Naar digitaal werken in de strafrechtsketen.
Perspectief en richting.

aanleiding

De strafrechtspleging digitaliseert. Dit raakt niet alleen de ondersteuning, maar ook rechtstreeks het primaire proces. Digitalisering is immers de - door technologische innovaties voortgedreven - maatschappelijke ontwikkeling die ertoe leidt dat alle verwerkingen van informatie worden ondersteund door en (kunnen) worden uitgevoerd met behulp van computers.[1] Zij biedt kansen om werk effectiever en efficiënter te doen, administratieve lasten en fouten in registraties terug te dringen, nieuwe manieren van werken te realiseren, functionarissen, belanghebbenden en burgers een betere informatiepositie te geven. In tal van projecten worden deze kansen al benut.[2] Een beheerste overgang naar volledig digitaal werken vereist echter een meerjarige, integrale, consistente, samenhangende aanpak. De werkwijzen van de (juridische) professionals, de wetgeving en de informatiesystemen moeten stapsgewijs en op elkaar afgestemd veranderen. Bestaande ICT-systemen en infrastructuren behoeven aanpassing, modernisering of vernieuwing. Dit vergt een visie met als belangrijkste elementen: de afstemming van verschillende systemen, de betrouwbaarheid van informatie en de verantwoordelijkheid voor de vastlegging en het beheer van informatie.[3]

Deze notitie schetst zo'n visie. Centraal daarin staat niet techniek, maar enerzijds de professional en diens informatiebehoefte, anderzijds het begrip "verantwoordelijkheid", dat wil zeggen de vele te onderscheiden verantwoordelijkheden voor gegevens, informatie en systemen. Doel is ook níet het creëren van één nieuw, alles omvattend informatiesysteem, maar het opbouwen van een coherent stelsel van voorzieningen die in een federatief model met elkaar kunnen communiceren: het “informatie-ecosysteem” van de strafrechtspleging. De term "voorziening" moet hier ruim worden opgevat: maatregel, middel om in een behoefte te voorzien, faciliteit; dus breder dan "informatie-systeem". Het gaat om een geheel van afspraken, gegevensverzamelingen, systemen en verbindingen daartussen.

Deze notitie schetst eerst de contouren van de visie, daarna een aantal bouwstenen. Als tijdshorizon is voorshands 2020 gekozen. Dat jaartal is echter tentatief. De notitie beoogt níet een "eindplaatje" te schetsen dat binnen die tijd zou moeten zijn gerealiseerd. Zulke "eindplaatjes" zijn niet aan de orde. De techniek staat immers niet stil en nieuwe mogelijkheden en inzichten blijven zich aandienen. In plaats van een "eindplaatje" geeft de notitie daarom de richting aan waarin de strafrechtspleging zich moet ontwikkelen om de digitalisering goed te absorberen. In een aantal bijlagen komen de achtergrond, de randvoorwaarden, de uitgangspunten en een aantal definities aan de orde.

[1] Vgl. Agenda voor Nederland. Inspired by technology (2015), p. 40.
[2] Bijlage 3 bij deze notitie presenteert een groot aantal initiatieven en projecten.
[3] Algemene Rekenkamer: Resultaten verantwoordingsonderzoek bij het Ministerie van Veiligheid en Justitie 2014, p. 26 (aangeboden aan de Tweede Kamer bij brief van 20 mei 2015, Kamerstukken II, 2014-2015, 34200 VI, nr. 2.

CONTOUREN

strafrecht

Het strafrecht is een van de middelen die de overheid ter beschikking staan om namens de samenleving te reageren op criminaliteit.[4] Om draagvlak in de samenleving te behouden en eigenrichting door burgers te voorkomen, dient de strafrechtspleging doeltreffend en rechtmatig te functioneren. De samenleving moet erop kunnen vertrouwen dat criminaliteit effectief wordt bestreden en dat tegelijkertijd de fundamentele rechten van burgers worden gerespecteerd. Daarnaast moet de samenleving erop kunnen vertrouwen dat het hiervoor ingezette belastinggeld efficiënt wordt besteed. Deze doelen brengen bepaalde verantwoordelijkheden met zich ten aanzien van de effectiviteit, zorgvuldigheid en efficiëntie van de strafrechtspleging (met inbegrip van de informatievoorziening).

strafrechtsketen

De strafrechtspleging omvat het opsporen, vervolgen en berechten van verdachten van strafbare feiten en het tenuitvoerleggen van strafrechtelijke sancties. Re-integratie na een vrijheids-benemende sanctie is het "open einde" van het strafrecht. Het is een noodzakelijk onderdeel van de reactie op (ernstige) criminaliteit, maar "loopt het strafrecht uit" naar maatschappelijk werk, gezondheidszorg, zorg voor huisvesting, werk en inkomen, et cetera. De vijf genoemde stappen constitueren de "strafrechtsketen".[5] Zij omvatten op hun beurt talrijke deelprocessen, die worden uitgevoerd door functionarissen binnen een groot aantal organisaties. Deze organisaties werken in allerlei netwerken met elkaar en met partijen buiten de keten samen. De meeste hebben niet alleen taken in de strafrechtsketen, maar ook in andere ketens.
Digitalisering raakt de hele keten; dit geldt ook voor de digitalisering van de strafrechtspleging. Digitalisering brengt als zodanig geen wijziging in de bestaande strafvorderlijke taken, bevoegdheden en verantwoordelijkheden van functionarissen en/of organisaties. Wel brengt zij wijziging in bestaande werkwijzen, routines en procedures. Daarnaast is het zo dat de "disruptieve kracht van digitale technologieën" onze maatschappij niet alleen tal van kansen biedt, maar ook nieuwe bedreigingen en maatschappelijke vraagstukken oplevert.[6] Dat geldt ook voor de strafrechtsketen. In bijlage 2 wordt getracht een aantal potentiële bedreigingen te duiden.

kernbegrippen: zaak - persoon, maatwerk - standaard

De strafrechtsketen werkt vanouds vooral zaakgericht. De weg waarlangs een zaak wordt afgehandeld, is principieel onvoorspelbaar. De functionarissen binnen het strafrechtelijk systeem zijn professionals en beschikken dikwijls over discretionaire bevoegdheden. Achteraf kan weliswaar worden vastgesteld dat 80% "standaard" is, maar voor een concrete zaak is vooraf nooit volstrekt zeker wat het verloop zal zijn.
Die "zaak" is een meerduidig begrip. Binnen één strafrechtelijk traject spelen zich allerlei deel-processen af, soms opeenvolgend, soms gelijktijdig (parallel). Voor de onderscheiden partijen in de

[4] Vgl. prof. mr Ybo Buruma: Veiligheid door repressie: emotie of verstand? WODC-lezing 2003. (http://www.wodc.nl/onderzoeksdatabase/ov-200301-veiligheid-door-repressie.aspx)
[5] Zie bijlage 3 voor een nadere uitleg van de strafrechtsketen.
[6] Met "disruptieve kracht" van ICT wordt gedoeld op het verschijnsel dat de toepassing van ICT markt- en/of arbeidsverhoudingen ingrijpend en blijvend kan doen wijzigen. Dit kan ook de juridische advisering en/of dienstverlening raken.

keten vormen die deelprocessen hun "zaak", i.e. hun bijdrage aan het traject. Hetzelfde geldt in de fase van "pre-opsporing" (fenomeenonderzoek, verkennend onderzoek e.d.) en voor het strafrechtelijk financieel onderzoek.
Naast de traditionele zaakgerichte aanpak heeft sinds het begin van deze eeuw de persoonsgerichte aanpak zijn plek opgeëist, niet alleen binnen de keten, maar in toenemende mate ook over de grenzen van ketens heen. Welke aanpak in een concreet geval gevolgd wordt, hangt onder meer af van beleidsregels en van de invulling die functionarissen geven aan hun rollen. In deze, het strafrecht overstijgende, benadering komt het zwaartepunt meer en meer te liggen bij het bestuur (de gemeente).

informatie
Strafrechtstoepassing bestaat voor het grootste deel uit het verwerken van informatie. "Verwerken" omvat verzamelen, vastleggen, verrijken, beoordelen, gebruiken, ontvangen, verstrekken, beheren, etc.; en ook "verwijderen" en "vernietigen" van gegevens zijn vormen van "verwerken". Informatie is de basis van alle strafrechtelijke beslissingen en handelingen. "Informatie" kan bestaan uit data, documenten, dossiers, audiovisuele media, etc. ("information is anything that can be digitized")[7]. De informatie die door een ketenpartij wordt gegenereerd (haar "output"), is vaak het startpunt (de "input") voor de activiteiten in een volgende fase van het traject.
De informatie moet, voor zover mogelijk, betrouwbaar, authentiek en volledig zijn.[8] "Betrouwbaar" wil zeggen dat de informatie een getrouwe weergave is van de activiteiten of feiten die hebben plaatsgevonden. "Authentiek" wil zeggen dat kan worden vastgesteld (dat de informatie nog is zoals die oorspronkelijk was en) wie deze heeft gecreëerd of verzonden. "Volledig" wil zeggen dat de informatie nog compleet en ongewijzigd is; dit laatste wordt ook wel aangeduid als de eis dat de informatie "integer" moet zijn. De informatiehuishouding moet voorts de professional in staat stellen te selecteren wat als "standaardzaak" kan worden afgedaan en waar "maatwerk" nodig is. Daarvoor heeft hij (meer of minder summiere) informatie nodig over de persoon en de context.
Binnen de grenzen van de regelgeving moet informatie ook voor anderen dan de opsteller toegankelijk zijn. Strafrechtelijke informatie is echter gevoelige informatie. Zij is immers de basis voor de toepassing van ingrijpende bevoegdheden, zelfs tot en met vrijheidsbeneming (detentie). Daarom is de vraag hoe we informatieposities reguleren van belang voor de kwaliteit van onze rechtsstaat.[9]
Behalve de professionals hebben ook verdachten, slachtoffers, benadeelden, advocaten, omwonenden, bestuurders, beleidmakers en politici. informatie nodig om hun rechten te kunnen effectueren, plannen te maken, beslissingen te nemen, verantwoording af te leggen, prestaties te beoordelen, etc. Tegelijkertijd mag er echter niet méér gevoelige informatie over personen worden verspreid ("verwerkt") dan de regelgeving toestaat. De informatiehuishouding dient beide belangen te waarborgen. Uiteindelijk lost de hele omgang met informatie zich op in taken, bevoegdheden en verantwoordelijkheden.

[7] Carl Shapiro en Hal R. Varian: Information Rules. A Strategic Guide to the Network Economy. p. 3.
[8] Brief van de staatssecretaris van Onderwijs, Cultuur en Wetenschap en de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties van 29 juni 2006, Kamerstukken II, 2005-2006, 29362 nr. 101 (Kabinetsvisie informatie op orde), p. 2.
[9] Aernout H.J. Schmidt: Bedreigen computers ons rechtssysteem? Oratie Leiden (2004), p. 21.

digitaal

Alle informatieproducten[10] worden in digitale vorm gegenereerd ("digital born") en vervolgens volledig digitaal verwerkt, uitgewisseld, opgeslagen, beheerd en uiteindelijk na afloop van de wettelijke bewaartermijn vernietigd. Inbeslaggenomen bewijsmateriaal wordt voor zover mogelijk eveneens gedigitaliseerd. Bijzondere aandacht wordt gegeven aan de eis van digitale duurzaamheid, onder meer voor het bewaren van veilig gestelde digitale of gedigitaliseerde sporen.[11] Transacties[12] c.q. proceshandelingen worden digitaal verricht. Rechtspersonen en juridische professionals, zoals advocaten, communiceren uitsluitend nog digitaal met de strafrechtelijke overheid, bijvoorbeeld waar het gaat om het indienen van stukken of het doen van verzoeken. (In geval van een zitting, verhoor of vergelijkbare situatie waarin een advocaat of een vertegenwoordiger van de rechtspersoon - al dan niet digitaal, bijvoorbeeld via telehoren of videoconferencing - vis-à-vis contact heeft met een strafrechtelijke functionaris, kan hij nog steeds ook mondeling verzoeken indienen.) Ook natuurlijke personen die niet handelen vanuit een bedrijf of namens een rechtspersoon communiceren digitaal met de strafrechtelijke overheid, tenzij zij geen gebruik kunnen of willen maken van de digitale mogelijkheden ("digital first"). Dit geldt zowel voor verdachten en veroordeelden als voor andere betrokkenen, zoals getuigen, slachtoffers, benadeelden, aangevers van strafbare feiten: zij halen en brengen hun informatie (tekst, geluid, beeld) als regel digitaal. De informatiehuishouding ondersteunt de verwerking van alle[13] zaakstromen, van eenvoudig tot complex. Zij ondersteunt ook de persoonsgerichte aanpak c.q. het persoonsgericht werken, zowel binnen de keten als over haar grenzen heen, alsook de aanpak van (criminele) groepen.

menselijke maat[14]

"Technology is a useful servant but a dangerous master."[15] In de digitalisering van de strafrechts-pleging blijft de burger degene waar het ten slotte om gaat. De zeggenschap van burgers (en vooral van verdachten en veroordeelden) over de strafrechtelijke informatie die hen betreft, is echter noodzakelijkerwijs beperkt. Om de naleving van de privacy te bevorderen, worden nieuwe systemen ontworpen en gebouwd volgens het principe van "privacy by design". Vóór de introductie van nieuwe regels of systemen wordt een privacy impact assessment uitgevoerd. Beveiliging van de strafrechtelijke gegevens en informatiestromen voldoet aan hoge eisen, mede ter voorkoming van ongewenste beïnvloeding van de uitkomst van het strafgeding (bijvoorbeeld via cybercrime).

---

[10] Zie bijlage 5 voor een nadere uitleg van de term "informatieproduct".

[11] De "chain of evidence" vertelt waar het digitale opsporingsmateriaal is geweest en wat er mee is gebeurd.

[12] De term "transactie" wordt hier niet gebruikt in de juridische betekenis (een vorm van buitengerechtelijke afdoening van een strafzaak), maar in de informatiekundige betekenis (het aangaan van overeenkomsten of het geven en/of ontvangen van opdrachten via computers; bijvoorbeeld: het kopen van een product via internet, of het online boeken van een verblijf in een hotel).

[13] Om redenen van efficiëntie kan het wijs zijn niet te streven naar "100% automatiseren", maar - conform de "80/20 regel" - tevreden te zijn met 80%. Uitzonderingen laten zich immers moeilijk automatiseren.

[14] Vgl. Raad voor het openbaar bestuur: Van wie is deze hond? Politieke sturing op dienstverlening en ICT (2013).

[15] De uitspraak wordt toegeschreven aan Noorse Nobelprijswinnaar Christian Lous Lange; zie http://ebookfriendly.com/best-technology-quotes/ (geraadpleegd 1 december 2015).

De "menselijke maat" geldt ook voor de professional. De digitale werkomgeving en de daarin ondergebrachte informatiesystemen zijn afgestemd op de gebruikers en niet andersom. Zij bieden een optimale gebruikerservaring.[16]

strategische uitgangspunten

"Digitalisering" en "digitaal werken" dragen bij aan het realiseren van verbeterdoelen, zoals het verhogen van efficiëntie en effectiviteit, het waarborgen van kwaliteit en legitimiteit, het vergroten van omgevingsgerichtheid en transparantie en het genereren van betrouwbare informatie over (de prestaties van) de keten. De digitalisering vergt een evenwichtig samenstel van maatregelen op het gebied van regelgeving, organisatie en techniek. Rechtsstatelijke en strafvorderlijke waarden en beginselen blijven gewaarborgd. Verschillende wetgevingscomplexen, zoals het Wetboek van Strafvordering, de Wet bescherming persoonsgegevens, de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens, zijn - met inachtneming van de strafvorderlijke taken, bevoegdheden en verantwoordelijkheden van functionarissen en organisaties - in samenhang bezien en aangepast om een bruikbaar fundament onder digitaal werken te vormen.[17]

BOUWSTENEN

bereikbaarheid

Alle benodigde informatie is digitaal beschikbaar en met slechts enkele simpele handelingen bereikbaar. Daarbij doet het er niet toe van welk apparaat de functionaris zich bedient, noch waar hij zich bevindt of wanneer hij de informatie zoekt ("any place, any time, any device"; APATAD). Wel kan het zo zijn dat bijvoorbeeld uit oogpunt van beveiliging op apparatuur die buiten het kantoor wordt gebruikt niet alle informatie beschikbaar is die vanaf werkplekken op kantoor te bereiken is.

eenmalige opslag, meervoudig gebruik

Informatieproducten (data, documenten, dossiers) worden in beginsel eenmalig ingevoerd en technisch op één plaats opgeslagen en onderhouden, maar kunnen meervoudig worden gebruikt. Deze informatieproducten worden idealiter "bij de bron beheerd". De bron is diegene die verantwoordelijk is voor de primaire vastlegging van het informatieproduct. Wie een informatie-product nodig heeft, kan het - indien hij daartoe gerechtigd is - bij de bron inzien, raadplegen en eventueel ook ophalen. Heen en weer sturen van documenten, ze kopiëren en die kopieën vervolgens op diverse plaatsen opslaan (bewaren) is overbodig en in beginsel ook onwenselijk. De overdracht van een "zaak" vereist op technisch niveau niet langer het toezenden van een document of een dossier, maar kan worden geëffectueerd door het verzenden van een signalering of een link naar een zaak, dossier of stuk. Als de ontvanger van dat bericht het informatieproduct van de ander downloadt, is dat alleen voor de duur van het eigen gebruik; daarna wordt het vernietigd volgens de regels die daarvoor gelden.

De techniek die gebruikt wordt, brengt echter geen verandering in de verantwoordelijkheden. Die verantwoordelijkheden zijn immers gekoppeld aan het "verwerken" van gegevens in de betekenis die

[16] Een ander aspect van de "menselijke maat", nl. de vraag in welke fasen van de strafrechtsketen voor welke beslismomenten, gegeven de voortschrijdende digitalisering, menselijke tussenkomst nodig is en blijft, komt aan de orde in bijlage 2.

[17] Zie ook de brief van de minister van Veiligheid en Justitie van 23 juni 2014, Kamerstukken II, 2013-2014, 33842, nr. 2 (beleidsreactie evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens), p. 3.

de Wet bescherming persoonsgegevens daaraan geeft. Ook reeds het enkele "inzien" of "raadplegen" zijn juridisch bezien vormen van "verwerken van persoonsgegevens". Het beginsel van eenmalige opslag, meervoudig gebruik kan betekenen dat de verantwoordelijkheid voor het beheer (bewaren, verstrekken, onderhouden, vernietigen, etc.) van een bepaalde hoeveelheid informatie of informatieproducten overgaat van de ene partij op de andere. Die verantwoordelijkheid kan zelfs bij meer dan één partij tegelijk komen te liggen.

voorzieningen voor het delen van informatie

Het uitgangspunt van "eenmalige opslag" betekent níet dat alle informatie ook in één centraal systeem moet of zal worden opgeslagen. De ketenorganisaties zijn in beginsel verantwoordelijk, en daarmee vrij, om te beslissen hoe zij de informatieproducten waarvan zij “de bron” zijn, beheren. Deze vrijheid is begrensd door o.a. de voorschriften en eisen inzake beveiliging van data en datacommunicatie. Voor zover dat noodzakelijk is voor de consistentie en samenhang binnen de keten en met andere ketens, wordt een beperkte set van gegevens opgenomen in gemeenschappelijke, centraal beheerde gegevensverzamelingen. Dit betreft met name de identiteitsgegevens betreffende verdachten en veroordeelden, de antecedenten (justitiële documentatie) en de verwijzingen (informatie over de status van een zaak of incident).
Meervoudig gebruik van informatie brengt mee dat functionarissen toegang moeten hebben tot informatie die "in de bron" – dus mogelijk bij andere partijen - aanwezig is. Sommige informatie-systemen van ketenorganisaties bevatten dus informatie die ook toegankelijk moet zijn voor andere partijen die aan dezelfde zaak werken ("tweeden")[18]. De desbetreffende informatiesystemen moeten daarom voldoen aan een gemeenschappelijk opgestelde set van eisen ten aanzien van betrouwbaar-heid, kwaliteit (van de gegevens), beschikbaarheid ("performance"), toegang en toegankelijkheid, beveiliging, beheer, transparantie ("chain of custody"), organisatie en inrichting van het toezicht. De informatie die wordt uitgewisseld en de relaties tussen de informatieobjecten, zijn beschreven in het Canoniek Datamodel (CDM) van de strafrechtsketen. Dit CDM is de basis van het gegevens-woordenboek voor de keten.
De voorzieningen (systemen, applicaties) voor het delen van informatie bieden functionaliteit voor bevragen, wijzigen (muteren; alleen voor daartoe bevoegde afnemers), abonneren op bepaalde gegevens of soorten gegevens (om actief te worden geïnformeerd over nieuwe of gewijzigde gegevens van bijvoorbeeld een subject) en terugmelden (indien bij een afnemer een vermoeden bestaat dat geregistreerde gegevens onjuist of onvolledig zijn).

regelgeving

De wet – dus niet degene aan wie informatie wordt gevraagd – bepaalt wie kennis mag nemen van een gegeven of document.[19] Iedere partij in de keten is zelf verantwoordelijk voor de naleving van de regelgeving inzake de bescherming van persoonsgegevens. Dit geldt zowel voor het ontvangen (bevragen, raadplegen, etc.) als voor het verstrekken van informatie. De eenduidige toepassing van

[18] "Tweeden" zijn actoren of instanties die werken aan dezelfde zaak en/of met dezelfde verdachte of veroordeelde. "Derden" zijn alle overige actoren of instanties aan wie gegevens worden verstrekt of met wie informatie wordt uitgewisseld. Voor beide categorieën gelden in beginsel dezelfde regels voor het verwerken van persoonsgegevens.

[19] Cf. brief van de minister van Veiligheid en Justitie van 23 juni 2014, Kamerstukken II, 2013-2014, 33842, nr. 2 (beleidsreactie evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens), p. 4.

die regels, die rekening houdt met en recht doet aan de bijzondere kenmerken van de keten en met de eisen van beveiliging, is geborgd in een stelsel van afspraken op ketenniveau.

toegang en toegankelijkheid

De toegankelijkheid en de regeling van de kennisneming c.q. verstrekking zijn geborgd in systemen en processen. Zij worden gefaciliteerd via een of meer voorzieningen die een gestelde vraag geleiden naar de bronnen van de informatie en de daar opgehaalde informatie in samenhang presenteren ("assembleren") aan degene die om de informatie heeft gevraagd. Daarbij wordt tevens - voor zover mogelijk digitaal - getoetst of aan de regels voor kennisneming c.q. verstrekking van die gegevens is voldaan. De mechanismen die daarvoor nodig zijn, zijn eenduidig ingericht op basis van ketenbrede afspraken ("AAA": authenticatie, autorisatie en accountability).[20] Dit betreft zowel de toegang voor functionarissen binnen (en buiten) de strafrechtspleging, als de toegang voor advocaten en burgers, bijvoorbeeld in de hoedanigheid van verdachte, veroordeelde, aangever, getuige, slachtoffer, benadeelde, belanghebbende, ouder of voogd van een minderjarige verdachte, vertegenwoordiger van de verdachte rechtspersoon. De toegang wordt conform de geldende regelgeving onder meer bepaald door de noodzaak van kennisneming van de gevraagde informatie. Het "noodzaak"-vereiste wordt geoperationaliseerd door bijvoorbeeld de toegang tot informatie te beperken tot een nader te bepalen aantal functionarissen binnen een organisatie, of te binden aan de eis dat informatie alleen wordt verstrekt aan een functionaris die betrokken is bij de behandeling van de zaak. Geborgd is dat bijvoorbeeld de gegevens van het slachtoffer en het strafdossier ontvlochten kunnen worden, opdat een psychologisch rapport over het slachtoffer niet zo maar in het strafdossier belandt. Aan de kant van de data kan de toegang worden beperkt door gegevens te classificeren.

origineel en kopie

Technisch is er in een digitale omgeving geen onderscheid meer te maken[21] tussen origineel en kopie; maar uit oogpunt van bevoegdheden en verantwoordelijkheden blijft het onderscheid van belang. Wat in de digitale omgeving heeft te gelden als "origineel" en wat als "kopie" is een kwestie van afspraken. Partijen kunnen ervoor kiezen de door hen opgestelde informatieproducten zelf te beheren en te bewaren, dan wel technisch onder te brengen in een, al dan niet gemeenschappelijk, depot of bij een Trusted Third Party (en dan te verwijderen uit hun eigen systemen); dit brengt evenwel geen verandering in de (juridische) verantwoordelijkheid voor het informatieproduct, tenzij dat uitdrukkelijk is geregeld bij de overdracht aan het depot. Creatie van een "depot" brengt ook geen verandering in de rechten en verplichtingen rond verstrekken of kennisnemen van gegevens. Het is dus níet een bak waar iedereen maar in kan graaien. Om data, documenten en dossiers terug te kunnen vinden, worden daaraan metadata toegevoegd volgens ketenbrede afspraken. Voor informatieproducten die nog wel (mogen) worden gewijzigd c.q. die opgevolgd (kunnen) worden door nieuwere versies, is het versiebeheer ketenbreed en uniform geregeld. Doordat in een volledig digitale omgeving het reproduceren en verspreiden van informatie en informatieproducten steeds

[20] "Authenticatie" betreft de procedure om met behulp van technische middelen de – geclaimde – identiteit van de afzender van een elektronisch bericht, en de integriteit van het bericht (is het na verzending gewijzigd?), vast te stellen en/of te verifiëren. "Autorisatie" betreft de procedure om de – geclaimde – bevoegdheid van de afzender van een elektronisch bericht vast te stellen en/of te verifiëren. Zo'n elektronisch bericht kan een vraag om informatie zijn. "Accountability" betreft het afleggen van verantwoording over het gebruik van gegevens, bijvoorbeeld door het inrichten van logging van en het toezicht op het verwerken en het gebruik van de gegevens.

[21] Tenzij daartoe speciale voorzieningen worden getroffen ("digital rights management").

eenvoudiger wordt, wordt ook het risico van ongeoorloofde verspreiding en te lang c.q. ongeoorloofd bewaren, navenant groter. Er zijn daarom voorzieningen om dat tegen te gaan, op organisatorisch vlak (o.a. procedures) en zo nodig ook op technisch vlak.[22]

digitaal samenwerken

Digitale samenwerkingsvoorzieningen bieden de mogelijkheid om, al dan niet op afstand, informatie en informatieproducten met elkaar te delen en er desgewenst gelijktijdig aan te werken. Participanten in die samenwerking kunnen dezelfde informatie inzien, alsook gebruik maken van videoconferencing en social groupware. Dit geldt binnen de keten én in de samenwerking met (professionals uit) andere ketens. Er wordt, binnen de grenzen van de regelgeving, maximaal (her)gebruik gemaakt van reeds elders aanwezige informatie, binnen of buiten het strafrechtelijk systeem.

eenduidige identificatie

Essentiële informatieobjecten in de strafrechtspleging zijn (1) het individu, i.e. de persoon van de verdachte of veroordeelde, (2) het incident dat aanleiding heeft gegeven tot de strafzaak, (3) de interventie, i.e. de opgelegde sanctie(s), en (4) het inbeslaggenomen bewijsmateriaal. Deze worden, mét hun onderlinge relaties, eenduidig en uniek geïdentificeerd en kunnen door alle betrokkenen worden gevolgd c.q. teruggevonden door heel de keten heen. Individuen kunnen voor zover nodig over de diverse ketens heen worden geïdentificeerd, bijvoorbeeld in het geval van verdachte vreemdelingen. Inbeslaggenomen voorwerpen worden digitaal gemerkt (geïdentificeerd), zodat ook die kunnen worden gevolgd in hun gang door het ketenproces en de "chain of custody" wordt gewaarborgd.

De unieke en eenduidige identificatie van het *incident* vanaf de start van het traject tot en met het einde dient drie belangen.

- Ten eerste wordt zij gebruikt om de individuele zaak door de keten heen te (kunnen) sturen (ketenlogistiek), zodat er geen zaken meer tussen wal en schip vallen.
- In de tweede plaats is een dergelijke identificatie de basis voor "tracking & tracing", d.w.z. het (kunnen) volgen van de zaak door heel de keten heen. Dit is van belang voor de functionaris, bijvoorbeeld een opsporingsambtenaar die wil weten welk gevolg een door hem opgemaakt proces-verbaal krijgt, maar ook voor de aangever, het slachtoffer en de verdachte en diens raadsman, die willen weten hoe ver de behandeling van "hun" zaak is gevorderd.
- In de derde plaats wordt zij gebruikt om de prestaties van de strafrechtsketen te verantwoorden en de effecten daarvan te beoordelen.[23]

Behalve de vier genoemde informatieobjecten worden ook de functionarissen en hun relaties tot de "zaak" eenduidig en uniek geïdentificeerd en geregistreerd.

veiligheid en rechtmatigheid

De veiligheid en de rechtmatigheid van het gegevensverkeer zijn gewaarborgd. Alleen bevoegde gebruikers krijgen, na identificatie, authenticatie en autorisatie,[24] toegang tot gegevens of systemen.

[22] In de technische sfeer kan worden gedacht aan het blokkeren van het maken van kopieën ("downloaden") of het na verloop van tijd automatisch vernietigen van kopieën.

[23] Het eerste en het derde hier genoemde belang zijn geadresseerd in het rapport van de Algemene Rekenkamer over prestaties in de strafrechtsketen (Kamerstukken II, 2011-2012, 33173, nr. 2).

Toegang is niet alleen gekoppeld aan iemands functie, maar waar mogelijk ook aan diens betrokkenheid bij een strafrechtelijk relevante persoon, zaak, incident (gebeurtenis), voorwerp of plaats. Een geautomatiseerde vraag om gegevens wordt geautomatiseerd getoetst aan de regelgeving ("rule based access control"). Identificatie, authenticatie en autorisatie worden grotendeels aan de kant van de vragende partij geregeld. Daarover zijn ketenbrede eisen geformuleerd - en in afspraken vastgelegd - uit oogpunt van kwaliteit, beheer en onderhoud, transparantie en toezicht op de naleving van de eisen. De kennisneming en verstrekking van gegevens worden gelogd. Deze loggegevens worden gebruikt om achteraf toezicht te houden op de naleving van de regels.

stelsel van ketenbrede afspraken

In een stelsel van ketenbrede afspraken zijn - met inachtneming van de wettelijk verankerde posities van de onderscheiden partijen in de keten - al die onderwerpen geregeld die niet bij wet geregeld hoeven te worden. Behalve op de hiervoor al genoemde onderwerpen hebben deze afspraken betrekking op de kwaliteit van gegevens, de aansluiting op het stelsel van basisregistraties, de inrichting en het gebruik van gemeenschappelijke voorzieningen (onder meer voor het waarmerken, tekenen en valideren van digitale documenten), standaarden (onder meer ten aanzien van biometrie), definities, referentiegegevens, de inrichting en het gebruik van portals, de identificatie en authenticatie van medewerkers in het stelsel van federatieve authenticatie, de beveiliging, het toezicht op het rechtmatig gebruik van gegevens door de functionarissen (medewerkers van de betrokken organisaties), het toezicht op de naleving van de ketenafspraken (standaarden) door de organisaties, en op het beheer en onderhoud zowel van de afzonderlijke afspraken als van het stelsel als geheel.

Er is een voorziening - binnen de keten of op het niveau van het hele domein van Veiligheid en Justitie - om discussies over de inrichting, ontwikkeling en het beheer van het informatiestelsel als geheel (het "digitale ecosysteem") te beslechten en daarover beslissingen te nemen. Dit betreft bijvoorbeeld de wijze van toegang tot bronnen, de betekenis van gegevens (definities), technische standaarden, de kwaliteit van informatie. Voor de feitelijke kwaliteit van de data en voor het toezicht op de kwaliteit en het gebruik van gegevens blijven de ketenorganisaties zelf verantwoordelijk.

naar een strategisch plan

Op deze visie moet een strategie volgen. Kern daarvan is het bepalen hoe de overgang van de huidige, nog grotendeels op papier gebaseerde werkwijze, met heel de daarbij behorende "legacy" aan processen, procedures en systemen, naar de volledig digitale werkwijze moet verlopen; beheerst, stapsgewijs, met betrokkenheid van de gebruikers[25] en met inachtneming van de rechtsstatelijke waarden en de constitutionele "checks and balances". In zo'n strategisch plan moeten ten minste de volgende aspecten aan de orde komen:

- "I-governance": dit is het geheel van taken, verantwoordelijkheden en bevoegdheden ten aanzien van de verwerking van informatie. Het omvat een stelsel van afspraken dat beoogt een klimaat te scheppen waarin gewenst gedrag inzake de omgang met informatie wordt bevorderd. Onderdeel van dit stelsel is een raamwerk voor het afleggen van verantwoording.

[24] "Authenticatie" en "autorisatie" zijn hiervóór al gedefinieerd. "Identificatie" betreft de initiële vaststelling van de identiteit van een persoon, bijvoorbeeld van een medewerker op het moment van indiensttreding bij een organisatie.

[25] Cf. Irene Tiepel, Frank Kist en Henri Pieters: Digitalisering rechtspraak kan alleen agile. http://ibestuur.nl/podium/digitalisering-rechtspraak-kan-alleen-agile.

I-governance omvat processen, rollen, normen, standaarden, indicatoren en meetpunten. Bij de afronding van het programma Versterking prestaties strafrechtketen wordt een breed, permanent Bestuurlijk Strafrechtketenberaad in het leven geroepen, waar afspraken worden gemaakt tussen de minister en de ketenorganisaties over de samenwerking en de prestaties. Onder de regie van dat Beraad wordt een proces ingericht met de daarbij behorende taken en verantwoordelijkheden om tot een effectieve coördinatie op de keteninformatisering te komen.[26] Daarmee is de noodzakelijke bestuurlijke randvoorwaarde voor de ontwikkeling van een strategie gecreëerd.

- Architectuur: het formuleren en (doen) toepassen van de principes die richting geven aan het ontwerp en de ontwikkeling van de "digitale" strafrechtsketen en van de afzonderlijke voorzieningen daarbinnen. Dit omvat een nadere uitwerking van de strafrechtspleging als gecompliceerd samenspel van mens, proces, organisatie en techniek. In die uitwerking worden de gevolgen van digitalisering inzichtelijk gemaakt zowel voor de werkprocessen als voor de interactie met de samenleving.
- Programmering van inspanningen: het verder ontwerpen en ontwikkelen van de strafrechts-pleging vereist een portfolio aan inspanningen, gericht op het in samenhang veranderen van regelgeving, organisatie (cultuur, processen en structuren) en techniek (o.a. ontwikkelen van systemen).
- Stellen van nieuwe (ethische) grenzen. Digitalisering zal nieuwe mogelijkheden creëren in de toepassing van het strafrecht. Deze nieuwe mogelijkheden zullen, voorafgaand aan hun toepassing, moeten worden beoordeeld door de juridische professie en de samenleving. Maar niet alles wat mogelijk is, hoeft te worden gerealiseerd alleen omdat het technisch kan.[27] Er zullen nieuwe grenzen gesteld moeten worden aan het gebruik van hetgeen technisch mogelijk wordt (of al is). Als voorbeelden (niet beperkt tot het strafrecht) kunnen hier gelden: het steeds eenvoudiger kunnen verzamelen en combineren van data ('big data')[28], het anoniem kunnen melden van misdaad via internet[29], of de komst van de "zelfrijdende auto".[30]

Samenvatting

De strafrechtspleging digitaliseert. Digitalisering als "disruptive technology" biedt kansen en brengt bedreigingen met zich mee. Om de kansen optimaal te benutten en de bedreigingen zo goed mogelijk het hoofd te bieden, is een visie nodig op de betekenis van digitalisering voor de bedrijfsprocessen en voor het strafrechtelijk systeem als zodanig. In het bijzonder is aandacht nodig voor de samenhang tussen informatiesystemen, de betrouwbaarheid van informatie en de verantwoordelijkheid voor de vastlegging en het beheer van informatie. De samenhang tussen systemen moet zo worden georganiseerd dat de functionarissen (professionals) die informatie nodig hebben, op eenvoudige wijze daaraan kunnen komen, binnen de grenzen van wet- en

[26] Zie het "Besluit Duurzame samenwerking in de strafrechtketen. Besluit Stuurgroep VPS betreffende de beëindiging van het programma Versterking Prestaties Strafrechtketen en voortzetting van de duurzame samenwerking in de strafrechtketen" van 26 oktober 2015.

[27] Cf. Jaap-Henk Hoekman, Bert-Jaap Koops, Wouter Lueks: Anoniem misdaad melden via internet. In: Nederlands Juristenblad 2015, p. 3063.

[28] Vgl. Corien Prins: Big Data en de rechterlijke macht. In: Nederlands Juristenblad 2015, p. 2087.

[29] Vgl. het hiervóór genoemde artikel van Hoekman, Koops en Luek.

[30] Vgl. Kees de Vey Mestdagh en Jeroen Lubbers: 'Nee hoor, u wilt helemaal niet naar Den Haag…' Over de techniek, het recht en de toekomst van de zelfrijdende auto. In: Ars Aequi 2015 (april), p. 267 e.v.

regelgeving. Technisch is op dit gebied al heel veel mogelijk. Deze technieken betreffen de wijze van opslag en beheer van gegevens, de wijze waarop organisaties en systemen communiceren (interoperabiliteit)[31], de kwaliteit en betrouwbaarheid van informatie, de bereikbaarheid van gegevens en de manier waarop toegang wordt gegeven tot gegevens en gegevensverzamelingen, de mechanismen om te bewaken dat bij het verwerken van gegevens de regelgeving in acht wordt genomen, het beheer van gegevens gedurende hun gehele levenscyclus (vanaf de verwerving tot en met het vernietigen), de beveiliging en het toezicht op het rechtmatig gebruik van gegevens. Een goede absorptie van digitalisering in de strafrechtspleging vergt een coherent geheel van maatregelen ten aanzien van regelgeving, organisatie en techniek. Het aspect "organisatie" heeft in dit verband zowel betrekking op de afzonderlijke ketenpartijen (qua inrichting, processen, werkwijzen, cultuur, personeelsbeleid) als op de keten als geheel. Inzet van nieuwe digitale technieken brengt niet per se verandering in strafvorderlijke taken, bevoegdheden en verantwoordelijkheden. Het laat ook de verantwoordelijkheden voor de verwerking van informatie en voor de informatiesystemen onverlet. Wel vergt het nauwkeurige afspraken over de toedeling van die verantwoordelijkheden. De constitutionele en wettelijke posities van de onderscheiden organisaties hebben daarbij te gelden als randvoorwaarden. Het geheel mondt uit in een stelsel van ketenbrede afspraken. Sluitstuk is een ketenbrede besturing ("I-governance"), die de afspraken beheert en de goede werking van het "digitale ecosysteem" faciliteert en bewaakt. Deze besturing creëert, met respect voor de relatieve autonomie van de betrokken organisaties, de mogelijkheid tot niet-vrijblijvende ketenbrede besluitvorming over vraagstukken die inter-organisatorische besluitvorming vereisen.

[31] Met de term "interoperabiliteit" wordt gedoeld op de mogelijkheid van verschillende autonome, heterogene systemen, apparaten of andere eenheden (bijvoorbeeld organisaties of landen) om met elkaar te communiceren en interacteren.

BIJLAGE 1:
ACHTERGROND

aanleiding tot en doel van deze notitie
De samenleving digitaliseert. Die ontwikkeling raakt alle onderdelen van het werk van de overheid; ook de strafrechtspleging. Papieren werkstromen en werkprocessen maken plaats voor digitale. De vraag is niet óf dat gaat gebeuren - het gebeurt al -, maar alleen in welk tempo en hoe. Dat tempo wordt niet - in elk geval niet alleen - door de strafrechtspleging bepaald. *Niet* digitaliseren is geen optie; de strafrechtspleging zou daarmee haar legitimiteit verliezen.

Digitalisering moet primair ten dienste staan van de professional door hem beter toe te rusten voor zijn kerntaak: het nemen van juiste en rechtvaardige beslissingen. Daarnaast maakt digitalisering het mogelijk om:

- het werk effectiever te doen en met minder administratieve rompslomp en snellere toegang tot relevante informatie,
- in de opsporing beter te sturen (genereren en gebruiken van sturingsinformatie, informatie-gestuurd politiewerk),
- nieuwe manieren van (samen-)werken te realiseren,
- andere betrokkenen, zoals de verdachte en diens raadsman, het slachtoffer of de benadeelde, beter te informeren over de voortgang van "hun" zaak,
- zaken door het ketenproces heen te volgen (zonder de betrokken functionarissen te belasten met extra, voor het primaire proces niet noodzakelijke administratieve handelingen), beter te sturen (ketenlogistiek) en daarmee te voorkomen dat zaken "tussen wal en schip vallen",
- beter verantwoording af te leggen aan de samenleving en de politiek over de geleverde prestaties (op systeemniveau), alsook om
- effectiever en efficiënter wetenschappelijk onderzoek naar criminaliteit en rechtshandhaving te doen.

Moderne technologie (ICT) schept echter niet alleen nieuwe kansen, maar brengt ook nieuwe bedreigingen mee. Om de digitalisering van de strafrechtspleging in goede banen te leiden, is daarom een visie nodig. Daarnaast brengt de veelheid van actoren in de strafrechtsketen het risico mee van een onwenselijke diversiteit aan oplossingen en daarmee versnippering van systemen, vermindering van effectiviteit en verspilling van creativiteit, energie, tijd en geld. Daarom is in aanvulling op de *visie* een ketenbrede *strategie* nodig voor de overgang naar digitaal werken in de strafrechtsketen. Bij de vertaling van de visie naar concrete projecten is een integrale adequate beheersing vereist, zoals het werken met een business case (uitschrijven van een zakelijke rechtvaardiging).

In haar rapport van 16 februari 2012 over prestaties in de strafrechtsketen heeft de Algemene Rekenkamer aanbevolen een "informatiestrategie" te ontwikkelen voor de strafrechtsketen.[32] Tijdens het Algemeen Overleg van 4 november 2015 over een aantal strafrechtelijke onderwerpen heb ik

[32] Algemene Rekenkamer: Prestaties in de strafrechtsketen. Kamerstukken II, 2011-2012, 33173, nr. 2, p. 29.

toegezegd een visie op de informatievoorziening in de strafrechtsketen op te stellen.[33] In het bredere kader van het programma VPS (Versterking prestaties strafrechtsketen) wordt invulling en opvolging gegeven aan de uiteenlopende aanbevelingen van de Rekenkamer. Digitalisering is een onderdeel daarvan. Dit omvat twee sporen: het realiseren van de digitale uitwisseling van stukken tussen politie, openbaar ministerie en rechtspraak in 2016, en het opstellen van een visie op het vervolg.[34] De digitale uitwisseling van processtukken vormt een eerste stap in het volledig digitaal werken in de strafrechtketen. Met het onderhavige visiedocument wordt het tweede spoor ingevuld. In haar rapport van het verantwoordingsonderzoek 2014 bij het ministerie van Veiligheid en Justitie heeft de Rekenkamer aangegeven dat de door haar bedoelde informatiestrategie een visie zou moeten bevatten "op de afstemming van verschillende systemen, de betrouwbaarheid van informatie en de verantwoordelijkheid voor de vastlegging en het beheer van informatie."[35] In de onderhavige notitie wordt daar invulling aan gegeven. Deze invulling past binnen en geeft uitvoering aan de Enterprise Architectuur en de "Gouden Regels" van het ministerie van Veiligheid en Justitie. Zij is ook afgestemd met de vreemdelingenketen.

Deze notitie schetst de visie. Enkele elementen van deze visie zijn al in twee eerdere brieven al kort en schetsmatig benoemd.[36] De inhoud van deze notitie is op bestuurlijk niveau afgestemd met de betrokken organisaties in de keten. Daarnaast wordt permanent het gesprek met de professionals gezocht teneinde te waarborgen dat de visie recht doet aan de kenmerken en eisen van het primaire proces en aansluit bij de inzichten en behoeften van de professionals.

leeswijzer

De visie beoogt vanuit twee perspectieven tegelijk een beeld te schetsen van de digitalisering van de strafrechtspleging. Het ene perspectief betreft het primaire proces, i.e. de strafrechtspleging (de behoefte aan informatie), het andere de informatietechnologie (de manier waarop informatie beschikbaar wordt gesteld en beheerd); het primaire proces genereert de vraag naar informatie, de technologie faciliteert het aanbod. Achtergronden worden in de bijlagen gegeven.

- Bijlage 2 bakent de visie af en beschrijft een aantal uitgangspunten en randvoorwaarden.
- Bijlage 3 schetst enkele fundamentele kenmerken van de strafrechtsketen in relatie tot informatieverwerking.
- Bijlage 4 schetst een aantal technologische trends en ontwikkelingen.
- Bijlage 5 definieert een aantal kernbegrippen binnen de (digitale) informatiehuishouding; eenheid van taal is immers essentieel in een veld dat zo complex is als de strafrechtspleging en waarop ook zoveel spelers actief zijn.

[33] Kamerstukken II, 2015-2016,29 279, nr. 294, p. 18, 35. Zie ook de toezegging van mijn ambtsvoorganger, Kamerstukken II, 2013-2014, 33942, nr. 9, p. 5 (Rapporten van de Algemene Rekenkamer bij de jaarverslagen 2013 en bij de Nationale verklaring 2014; lijst van vragen en antwoorden, vastgesteld 11 juni 2014).
[34] Vgl. o.m. de brief van de minister van Veiligheid en Justitie van 12 november 2013, Kamerstukken II, 2013-2014, 29279, nr. 178 (GPS in relatie tot VPS en KEI), p. 3-4.
[35] Algemene Rekenkamer: Resultaten verantwoordingsonderzoek bij het Ministerie van Veiligheid en Justitie 2014, 26 (aangeboden aan de Tweede Kamer bij brief van 20 mei 2015, Kamerstukken II, 2014-2015, 34200 VI, nr. 2.
[36] Zie de brief van 12 november 2013, Kamerstukken II, 2013-2014, 29279, nr. 178 (GPS in relatie tot VPS, DWS en KEI), p. 3-5; brief van 23 juni 2014, Kamerstukken II, 2013-2014, 33842, nr. 2 (beleidsreactie evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens), p. 2-5.

BIJLAGE 2:
AFBAKENING, UITGANGSPUNTEN EN RANDVOORWAARDEN MET BETREKKING TOT DE VISIE

afbakening (focus van de visie)
Digitalisering wordt in Nederland nog steeds te veel beschouwd als onderdeel van de ondersteuning, en niet van het primaire proces van rechtspraak c.q. van "zaken afdoen": het onderzoeken, beslissen, c.q. de opvolgende partner in de keten daartoe (adequaat) in de gelegenheid stellen.[37] Deze visie kiest het primaire proces als uitgangspunt. Centraal staat de informatiepositie van de professional. De informatie moet worden georganiseerd "om de professional heen". De informatiehuishouding moet hem in staat stellen zo snel mogelijk, maar in ieder geval binnen de voorgeschreven termijnen, de juiste beslissingen te nemen en daarover verantwoording af te leggen. De moderne digitale techniek moet hem helpen snel, eenvoudig, trefzeker en efficiënt aan de relevante informatie te komen die ergens in die keten dan wel elders in het domein van Veiligheid en Justitie - of nog breder: binnen de overheid[38] - al aanwezig is. Dat betreft dus vooral die informatie die tussen partijen in de keten, dan wel vanuit de keten met partijen daarbuiten[39], wordt uitgewisseld c.q. gedeeld. De techniek moet hem eveneens helpen zijn eigen bijdrage aan het ketenproces snel en efficiënt te leveren (gegevens invoeren, informatie verstrekken, berichten uitwisselen, etc.). Het regelen van de informatiepositie van de professional is de kern van de visie én de basis voor de overige functies die de informatievoorziening moet vervullen.
Digitalisering van de keten raakt de informatiesystemen van de afzonderlijke partijen in die keten: zij zullen moeten voldoen aan de eisen die vanuit het ketenperspectief worden gesteld, hetzij via regelgeving, hetzij in een stelsel van (bindende) afspraken.

uitgangspunten (bedreigingen, vraagstukken, waarborgen)
"De disruptieve kracht van digitale technologieën biedt onze maatschappij tal van kansen, maar levert ook nieuwe bedreigingen en maatschappelijke vraagstukken op".[40] Dat geldt ook voor de strafrechtspleging. Cybercrime is uiteraard een evidente bedreiging voor alle digitalisering. Cybercriminelen kunnen met aanvallen de digitale strafrechtspleging platleggen of zich toegang verschaffen tot de digitale informatie en dan bijvoorbeeld onbevoegd gegevens inzien, wijzigen of vernietigen. Fysieke nabijheid is daarvoor in het geheel niet nodig. De veiligheid van de gegevens en van het gegevensverkeer moet dus - voor zover mogelijk - gewaarborgd worden. Maar ook moet ervoor worden gewaakt dat digitalisering de rechtsstatelijke kwaliteit van het strafproces niet aantast. Waar mogelijk zou zij die kwaliteit juist moeten verhogen. Zo kan bijvoorbeeld de elektronische handtekening niet alleen de echtheid op het moment van ondertekenen (de authenticiteit van het document) garanderen, maar ook de echtheid ervan op een later tijdstip (de integriteit van het document, d.w.z. dat het na ondertekening niet gewijzigd is). Dat is winst, want de klassieke "natte" handtekening ziet alleen op de authenticiteit van een document. Digitalisering kan

[37] Aldus P.A.M. Mevis in Delikt en Delinkwent 2014, p. 584.
[38] Dit betreft zowel de Nederlandse overheid, bijvoorbeeld het stelsel van basisregistraties, als buitenlandse overheden met wie Nederland samenwerkt op strafrechtelijk gebied.
[39] Bijvoorbeeld: in casusoverleggen, Veiligheidshuizen, aan burgemeesters, gemeenten, zorgprofessionals.
[40] Bart Schermer: Digitalisering: kans of bedreiging voor wetgeving? In: Recht der Werkelijkheid 2015, p. 34.

ook de inzage in en kennisneming van een dossier vergemakkelijken, en helpen tegen het zoekraken van stukken.

Uitgangspunt van de visie is het bestaande strafrechtsproces (in termen van wettelijk toegedeelde taken, bevoegdheden en verantwoordelijkheden), met alle rechtsstatelijke en procedurele waarborgen die daarbij horen. Daarbij zal het evenwicht tussen de verschillende in geding zijnde belangen ook bij voortschrijdende digitalisering in stand gehouden moeten worden en waar nodig opnieuw moeten worden bepaald. Uitgangspunt is dat "de keuze voor de wijze van de automatisering niet waardevrij is, maar in dienst staat van de wet".[41]

- Het beginsel van "equality of arms" bijvoorbeeld vergt dat de informatie waarover het openbaar ministerie beschikt, in beginsel ook beschikbaar is voor de verdediging. Dit geldt ook voor digitale informatie. Veel informatie wordt in de opsporingsfase niet in processen-verbaal vastgelegd. In een digitale omgeving wordt het technisch eenvoudiger om alle digitaal vastgelegde informatie, zoals de stuurinformatie (de informatie op basis waarvan beslissingen worden genomen over de richting en inrichting van het onderzoek), beschikbaar en toegankelijk te maken voor de verdediging. Die toegankelijkheid moet - op gelijke voet als voor de officier - gewaarborgd zijn, zowel in het voorbereidend onderzoek als op de terechtzitting.
- Het beginsel van berechting op tegenspraak vergt dat de verdachte zich moet kunnen uitspreken over alle informatie die voor de beslissing van belang is of kan zijn. En het beginsel van interne openbaarheid belet de rechter aan zijn beslissing gegevens of informatie[42] ten grondslag te leggen die niet voor beide partijen, officier van justitie en verdachte, beschikbaar zijn geweest en/of waarover zij zich niet hebben kunnen uitlaten. De informatie dient voor beide partijen toegankelijk te zijn en met het oog op later gebruik en/of verantwoording gedurende zekere tijd te worden bewaard.[43] Dit is een functionele eis voor de inrichting van de (digitale) informatiehuishouding.
- Functionarissen in de strafrechtsketen beschikken veelal over discretionaire bevoegdheden (de opsporingsambtenaar "is bevoegd …", de officier van justitie "kan …", de rechter "kan …"), die hun in beginsel in elke zaak ter beschikking staan. ICT moet die discretionaire bevoegdheden respecteren en dus geen processysteem creëren dat onvoldoende ruimte laat voor de uitoefening van bepaalde bevoegdheden.

[41] P.A.M. Mevis, 'Modernisering strafvordering bij de aanvang van het vervolg', *DD* 2015/69, p. 759.

[42] De termen "gegeven" en "informatie" worden in dit document niet in strikt technische betekenis gebruikt. De definitie van "gegevens" in artikel 80 quinquies Wetboek van Strafrecht ("Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken") is dienstig om de gedachten te bepalen, maar is niet per se leidend in dit visiedocument.

[43] "Op het moment van de schuldvaststelling dient alle daarvoor gebruikte bewijsinformatie schriftelijk of electronisch vastgelegd en beschikbaar te zijn en dient die informatie op een later tijdstip gereproduceerd te kunnen worden." (brief van de minister van Veiligheid en Justitie van 26 februari 2015, Kamerstukken II, 2014-2015, 29279, nr. 225, p. 3, over de praktijk van het opleggen van strafbeschikkingen). "Naast gebruik van het «klassieke» proces-verbaal kan in toenemende mate ook gebruik worden gemaakt van moderne technologie en journaalvorming, op basis waarvan achteraf kan worden herleid waarop een beslissing is gebaseerd." (idem, p. 4). De bewaartermijnen in de Wet politiegegevens en in de Wet justitiële en strafvorderlijke gegevens worden herzien; zie de brief van de minister van Veiligheid en Justitie aan de Tweede Kamer van 23 juni 2014, Kamerstukken II, 2013-2014, 33842, nr. 2 (beleidsreactie evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens).

- ICT moet de onafhankelijkheid van de rechter in diens oordeel (en de totstandkoming en verantwoording daarvan) respecteren. Uit dat oogpunt ligt het bijvoorbeeld niet voor de hand dat het beheer van de opslag van digitale informatie (data, documenten, dossiers) bij het openbaar ministerie wordt belegd.[44] Ook zal het (noodzakelijke) toezicht op de toegang tot, de omgang met en het gebruik van gegevens zo moeten worden ingericht dat de onafhankelijkheid van de rechtspraak wordt gewaarborgd.
- Aandacht verdient daarbij ook de wijze waarop de presentatie van informatie (mondeling, schriftelijk, audiovisueel) de oordeelsvorming van mensen kan beïnvloeden.[45] Zo is bekend dat het zien van gekleurde beelden - in plaats van het lezen van tekst - effect heeft op de oordeelsvorming van mensen (rechter en andere beslissers).[46]
- De wet kent bewijsminimumregels. Door de inzet van digitale apparatuur voor waarneming en vastlegging van strafbare feiten, bijvoorbeeld beeld en geluid, kunnen die onder druk komen te staan. Verkeersovertredingen onder de WAHV die via cameratoezicht worden geconstateerd, worden nu al geheel geautomatiseerd verwerkt, waarbij de menselijke factor alleen nog betrekking heeft op de inrichting van het geautomatiseerde proces.[47] Is het aanvaardbaar dat het bewijs van een misdrijf in de toekomst wordt aangenomen op basis van uitsluitend een beeld- en geluidsopname die aan de rechter wordt getoond?

actoren

De facto uitgangspunt van de visie is de huidige diversiteit van actoren in de strafrechtspleging en hun onderlinge juridische en bestuurlijke verhoudingen. De strafrechtsketen staat bovendien op allerlei manieren in verbinding met partijen buiten die keten. Er is sprake van intensieve samenwerking - en dus uitwisseling van informatie - met andere ketens, bijvoorbeeld met de vreemdelingenketen, het openbaar bestuur, de gezondheidszorg. De visie beoogt niet dit te wijzigen, de digitalisering moet de informatie-uitwisseling tussen al deze partijen faciliteren.

randvoorwaarden: transparantie en verantwoordelijkheid

transparantie

De strafrechtsketen staat niet op zichzelf, maar vindt haar plaats en functie in de samenleving - en ontleent haar bestaansrecht daaraan. Bovendien is in deze keten, evenals in de beide andere justitiële ketens: de vreemdelingenketen en de jeugdbeschermingsketen, het geweldsmonopolie van de overheid in geding. Alle voorzieningen dienen daarom zodanig te zijn ontworpen en ingericht en zodanig te worden beheerd dat niet alleen de partijen in de keten er vertrouwen in hebben, maar ook het slachtoffer en de verdachte of veroordeelde; en uiteindelijk ook de hele Nederlandse samenleving.[48] Dat vereist vóór alles rechtvaardige en goed gemotiveerde strafrechtelijke beslissingen. Maar ook het ontwerp, de inrichting en het beheer van de informatiehuishouding als geheel en van de afzonderlijke informatiesystemen moeten bestand zijn tegen kritische vragen, hetzij in de vorm van verweren in de rechtszaal of in de vorm van kritiek vanuit de politiek, vakgenoten, het publiek en

[44] Cf. M.E. van Wees, 'Modernisering en digitalisering van het strafproces', *DD* 2015/72, p. 810.
[45] Vgl. Jacob Jolij: De cognitieve ergonomie van het digitale dossier. Trema 2015 (oktober), p. 240-244.
[46] Cf. Gabry Vanderveen en Lotte van Dillen: Digitalisering maakt strafrechtspraktijk kleurig. Met alle onbekende gevolgen van dien. In: Proces 2013, p. 315-317.
[47] Gerechtshof Arnhem-Leeuwarden 5 juni 2014, ECLI:NL:GHARL:2014:4324.
[48] En vreemde mogendheden met wie ons land op strafrechtelijk gebied samenwerkt.

de media. Dit raakt bijvoorbeeld de eisen die worden gesteld aan de elektronische handtekening of aan het digitaliseren van fysiek bewijsmateriaal ("stukken van overtuiging").

verantwoordelijkheid

De regelgeving bestaat in de grond van de zaak in toedeling van taken, bevoegdheden en verantwoordelijkheden aan mensen (functionarissen) of aan organisaties. Tot dusver wordt ook in zaken die volledig geautomatiseerd worden afgehandeld, vastgehouden aan enige vorm van menselijke verantwoordelijkheid voor het opleggen van punitieve sancties.[49] Uiteindelijk moet een menselijke functionaris aanspreekbaar zijn op het opleggen van een punitieve beslissing. Dat betekent nog niet per se dat ook elke beslissing ondertekend moet zijn. "Mulder"-beschikkingen worden niet ondertekend en ook voor strafbeschikkingen stelt de wet die eis niet.[50]

[49] Gerechtshof Arnhem-Leeuwarden 5 juni 2014, ECLI:NL:GHARL:2014:4324 (inzake "Mulder"-sanctie).

[50] Vgl. de brief van de minister van Veiligheid en Justitie van 26 februari 2015, Kamerstukken II, 2014-2015, 23279, nr. 225 (beleidsreactie op het rapport van de procureur-generaal bij de Hoge Raad «Beschikt en Gewogen; over de naleving van de wet door het Openbaar Ministerie bij het uitvaardigen van straf-beschikkingen»), p. 6: "degene die het verzet moet beoordelen moet kunnen nagaan wie de beslissing heeft genomen in eerste aanleg. Voor de strafbeschikkingen die het OM uitvaardigt, is in GPS herleidbaar wie de beslissing heeft genomen".

BIJLAGE 3:
DE STRAFRECHTSKETEN

keten, netwerk, domein

De strafrechtspleging strekt ertoe wetsovertredingen te bestraffen en tegelijkertijd te beletten dat mensen onterecht worden bestraft.[51] Deze dienst of functie wordt gerealiseerd in een proces dat, op abstract niveau bezien, bestaat uit de volgende stappen:

opsporen → *vervolgen* → *berechten* → *tenuitvoerleggen* → *re-integreren*

Deze stappen geven de logische structuur van het proces weer. In een rechtsstaat moet aan de tenuitvoerlegging van een straf of maatregel noodzakelijkerwijs een beslissing van een bevoegd orgaan (rechter of officier van justitie) voorafgaan, aan die beslissing moet een gedegen onderzoek voorafgaan, et cetera. Het plaatje zegt níet dat alle afzonderlijke activiteiten in een strafproces per se na elkaar worden of moeten worden uitgevoerd. Digitalisering schept mogelijkheden om activiteiten die op logisch niveau op elkaar volgen, feitelijk simultaan uit te voeren (te parallelliseren), bijvoorbeeld door gelijktijdig aan een stuk te werken. Dat kan leiden tot tijd-, kwaliteits- en efficiëntiewinst. Ook kunnen er "lussen" optreden, bijvoorbeeld als een zaak wordt teruggewezen na vernietiging van een vonnis of arrest in hoger beroep of cassatie.

De strafrechtspleging staat niet op zichzelf. Zoals de re-integratie als het ware "aan de achterkant" het strafrecht uit loopt, zo is er ook "aan de voorkant" een gebied waar preventie (in haar diverse verschijningsvormen), handhaving van de openbare orde, controle, toezicht, grensbewaking en bestuurlijke handhaving kunnen overgaan in opsporing en daarmee de strafrechtspleging activeren. Ook preventie in de zin van het voorkómen van strafbare feiten in specifieke (categorieën van) gevallen gaat aan de eigenlijke keten vooraf; denk aan barrièremodellen, “tegenhouden”, het “stuk maken" van zaken etc. Al deze fenomenen fungeren - op hun tijd - als "voorportalen" van de strafrechtsketen. En dan zijn er ook nog "parallelle" of aanpalende ketens, instrumenten en domeinen, zoals de jeugdbescherming en de jeugdzorg,[52] de vreemdelingenketen, de Verklaring omtrent het gedrag (VOG), die ook allerlei raakvlakken en verbindingen hebben met de strafrechts-pleging.

In deze processen werken vele partijen samen.[53] Dit zijn niet per se alleen overheidsorganisaties of door de overheid gefinancierde organisaties, maar kunnen ook particuliere organisaties zijn.[54]

---

[51] Deze "dienst" kan vanuit systemisch-bedrijfskundig oogpunt worden aangeduid als het "product" of de "*output*" van het strafrechtelijk systeem. Als de gewenste "*outcome*" plegen onder meer te worden genoemd: preventie van criminaliteit, afschrikking, onschadelijkmaking, genoegdoening, gedragsverandering, recidive-vermindering, vergroten van veiligheid en leefbaarheid. Die effecten zijn echter doorgaans afhankelijk van tal van andere factoren dan alleen strafrechtelijk ingrijpen.

[52] Jeugdstrafrecht is begripsmatig bezien integraal onderdeel van het strafrecht, echter met een aantal bijzondere kenmerken. Alles wat in deze notitie wordt opgemerkt over strafrecht, geldt dus ook voor jeugd-strafrecht.

[53] De term "samenwerken" moet in dit verband niet verkeerd worden begrepen. Vanuit het stelsel van "checks and balances" kan het immers noodzakelijk zijn dat partijen elkaar juist "tegenwerken" of corrigeren. Hogere functionarissen binnen een organisatie moeten toezien op de rechtmatigheid van het werk van hun medewerkers, de officier van justitie moet de rechtmatigheid, legitimiteit en integriteit van de opsporing

Bijvoorbeeld: banken (in het kader van het "bankenteam" c.q. de Electronic Crimes Taskforce, of het Kennisprogramma Veiligheid Digitaal Betalingsverkeer), telecom- en internetbedrijven (bijvoorbeeld in het kader van het Centraal Informatiepunt Onderzoek Telecommunicatie), advocatuur, instellingen voor geestelijke gezondheidszorg (in het kader van forensische zorg). Volgens de gangbare definities is er sprake van een "keten".[55]
Tegelijk is elk van die partijen het centrum van haar eigen netwerk, doordat zij veelal in meer dan één keten participeert. Bijvoorbeeld (op operationeel niveau) in ZSM, Veiligheidshuizen, casus-overleggen, ketenunits; en op bestuurlijk niveau in het Arrondissementaal Justitieel Beraad (AJB). Voor sommige organisaties vormen de strafrechtelijke taken zelfs maar een klein onderdeel van hun totale takenpakket, zoals de gecertificeerde instellingen die onder de Jeugdwet de jeugdreclassering gaan uitvoeren, of de instellingen voor GGZ die in het kader van bijzondere voorwaarden trajecten verzorgen voor verdachten en veroordeelden.[56] In het geval van jeugdige verdachten kunnen jeugdzorg en jeugdbescherming aan de toepassing van het strafrecht voorafgaan (bijvoorbeeld: signalen van strafbaar gedrag) of in het verlengde daarvan liggen (bijvoorbeeld: nazorg en re-integratie).

Dit brengt mee dat op ketenniveau (strafrecht) én op ketenoverstijgend niveau (tussen twee of meer ketens, of op het niveau van VenJ, of rijksbreed) afspraken gemaakt moeten worden. Er is niet één universeel uitgangspunt ("keten" of "netwerk" of "domein"), maar er moet van geval tot geval bepaald worden op welk niveau een een afspraak gepositioneerd moet worden.

informatiehuishouding
De taken, bevoegdheden en verantwoordelijkheden zijn binnen het VenJ-domein sterk juridisch gereguleerd. Die regulering is procesgewijs - en dus ketengewijs - ingericht. Er zijn afzonderlijke regels voor het straf- en strafprocesrecht, voor het vreemdelingenrecht en voor de jeugd-bescherming. In het strafprocesrecht zijn de meeste bevoegdheden toegedeeld aan functionarissen, niet aan organisaties. De juridische grondslag voor een beslissing of handeling bepaalt welke bevoegdheden een functionaris heeft en welke informatie hij mag of moet uitwisselen. Strafrechtelijke informatie mag niet zomaar naar de vreemdelingenketen of de jeugdbescherming worden overgeheveld en omgekeerd evenmin. En ten slotte zijn er binnen het domein van VenJ ook besturende processen en besluitvormingsstructuren per keten ingericht. Deze fungeren als een tussenlaag tussen het niveau van het VenJ-domein als geheel (het concern-niveau) en het niveau van de afzonderlijke organisaties.

---

bewaken, de rechter moet de rechtmatigheid van het geding als geheel toetsen. Dit kan er onder omstandigheden toe leiden dat de ene functionaris (of "partij") binnen de keten belet wat een andere wil doen (bijvoorbeeld: de rechter-commissaris weigert een machtiging tot doorzoeken van een woning), of dat de ene ongedaan maakt wat een andere heeft verricht (bijvoorbeeld: de rechtbank verklaart de officier van justitie niet-ontvankelijk of stelt onrechtmatig verkregen bewijs ter zijde; of het gerechtshof vernietigt in hoger beroep het vonnis van de rechtbank).

[54] Waar in deze notitie wordt gesproken van "functionarissen", worden personen in dienst van zulke particuliere organisaties, voor zover zij werkzaam zijn binnen de strafrechtsketen, daar mede onder begrepen.

[55] Onder "keten" wordt in deze notitie verstaan "een lineair proces waarin verschillende organisaties buiten hun eigen organisatiegrenzen werken aan een gemeenschappelijk resultaat" (cfm. WRR 2011: iOverheid, p. 72).

[56] De advocatuur is geen onderdeel van de keten, maar wel een primaire belanghebbende. De advocatuur kan ook het functioneren van de keten sterk beïnvloeden.

Omdat de juridische regulering zo dominant is, moet de informatiehuishouding het ketenverband volgen. Maar zij moet ook het netcentrisch werken van de ketenpartners faciliteren. De eisen vanuit de verschillende ketens kunnen conflicteren en daardoor binnen de organisaties tot spanningen leiden. Om die beheersbaar te maken, moeten op ketenniveau en tussen ketens afspraken over de informatiehuishouding en –uitwisseling worden gemaakt.

gegevensbescherming

Informatie is macht. Het vergaren, vastleggen, opslaan, gebruiken en uitwisselen van informatie over burgers is in zichzelf een machtsmiddel en mag daarom alleen worden toegepast binnen de grenzen van wet en recht. Onjuiste of ontijdige - te late - informatie kan leiden tot onjuiste beslissingen, bijvoorbeeld onterechte veroordeling of een onterechte vrijspraak, of onterechte handelingen, bijvoorbeeld: een inval in een woning waar de verdachte ten onrechte vermoed wordt aanwezig te zijn.[57] Zulke fouten kunnen grote impact hebben op de justitiabelen zelf (verdachten, veroordeelden), op hun directe omgeving, op het slachtoffer en andere betrokkenen, en op de samenleving als geheel.

De wetgeving laat zien dat de samenleving de omgang met informatie over personen strikt wil reguleren. Hoe opener de omgeving waarin gegevens circuleren, des te groter zijn de gevaren van oneigenlijk gebruik van gegevens en verlies van context. Als gegevens eerst worden "gedecontextualiseerd" en vervolgens worden "gehercontextualiseerd", brengt dat risico's mee voor hun kwaliteit en integriteit en daarmee voor het gebruik van die gegevens.[58] De omgang met informatie is daarom via de wet gereguleerd. Die regulering volgt grosso modo het patroon van de ketens, bijvoorbeeld via het vereiste van doelbinding.

huidige situatie

De informatiestroom in de strafrechtketen is grotendeels gebaseerd op de uitwisseling van papieren dossiers en documenten. Voor zover deze in de keten digitaal worden uitgewisseld, gebeurt dit op bilaterale basis, zoals tussen het OM en de ZM of tussen de politie en het CJIB. De zgn. "kopie-conform" procedure is de norm. Stukken worden digitaal gemaakt (met de computer: "digital born"), al dan niet geprint, en vervolgens gedigitaliseerd en digitaal verzonden. De papieren en de digitale verschijningsvormen van "stukken" zijn in de memorie van toelichting bij het wetsvoorstel "elektronische processtukken" gelijkwaardig verklaard.[59] De elektronische aangifte en het elektronische proces-verbaal van opsporing zijn al in de wet geregeld.[60] Een wetsvoorstel om het gebruik van elektronische processtukken in de volle breedte te regelen, is in behandeling.[61] Andere voorzieningen, initiatieven en programma's om te komen tot (meer) digitaal werken in de strafrechtsketen zijn:

[57] Dit laatste was aan de orde in EHRM 18 juli 2006, appl. no. 28867/03 (Keegan/UK).
[58] Vgl. WRR (2011): iOverheid.
[59] Wetsvoorstel tot wijziging van het Wetboek van Strafvordering en de Wet op de economische delicten in verband met het gebruik van elektronische processtukken (digitale processtukken Strafvordering), Kamerstukken II, 2014-2015, 34090, nr. 3 (MvT), p. 6.
[60] Art. 163, derde lid, resp. 153, tweede lid, Wetboek van Strafvordering.
[61] Wetsvoorstel tot wijziging van het Wetboek van Strafvordering en de Wet op de economische delicten in verband met het gebruik van elektronische processtukken (digitale processtukken Strafvordering), Kamerstukken II, 2014-2015, 34090, nrs. 1-3.

- de introductie en het gebruik van het strafrechtketennummer (SKN);[62]
- digitale standaarden in het domein van VenJ: de justitie-brede berichtenbus JUBES en de Externe Politie Broker (EPB);[63]
- het programma Versterking Prestaties in de Strafrechtketen (VPS), dat voorziet in samenwerking tussen een aantal van de belangrijkste ketenpartijen;
- het project Digitaal Werken in de Strafrechtketen (DWS; onderdeel van VPS), dat tot doel heeft om in 2016 de processtukken digitaal uit te wisselen tussen politie, openbaar ministerie en Rechtspraak;
- het Bijgestelde Aanvalsprogramma Politie (bAVP);
- het project MEOS (Mobiel Effectiever Op Straat), dat voorziet in compacte mobiele apparatuur waarmee de politieman- of vrouw op straat snel en eenvoudig informatie over individuen kan raadplegen (voor zover over hen reeds informatie is vastgelegd in de systemen van politie en justitie) en digitale bekeuringen kan uitschrijven;
- het Programmaplan Vernieuwing Informatievoorziening DJI (VIDJI);
- het programma Uitvoeringsketen strafrechtelijke beslissingen (USB). In de nieuwe regeling van de tenuitvoerlegging van strafrechtelijke beslissingen (boek 6 van het Wetboek van Strafvordering) is de mogelijkheid van elektronisch betekenen van dagvaardingen en andere processtukken voorzien.[64]

Ook het Programma Kwaliteit en Innovatie (KEI) binnen de Rechtspraak en het wetsvoorstel "vereenvoudiging en digitalisering van het procesrecht" moeten in dit verband worden genoemd, met dien verstande dat het wetsvoorstel alleen betrekking heeft op het civiel en bestuursrecht, niet op het strafrecht.[65]

Voor de identiteit van de verdachte of veroordeelde is reeds een ketenbrede voorziening getroffen: de strafrechtsketendatabank (zie artikel 27b, vierde lid, Wetboek van Strafvordering en het Besluit identiteitsvaststelling verdachten en veroordeelden). Voor de bij het openbaar ministerie ingeschreven strafzaken en de beslissingen van officieren van justitie en rechters in strafzaken is een ketenbrede uniforme voorziening getroffen in de vorm van de justitiële documentatie (zie de Wet en het Besluit justitiële en strafvorderlijke gegevens).[66]

De Justitiële Informatiedienst (onderdeel van het Ministerie van Veiligheid en Justitie) beheert een aantal gemeenschappelijke voorzieningen ("ketenvoorzieningen") van de strafrechtsketen, zoals de strafrechtsketendatabank (SKDB), de Voorziening voor verificatie en identificatie (VVI), de "Spelverdeler", het Justitieel Documentatiesysteem (JDS), het Centraal digitaal depot (CDD), het

[62] Dit SKN heeft een wettelijke basis in artikel 27b, eerste lid, Wetboek van Strafvordering (in werking getreden op 1 oktober 2010).
[63] Beide zijn sectorale berichtenbussen/knooppunten, sluiten aan op de standaarden van de Overheid Service Bus (OSB) en zijn verplicht voor alle ketenpartners. De centrale Justitie Berichten Service “JUBES“ is een Justitiebrede voorziening, die het elektronische berichtenverkeer tussen de onderdelen van VenJ en met partijen buiten VenJ faciliteert. De centrale Externe Politie Broker (EPB) is een politie-brede voorziening, die het elektronische berichtenverkeer tussen de verschillende politieonderdelen met partijen buiten de politie faciliteert.
[64] Kamerstukken II, 2014-2015, 34086, nrs. 1-3.
[65] Kamerstukken II, 2014-2015, 34059, nrs. 1-3.
[66] Ook de politiële, de bestuurlijke en de fiscale strafbeschikkingen worden geregistreerd in de justitiële documentatie.

elektronisch berichtenverkeer (EBV), de elektronische handtekening ("Gemeenschappelijke Authenticatie, Associatie en Validatie", GAAV) en het Gegevenswoordenboek voor de strafrechtsketen, en is daarnaast een service provider voor het VenJ-domein.

In zijn rapport "Prestaties in de strafrechtsketen" constateerde de Algemene Rekenkamer onder meer dat een onbekend aantal zaken uitstroomt uit de keten zonder dat daarvoor de redenen die bekend of gedocumenteerd zijn, dat de cijfers over uitstroom van de ene schakel en instroom in de andere schakel niet op elkaar aansluiten, dat de doorlooptijden te lang zijn en dat de informatie-voorziening over prestaties niet voldoet. De Rekenkamer beval daarom onder meer aan een informatiestrategie voor de strafrechtketen te ontwikkelen, die als uitgangspunt heeft dat sturing op gewenste prestaties en het voorkomen van ongewenste prestaties mogelijk wordt.[67] In haar rapport over de verantwoording van VenJ over 2014 heeft de Rekenkamer gespecificeerd wat de informatie-strategie zou moeten inhouden: zij zou betrekking moeten hebben op "de afstemming van verschillende systemen, de betrouwbaarheid van informatie en de verantwoordelijkheid voor de vastlegging en het beheer van informatie".[68] Daarover gaat de visie die hier wordt geboden, als onderdeel van het bredere programma Versterking prestaties strafrechtsketen (VPS).

[67] Algemene Rekenkamer: Prestaties in de strafrechtsketen. Kamerstukken II, 2011-2012, 33173, nr. 2.
[68] Algemene Rekenkamer: Resultaten verantwoordingsonderzoek bij het Ministerie van Veiligheid en Justitie 2014, p. 26 (aangeboden aan de Tweede Kamer bij brief van 20 mei 2015, Kamerstukken II, 2014-2015, 34200 VI, nr. 2.

BIJLAGE 4:
TRENDS EN ONTWIKKELINGEN

De strafrechtsketen staat niet op een eiland en Nederland evenmin. Dit hoofdstuk schetst achtereenvolgens een aantal Rijksbrede ontwikkelingen, een aantal ontwikkelingen in het buitenland en een aantal trends en ontwikkelingen op het gebied van de technologie (ICT), voor zover van belang voor deze visie.

Nederland
De samenleving stelt hoge eisen aan de strafrechtketen. Zij verwacht dat strafbare feiten snel, transparant en foutloos worden afgehandeld. De doorlooptijden worden als te lang ervaren. Er is een behoefte aan transparante informatievoorziening gedurende het proces; statusinformatie moet op elk moment beschikbaar zijn. Er bestaat een toenemende spanning tussen transparantie en waarborging van de privacy. Mag bijvoorbeeld persoonlijke informatie over een mogelijke dader beschikbaar worden gesteld om de opsporing te versnellen? Mag de (strafrechtelijke) overheid alle informatie die mensen over zichzelf op internet plaatsen, onbeperkt gebruiken?

Mensen beschikken over twee identiteiten: een digitale en fysieke identiteit. In de digitale wereld is het eenvoudig mogelijk om nog meer identiteiten aan te nemen; eenvoudiger in elk geval dan in de fysieke wereld. Dat heeft consequenties in een context waarin die identiteit essentieel is, zoals de strafrechtspleging. De professional binnen de strafrechtketen stelt nieuwe eisen aan mobiliteit en wil beschikken over de informatie op elke locatie, tijdstip (24x7) en apparaat. De burger heeft toegang tot nieuwe technologie, zoals mobiele telefonie, apps, foto- en videoapparatuur en sensoren, en wil deze gebruiken en proactief inzetten, bijvoorbeeld als bewijsmateriaal - maar onder omstandigheden ook om zich aan opsporing en berechting te onttrekken. De juridisering van de samenleving leidt tot steeds complexere wet- en regelgeving, hetgeen snelle en effectieve rechtspraak kan bemoeilijken.

Vanuit de politiek is er druk op een verhoging van de effectiviteit en verlaging van de kosten. Het Uitvoeringsprogramma Compacte Rijksdienst is de eerste stap op weg naar de totstandkoming van de afspraak uit het regeerakkoord 2012 om te komen tot een krachtige, kleine en dienstverlenende overheid.[69] Beoogd wordt een overheid die zich richt op haar kerntaken, met een effectieve besturing en lagere kosten. De Compacte Rijksdienst vertaalt zich onder andere in het samenvoegen van organisatieonderdelen, harmonisatie van processen (bijvoorbeeld inkoop, personeel), gemeenschappelijke ICT-standaarden en gebruik van gemeenschappelijke ICT-infrastructuur.

internationaal
In opdracht van het WODC heeft de Rijksuniversiteit Groningen een onderzoek uitgevoerd naar ervaringen met digitalisering van de strafrechtsketen in Engeland, Denemarken, Oostenrijk en Estland. De ervaringen in die landen blijken belangrijke parallellen te vertonen met de ervaringen in ons land.[70]

[69] "Bruggen slaan". Kamerstukken II, 2012-2013, 33410, nr. 15.
[70] Digitalisering in strafrechtketens. Ervaringen in Denemarken, Engeland, Oostenrijk en Estland vanuit een supply chain perspectief (2014). Zie ook Carolien de Blok, Aline Seepma, Dirk Pieter van Donk en Inge Roukema: Ervaringen met digitalisering in vier Europese strafrechtketens. NJB 2015, p. 612-618.

Digitalisering moet, blijkens dit onderzoek, vooral onderdeel zijn van een continu / langlopend verbetertraject dat streeft naar betere afstemming en stroomlijning in een keten van organisaties, gevolgd door en ondersteund door inpassing van adequate ICT. Er bestaat geen "ideale" aanpak; wat de beste aanpak is, is afhankelijk van de context van een land en de doelstelling van digitalisering. Drie aspecten komen in zo'n digitaliseringstraject bij elkaar: organisatie (processen, structuren, cultuur), technologie (ICT) en wetgeving. Belangrijke voorwaarden voor het slagen van dergelijke trajecten zijn het zoeken van aansluiting bij specifieke omstandigheden en kleinschalige verbeteractiviteiten binnen en tussen de partners in de keten en het aansturen van de keten door het ministerie vanuit een op ketenintegratie gerichte visie. Daarbij moet digitalisering geen doel op zich zijn, maar een middel, dat samen met bijvoorbeeld het wettelijke kader, de stroomlijning verder faciliteert. Digitalisering moet onderdeel worden van de wijze waarop de keten werkt en niet als een additioneel werkproces worden opgetuigd. Organisatorische belemmeringen, veelal gegroeid uit gewoonte en historie, bemoeilijken die stroomlijning en dienen doorbroken te worden. Het werken vanuit een ketenvisie vraagt van alle ketenpartijen een omslag. Een belangrijke uitdaging blijft om een balans te vinden tussen enerzijds inhoudelijke zorgvuldigheid en professionele autonomie en anderzijds kosten, procedurele afstemming door de keten en snelheid.

In Denemarken werd gestreefd naar het vervangen van alle bestaande systemen door één systeem, maar door de omvang daarvan en omdat alle ketenpartijen de eigen oorspronkelijke functionaliteiten in dit systeem wilden onderbrengen, bleek het uiteindelijk te instabiel om mee te werken. In Engeland en Estland blijven de ketenpartners gebruik maken van de eigen informatie-systemen. Deze verschillende systemen zijn in Engeland door een groot aantal koppelingen met elkaar verbonden. In Estland is één centrale architectuur ontwikkeld waar alle bestaande systemen op aansluiten, waardoor deze met elkaar kunnen communiceren. De combinatie van het eigenaarschap over het eigen systeem en tegelijkertijd het inbrengen van een ketenperspectief en creëren van uitwisselingsmogelijkheden tussen de ketenpartners, lijkt in deze landen tot succesvolle digitalisering geleid te hebben.

Ook de aanpak en ervaringen in Zweden blijken veel overeenkomsten te vertonen met die in ons land.[71] Eind december 2013 is daar een digitale uitwisseling van documenten gerealiseerd tussen de politie, het openbaar ministerie en de Rechtspraak. Het project wordt nu uitgebreid naar meer informatie en meer ketenorganisaties. Het project wordt bestuurd door een Council for Information Management in the Judicial System. Deze "Council" lijkt sterk op de Coördinatiegroep Informatie-voorziening Strafrechtsketen (CIS), zoals die is ingesteld bij besluit van de minister van Justitie van 13 april 2005 (Stcrt. 2005, 80): een brede samenstelling, besluitvorming op basis van consensus, verantwoordelijkheid voor de implementatie van hetgeen gezamenlijk besloten is bij de afzonderlijke partners en financiering in beginsel binnen de bestaande kaders. Ook de gekozen oplossingen op het meer technische vlak komen in veel opzichten overeen met hetgeen in deze visie is geschetst . Een voorziening om het "incident" dat aanleiding gaf tot de strafrechtelijke actie, vanaf het begin tot het eind van het strafrechtelijke traject uniek en eenduidig te identificeren, is in Zweden al gerealiseerd.

[71] Zie de factsheet "A digitally joined-up judicial chain" (http://www.government.se/contentassets/0d64212eac554a268396de58c11f9f1f/a-digitally-joined-up-judicial-chain).

Er is sprake van toenemende harmonisatie en samenwerking tussen Europese lidstaten en de aanpak van grensoverschrijdende criminaliteit (o.a. cyber-security). Enkele belangrijke internationale initiatieven die de strafrechtspleging raken, zijn:

- het Europese project e-CODEX ("e-Justice Communication via Online Data Exchange"), een Europees project met als doel het verbeteren van toegang tot rechtspraak over de grens voor burgers en bedrijven, en het verbeteren van digitale informatie-uitwisseling tussen de autoriteiten in de EU;
- de toekomstige Europese Verordening ter vervanging van de huidige Europese privacyrichtlijn uit 1995 en de toekomstige Richtlijn gegevensbescherming opsporing en vervolging;
- Europese digitale identiteit: niet alleen in Nederland wordt gewerkt aan de volgende versie van digitale identiteit, ook binnen Europa is er aandacht voor het onderling (h)erkennen van de digitale identiteiten van burgers van de lidstaten. Scoping the Single European Digital Identity Community (SSEDIC) is een platform waarin Europese e-ID belanghebbenden samenwerken om dit doel te bereiken.

technologie (ICT)

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. De hoeveelheid beschikbare informatie verdubbelt elke twee jaar.[72] "Delen" van digitale informatie betekent vermenigvuldigen ervan en digitaal werken betekent dat het werk onafhankelijk is van tijd, plaats of gebruikt middel ("APATAD": any place, any time, any device). Informatie is alom (digitaal) aanwezig en bereikbaar. De fysieke aanwezigheid van een stapel papier bepaalt niet langer wie er aan het dossier werkt. Informatie hoeft daarom niet langer rond het werk te worden georganiseerd, maar werk kan rond informatie worden georganiseerd. De professional hoeft, als de digitalisering goed wordt ingericht, minder administratieve handelingen te verrichten en kan zich dus meer concentreren op zijn kerntaken[73]; digitale gegevensuitwisseling verkleint de kans op fouten doordat gegevens niet langer telkens opnieuw hoeven te worden overgetypt (invoeren, "inkloppen").

In de digitale wereld zijn mogelijkheden voorhanden om de authenticiteit en de integriteit van documenten of gegevens te waarborgen, die in de papieren wereld niet of nauwelijks bestaan. Een "natte" handtekening op een stuk papier bijvoorbeeld, kan alleen de authenticiteit van het document waarborgen, d.w.z. de echtheid op het moment van ondertekenen, maar niet de integriteit (d.w.z. dat het nadien niet gewijzigd is). De elektronische handtekening kan beide. De "natte" handtekening was trouwens ook zonder al te veel moeite te vervalsen; de digitale wereld kan betere bescherming daartegen bieden.

Daar staat tegenover dat inbreuken op de integriteit van informatie in de digitale wereld veel verder kunnen reiken dan in de papieren wereld. Stelen en/of onbevoegdelijk wijzigen, verspreiden, kopiëren of vernietigen van papieren dossiers is, ervan uitgaande dat de "dief" eenmaal kans heeft

[72] Bron: http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm (geraadpleegd 4 november 2015).

[73] Geschat wordt dat professionals nu 19 tot 38% van hun tijd bezig zijn met het zoeken naar en ordenen van informatie. Bronnen: Michael Mcdermott (2005): Knowledge Workers: You can gauge their effectiveness. Leadership Excellence 22 (10): 15–17 (38%); McKinsey Global Institute (2012): The social economy: Unlocking value and productivity through social technologies (19%).

gezien binnen te dringen in het systeem, een stuk bewerkelijker dan van digitale data. Het kan bovendien digitaal allemaal op afstand worden uitgevoerd, fysieke nabijheid speelt geen rol meer.

Het gebruik van mobiele apparaten (tablets, smartphones) stelt professionals en andere betrokkenen eenvoudig in staat om 24 uur per dag en 7 dagen per week vanaf elke locatie toegang tot informatie te hebben. Het zakelijk gebruik van social media toepassingen neemt toe, waardoor professionals eenvoudiger kunnen samenwerken en informatie onderling kunnen delen. Het geautomatiseerd kunnen analyseren en interpreteren van grote hoeveelheden informatie biedt mogelijkheden voor beslisondersteuning ook op inhoudelijk vlak ("in een vergelijkbare zaak heeft een rechter de volgende uitspraak gedaan").

Datzelfde gebruik van - al dan niet mobiele - digitale apparatuur leidt er ook toe dat veel grotere hoeveelheden informatie beschikbaar komen in de opsporing, bijvoorbeeld via op straat opgenomen video's van gebeurtenissen in relatie tot een strafbaar feit, of via internet (social media). Daarnaast leidt het toenemend gebruik van bodycams, drones, sensing, en het "internet of things" ("ubiquitous computing") tot een explosieve toename van de hoeveelheid beschikbare informatie. Dat beïnvloedt de opsporing en dus potentieel ook de informatie die in de keten wordt gedeeld en de manier waarop dat gebeurt. Kan - op termijn - een op straat door de politie opgenomen video als bewijs van een strafbaar feit het ambtsedig proces-verbaal vervangen? En een door een willekeurige voorbijganger opgenomen video? En is dat ook wenselijk?

"Digitalisering van de strafrechtspraak, zeker van de totale keten, is uiterst moeilijk en complex en het (mis)lukken is van zeer veel, en zeer verschillende factoren afhankelijk".[74] De introductie van nieuwe technologieën gaat gepaard met structurele en procedurele veranderingen. Digitalisering gaat dikwijls gepaard met standaardisatie van werkprocessen. Dat kan spanning opleveren met de professionele autonomie en de discretionaire bevoegdheden van functionarissen.[75] Gebruik van audiovisuele media voor bijvoorbeeld het registreren van verhoren van verdachten en getuigen in het vooronderzoek heeft onmiskenbaar waarde, maar kan ook het evenwicht tussen het voorbereidend onderzoek en het onderzoek op de terechtzitting zoals dat in ons land is gegroeid, onder druk zetten: een terechtzitting is er in de huidige omstandigheden niet op berekend dat vele uren aan beeld- of geluidsmateriaal wordt afgespeeld. Daar komt bij dat het werk in de strafrechts-keten kennisintensief is; de complexiteit van de informatiehuishouding is groot en de betrouwbaar-heid en de bedrijfszekerheid van de informatiesystemen cruciaal.

Wat de gevolgen zijn van de digitalisering in en voor de dagelijkse praktijk van de professionals is nog niet duidelijk. Om hier ervaring mee op te doen, zijn op een aantal plaatsen in het land proeftuinen ingericht. In aanvulling daarop wordt nu een onderzoek uitgevoerd dat zich richt op de impact van digitalisering op de rechtsstatelijke waarden en beginselen van de strafvordering; de resultaten daarvan worden medio dit jaar verwacht.

[74] Aldus P.A.M. Mevis in Delikt en Delinkwent 2014, p. 584.
[75] Cf. W.K.F. Hangelbroek: Digitale revolutie in de Nederlandse rechtspraak. In: Holland/Belgium Management Review, nummer 148 - 2013, p. 5; Thomas P. Hughes: The Evolution of Large Technological Systems. In: The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology. Cambridge, MA: M.I.T. Press, 1987, p. 54.

BIJLAGE 5:
KERNBEGRIPPEN BINNEN DE DIGITALE INFORMATIEHUISHOUDING

automatiseren, informatiseren, digitaliseren
"Digitalisering" wordt in deze notitie gebruikt in contrast met "automatisering" en "informatisering". Onder "automatisering" wordt in deze notitie verstaan het vervangen van menselijk-handmatige werkzaamheden door werk van apparaten, zoals computers. Onder "informatisering" wordt verstaan het tijdig en efficiënt (geautomatiseerd) voorzien van professionals van de juiste informatie. Onder "digitalisering" wordt verstaan de maatschappelijke ontwikkeling dat alle verwerkingen van informatie worden ondersteund en (kunnen) worden uitgevoerd door computers.[76, 77]

Digitalisering in deze brede betekenis is niet slechts - en zelfs niet in de eerste plaats - een technische aangelegenheid. Digitalisering van de strafrechtspleging is ook meer dan het "digitaliseren van de postbode". Het raakt de werkprocessen van de professional en de manieren waarop het werk is georganiseerd. Digitaal werken is het inrichten van een werkomgeving voor de professional waarbinnen alle informatie verwerkingen worden uitgevoerd met behulp van ICT. De digitale werkomgeving is afgestemd op en gepersonaliseerd/te personaliseren naar een optimale ondersteuning van de werkzaamheden van de professional.

informatieproduct, informatiepositie, informatiehuishouding
Het patroon van de strafrechtsketen zoals geschetst in bijlage 3, is - op dit hoge abstractieniveau - stabiel. Naarmate wordt ingezoomd op detailniveau wordt het beeld navenant veranderlijker, minder stabiel. Werkprocessen en samenwerkingsprocessen worden immers voortdurend aangepast, verbeterd en/of opnieuw ingericht, bijvoorbeeld in het kader van VPS, USB, ZSM, (Lean) Six Sigma. De informatiehuishouding moet zo zijn ingericht dat niet elke verandering in de werkprocessen meteen noodzaakt tot veranderingen in de informatiehuishouding. Bovendien is in beginsel in vrijwel elke strafzaak een veelheid van procesgangen mogelijk: opsporingsambtenaren, officieren van justitie en rechters kunnen in beginsel zelfs in de "kleinste" zaak gebruik maken van tal van discretionaire bevoegdheden. Dat mag niet worden gefrustreerd door - in het kader en ten behoeve van de digitalisering - processen te standaardiseren.

De term "informatieproduct" wordt in dit visiedocument gebruikt als verzamelterm voor data, documenten en dossiers. Tot die documenten behoren in ieder geval alle door het Wetboek van Strafvordering voorgeschreven of veronderstelde documenten, zoals processen-verbaal van opsporingsambtenaren, vorderingen, bevelen, machtigingen, dagvaardingen, rechterlijke beslissingen, akten van uitreiking (betekeningsformulieren), bezwaarschriften, akten voor het instellen van een rechtsmiddel (hoger beroep, cassatie). Als "document" worden voorts aangemerkt

[76] In zijn proefschrift "De digitale strafrechtspleging" (1996) heeft J. Rademaker de geschiedenis van de eerste decennia van de aanloop naar een digitale strafrechtspleging uitvoerig beschreven.
[77] Het Engels kent twee verschillende woorden: "In the Oxford English Dictionary, *digitization* refers to 'the action or process of digitizing; the conversion of analogue data (esp. in later use images, video, and text) into digital form.' *Digitalization*, by contrast, refers to 'the adoption or increase in use of digital or computer technology by an organization, industry, country, etc.'." Aldus Scott Brennen and Daniel Kreiss: Digitalization and Digitization · September 8, 2014 (bron: http://culturedigitally.org/2014/09/digitalization-and-digitization/, geraadpleegd 19 november 2015).

allerlei andere, niet in dat Wetboek genoemde of geïmpliceerde documenten die in het kader van de strafrechtspleging geproduceerd kunnen worden, zoals een transportopdracht van een gedetineerde van de PI naar de rechtbank of het strafblad (uittreksel uit de justitiële documentatie) van een veroordeelde.[78] Deze documenten markeren, juridisch bezien, de vastlegging van handelingen ("verrichtingen") en waarnemingen ("bevindingen"), beslissingen en wilsuitingen. Informatorisch bezien kunnen ze worden aangemerkt als meer of minder gestructureerde sets van gegevens. De bedoelde handelingen, waarnemingen, beslissingen en wilsuitingen constitueren gezamenlijk het strafgeding. De vorm en opmaak van het document zijn veelal toegesneden op de strekking ervan: de hiervoor genoemde documenten maken zich reeds door hun vorm en opmaak expliciet als zodanig, dus als proces-verbaal, vordering, dagvaarding, vonnis, etc., bekend. Begin vorige eeuw, toen het Wetboek gemaakt werd, was er echter nog geen sprake van documenten in digitale verschijnings-vorm. De verschijningsvorm doet er ook niet toe: het gaat om de inhoud, d.w.z. om de informatie die is vastgelegd. Alle werkprocessen zijn er in feite op gericht deze documenten te produceren. Het doet er ook niet zoveel toe in welke fase een zaak zich bevindt: of er nu sprake is van een verdenking, van ernstige bezwaren, een tenlastelegging of een bewezenverklaring, de informatieproducten blijven gelijk. Als zodanig zijn deze informatieproducten stabiel, stabieler in elk geval dan de werkprocessen waarin ze worden gemaakt. Wanneer men een strafdossier pakt van honderd jaar geleden, zijn in dat dossier dezelfde informatieproducten terug te vinden als in een dossier van vandaag de dag: het proces-verbaal, de akte van uitreiking, de dagvaarding, het vonnis, etc. En de informatieproducten van toen, bijvoorbeeld een proces-verbaal wegens een inbraak, verschillen qua inhoud ook niet wezenlijk van de huidige; ook de (juridische) kwaliteitseisen zijn nog dezelfde. Beslissingen en handelingen moeten nu eenmaal op een kenbare en betekenisvolle manier worden vastgelegd ten behoeve van de overdracht en de verantwoording. Om al deze redenen moeten voor de inrichting van de informatiehuishouding niet de processen als aanknopingspunt worden gebruikt, maar de informatieproducten.

De informatie die iemand nodig heeft en waartoe hij gerechtigd is en die voor hem effectief beschikbaar en toegankelijk is, wordt in deze notitie aangeduid als de "informatiepositie" van de gebruiker (professional, justitiabele, belanghebbende, etc.).

De "informatiehuishouding" is het totaal aan regels en voorzieningen gericht op de informatie-stromen en -opslag of archivering ter ondersteuning van de primaire processen.[79]

zaak, dossier
Gegevens en informatieproducten hebben betrekking op iets in de werkelijkheid, zoals personen, objecten, locaties, relaties, situaties, gebeurtenissen. De kern van de strafrechtspleging is, zoals hiervóór uiteengezet, het verbinden van interventies aan incidenten. De "incidenten" zijn de gebeurtenissen die strafrechtelijk worden geduid: misdrijven en overtredingen. De "interventies" zijn

[78] In de opsporingsfase wordt veel informatie gegenereerd die niet wordt vastgelegd in een ambtsedig proces-verbaal als bedoeld in art. 152 WvSv. Voor die informatie - en voor informatie die wordt gegenereerd en uitgewisseld in het kader van rechtshulpverzoeken of in een verkennend onderzoek (onderzoek ter voorbereiding van de opsporing, art. 126gg WvSv) - gelden in beginsel dezelfde uitgangspunten als voor alle overige informatieproducten.
[79] Cfm. de brief van staatssecretaris van Onderwijs, Cultuur en Wetenschap en de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties van 29 juni 2006, Kamerstukken II, 2005-2006, 29362 nr. 101 (Kabinetsvisie informatie op orde), p. 1.

de sancties uit het strafrechtelijke arsenaal: straffen en maatregelen. De strafrechtsketen "produceert" interventies die hun rechtvaardiging vinden in wetsovertredend gedrag van individuen, d.w.z.: verdachten en veroordeelden.[80] Daaruit volgt dat in ketenperspectief het incident, het individu en de interventie de kernbegrippen zijn. Hierover moet eenduidig voor heel de keten - alle ketenpartijen - informatie worden vastgelegd.

De verbinding tussen deze drie entiteiten (incident, individu, interventie) pleegt van oudsher te worden aangeduid als "de zaak", het pakket informatie (of informatieproducten) dat op zo'n "zaak" betrekking heeft als "het dossier". Een "zaak" kan informatiekundig worden gezien als een samenhangende hoeveelheid werk om voortgang te krijgen met betrekking tot het ophelderen van een incident, het creëren van een afdoening of het tenuitvoerleggen van een interventie. Zo geformuleerd, is het duidelijk dat de inhoud van hetgeen wordt aangeduid als "de zaak" voortdurend aan verandering onderhevig is in de loop van het traject.[81] In de fase van de opsporing staat het incident centraal en wordt gepoogd dit te relateren aan een individu. Als dit is gelukt, is de zaak "opgehelderd"; als bij een incident een verdachte is gevonden, wordt dit in de politiestatistiek geregistreerd als een "opgehelderde" zaak. In de fase van de vervolging en berechting gaat het erom aan de combinatie van incident (ten laste gelegd feit) en individu (verdachte; na bewezenverklaring: dader) een interventie (straf, maatregel) te verbinden.[82] In de fase van de tenuitvoerlegging gaat het uitsluitend nog om de combinatie van interventie (sanctie) en individu (verdachte, veroordeelde). Het "strafdossier" of "procesdossier",[83] op te vatten als een verzameling gegevens en/of informatie-producten, is de fysieke of digitale belichaming van de "zaak". Daarom verandert ook de inhoud van het "dossier" voortdurend in de loop van het traject. Een "dossier" kan informatiekundig worden gezien als een elastiekje om een stapel papier die geselecteerd en samengesteld is met het oog op een te nemen beslissing of een uit te voeren handeling. Die selectie is voorbehouden aan de bevoegde functionaris en de informatiehuishouding moet die selectie faciliteren en niet proberen haar uit handen te nemen van de bevoegde functionaris. De digitalisering moet de bevoegde functionaris de mogelijkheid geven een "digitaal elastiekje" te doen om een door hem geselecteerde hoeveelheid informatieproducten (data, documenten) op basis waarvan hij een beslissing moet nemen of wil uitlokken, dan wel op basis waarvan hij een handeling moet uitvoeren. En zij moet de verdediging en het slachtoffer in staat stellen daar kennis van te nemen en hun stukken aan het dossier toe te voegen.

gegeven, document, depot, archivering

Aan een beslissing liggen gegevens ten grondslag. Die gegevens zijn veelal vervat in documenten. Een "document" kan technisch worden beschouwd als een "bevroren" verzameling gegevens. Als zodanig markeert het een punt in de tijd. Documenten, zoals een proces-verbaal van opsporing, een

[80] Het Nederlands strafrecht kent ook daderschap van rechtspersonen.

[81] Onder "traject" wordt in deze notitie verstaan de gang van een individuele casus of cliënt door het keten-proces (vgl. Ministerie van BZK: Naar een methodisch kader voor ketenregie in het openbaar bestuur. Eindrapportage. BMC, Berenschot, De Verbinding, 16 oktober 2002, par. 2.2 en bijlage 2.)

[82] Het uitvaardigen van een strafbeschikking is door de wetgever gerubriceerd onder "vervolging", maar moet functioneel worden aangemerkt als een vorm van "berechting"; het impliceert de vaststelling van schuld aan een strafbaar feit en van de daarbij behorende sanctie.

[83] Vgl. art 1, onder c, Besluit processtukken in strafzaken: "In dit besluit wordt verstaan onder procesdossier: verzameling van processtukken die tijdens het opsporingsonderzoek aan het dossier zijn of worden toegevoegd".

dagvaarding, een beschikking, een vonnis, een akte van uitreiking of van het instellen van een rechtsmiddel, mogen in de strafrechtspleging doorgaans na het moment van "vaststelling" niet meer worden veranderd; een wijziging, bijvoorbeeld een aanvulling van de tenlastelegging ter zitting, impliceert (informatiekundig bezien) een nieuw document.[84] De informatiehuishouding moet dit punt markeren en de onveranderbaarheid (integriteit) van de documenten waarborgen.[85]

Semantisch kan een "document" worden beschouwd als een betekenisvolle verzameling van samenhangende gegevens in een bepaalde vorm. De samenhang en vorm bepalen vaak mede de betekenis van het document als geheel. Een stuk heeft de status van "proces-verbaal van opsporing" of "dagvaarding" of "vonnis". Verslaglegging is bijvoorbeeld van groot belang om de rechtmatigheid van de opsporing te kunnen controleren.[86] Tevens bepalen de samenhang en de vorm in belangrijke mate de betekenis van de afzonderlijke gegevens. De "gegevens" in dit soort documenten zijn vaak beweringen van mensen, zoals aangevers van strafbare feiten, opsporingsambtenaren, verdachten, getuigen, deskundigen etc., en deze beweringen bezitten een nader te bepalen graad van waarschijnlijkheid. Bijvoorbeeld: dat iets op een bepaalde plaats en tijd is gebeurd, heeft een verschillende betekenis naar gelang het onderdeel uitmaakt van een verklaring van een verdachte of van een getuige in een proces-verbaal van een opsporingsambtenaar, of van een bewezenverklaring in een vonnis van een rechter.

Losse "gegevens" hebben informatiekundig en juridisch in beginsel dezelfde status als "documenten". Wel geldt de eis dat met het oog op de betekenis die het gegeven kan of mag of moet krijgen in de strafzaak te allen tijde ook de status van de drager - als dat niet een document is - helder moet zijn. Anders gezegd: er moet voorzien zijn in een manier waarop of een weg waarlangs het gegeven in het strafgeding kan worden gebracht, die de mogelijkheid van tegenspraak en van duurzame vastlegging en toegankelijkheid waarborgt. Ook moet ervoor gewaakt worden dat een gegeven niet los van zijn context wordt verstrekt c.q. gebruikt. En tot slot kan van burgers niet worden geëist dat zij (uitsluitend) digitaal met de overheid communiceren. Een en ander brengt mee dat "documenten" - digitaal of op papier - een blijvende betekenis hebben in de strafrechtspleging, ook in een volledig digitale werkomgeving.[87] Voor zover de wet eisen stelt aan stukken wat betreft hun vorm of inhoud of ondertekening (fysiek of digitaal), gelden die voor alle soorten zaken, ook voor die welke buiten de rechter om worden afgedaan. Het gaat immers in al die gevallen om de kwaliteit van de informatie die een strafrechtelijke interventie moet dragen. En bovendien: er zijn wel veel strafzaken die de rechter niet bereiken, maar er zijn geen strafzaken die de rechter niet *kunnen* bereiken.

---

[84] Volgens artikel 314 Wetboek van Strafvordering "wordt aan de verdachte door de griffier een gewaarmerkt afschrift van de gewijzigde telastlegging op de terechtzitting verstrekt, tenzij de rechtbank oordeelt dat met de uitreiking van een door de griffier gewaarmerkt afschrift van de wijzigingen kan worden volstaan".

[85] Vgl. bijvoorbeeld de brief van de minister van Veiligheid en Justitie van 26 februari 2015, Kamerstukken II, 2014-2015, 23279, nr. 225 (beleidsreactie op het rapport van de procureur-generaal bij de Hoge Raad «Beschikt en Gewogen; over de naleving van de wet door het Openbaar Ministerie bij het uitvaardigen van strafbeschikkingen»), p. 3: "Op het moment van de schuldvaststelling dient alle daarvoor gebruikte bewijsinformatie schriftelijk of electronisch vastgelegd en beschikbaar te zijn en dient die informatie op een later tijdstip gereproduceerd te kunnen worden".

[86] M.J. Borgers in Delikt en Delinkwent 2015, p. 148.

[87] Ook gebruikersgemak en ergonomische overwegingen kunnen rechtvaardigen dat mensen tot op zekere hoogte met "papier" (blijven) werken.

verantwoordelijkheid

Centraal in de visie staat "verantwoordelijkheid" in bestuurlijke, juridische en politieke zin. Een informatieproduct kan op technisch (c.q. "fysiek") niveau eenmalig worden beheerd, maar functioneel c.q. in juridische zin kan er sprake zijn van meer dan één "verantwoordelijke" (in de zin van de Wet bescherming persoonsgegevens) voor de verwerking van een bepaald persoonsgegeven. Die verantwoordelijkheid heeft immers betrekking op alles wat met informatieverwerking te maken heeft: gegevens (data), informatie, semantiek (betekenis), berichtenverkeer, systemen, verbindingen, datatransport. Zij omvat dus het verzamelen, opslaan, gebruiken, bewaren, archiveren, regelen van toegang en (duurzame) beschikbaarheid en toegankelijkheid, beheer en onderhoud, kwaliteit, verstrekken, uitwisselen, muteren en vernietigen van gegevens, continuïteit van systemen, verbindingen en bedrijfsvoering (business continuity management), beveiliging van gegevens, verbindingen en systemen, naleving van regelgeving. De verantwoordelijkheden ten aanzien van al deze aspecten moeten worden beschreven en vastgelegd. Daarbij is het mogelijk dat met betrekking tot verschillende aspecten van eenzelfde gegeven of type gegeven, verantwoordelijkheden bij verschillende partijen tegelijk komen te liggen. Sterker nog, dit kan zelfs ten aanzien van een-en-hetzelfde aspect het geval zijn. Wanneer bijvoorbeeld een gegeven volgens de regels die voor partij A gelden moet worden vernietigd, maar volgens de regels die voor partij B gelden nog moet worden bewaard, geldt (uiteraard) de langste bewaartermijn; gewaarborgd moet dan worden dat partij A er niet meer bij kan. Dat is nu, in de papieren wereld, ook al zo, met dien verstande dat er nu sprake is van een veelheid van documenten in technische c.q. fysieke zin, die zich op meer dan één plek bevinden. In een digitale omgeving waarin enkelvoudig technisch beheer is gerealiseerd, vergt dit nieuwe doordenking, niet alleen aan de kant van de techniek maar ook aan de kant van de regelgeving.[88]

Die verantwoordelijkheden bestrijken ook alle niveaus van de organisatie: het operationele niveau, de inrichting en het beheer van de processen en het strategische niveau, en dienen op al die niveaus te zijn belegd.

verantwoordelijkheden in digitale omgeving

Technisch is een gegeven of een document - op fysiek niveau - niets anders dan een hoeveelheid elektromagnetische signalen in een machine. Op iets hoger niveau is het een verzameling "nullen en enen" ergens op een server. Ook dat is nog zonder enige "betekenis" in de gangbare zin; gebruikers kunnen hier nog niets mee. Pas op de "hoogste" laag in het informatiesysteem, de toepassingslaag (applicatielaag), wordt het gegeven of document betekenisvol voor de gebruikers.[89] Hier ligt een wezenlijk verschil met de papieren wereld, waarin de fysieke verschijningsvorm volledig samenvalt met het document-met-betekenis (de semantische verschijningsvorm). Dit heeft consequenties voor discussies over het beheer van informatie en gegevens. De integriteit moet door heel het keten-proces heen en op alle lagen gewaarborgd zijn. Een "slotgracht"-conceptie ("wij zijn verantwoordelijk voor de documenten die wij zelf bezitten en schermen die af") werkt niet meer,

[88] Dit laatste in het kader van de herziening van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens in hun onderlinge samenhang, zoals aangekondigd in de brief van 23 juni 2014, Kamerstukken II, 2013-2014, 33842, nr. 2 (beleidsreactie evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens).

[89] De "applicatielaag" is de hoogste van de zeven lagen in het "OSI-model". Het OSI-model is een door ISO gestandaardiseerd referentiemodel voor datacommunicatiestandaarden, ter bevordering van de inter-operabiliteit tussen heterogene netwerktopologieën. "OSI" staat voor "Open Systems Interconnection".

verantwoordelijkheden moeten op een nieuwe manier worden ingevuld. Omgang met informatie is ook niet iets wat in de kolom van beheer (ondersteuning) kan worden gepositioneerd; het is een integraal onderdeel van het primaire proces en hoort dus thuis in de kolom van het "gezag". De digitalisering brengt sowieso mee dat de verantwoordelijkheid voor wat er met een gegeven, document of dossier gebeurt, veel directer dan tot nu toe bij de professional zelf komt te liggen. Veel van de ondersteunende administratieve functies die ten aanzien van papieren documenten door anderen dan de professional plegen of plachten te worden uitgevoerd, zoals archiveren, beheren of distribueren (waaronder kopiëren), worden immers overbodig.

Alle informatieproducten (data, documenten, dossiers) moeten voorts gedurende een door de wet bepaalde tijd worden bewaard. Voor ieder gegeven of informatieproduct moet er een instantie zijn die rechtens verantwoordelijk is voor het beheer gedurende die periode en voor de vernietiging ervan als de bewaartermijn is verstreken.[90] Dit wordt niet anders als de verantwoordelijke voor de opslag en archivering gebruik maakt van de diensten van anderen, bijvoorbeeld van dienstverleners in de informatiesamenleving (cloud, digitaal depot, Trusted Third Party). De aansprakelijkheid van die dienstverleners varieert naar gelang van de handelingen die zij zelf met de aan hen toevertrouwde informatie uitvoeren.[91]

[90] Vgl. artt. 1, onder d, 13, 15 Wet bescherming persoonsgegevens (Wbp).
[91] Zie artikel 6:196c Burgerlijk Wetboek (BW).