which positive and negative consequences for the fundamental principles derived from treaty law and statutory law can be discerned in criminal justice administration.

The central question comprised the following subquestions:

1. Which principles of criminal justice administration can be related to IT-developments?
2. Which changes in the criminal justice chain, as visible over the last five years, are the consequence of developments in IT?
3. What aspects of these already visible changes can we appreciate as support for the fundamental principles derived from treaty and statutory law and which as a cause for tension?
4. Which IT-developments, relevant for the Dutch criminal justice chain, can be expected in the next ten years?
5. On what points will the expected changes support the fundamental principles of criminal justice administration, as derived from treaty and statutory law, and where can tension be expected to arise?

This report concludes, that for the procedural stages of prosecution and trial the fundamental legal principles of criminal justice administration can be upheld in the digitalisation development. In chapter 2 the relevant legal principles are described as well as the leading principles for developing information systems. After confronting those two sets of principles the conclusion is reached, that the principles for information systems do not by nature provide a contradiction with the fundamental legal principles. Chapter 3 describes the recent transition from paper to digital for criminal case files. This changing operation is put to the test whether tensions have arisen with the fundamental principles of criminal justice administration. Tension is observed but is not ascribed to IT itself. A possible scenario for future IT-induced changes is subjected in chapter 4 to the framework that the legal fundamentals provide, where it is found that violation of these principles is not inevitable. Digitalisation can support the realisation of the legal fundamental principles, or at least be neutral to those principles.

It is obvious that there are issues at the moment and will be in the future where tension arises. Those issues however should not simply be linked to digitalisation itself. They have to do with lack of direction and lack of knowledge, proximity and coordination on the side of the professionals from the separate expertise areas, that are involved in the digitalisation of this complex system. Regarding the tension issues IT-developments or applications themselves cannot be put forward, neither as a cause nor as a solution, for now and for the future.

In the prospective digitalised criminal justice administration the relation between IT-specialists and legal professionals should not be characterised as a producer-consumer relation. Both sides will have to focus on the other discipline and the roles will have to become combined to that of ‘conducers’ of the digital disposal of criminal cases. The changes in acting and decision making will surely lead to new realisations of the fundamental legal principles. When both professional disciplines lead the process of change, working from the respective basic principles, the new situation can be as much in conformity with the legal-normative framework as it is in the current situation. Even progress can be expected.

Bijlage 1 Leden van de begeleidingscommissie

naam	*affiliatie*
mr. dr. W.L. Borst	Ministerie van Veiligheid en Justitie
mr. dr. B.W. Schermer	Universiteit Leiden
dr. S.A. de Blok	Rijksuniversiteit Groningen
mr. dr. J.B.J. van der Leij	Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) Ministerie van Veiligheid en Justitie
prof. mr. A.R. Lodder (voorzitter)	Vrije Universiteit Amsterdam

Bijlage 2 Lijst met geïnterviewde personen

naam	*functie*	*reden betrokkenheid*	*datum interview*
mr. S.S. Hensels-van Straaten	Officier van Justitie te Rotterdam	Deelprojectleider Digitaal Dossier binnen de Rotterdamse Pilot Implementatie GPS Maatwerk	22-06-2016
drs. B. Hogemans	Adviseur bij SYSQA expertise: kwaliteitsmanagement en ICT	Hij is binnen zijn organisatie verantwoordelijk voor het domein ministeries & overheid. En hij is actief in de commissie ICT en overheid	13-05-2016
mr. A. Huigen	Senior rechter te Amsterdam	(voormalig) programmaleider DWS	11-05-2016
mr. V. Mul	Vice-president Rechtbank Rotterdam	Betrokken bij Rotterdamse pilot	01-06-2016
mr. K. Pieters	Officier van Justitie te Rotterdam	Heeft vanaf het prille begin gewerkt met DDV en is in dat opzicht te beschouwen als een 'early adapter'.	22-06-2016
dr. T. Rodrigues	Adviseur op het gebied van verandermanagement en moderniseringsvraagstukken	Programma adviseur voorDWS. Tevens als adviseur betrokken bij verschillende overige ketenpartners	18-05-2016
ir. H.M. Sasse	Business Architect bij De Rechtspraak	Als business architect betrokken bij de digitaliseringsontwikkelingen	20-04-2016
mr. M.E. van Wees	Raadsheer in het Hof Arnhem-Leeuwarden	Lid van Rechtspraak-projectteams digitalisering	20-05-2016

Bijlage 3 Lijst met personen en affiliaties expertmeeting Utrecht, 7 september 2016

N.B.: de leden van de begeleidingscommissie waren ook uitgenodigd. Aanwezig waren prof. dr. A. Lodder, VU Amsterdam, en mr. dr. W. Borst, Ministerie van Veiligheid en Justitie.

naam	*affiliatie*
Marie-José Bonthuis	It's privacy
S. Fieten	Fieten IT, Leiden
F. Heida	informatiemanager CIO office Openbaar Ministerie
F. Hendriksen	programma Digitaal Werken Strafrechtsketen Principal adviseur – enterprise architectuur M&I Partners Zeist
S.S. Hensels-van Straaten	senior officier van justitie, teamleider team opleidingen, afdeling interventies Arrondissementsparket Rotterdam
P.A.O. Josephus Jitta	directeur Strategie en Middelen Justitiële informatiedienst Almelo
M. Kessler	Professor of Criminal Law Institute of Criminal Law and Criminology Leiden University
K.W. Keuzenkamp	programmamanager Keteninformatisering Ministerie van Veiligheid en Justitie Directoraat-Generaal Vreemdelingenzaken Directie Regie Vreemdelingenketen
E. Koedam	beleidsadviseur Politie, Staf Korpsopleiding, Directie Informatievoorziening Den Haag
A.W.M. de Koning	adviseur Digitalisering Strafrechtsketen Ministerie van Veiligheid en Justitie Directoraat Generaal Rechtspleging en Rechtshandhaving Directie Veiligheid en Bestuur Den Haag
H.C.D. Korvinus	Raadadviseur Veiligheid & Recht Kabinet Minister President Ministerie van Algemene Zaken Den Haag
C.H. Lucassen	informatiearchitect Politie, Dienst Informatiemanagement, IV experts
R.F. Meijer	Ministerie van Veiligheid en Justitie Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) Afdeling Statische Informatievoorziening en Beleidsanalyse (SIBa) Den Haag
J.G. Pot	programma Digitaal Werken Strafrechtsketen

A. Ruifrok	Forensische Biometrie & Identificatie Nederlands Forensisch Instituut Den Haag
H.M. Sasse	Business architect, QA, teamcoördinator LDCR – Informatievoorziening Team informatiemanagement De Rechtspraak
W. Ph. Stol	Politieacademie bijzonder hoogleraar Cybercrime Open Universiteit NHL University of Applied Sciences
A.L.J. van Strien	raadsheer in de Hoge Raad
R.P. Tuinenburg	officier van justitie Openbaar Ministerie Arrondissementspakket Den Haag
P. Verloop	advocaat
M.E. van Wees	coördinerend raadsheer-commissaris Afdeling Strafrecht De Rechtspraak Gerechtshof Arnhem-Leeuwarden
R. van Wees	architect programma Digitaal Werken Strafrechtsketen (consulting) Ministerie van Veiligheid en Justitie Capgemini

Bijlage 4 **Lijst met stellingen die in de voorbereiding van de expertmeeting gevoegd was bij de uitnodiging**

Uw naam:

Ik voel mij in op de eerste plaats (geef één antwoord: a, b of c):

a jurist
b IT-er
c anders

Geef van elk van de onderstaande 10 stellingen uw mening met een cijfer van 0-5:
0: weet niet/geen mening
1: pertinent oneens
2: oneens, maar…
3: om het even
4: eens, maar…
5: mee eens

Stelling	Score
1. De digitalisering in de strafrechtspleging vormt een bedreiging voor de autonomie van de relevante actoren (bijv. politie, OM, rechter, advocatuur, reclassering).	
2. Privacy gaat voor functionaliteit.	
3. Semantische technologie (bijv. regelsystemen, slim zoeken, Big Data(mining)) zal binnen vijf jaar een belangrijke rol spelen binnen de strafrechtsketen.	
4. Digitalisering bevordert het goed functioneren van de strafrechtspleging als keten.	
5. Het digitale zaaksdossier bevordert de gelijkwaardigheid (equality of arms) van partijen in het strafproces.	
6. De toenemende digitalisering in de strafrechtsketen zal een negatief effect hebben op de toegankelijkheid van het recht.	
7. De equality of arms brengt met zich mee dat de resultaten van digitalisering bij de overheid onbeperkt beschikbaar moeten komen voor de verdediging.	
8. Het publieke karakter van de strafrechtspleging brengt met zich mee dat de overheid voor het digitaal werken onafhankelijk moet kunnen zijn van marktpartijen.	
9. Onrechtmatig handelen door een informatiesysteem is een acceptabel risico.	
10. Sterke beveiligingsmaatregelen leveren veiligheidsrisico's op.	

Bijlage 5 Personalia onderzoekers

M. (Marloes) Dijkstra Msc	Onderzoeker Ordina
prof. dr. ir. S.M.M. (Stef) Joosten	Hoogleraar Ontwerpen van informatiesystemen Open Universiteit Management consultant Ordina
prof. mr. E.F. (Evert) Stamhuis	Hoogleraar straf(proces)recht Open Universiteit Raadsheer-plaatsvervanger Gerechtshof 's Hertogenbosch
mr. M. (Mark) Visser	promovendus straf(proces)recht Open Universiteit

Bijlage 6 Register van geraadpleegde bronnen

Literatuur

Aarde & Prins 2016
C.M. Aarde & J.E.J. Prins, 'Digitalisering binnen de rechtspraak: van KEI naar Big Data', in: *RMThemis* 2016, 2.

Balkema 2016
J.P. Balkema, 'Het strafrechtelijk sanctiestelsel. Een terugblik op vijfentwintig jaar', *Sancties* 2016, 2.

Bauw 2016
E. Bauw, 'KEI, een gamechanger voor de civiele en bestuursrechtspraak?', in: *RMThemis* 2016, 2.

Berkhout-van Poelgeest 2001
A.M. Berkhout-van Poelgeest, 'Enkele vragen over de legaliteit in het strafproces (artikel 1 Sv)', in: C. Brants, P.A.M. Mevis en E. Prakken (red.), *Legitieme strafvordering. Rechten van de mens als inspiratie in de 21ste eeuw*, Antwerpen-Groningen: Intersentia Rechtswetenschappen, 2001.

De Blok e.a. 2015
C. de Blok e.a., *Digitalisering in strafrechtsketens. Ervaringen in Denemarken, Engeland, Oostenrijk en Estland vanuit een supply chain perspectief*, RuG/WODC 2015.

Boksem 2015
J. Boksem, 'Nader onderzoek geboden?', in: J. Boksem & D. de Wolf, *Nader strafrechtelijk onderzoek vanuit verdedigingsperspectief (*Pre-advies voor de jaarvergadering van de Nederlands-Vlaamse Vereniging voor Strafrecht), Oisterwijk: WLP 2015.

Brants e.a. 2003
C.H. Brants, P.A.M. Mevis, E. Prakken en J.M. Reijntjes, 'Op zoek naar grondslagen', in C.H. Brants e.a. (red.) *Op zoek naar grondslagen. Strafvordering 2001 ter discussie*, Den Haag: Boom Juridische uitgevers 2003.

Brinkhoff 2016
S. Brinkhoff, 'Big data datamining door de politie', *NJB* 2016, 994

Corstens/Borgers 2014
G.J.M. Corstens (bewerkt door M.J. Borgers), *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2014.

Van Essen 2016
B. van Essen, *Het kan dus wel: succesvol automatiseren door de overheid*, Rijkswaterstaat, 2016.

Feteris 2016
M. Feteris, 'Komt het ooit tot robotrechters?', *Rechtspraak*, Magazine van de Raad voor de rechtspraak, juni 2016.

Groenhuijsen & Knigge 2004
M.S. Groenhuijsen & G. Knigge, 'Afronding en verantwoording. Algemeen deel', in M.S. Groenhuijsen & G. Knigge (red.), *Afronding en verantwoording. Eindrapport Strafvordering 2001*, Deventer: Kluwer 2004.

Hesselink 2016
L. Hesselink, 'Ervaringen met digitaal procederen over asiel en bewaring. We moeten eraan', in: *A&MR* 2016, 2.

Hijmans 2014
H. Hijmans, 'De ongeldigverklaring van de Dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof van Justitie', in: *NtEr* 2014, 7.

Hildebrandt 2016
M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht', in: *Homo Digitalis* (Handelingen Nederlandse Juristen-Vereniging 2016-I), Deventer: Kluwer 2016.

Homan 2012
K. Homan, 'Oorlogvoering in de digitale ruimte', in: *Internationale Spectator*, 66, februari 2012.

Van den Hoogen 2007
R.H. van den Hoogen, *E-justice, beginselen van behoorlijke elektronische rechtspraak*, Den Haag: Sdu 2007.

Joosten, Wedemeijer & Van der Woude 2013
S. Joosten, L. Wedemeijer en J. van der Woude: Rule Based Design, Open Universiteit, 2013.

Keulen & Knigge 2016
B.F. Keulen & G. Knigge, *Strafprocesrecht,* Deventer: Kluwer 2016.

Koops, Konings & Verbruggen 2016
B-J. Koops, C. Konings en F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht*, preadvies NVVS 2016, Oisterwijk: Wolf Legal Publishers 2016.

Langbroek & Tjaden 2008
P. Langbroek & M. Tjaden, 'ICT in de strafrechtsketen, de ontwikkeling en implementatie van nieuwe systemen bij het Openbaar Ministerie, '*Proces, februari* 2008.

Van der Leij 2005
J.B.J. van der Leij, *Ontwikkelingen in het strafrecht-een aperitief*, in: *Systeem in ontwikkeling: liber amicorum G. Knigge*. Nijmegen: Wolf Legal Publishers, 2005.

Leukfeldt 2016
R. Leukfeldt, *Cybercriminal networks. Origin, growth and criminal capabilities* (diss. OU), Den Haag: Eleven International Publishing 2016.

Lodder & Schuilenburg 2016
A.R. Lodder & M.B. Schuilenburg, 'Politie-webcrawlers en predictive policing' in: *Computerrecht* 2016/81.

Mamykina e.a. 2016
L. Mamykina et. al., 'Learning From the Crowd: Observational Learning in Crowdsourcing Communities', in: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, New York: ACM 2016.

Van der Meij 2014
P.P.J. van der Meij, 'De laatste duit in het zakje. Over waarheidsvinding in strafzaken en de beperkingen van de verdediging', in: *Strafblad* december 2014.

Moerel & Prins 2016
E.M.L. Moerel & J.E.J. Prins, 'Privacy voor de Homo Digitalis', in: *Homo Digitalis* (Handelingen Nederlandse Juristen Vereniging 2016-I), Deventer: Kluwer 2016.

Rademaker 1996
J. Rademaker, De digitale strafrechtspleging. Strafrechtelijke informatisering in meervoudig perspectief, Zwolle, Tjeenk Willink, 1996.

Reijntjes 2009
J.M. Reijntjes, *Minkenhof's Nederlandse strafvordering*, Deventer: Kluwer 2009.

Ros 2016
A.W.J. Ros, 'KEI: Kans of keurslijf', *NJB* 2016, 5.

Schuyt 2015
P.M. Schuyt, 'Nieuwe strafvorderingsrichtlijnen voor het openbaar ministerie', *Sancties* 2015, 10.

Snellen & Schokker 1993
I.Th.M. Snellen, J T. Schokker, *Wetgeving en systeemontwikkeling*, 's-Gravenhage 1993.

Van Stekelenburg 2010
M. van Stekelenburg, *De betere byte in de strijd om het gelijk*, dissertatie VU Amsterdam, Delft: Eburon 2010.

Verheij 1999
B. Verheij, Automated Argument Assistance for Lawyers, proceedings ICAIL-99, Oslo.

Verhoef, Hiemstra & Cachet 2013
J. Verhoef, R. Hiemstra en A. Cachet, 'Politie, ICT en toekomstvisie', *Tijdschrift voor de Politie* 2013, 75 (4).

Vermaas 2007
P. Vermaas, 'GPS wordt steeds beter. Interview met H. van Brummen', in: *Opportuun* 2007.

Van Wees 2015
M.E. van Wees, 'Modernisering en digitalisering van het strafproces', *DD* 2015, 72.

WRR 2016
Wetenschappelijke Raad voor het Regeringsbeleid (WRR), *Big Data in een vrije en veilige samenleving*, Amsterdam University Press, 2016.

Willems 2014
D. Willems, 'Predictive Policing — wens of werkelijkheid?', *Tijdschrift voor de Politie*, 2014 jrg.76, nr. 4/5/14, p. 39v.

Wisse 2008
P. Wisse, *Interoperabiliteit voor informatieverkeer in publiek domein*, UvA PrimaVera Working Paper 2008-08.

Wolters Ruckert & Van Sloten 2016
N. Wolters Ruckert & L. van Sloten, 'Big Data: Big privacy challenges', in: *Computerrecht* 2016/2.

Zuiderwijk e.a. 2012
A.M.G. Zuiderwijk et al., Doorlooptijden in de strafrechtsketen, *Cahier* 2012-1, Den Haag: WODC 2012.

Kamerstukken

Kamerstukken II 2015/16, 29279, 298.
Kamerstukken II 2014/15, 34090, 3.
Kamerstukken II, 2014/15, 34090, 5.
Kamerstukken II, 2012/13, 29279, 165.
Kamerstukken II 2013/14, 29 279, nr. 178.
Kamerstukken II 2011/12, 29279, 165.
Kamerstukken II 2011/12, 33173, 1.
Kamerstukken II 2008/09, 31 700 VI, nr. 155.

Kamerstukken I 2013/14, 33750, VI, nr. AB.

Rechtspraak

EHRM 5 oktober 2006, 45106/04 *(Marcello Viola/Italie).*
EHRM 16 februari 2000, nr. 28901/95, *(Rowe en Davis/Verenigd Koninkrijk).*
EHRM 18 maart 1997, nr. 21497/93, *NJ* 1998, 278, m.nt. H.J. Snijders *(Mantovanelli/Frankrijk).*
EHRM 27 oktober 1993, nr. 14448/88, *NJ* 1994, 534, m.nt. H.J. Snijders & E.J. Dommering, *(Dombo/Nederland).*
EHRM 24 juni 1993, nr. 14518/89 *(Schuler-Zgraggen/Zwitserland).*

HvJ EU 8 april 2014, C293/12 en C594/12 *(Digital rights Ireland en Seitlinger).*

HR 16 februari 2016, ECLI:NL:HR:2016:240, *NJ* 2016/404.
HR 19 februari 2016, ECLI:NL:HR:2016:296.

Hof Den Haag 20 februari 2012, gepubliceerd in *NBSTRAF* 2012/277.

Rb. Amsterdam 2 december 2014, gepubliceerd in *NBSTRAF* 2015/122.

Digitale bronnen

A. Das, *Waarom de rechtspraak fishing expeditions niet moet faciliteren*, http://njb.nl/blog/waarom-de-rechtspraak-fishing-expeditions-niet.19962.lynkx (laatst geraadpleegd 30-11-2016)

A Ernes, *Eigendom in de virtuele dimensie*, https://www.ou.nl/web/rechtswetenschappen/webcolumn-RW (laatst geraadpleegd 30-11-2016)

J. Kohnstamm, *Het spiegelkabinet van de argwaan*, speech 8 april 2005, te vinden op https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/artikelen/art_jko_2005_speech_njcm.pdf.

Professionele standaarden strafrecht
https://www.om.nl/organisatie/beleidsregels/@88217/aanwijzing-kader-0/.

https://www.rechtspraak.nl/SiteCollectionDocuments/20160220-professionele-standaarden.pdf.

M. Roessingh, 'iColumbo kan meer dan hij mag', *Trouw,* 2 november 2013
http://www.trouw.nl/tr/nl/5009/Archief/article/detail/3537791/2013/11/02/iColumbo-kan-meer-dan-hij-mag.dhtml.

M. Slaghekke, Column: Digitalisering en kennisneming van het procesdossier: 1-0 voor het OM
www.bijzonderstrafrecht.nl/2015/column-digitalisering-en-kennisneming-van-het-procesdossier-1-0-voor-het-OM/ (inmiddels dode link; 17 okt. 2016).

Symantec, Internet Security Threat Report, vol. 21, april 2016 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

Task Force OM-ZM, Recht doen: Samenwerken loont, Openbaar Ministerie & Rechtspraak, Februari 2014
https://www.**om**.nl/publish/pages/23332/rapport_**task_force_om_zm**.pdf.

J. van der Veen & B. Bokhorst, Normen IT-voorzieningen, e-Overheid
https://www.digitaleoverheid.nl/images/stories/nieuws_2010/normenit_noradossier_informatiebeveiliging.pdf.

https://www.om.nl/vaste-onderdelen/zoeken/@53989/bepaalt-officier/.

https://www.nrc.nl/handelsblad/2016/03/19/bij-de-gewonemensenrechter-1600515.

http://nos.nl/artikel/2091635-privegegevens-rotterdammers-op-straat-door-fout-ambtenaar.html.

https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Wetten-digitaal-procederen-aangenomen.aspx.

https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Toegang-tot-kantonrechter-blijft-gewaarborgd.aspx.

https://e-justice.europa.eu/content_ecli_search_engine-430-nl.do.

https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Miljoenen-uitspraken-uit-Europese-landen-nu-online-doorzoekbaar.aspx.

http://www.volkskrant.nl/economie/wet-asscher-werkt-averechts-personeel-ontslaan-alleen-maar-moeilijker~a4330296/.

https://www.rechtspraak.nl/Voor-advocaten-en-juristen/modernisering-rechtspraak/Paginas/Animatie-modernisering-rechtspraak.aspx.

https://www.rechtspraak.nl/Voor-advocaten-en-juristen/modernisering-rechtspraak.

https://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties/stelselvoorzieningen/stelselcatalogus/authentieke-gegevens.

http://www.daardan.nl/2012/01/taakstraf-voor-agentbeuker-dankzij-softe-polaris-richtlijnen/.

https://loket.rechtspraak.nl/Professionals/Advocatuur/45.

http://www.mr-online.nl/juridisch-nieuws/31449-advocaten-slaan-handen-ineen-voor-digitaal-procederen.

https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Jaarlijks-35-miljoen-extra-voor-Rechtspraak.aspx.

https://www.computable.nl/artikel/nieuws/wie-gunt-wat/5084183/3152533/ind-kiest-capgemini-voor-beheer-indigo.html.

https://www.rathenau.nl/nl/publicatie/het-gaat-niet-om-technologie-het-gaat-om-ons.

https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/De-zachte-kant-van-digitalisering.aspx.

http://www.gartner.com/newsroom/id/3143521.

http://www.amberalert.nl/.

http://www.sciencemag.org/news/2016/09/can-predictive-policing-prevent-crime-it-happens.

http://wabp.nl/.

https://beveiligingnieuws.nl/nieuws/politie-wil-drugshonden-robots-vervangen.

http://rechtennieuws.nl/42277.

http://portal.ou.nl/web/rule-based-design.

https://www.propublica.org/article/machine-bias-risk-assessment-in-criminal-sentencing.

Overige bronnen

Digitaal werken in de strafrechtsketen, E-Zine van DWS, maart 2016.

Digitaal werken in de strafrechtsketen, E-Zine van DWS, oktober 2015.

Begroting Veiligheid en Justitie 2017, *NJB* 2016/33.