DE VERDACHTE IN DE KETENS

Informatie delen
in ketens en netwerken

Wim Borst

Boombestuurskunde

De verdachte in de ketens

De verdachte in de ketens

Informatie delen in ketens en netwerken

Wim Borst

Boom bestuurskunde
Den Haag
2019

Omslagontwerp: Textcetera, Den Haag
Opmaak binnenwerk: Textcetera, Den Haag

ISBN 978-94-6236-892-7
ISBN 978-94-6274-971-9 (e-book)
NUR 741

www.boombestuurskunde.nl

What is important is not the tools. It is the concepts behind them.

Peter Drucker

(The Essential Drucker)

VOORWOORD

'Informatie delen moet', aldus de openingszin van dit boek. Alhoewel het uitwisselen en daarmee verspreiden van informatie in de huidige tijd welhaast ongebreidelde vormen lijkt te hebben aangenomen, is de noodzaak tot het delen van informatie van alle tijden. Grottekeningen, kleitabletten, gebaren en zelfs muziekstukken: slechts enkele voorbeelden van systemen die wij mensen door de eeuwen heen hebben ontwikkeld en benut om informatie te delen. En ook destijds gold: informatie delen moet, wilde immers de mens overleven, innoveren of gewoon ontspannen.

In dit boek staan twee begrippen centraal die vrijwel onlosmakelijk zijn verbonden met ons hedendaagse instrumentarium voor het delen van informatie: netwerken en ketens. Het eerste verwijst naar een relatief open verband waarbij verschillende onderdelen (knooppunten) in relatie staan tot andere onderdelen via veelvoudige, doorkruisende en vaak redundante verbindingen. Via deze verbindingen wordt informatie gedeeld. Anders dan bij netwerken, wordt informatie in ketens in een lineair proces gedeeld. Verschillende organisaties werken buiten hun eigen organisatiegrenzen aan een gemeenschappelijk resultaat en delen daartoe via een gestructureerde uitwisseling hun informatie. De volgorde waarin onderdelen en actoren hun plaats in de keten innemen, wordt bepaald door het probleem dat opgelost moet worden, dan wel de dienst die of het product dat geleverd moeten worden.

Wie een blik werpt op de terminologie die de Nederlandse overheid in haar officiële stukken hanteert, stelt vast dat bij informatie-uitwisseling veelal wordt gesproken in termen van 'ketens' en een 'ketenbenadering'. Niet verrassend. Binnen de overheid is het delen van informatie immers in principe gereguleerd en die stroomt daarmee niet 'vrij' tussen actoren, maar volgens afgesproken routes. Toch is de dagelijkse realiteit dat ook binnen de overheid informatie wordt

gedeeld via verbindingen die dynamisch, flexibel en adaptief zijn. De term netwerk is in dat geval veel meer op z'n plaats.

Startpunt van het betoog waar Wim Borst ons in dit inspirerende, rijke en uiterst verhelderende boek in meeneemt, is de constatering dat nogal eens wordt geroepen dat het denken in ketens verouderd is. Netwerken zouden de toekomst hebben. Ook binnen de overheid. Ten onrechte, aldus Borst. De twee hebben elkaar nodig. Sterker nog, zo luidt een van zijn conclusies, het begrip keten is onmisbaar als verankering van de rechtsstaat. Dat geldt in het bijzonder voor het domein waar dit boek zich specifiek op richt: de strafrechtspleging.

Het belang van de analyse en het betoog van Wim Borst wil ik, afrondend, onderstrepen met de volgende observatie. We hanteren allemaal weleens, met een zeker gemak, de termen ketens en netwerken. Alsof ze inwisselbaar zijn. Alsof er van de typerende en daarmee onderscheidende kenmerken van elk van deze twee te abstraheren valt. Maar zeker voor de huidige tijd geldt dat het instrumentarium waarmee we informatie delen vrijwel nooit neutraal is. Technologie en daarmee op technologie gebaseerde ketens en netwerken veranderen, beide vanuit hun specifieke kenmerken, onze wereld. Zo ook veranderen ze de mogelijkheden, rol, positie en zelfs macht van het openbaar bestuur. Met vervolgens de nodige implicaties voor de (rechts)positie van burgers. Wie zich een goed beeld wil vormen van deze veranderingen kan niet anders dan een scherp oog hebben voor de intrinsieke waarde van het onderscheid tussen netwerken en ketens.

Corien Prins
Voorzitter Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en hoogleraar recht en informatisering, TILT/Universiteit Tilburg

LEESWIJZER

Informatie delen móet. Wij leven in een netwerksamenleving. Ketensamenwerking is de sleutel voor de aanpak van veel maatschappelijke problemen. Drie open deuren. Samen leiden zij naar de kernvraag waar dit boekje over gaat: hoe verhouden de begrippen 'keten' en 'netwerk' zich tot elkaar en wat betekent dat voor de rechtsstaat Nederland? Er wordt nogal eens geroepen dat we af moeten van het idee van ketens, dat zou verouderd denken zijn. In plaats daarvan zouden we moeten spreken van netwerken. Mijn stellingen zijn: (1) de twee begrippen hebben elkaar nodig, en (2) het ketenconcept is onmisbaar als verankering voor de rechtsstaat. Het boek is daarmee geen handleiding voor het maken van ICT-systemen of privacy impact assessments (PIA's); het gaat over de *concepts*, niet over de *tools*.

In het eerste hoofdstuk werk ik de centrale stellingen uit. Ik doe dat vanuit de invalshoek van informatievoorziening (hierna: IV) en vanuit het uitgangspunt 'keteninformatisering heeft de toekomst' (zoals Corien Prins het eens uitdrukte tijdens een lezing op 9 maart 2010 in een achterafzaaltje aan het Plein in Den Haag). In de daaropvolgende hoofdstukken spits ik mijn kernboodschap toe op de thema's gegevensbescherming en strafrechtspleging. In de meeste handhavingsarrangementen is strafrecht immers de harde kern. Dus als het gaat om informatie delen in ketens en netwerken, komen we vaak uiteindelijk bij strafrecht uit. Bovendien is strafrecht mijn eigenlijke vak. Daarom zal ik vooral daaraan mijn voorbeelden en toepassingen ontlenen.

Ik mik op drie kringen van lezers:

1. Degenen die werken *aan* de informatievoorziening (automatisering, informatisering, digitalisering). Dat betreft onder meer informatiemanagers, architecten, ICT'ers, beleidmakers, juristen, adviseurs, consultants, wetgevers, professionals die participeren in programma's en projecten, project- en programmaleiders, managers, bestuurders.

2. De wetenschappelijke wereld. Dat betreft bestuurskundigen, juristen en informatici die zich bezighouden met de bestudering van organisaties, ketens en netwerken. Zij zijn ook vaak de externe adviseurs van organisaties die hun plek in een keten moeten vinden. Vanwege mijn achtergrond heb ik meer in het bijzonder de wereld van de strafrechtswetenschap op het oog.
3. Degenen die in de praktijk – binnen en buiten de strafrechtspleging – werken *met* de IV die hun ten dienste staat. Dat betreft de professionals in het primaire proces. Velen van hen worden geconfronteerd met een wirwar aan systemen en zien door de bomen het bos niet meer. Dit boekje wil hen, voor zover het de strafrechtsketen betreft, helpen het bos te zien: niet de losse systemen, maar de IV in haar samenhang.

Ik verwijs in dit boek nog naar de artikelen uit het huidige Wetboek van Strafvordering van 1926. Dat wetboek wordt helemaal gemoderniseerd, lees: opnieuw geschreven. Maar voordat dat allemaal in het *Staatsblad* staat en in werking is getreden, duurt nog wel even; dat maak ik in mijn ambtelijke leven niet meer mee.

Voor hun commentaar op conceptversies van de tekst ben ik dank verschuldigd aan (in alfabetische volgorde) Adri van Amelsvoort, Rocus Brasz, Klaas Brongers, Ronald van den Hoogen, Annelise van Kleef, Daan de Koning, Ronald Meijer, Marcella van Ommen, Mirjam de Natris, Bertine Steenbergen, Kam Mai Tan, Albert Vermeer, Richard de Wit en Merel Zwaaneveld. Tevens dank ik het ministerie van Justitie en Veiligheid, en in het bijzonder het directoraat-generaal Rechtspleging en Rechtshandhaving (DGRR), dat het mij de ruimte heeft geboden om dit boek – en ook mijn vorige boek[1] – te schrijven.

Wim Borst
Zoetermeer/Den Haag, oktober 2018

Noot

1 Jegens en Wegens; Over persoonsgebonden informatie in de strafrechtsketen, tweede druk, 2010.

INHOUD

AFKORTINGEN

AICE	Administratie- en informatiecentrum voor de executieketen
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming (EU 2016/679)
Bibob	Wet bevordering integriteitsbeoordelingen openbaar bestuur
Bivv	Besluit identiteitsvaststelling verdachten en veroordeelden
Bjsg	Besluit justitiële en strafvorderlijke gegevens
BRP	Basisregistratie Personen
BSN	burgerservicenummer
BVID	Basisvoorziening identiteitsvaststelling
CBP	College bescherming persoonsgegevens (voorloper van de AP)
CDD	Centraal Digitaal Depot
CDM	Canoniek datamodel
CJIB	Centraal Justitieel Incassobureau
DJI	Dienst Justitiële Inrichtingen
DPIA	Data Protection Impact Assessment
EBV	elektronisch berichtenverkeer
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
IIPB	integraal en integer (strafrechtelijk) persoonsbeeld
IV	informatievoorziening
JD	Justitiële documentatie
JDS	Justitieel documentatiesysteem
Justid	Justitiële Informatiedienst
NAW	naam, adres, woonplaats
NFI	Nederlands Forensisch Instituut
NIFP	Nederlands Instituut voor Forensische Psychiatrie en Psychologie
NSCR	Nederlands studiecentrum voor criminaliteit en rechtshandhaving
OM	Openbaar Ministerie
OvJ	officier van justitie
PIA	privacy impact assessment

pv	proces-verbaal
Rgbs	Richtlijn gegevensbescherming strafrecht (EU 2016/680)
RIEC	Regionaal Informatie- en Expertisecentrum
SKDB	strafrechtsketendatabank
SKN	strafrechtsketennummer
Sv	Wetboek van Strafvordering
TBV	taken, bevoegdheden en verantwoordelijkheden
(Wet) USB	(Wet) herziening tenuitvoerlegging strafrechtelijke beslissingen
VIP(S)	Verwijsindex Personen (Strafrechthandhaving)
VOG	Verklaring omtrent het gedrag
Wahv	Wet administratiefrechtelijke handhaving verkeersvoorschriften (ook wel genoemd Wet-Mulder)
Wbp	Wet bescherming persoonsgegevens
Wet JD	Wet op de justitiële documentatie en de verklaringen omtrent het gedrag (= voorloper van de Wjg)
Wivvg	Wet identiteitsvaststelling verdachten, veroordeelden en getuigen
Wjg	Wet justitiële gegevens (= voorloper van de Wjsg)
Wjsg	Wet justitiële en strafvorderlijke gegevens
WODC	Wetenschappelijk onderzoek- en documentatiecentrum (van het ministerie van Justitie en Veiligheid)
Wpg	Wet politiegegevens
ZSM	'Zo Snel, Slim, Selectief, Simpel, Samen en Samenlevingsgericht Mogelijk'

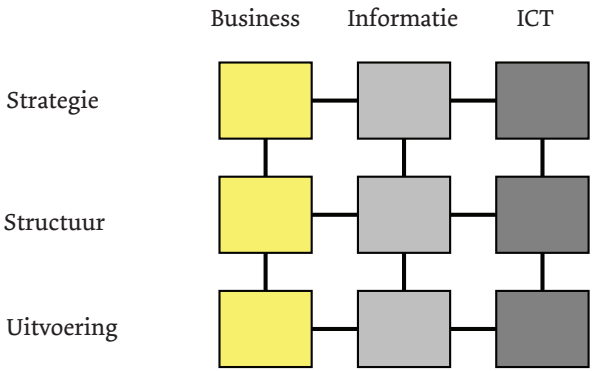
HOOFDSTUK 1

KETENS, NETWERKEN EN DE RECHTSSTAAT

1.1 IV is iets anders dan ICT

Informatievoorziening (IV) is in dit boekje mijn belangrijkste invalshoek. Daarom (voor de niet-informatici onder de lezers) in deze paragraaf eerst wat elementaire begrippen rond IV.

Allereerst: IV is niet hetzelfde als ICT. Het Amsterdamse negenvlak maakt dat in één oogopslag duidelijk:[1]



Business gaat over wat de organisatie feitelijk doet, dat waartoe zij bestaat. Vanuit de linkerkolom, de *business*, ontstaat de informatiebehoefte. Die wordt in de middelste kolom vertaald naar gegevenssoorten en informatiestromen. En die worden op hun beurt vertaald naar systemen, applicaties, programmatuur (software), apparatuur (hardware, stekkers en dozen); dat is de rechterkolom. Omgekeerd: van rechts naar links gaat het achtereenvolgens om beschikbaar

stellen, interpreteren en gebruiken van informatie. De business creeert de vraag, de techniek (ICT) het aanbod.

De drie *rijen* betreffen de bedrijfsvoering en de sturing:
- Uitvoering (*verrichten*) is het niveau waar het eigenlijke werk wordt gedaan: lesgeven aan leerlingen, behandelen en verplegen van zieken, produceren van fietsen, verwerken van belastingaangiften, opsporen, berechten en bestraffen van wetsovertredingen respectievelijk wetsovertreders. Dit is het niveau van het primaire proces.
- Structuur (*inrichten*) faciliteert de uitvoering en maakt de productie mogelijk. Het gaat op dat niveau om het zorgen dat er voldoende personeel is, dat er opleidingen zijn, machines, grondstoffen, gebouwen, werkinstructies, werkplanningen, dat de producten worden verkocht, enzovoort.
- Strategie ten slotte (*richten*) gaat over de vraag welke producten de organisatie wil maken, welke markten zij wil bedienen, welke waarden zij wil realiseren. Strategie betreft de vraag 'doen we de goede dingen (= wat, waarom, waartoe, voor wie)', structuur betreft de vraag 'doen we de dingen goed (= hoe)'.

Dit negenvlak is geen organisatiemodel en schrijft ook niets voor. Het is een landkaartje, handig om te bepalen wáár je op een bepaald moment in een onderzoek of in een discussie bent. Dit boekje gaat over de middelste kolom: informatie.

In de tweede plaats: het begrip *informatie* is dubbelzinnig. Het wordt op twee niveaus gehanteerd: op casusniveau en op geaggregeerd niveau. Iedereen snapt dat de chirurg die een operatie uitvoert, daarvoor andere informatie nodig heeft dan de directeur die het ziekenhuis economisch en financieel draaiende moet houden. De chirurg heeft medische kennis nodig en informatie over de individuele patiënt die aan zijn zorg is toevertrouwd. De directeur heeft

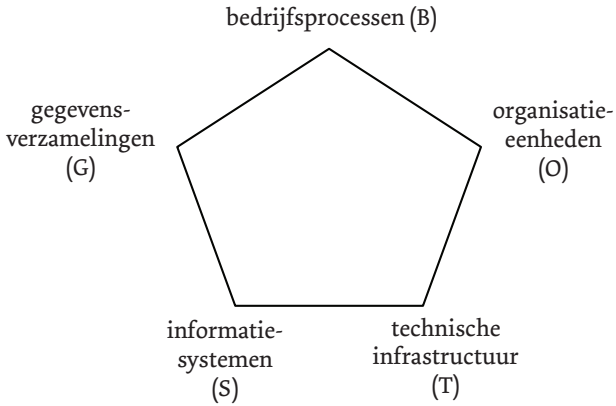
bedrijfskundige kennis nodig en geaggregeerde informatie: cijfers over aantallen patiënten, soorten behandelingen, personeel, doorlooptijden, kosten, prijzen, enzovoort. Die cijfers interesseren de chirurg niet op het moment dat hij staat te opereren (dat hoop ik tenminste als ik de patiënt ben). Omgekeerd is de directeur niet geïnteresseerd in de medische informatie. Sterker nog, die mág hij zelfs niet weten: de arts is ook naar de directeur toe tot medische geheimhouding verplicht.

De geaggregeerde informatie (voor de directeur) duid ik aan als informatie *over* de keten, de informatie in en voor het primaire proces (voor de chirurg) noem ik informatie *in* de keten. Informatie *in* de keten betreft informatie over de individuele casus: de zaak, de feiten en omstandigheden, de verdachte, de patiënt, enzovoort. Dat gaat over persoonsgegevens in juridische zin.

In de strafrechtspleging spreken we sinds een jaar of vijftien over het *integraal en integer (strafrechtelijk) persoonsbeeld* (IIPB). Dat heeft betrekking op informatie *in* de keten. Het IIPB is onderdeel van de informatiepositie van de professional. Maar als je met managers praat, gaat het meestal over beleids- of managementinformatie en over systemen. Bij beleidmakers ook. In dit boekje richt ik mij op de informatie *in* de keten, de operationele informatie.

Heel wat brieven aan de Tweede Kamer staan vol met verwijzingen naar allerlei systemen. Terecht? Nee. Systemen (= stukken hardware en software) horen thuis in de rechterkolom, de ICT. Dat zijn slechts hulpmiddelen, *tools*, net als de auto's waarin politieagenten rijden. Het politieke debat hoort te gaan over wat we met die hulpmiddelen dóen. En dat vind je in de middelste en de linkerkolom: het verwerken en het gebruiken van informatie. Het is daarom van

belang goed onderscheid te maken tussen informatiesystemen en gegevensbestanden. De *informatiester* maakt dit duidelijk:[2]



We kunnen de informatiester vertalen naar de taal van privacy en gegevensbescherming:

- 'gegeven' c.q. 'gegevensverzameling' refereert aan 'verwerken' (wat doe je met of aan de gegevens),
- 'proces' refereert aan 'noodzaak' (*need to know*, doelbinding), en
- 'organisatie' refereert aan 'verwerkingsverantwoordelijke'.

De onderste twee punten van de ster, informatiesysteem en infrastructuur, refereren aan techniek en zijn daarom uit oogpunt van privacy en gegevensbescherming niet van belang. Met deze conceptuele *toolkit* kun je 80% van de privacyvraagstukken zelf oplossen, zonder hulp van juristen. De resterende 20% behandel ik in de hoofdstukken 2 en 5 van dit boek.

Zo is bijvoorbeeld de justitiële documentatie (JD; zie par. 5.4) een gegevensverzameling, het Justitieel documentatiesysteem (JDS) een informatiesysteem. De JD heeft als zodanig een wettelijke grondslag, namelijk in de Wet justitiële en strafvorderlijke gegevens (zie par. 5.1), het JDS niet. Scherper gezegd: je zou de Justitiële documentatie (JD) als gegevensverzameling in principe overal kunnen onderbrengen, voor mijn part in Baidu (de Chinese *cloud*) of bij wijze van spreken op de maan. Er zijn misschien goede redenen om dat niet te doen, maar de wet staat er niet aan in de weg – en de techniek ook niet.

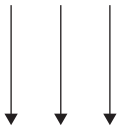
1.2 Een keten is iets anders dan een netwerk

Het onderscheid tussen *keten* en *netwerk* is het centrale thema in dit boekje. Ik signaleer aan de ene kant dat er te pas en te onpas wordt gesproken over ketens. Zodra een situatie een beetje ingewikkeld wordt, met meer dan twee partijen, roepen mensen al gauw: 'Dit is een keten!' Aan de andere kant signaleer ik een tendens om het ketenbegrip af te schrijven en te vervangen door het begrip netwerk. 'Eigenlijk moeten we niet van ketens spreken, maar meer van netwerken', heet het dan. Ik houd het in beide gevallen op een gebrekkige begripsvorming. Ik ga daarom eerst uitleggen wat ik bedoel als ik spreek over keten en netwerk.[3] Ik doe dat aan de hand van een artikel van Henry Mintzberg, de Canadese managementgoeroe, en Ludo Van der Heyden uit 1999 (*Harvard Business Review*), dat ik hierna parafraseer.

Ketens en netwerken zijn vormen van *afhankelijkheid*. Afhankelijkheid kent volgens Mintzberg en Van der Heyden vier vormen:

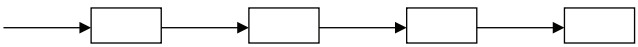
1. de *set*;
2. de keten (*chain*);
3. het wiel (*hub*);
4. het netwerk (*web*).

De eerste vorm, de *set*, ziet er zo uit (de plaatjes in deze paragraaf komen uit het genoemde artikel):



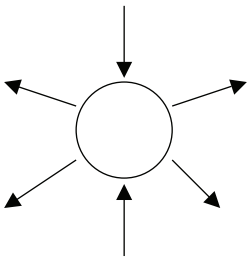
Veel dienstverlenende bedrijven, bijvoorbeeld advocatenkantoren, vertonen de structuur van de *set*. De advocaten werken hoofdzakelijk met hun eigen cliënten. Zij zijn losjes met elkaar verbonden (*loosely coupled*) en delen vooral een aantal gezamenlijke bronnen (*pooled interdependence*): huisvesting, facilitaire diensten, infrastructuur, administratieve ondersteuning, financiële middelen, de *branding*, bestuursstructuren – anders zouden ze überhaupt geen deel uitmaken van dezelfde organisatie. In dat opzicht zijn ze – tot op zekere hoogte – afhankelijk van elkaar. Voor het overige werken ze goeddeels op zichzelf.

Een iets geavanceerdere vorm van samenwerking is de *chain*, de keten. Als prototype daarvan dient de assemblagelijn van een auto (lopende band). De *chain* ziet er als volgt uit:



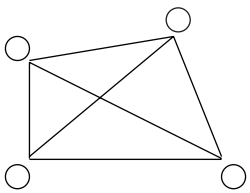
De keten kent seriële afhankelijkheid (*sequential interdependence*). Elke eerdere stap is een noodzakelijke voorwaarde voor elke latere. Het is niet per se ook een voldoende voorwaarde: een zaak hoeft niet per se de hele keten te doorlopen, trajecten kunnen halverwege worden afgebroken. Denk bijvoorbeeld aan een sepot in een strafzaak: het komt dan nooit tot tenuitvoerlegging van een straf. Het sequentiële moet vooral logisch gedacht worden; volgtijdelijkheid is bijkomstig.

Veel sociale en fysieke processen zijn ingewikkelder. Er zijn twee alternatieven voor de keten. De eerste is de *hub*, het wiel (*hub* = naaf, spil, middelpunt):



In een wielstructuur is sprake van een coördinerend middelpunt. Het is een fysiek of een virtueel punt waar mensen en dingen of informatie naartoe gaan of vandaan komen. Een gebouw kan zo'n middelpunt zijn, bijvoorbeeld een school of een vliegveld. Maar het kan ook een machine zijn, bijvoorbeeld een computer, of een mens, bijvoorbeeld een coach. Teken bijvoorbeeld een grote cirkel om een fabriek heen, die ook de hele productielijn omvat, en de hele plek gaat eruit zien als een wiel, waar dingen en mensen in en uit gaan.

De meest complexe vorm van afhankelijkheid is het *web*, het netwerk. Hier is sprake van *reciprocal interdependence*, wederzijdse afhankelijkheid en beïnvloeding:



Netwerken zijn rasters zonder middelpunt (*grid with no center*). Ze laten communicatie in alle richtingen toe en een onafgebroken beweging van mensen en ideeën. Het *world wide web* (www) is een typisch voorbeeld van een netwerk. Ook de meeste samenwerkingsverbanden hebben de structuur van een netwerk.

De vier vormen hoeven elkaar niet uit te sluiten, ze kunnen gelijktijdig bestaan, zoals het voorbeeld van de cirkel om de fabriek laat zien. Ze kunnen ook in elkaar genesteld zijn, bijvoorbeeld ketens binnen *hubs* of netwerken. Ook door één organisatie kunnen meer ketens lopen. Een goed voorbeeld is de politie. Die heeft taken in (onder meer) het strafrecht (namelijk: opsporing), het vreemdelingenrecht, het verkeersrecht, het bestuursrecht, de openbare orde, de hulpverlening. Dat zijn allemaal verschillende ketens. De meeste organisaties in het strafrechtelijke domein hebben ook rollen (taken, bevoegdheden, verantwoordelijkheden) in andere ketens.

Bij *pooled interdependence* functioneren de onderdelen min of meer los van elkaar. Disfunctioneren van een onderdeel heeft doorgaans geen directe consequenties voor andere onderdelen, maar schaadt wel het geheel. Voorbeeld: een advocaat die door een beroepsfout een zaak verliest en daarmee tegelijk zijn kantoor in opspraak brengt. Bij *sequential interdependence* leidt disfunctioneren in een vorige schakel (= stap in het proces) al gauw tot problemen in één of meer volgende schakels. *Problems and errors have a tendency to travel downstream*. Voorbeeld: een verdachte geeft bij aanhouding een valse naam op, onder die naam gaat de zaak de keten door en aan het eind komt er een veroordeling op een verkeerde naam.

1.3 Het analyseren van een keten

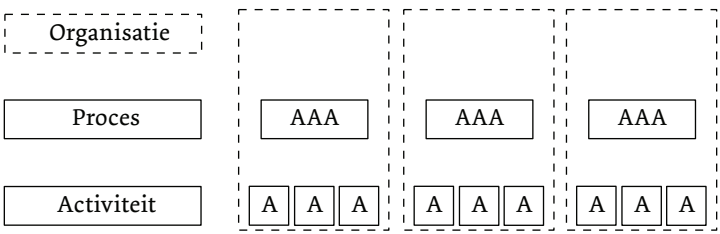
In deze paragraaf werk ik het ketenconcept nog wat verder uit, om het in de volgende paragraaf te confronteren met het netwerkconcept. Vraag bijvoorbeeld een willekeurige persoon hoe de strafrechtsketen eruit ziet en hij zal in de meeste gevallen zeggen: dat is politie, openbaar ministerie, rechtspraak, gevangeniswezen en reclassering. Ook in wetenschappelijke en beleidsdocumenten kun je omschrijvingen van dit type aantreffen. Ze definiëren de keten vanuit de *organisaties*. Ik geef de voorkeur aan een definitie vanuit het *proces*. Want de gegeven definitie van de strafrechtsketen laat al zien dat die ondeugdelijk is. Alle organisaties hebben immers taken in meer dan één fase van het

proces. De politie moet niet alleen strafbare feiten ophelderen (= een verdachte vinden), maar ook veroordeelden aanhouden; de officier van justitie (hierna: OvJ) gaat over de opsporing en brengt een zaak aan bij de rechter; de rechter moet beslissingen geven in de voorfase (over de voorlopige hechtenis) en op de terechtzitting en in de fase van tenuitvoerlegging, enzovoort. Hoe kun je dan een goed beeld van de keten opbouwen als de organisaties zo door elkaar lopen?

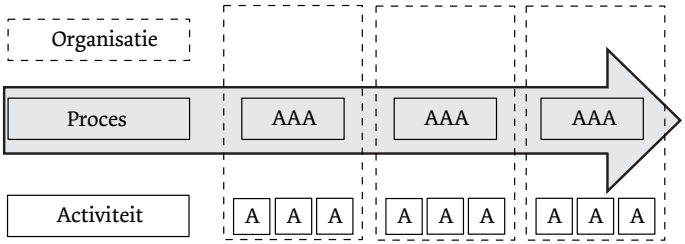
De analyse van de keten moet beginnen bij datgene waar het uiteindelijk om te doen is: het resultaat. Om te overleven, hebben wij goederen en diensten nodig. Dat noemen wij *producten*. Producten komen niet uit de lucht vallen, er moet iets worden gedaan om ze te produceren. Dat noemen we *activiteiten*:

Een aantal samenhangende activiteiten noemen wij een *proces*:

En om processen heen bouwen wij *organisaties*. Dat vergemakkelijkt de samenwerking en maakt die robuuster.



Een aantal processen door verschillende organisaties heen noemen wij een *keten*. Een keten ziet er dus zo uit:



De organisaties zijn, oneerbiedig gezegd, in meer of mindere mate toevallige passanten op de weg. Organisaties komen en gaan, zij veranderen, worden gereorganiseerd, opgeheven, samengevoegd, gesplitst. Processen daarentegen zijn stabieler, in elk geval op een wat hoger niveau van abstractie.

De keten is dus een productieproces. Nauwkeuriger gezegd: *een keten is een sequentieel proces waarin diverse, onderling in bestuurlijk opzicht onafhankelijke actoren werken aan een gemeenschappelijk resultaat*.[4] Dat resultaat, het ketenproduct, wordt gedefinieerd in termen van *output*, dat is het product – dienst of goed – dat de organisatie maakt, niet in termen van *outcome* (dat is: het beoogde maatschappelijk effect van dat product). Dus bijvoorbeeld in het domein van de zorg: niet gezondheid, maar een medisch advies of een medische interventie die bijdraagt aan betere gezondheid. En in het domein van het strafrecht: niet criminaliteitsbeheersing of vergroten van de veiligheid, maar een strafrechtelijke interventie die wordt toegepast tegen een verdachte vanwege een gepleegd strafbaar feit dat die heeft gepleegd. Of kortweg: 'de wetsovertreding wordt bestraft'. Dát is de maatschappelijk relevante prestatie van de strafrechtsketen, het ketenproduct (zie par. 3.1).

Een *traject* bestaat uit alle activiteiten in een keten waar er sprake is van een contact tussen een cliënt en een professional en waar afspraken tussen de betrokken professionals of tussen de professionals en de cliënt worden gemaakt. De keten is het abstracte institutionele

arrangement, het traject is de concrete gang van de afzonderlijke cliënt door de keten. Bijvoorbeeld: bij elke nieuwe verdenking wordt een nieuw traject gestart en wordt de identiteit van de verdachte vastgesteld. Dan kan blijken dat de keten hem al kent, dat wil zeggen herkent: hij is al eens geregistreerd en heeft al antecedenten (eerdere verdenkingen, veroordelingen) op zijn naam staan. Zo niet, dan moet hij alsnog geregistreerd worden.

Organisaties of functionarissen worden aangeduid als *actoren*. Een actor is een persoon, afdeling, organisatie, die handelingen verricht of beslissingen neemt; kortom: een actieve partij in de keten. Een stap of activiteit in het proces wordt beschreven met een werkwoord. De organisatie is de plek waar de activiteit wordt uitgevoerd. De organisaties in een keten zijn operationeel van elkaar afhankelijk (niemand kan het ketenproduct in z'n eentje produceren), maar bestuurlijk in meer of mindere mate autonoom, in elk geval ten opzichte van elkaar.

Een keten wordt dus gedefinieerd door drie P's: product, proces en partijen. De analyse van een keten kan en moet dan ook een eenvoudig, vast stramien volgen:

1. Bepaal allereerst wat het gemeenschappelijke resultaat, het gezamenlijke *product* is.
2. Teken vervolgens het *proces* waarin dat product wordt gemaakt, als logisch geordend geheel van activiteiten.
3. Kijk ten slotte welke *partijen* (organisaties, actoren) die activiteiten uitvoeren. Soms is een activiteit exclusief belegd bij één actor, soms kan een activiteit door meer dan één actor worden uitgevoerd. Een dagvaarding uitbrengen kan alleen de OvJ; maar een vrijheidsbenemende of vrijheidsbeperkende sanctie kan worden ten uitvoer gelegd door honderden partijen in het domein van detentie en forensische zorg.

Mensen beginnen de analyse vaak vanaf de verkeerde kant. Ze kijken met welke partijen ze aan tafel zitten (vaak is dat min of meer zo ontstaan) en vervolgens wat die partijen daar zo ongeveer doen. En dan lopen ze vast in de complexiteit. Logisch, want netwerken creëren onduidelijkheden (zie par. 1.5).

Binnen het domein van Justitie zijn er volgens de hier gegeven definitie drie ketens: de strafrechtsketen, het vreemdelingenrecht (misschien bestaat vreemdelingenrecht wel uit diverse ketens, dat weet ik niet precies) en jeugdbescherming (JB). JB betreft het gedwongen kader, dus jeugdzorg die verplicht wordt opgelegd op grond van het Burgerlijk Wetboek, waar een rechter aan te pas komt. (Daarnaast hebben we jeugdzorg en jeugdstrafrecht. Jeugdzorg gaat buiten Justitie om. Jeugdstrafrecht is gewoon een onderdeel van het strafrecht, maar met wat bijzondere wettelijke bepalingen en wat bijzondere partijen.) De justitiële ketens zijn van A tot Z juridisch gereguleerd en die regelgeving is ketengewijs opgezet. De keten bepaalt de taken en bevoegdheden en daarmee (meestal impliciet) ook de verantwoordelijkheden. Binnen Justitie wordt ook wel gesproken over de civiele keten en de bestuursrechtelijke keten; maar dat zijn volgens de hier gegeven definitie geen ketens. *De* jeugdketen bestaat ook niet, dat zijn drie ketens: jeugdstrafrecht, jeugdbescherming en jeugdzorg. De slachtofferketen is een soort van parallelketen naast of subketen binnen de strafrechtsketen, waarin niet de verdachte maar het slachtoffer centraal staat als cliënt.

1.4 Een keten is altijd tevens een netwerk (maar niet omgekeerd)

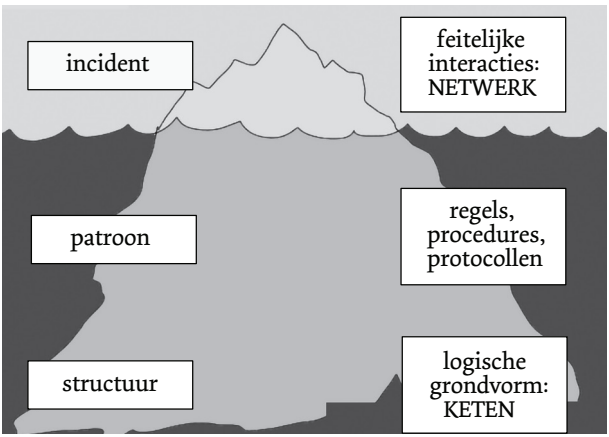
De definities van keten en netwerk zijn geen absolute waarheden; het zijn mentale constructies die je helpen de goede dingen te doen, stukken conceptueel gereedschap die je helpen ordening aan te brengen in een complexe werkelijkheid. *Een keten is altijd tevens een netwerk*. Op het actorniveau is er in een keten immers conform de gangbare definitie altijd sprake van over organisatiegrenzen heen samenwerkende partijen. Het omgekeerde geldt niet: een netwerk hoeft geen keten te zijn.

Keten en netwerk zijn metaforen en vullen elkaar aan. (Ik heb het hier niet over netwerken in fysieke, maar in sociale zin.) Ik sluit aan bij de gangbare definities van keten en netwerk, maar scherp ze nog wat meer aan. Keten en netwerk verschillen in veel opzichten van elkaar (voor de helderheid zet ik de verschillen zwart-wit neer):

- Een keten is een *proces*. Een proces is een logisch geordend geheel van activiteiten, gericht op het produceren van een resultaat. Een netwerk is een *configuratie* die processen kan faciliteren. Een configuratie is volgens Van Dale een systeem van punten en lijnen.
- Een keten is opgebouwd uit *stappen* (activiteiten) in een logische volgorde, een netwerk uit *entiteiten* (*nodes*, knopen) en *relaties* tussen entiteiten.
- Een keten beschrijf je met *werkwoorden*, een netwerk met *zelfstandige naamwoorden*. (Juristen hebben de slechte gewoonte werkwoorden om te bouwen tot zelfstandige naamwoorden. Dus bijvoorbeeld: 'De *tenuitvoerlegging* van rechterlijke beslissingen (…) *geschiedt* door Onze Minister' (art. 6:1:1, eerste lid, Sv, zoals dat komt te luiden na inwerkingtreding van de Wet USB, ter vervanging van het huidige art. 553 Sv), in plaats van 'Rechterlijke beslissingen *worden ten uitvoer gelegd* door Onze Minister'. Dat is lelijk en het vertroebelt het onderscheid tussen keten en netwerk.)
- De keten wordt volgens de gangbare literatuur over maatschappelijke ketens gedefinieerd vanuit het gezamenlijke *product*. Netwerken organiseren zich rondom gedeelde *waarden en/of belangen*.[5] Een netwerk hoeft, anders dan de keten, geen gezamenlijk product te hebben waaraan het zijn bestaan ontleent. Partijen vormen een netwerk om samen sterker te staan, er beter van te worden, enzovoort. Ieder kan daarbinnen zijn eigen doelen nastreven, zonder dat dat het netwerk hoeft aan te tasten. Netwerksamenwerking is een kluwen van doelen, belangen en verwachtingen.[6]
- Het ketenbegrip heeft betrekking op de abstracte, logische processtructuur, het netwerk op de concrete invulling daarvan: mensen van vlees en bloed, en hun onderlinge afstemming en besluitvorming, de feitelijke interacties. De keten staat *op* de tekentafel, het netwerk zit *aan* de vergadertafel (of de borreltafel of welke andere tafel dan ook).

KETEN	NETWERK
proces	structuur (configuratie van punten en lijnen)
activiteiten (stappen)	entiteiten (*nodes* en relaties)
werkwoorden	zelfstandige naamwoorden
product (goed of dienst)	gedeelde waarden en/of belangen
staat op de tekentafel	zit aan de (vergader-, werk-, borrel-, enz.) tafel

Wat je hoort en ziet als je rondkijkt op een kantoor of in een bedrijf, is vooral het functioneren van het netwerk. Het ketenconcept ligt daar als abstract ordenend principe aan ten grondslag, maar dat kun je als zodanig niet zien. In de metafoor van de ijsberg is het *netwerk* het zichtbare topje dat boven het water uit steekt. De *keten* zit als abstract concept diep onder water. Tussen die twee niveaus zit doorgaans nog een geheel van wetten, regels, procedures, afspraken, standaarden, protocollen, werkbeschrijvingen, enzovoort. Die zitten deels onder water, men is er niet dagelijks mee bezig, maar je kunt ze wel 'boven water halen', hetzij vanuit de kast of op het beeldscherm.



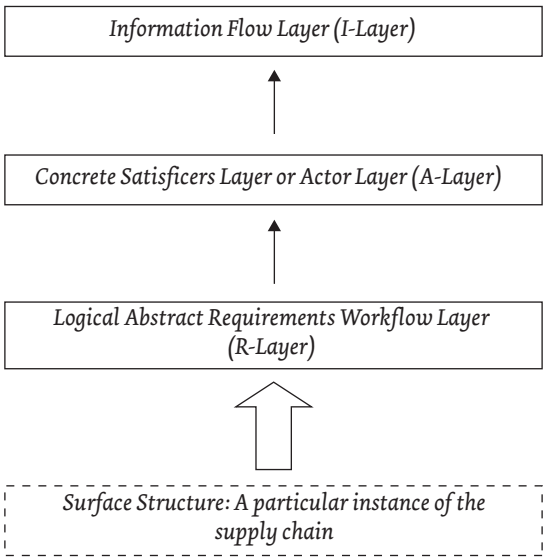
Een voorbeeld. De voorzitter van de strafkamer van de rechtbank leest tijdens een terechtzitting allerlei stukken uit het dossier voor of deelt de korte inhoud daarvan mee. Waarom doet zij dat? De verdachte weet toch al wat er in die stukken staat? Is dat geen tijdverspilling?

Iemand die relgelmatig zittingen bezoekt, zal kunnen antwoorden: 'Dat doet ze altijd.' Dat antwoord zit op de laag van het waarneembare, de acties en interacties die je kunt zien en horen, 'boven water'.

Iemand die wel eens een blik heeft geworpen in het Wetboek van Strafvordering zal kunnen antwoorden: 'Omdat de wet dat voorschrijft.' Inderdaad, de wet zegt dat 'ten bezware van de verdachte geen acht wordt (lees: mag worden) geslagen op stukken die niet zijn voorgelezen of waarvan de korte inhoud niet is meegedeeld' (art. 301, vierde lid, Sv). Daarmee gaan we al een eindje de diepte in, naar de regels en procedures. De voorzitter van de strafkamer vermeldt die regel er niet elke keer bij. Maar je kunt hem, als je dat wilt, wel vinden in de wetboeken die in de kast staan, en op de tafel van de rechtbank, en op internet (www.wetten.nl).

Maar waarom staat dat voorschrift in de wet? En trouwens, waar haalt de voorzitter al die stukken vandaan? Hoe komt ze eraan? Dat lees je niet in de wet. Daarvoor met je nog een laag dieper, naar het ketenconcept. Een terechtzitting ontleent haar betekenis aan het concept van de strafrechtsketen (zie par. 3.1). Het 'product' van die keten is: 'de wetsovertreding wordt bestraft'. In onze rechtsstaat willen we niet dat mensen worden bestraft in geheime processen. Aan die waarde ontleent – even heel kort gezegd – het voorschrift van art. 301 zijn betekenis. En hoe de voorzitter aan de stukken komt, vloeit voort uit datzelfde ketenconcept. In een rechtsstaat willen wij niet dat mensen zo maar worden veroordeeld en vastgezet, daar moet deugdelijk bewijs aan ten grondslag liggen. Dat komt bij de opsporingsdiensten vandaan, uit een eerdere fase in de keten. Maar dat ziet de bezoeker van de terechtzitting allemaal niet.

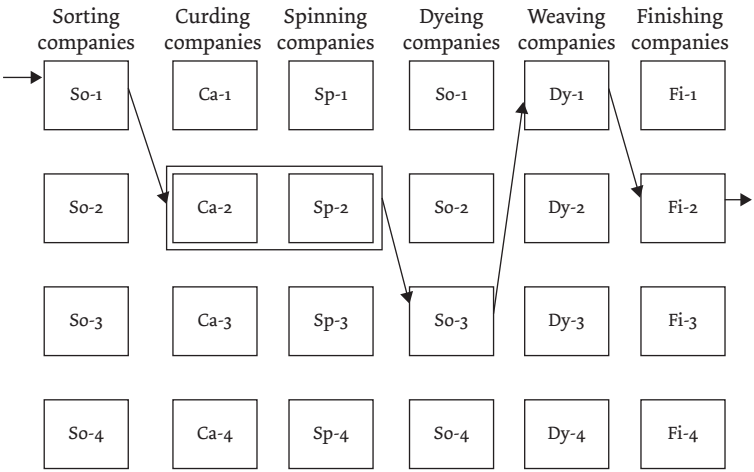
Een andere manier om het verschil – en tegelijk ook het verband – tussen keten en netwerk te illustreren, is het lagenmodel van Kumar et al. Dit ziet er als volgt uit:[7]



Vanuit de werkprocessen zoals deze zich in de dagelijkse werksituatie voordoen, de *surface structure*, ga je op zoek naar de logische grondvorm of het technologisch substraat, dat aan dat dagelijkse werk ten grondslag ligt en er betekenis aan geeft: de *R-Layer*. Het gaat daarbij om de taken of stappen in het proces van waardetoevoeging (de activiteiten die tezamen het proces uitmaken), die logisch noodzakelijk zijn om 'van A naar B te komen' c.q. het ketenresultaat te produceren. Dit is het ketenniveau. Vervolgens kun je bepalen welke actoren die taken uitvoeren: de *A-layer*. Dit is het netwerkniveau. En van daaruit kun je bepalen welke informatie nodig is om het ketenproces uit te voeren en hoe de informatiestroom moet worden ingericht: de *I-layer*.

Een keten omspant per definitie altijd een aantal organisaties of actoren. Een netwerk ook. Door één organisatie of netwerk kunnen meer ketens lopen. Ketens kunnen elkaar kruisen binnen een organisatie of netwerk. Dit valt te illustreren met het volgende plaatje:[8]

Network of independent companies in the industrial district of Prato



De entiteiten in het plaatje zijn onafhankelijke bedrijven die deel uitmaken van een netwerk. Dat netwerk is in dit geval regionaal gedefinieerd: *the industrial district of Prato*. Door dit netwerk heen loopt in het plaatje één ketenproces, maar dat zullen er waarschijnlijk meer zijn. Blijkbaar hebben de bedrijven in het district iets met elkaar, een gedeeld belang dat hen in het netwerk bij elkaar brengt. En tegelijk hebben enkele bedrijven deel aan eenzelfde productieproces, oftewel: een keten. Andere bedrijven in het netwerk zullen allicht deel uitmaken van andere ketens. Ook dit plaatje maakt weer duidelijk dat keten en netwerk geen concurrerende, maar complementaire begrippen zijn.

1.5 De rechtsstaat: verankerd in ketens, verstrikt in netwerken

Waarom is het onderscheid tussen ketens en netwerken nu zo belangrijk? Roel Bekker, onder meer voormalig Secretaris-Generaal van het ministerie van VWS en voormalig hoogleraar te Leiden, zei eens (op het congres 'Rijk met Wetenschap: Bestuur is Informatie' op 7 juni 2012 in Tilburg): 'netwerken creëren onduidelijkheden'. Ketens daarentegen zijn de ankerpunten van de rechtsstaat.

Toen ik in de jaren 2005-2009 mijn boek *Jegens en Wegens* schreef, heeft een aantal mensen het concept welwillend van commentaar voorzien. Eén van hen stelde de vraag: 'Dat hele hoofdstuk 3, vijftig pagina's theorie over ketens en netwerken, wáárom moet ik dat allemaal lezen?' Eigenlijk had ik daar toen nog geen goed antwoord op. Ik vond – en vind nog steeds – het onderscheid verhelderend. Maar als iemand anders dat niet vindt, *so what?* Het antwoord werd mij pas kort geleden in alle helderheid duidelijk, toen ik aan dit boekje werkte. Het gaat om meer dan alleen conceptuele helderheid; het gaat om ankerpunten van de rechtsstaat.

Onduidelijkheid zit hem in de eerste plaats in de *taken, bevoegdheden en verantwoordelijkheden* (TBV). Die zijn, in elk geval binnen het domein van Justitie, ketengewijs bepaald. Het proces waarin een justitiabele zit en de regels die voor dat proces gelden, bepalen de toepasselijke TBV.

Bijvoorbeeld: de politie houdt op straat iemand staande. Vanwege een strafbaar feit, in het kader van vreemdelingentoezicht of voor een verkeerscontrole? Dat maakt nogal verschil.

Ander voorbeeld: als een aantal partijen in een casusoverleg om de tafel zit en er wordt besloten verdachte X niet het strafrechtelijke traject in te sturen maar een zorgtraject aan te bieden, wie is dan precies waarvoor verantwoordelijk? De OvJ en niemand anders is verantwoordelijk voor de beslissing om iemand niet het strafrechtelijke traject in te sturen, want dat is juridisch gewoon een sepot. Die verantwoordelijkheid mag niet verdampen, collectieve verantwoordelijkheid voor zo'n beslissing kent ons strafprocesrecht niet. En omgekeerd: voor bijvoorbeeld controle (toezicht, bestuurlijke handhaving) is de officier van justitie niet verantwoordelijk, ook niet als hij onderdeel is van een samenwerkingsverband.

In het verlengde hiervan ligt de *verantwoordelijkheid voor de omgang met informatie*. De meeste overheidsorganisaties zijn informatieverwerkende bedrijven. Hun primaire proces bestaat in het verwerken van informatie. De TBV in het primaire proces gaan dus een-op-een over in TBV voor de informatieverwerking. Dat is ook het uitgangspunt van de regelgeving over gegevensbescherming (zie hoofdstuk 2).

> In samenwerkingsverbanden wil er nog wel eens onduidelijkheid ontstaan over de verantwoordelijkheden rond gegevensverwerking. Die onduidelijkheid is het gevolg van onduidelijkheid rond de TBV van het primaire proces. Om tot helderheid te komen over de gegevensverwerking moet je dus terug naar de tekentafel. Bepaal (1) wat het gezamenlijke *product* is, (2) hoe het *proces* eruitziet waarin dat product wordt gerealiseerd, en ten slotte (3) welke *partijen* in dat proces zijn betrokken (zie par. 1.3). En teken aan de hand van die analyse je primaire ketenproces. (Voor de drie justitieketens doe je dat vooral aan de hand van de relevante wetgeving.) Zo krijg je helderheid over de TBV en dat is, zoals gezegd, de basis voor de verantwoordelijkheden voor de gegevensverwerking.

De derde onduidelijkheid betreft de *gegevensuitwisseling* en daarmee de gegevensbescherming. Wie mag welke gegevens uitwisselen met wie en onder welke voorwaarden? De wettelijke eis van doelbinding is, net als de eis van een toereikende wettelijke grondslag voor het verwerken van gegevens, tot op zekere hoogte gekoppeld aan de keten (meer hierover in par. 2.4). Het netwerk biedt daarentegen geen handvat om deze vragen over gegevensuitwisseling te beantwoorden; zie het zojuist gegeven voorbeeld van de informatie-uitwisseling in samenwerkingsverbanden.

De vierde onduidelijkheid betreft de *betekenis van informatie*. Gegevens komen tot stand in processen. De keten is zo'n proces. De keten bepaalt daarmee de betekenis van een gegeven. De drie justitieketens bijvoorbeeld, strafrecht, vreemdelingenrecht en jeugdbescherming, hebben elk hun eigen regelgeving en begrippen. Die bepalen de bete-

kenis van de gegevens die worden verzameld en verwerkt. Een keten is als zodanig, ook al bevat zij soms open einden, een min of meer begrensde omgeving. Het netwerk daarentegen is principieel open en onbegrensd. Het gevaar is dat gegevens van hun context worden ontdaan (gedecontextualiseerd) en in een andere context worden geplaatst (gehercontextualiseerd). Dat leidt tot verlies van betekenis en bedreigt de kwaliteit en integriteit van de gegevens. (Zie het prachtige rapport van de WRR *iOverheid* uit 2011.) Een adres bijvoorbeeld kan een andere betekenis hebben in de context van de Basisregistratie Personen (BRP) dan in de strafrechtstoepassing (dus in de SKDB; zie nader par. 5.4). En het aantal inkomensbegrippen in de regelgeving is legio.

De vijfde en laatste onhelderheid betreft de besturing van het ketenproces of het samenwerkingsverband. Want als je niet weet wat precies ieders aandeel in het primaire proces is, hoe kun je dan bepalen wie er in het besturende orgaan moeten zitten? En hoe de rollen daarbinnen moeten worden verdeeld? Over ketenregie en ketenbesturing zijn al veel waardevolle rapporten en studies geschreven.[9] Ik heb daar weinig aan toe te voegen en laat dat onderwerp daarom rusten.

Ik hang het belang van het onderscheid tussen keten en netwerk dus op aan de regelgeving. Je zou je kunnen afvragen of die regelgeving er niet heel anders uit zou kunnen zien. Zouden de regels niet netwerkgewijs in plaats van ketengewijs kunnen worden opgesteld? Misschien. Maar dat is nu eenmaal niet de situatie. Het zou een totaal andere indeling van onze wetgeving vergen. De vraag is of we van zo'n fundamentele omvorming van de wetgeving veel wijzer worden. Er is bij mijn weten in elk geval nog niemand die dit heeft bepleit en ik zie het ook niet gebeuren.

1.6 Misverstanden over ketens

Zoals gezegd, er valt nogal eens te beluisteren dat we af moeten van het denken in ketens. Daartoe worden tal van bezwaren tegen dat denken aangevoerd. Ik geef hieronder een bloemlezing. Voor zover nog nodig na het voorgaande, geef ik de weerlegging erbij.

Ketens vervagen.

Dit misverstand berust op een verwarring van de begrippen *keten* en *netwerk*. Natuurlijk werken actoren uit diverse ketens met elkaar samen in netwerken (*cross chain collaboration*). Maar dat mag er niet toe leiden dat de ketens vervagen. Anders loopt de rechtsstaat gevaar. Die eist immers een heldere toedeling van taken, bevoegdheden en verantwoordelijkheden (TBV). Als ketens vervagen, dan vervagen de TBV. Dat mag niet gebeuren.

Ketendenken dwingt tot sequentieel werken, dus op elkaar wachten, ook als dat praktisch gesproken niet nodig zou zijn.

Dit misverstand berust op een verwarring van niveaus. De keten is sequentieel op een abstract conceptueel niveau, bijvoorbeeld dat van de noodzakelijke volgorde van opsporen, vervolgen, berechten, ten uitvoer leggen en re-integreren. Die sequentiële volgorde wordt ingegeven door rechtsstatelijke argumenten; totalitaire staten laten zien dat het ook heel anders kan. Maar Veiligheidshuizen en ZSM ('Zo Snel, Slim, Selectief, Simpel, Samen en Samenlevingsgericht Mogelijk') bewijzen dat op het praktische niveau, in het netwerk, mensen helemaal niet op elkaar hoeven te wachten, maar prima tegelijkertijd aan een zaak kunnen werken. Sterker nog, op dat niveau is de tijdsvolgorde helemaal niet van belang, het gaat er simpelweg om zo effectief en efficiënt mogelijk te werken. Technisch gesproken zou een boete voor een verkeersovertreding die door een digitale camera is 'vastgesteld', nog op datzelfde moment van de bankrekening van de overtreder kunnen worden afgeschreven; het hele proces is dan in een *split second* afgewikkeld, met de snelheid van het licht; maar conceptueel is toch de hele keten van opsporen tot en met ten uitvoer leggen doorlopen.

Er wordt niet alleen volgtijdelijk aan zaken of problemen gewerkt, maar ook gelijktijdig.

Dit hangt samen met de vorige tegenwerping. Ketendenken dwingt helemaal niet tot wachten op elkaar als dat praktisch gesproken niet nodig is.

Ketendenken verplicht tot samenwerking, ook waar dat geen toegevoegde waarde heeft.

Dit is simpelweg onjuist. Ketendenken is alleen maar een denkmodel, een mentale constructie, om een complexe werkelijkheid beter te kunnen begrijpen. Het schrijft niets voor. Voor samenwerking geldt het Afrikaanse spreekwoord: Als je snel wilt gaan, ga dan alleen, als je vér wilt komen, ga dan samen. In de strafrechtsketen moeten we soms snel zijn, maar vrijwel altijd willen we vér komen. Maar ordentelijke overdracht van dossiers of zaken (estafettemodel) is in veel gevallen al voldoende.

Partijen als de politie en rechtspraak maken ook deel uit van andere ketens.

Dat is juist, het geldt voor de meeste partijen in de strafrechtsketen. Ze maken ook deel uit van verschillende netwerken. Ik zie niet in hoe dit een argument kan zijn om het ketenbegrip ter zijde te schuiven.

De meeste zaken doorlopen niet de gehele keten.

Ook dit is juist. Sterker nog, het volgt regelrecht uit de definitie van een keten: elke vorige stap is wel een noodzakelijke, maar niet per se ook voldoende voorwaarde voor een volgende. Een zaak hóeft niet de hele keten te doorlopen. Iets abstracter gezegd: deze tegenwerping miskent het onderscheid tussen *keten* en *traject*.

De ketenlogistiek is vaak minder soepel dan het beeld van een keten suggereert.

Wie beweert er dat het beeld van een keten een soepele ketenlogistiek suggereert?

De keten werkt in een dynamische leefwereld met fluïde overgangen.

Zeker! Juist daarom hebben we het ketenconcept zo hard nodig als houvast voor de rechtsstaat, is mijn stelling.

De partijen in de strafrechtsketen verschillen qua omvang, (grond)wettelijke positie, taken, en cultuur.

Zeker! Dat geldt niet alleen binnen de strafrechtsketen, maar ook binnen vele andere ketens, ook in de commerciële sector. Hoezo zou er dan geen sprake kunnen zijn van een keten?

Noten

1 Het model is ontwikkeld door Prof. Rik Maes en zijn medewerkers aan de Universiteit van Amsterdam, vandaar de naam 'Amsterdams negenvlak'.
2 Ontleend aan Eleanor Pascoe-Samson, *Organisatie, besturing en informatie* (tweede druk), Deventer: Kluwer BedrijfsInformatie 1988, p. 231. Ik heb het een klein beetje aangepast.
3 Ik doe dat in dit boekje heel kort. Voor een uitvoerige toelichting (en verantwoording van bronnen) verwijs ik naar hoofdstuk 3 van mijn boek *Jegens en Wegens. Over persoonsgebonden informatie in de strafrechtsketen* (tweede druk), Nijmegen: Wolf Productions 2010.
4 Dit is de definitie van de Wetenschappelijke Raad voor het Regeringsbeleid in zijn rapport *iOverheid*, Amsterdam: Amsterdam University Press 2011, p. 72.
5 M. van der Steen, R. Peeters en M. van Twist, *De Boom en het Rizoom. Overheidssturing in een Netwerksamenleving*, Den Haag: Ministerie van VROM 2009, p. 30.
6 P. Oude Luttighuis en J. Gordijn, De boetvaardige architect. Knoper van netwerksamenwerking, *Informatie* 2015 (november), p. 20.
7 K. Kumar en E. Christiaanse, *From Static Supply Chains to Dynamic Supply Webs: Principles for Radical Re-Design in the Age of Information*, PrimaVera Working Paper, p. 99-14.
8 Ontleend aan K. Kumar, H.G. van Dissel en P. Bielli, The Merchant of Prato – Revisited: Toward a Third Rationality of Information Systems, *MIS Quarterly* 1998 (June), p. 199-226.
9 Ik volsta hier met verwijzing naar drie van die rapporten: Ministerie van BZK (2002): *Naar een methodisch kader voor ketenregie in het openbaar bestuur. Eindrapportage* (BMC, Berenschot, De Verbinding); NORA (2013): *Ketens de baas. Pijlers en bouwstenen voor ketensturing*; Morgens (2014): *Samen succesvol werken. Een onderzoek naar de succesfactoren voor ketensamenwerking binnen de overheid*. Zie ook *Jegens en Wegens* par. 3.4 (p. 126-138).

HOOFDSTUK 2

INFORMATIE DELEN IN KETENS EN NETWERKEN

2.1 Van privacy naar gegevensbescherming

Ik heb rechten gestudeerd van 1971 tot 1976. Privacy en/of gegevensbescherming behoorden nog niet tot de lesstof. Mensenrechten trouwens ook niet. Ik wist aan het eind van mijn studie het verschil nog niet tussen 'Straatsburg' (het Europese Hof voor de Rechten van de Mens, EHRM) en 'Luxemburg' (het Hof van Justitie van de Europese Unie). En ook niet tussen de Europese Gemeenschap (tegenwoordig: EU) en de Raad van Europa. In de tijd dat ik les gaf aan de Universiteit Leiden (1978-1985) werd dat nog niet veel anders. Een paar collega's werden beschouwd als de specialisten op het gebied van de mensenrechten en het internationaal strafrecht. Maar in mijn proefschrift over 'De bewijsmiddelen in strafzaken' heb ik geen woord vuil gemaakt aan deze onderwerpen, noch aan de internationale dimensie van het bewijsrecht. Anno 2018 is dat niet meer voor te stellen. Pas in mijn tijd als gerechtsauditeur bij het Wetenschappelijk Bureau van de Hoge Raad (1986-1989) kwam ik in aanraking met 'Straatsburg', want de jurisprudentie van het EHRM werd daar nauwkeurig bijgehouden en diepgaand bediscussieerd. En wat de regelgeving rond strafrechtelijke gegevens betreft (zie par. 5.1), in de leerboeken werd die wel in een apart hoofdstuk behandeld, maar dat behoorde tot de hoofdstukken die je voor het tentamen mocht overslaan. En dat is nog steeds zo.

Ooit zeiden leidinggevenden tegen mij: 'Jij bent beleidsadviseur keteninformatisering; jij moet je niet bezighouden met privacy, daar hebben we gespecialiseerde juristen voor.' Ik heb enige tijd geprobeerd mij aan die instructie te houden, maar dat heeft niet lang geduurd. Zoals IV niet iets van de 'techneuten' is (zie par. 1.1), zo is gegevensbescherming (privacy) niet een dingetje van juristen, iets dat je kunt uitbesteden. Dat houdt verband met je visie op de plaats van IV binnen de bedrijfsvoering. Informatie wordt nog steeds door velen gezien als een element van PIOFACH.[1] Dat zijn ondersteunende functies, ze maken geen onderdeel uit van het primaire proces. In de informatiekunde is deze visie allang achterhaald. IV is, zeker in gegevensverwerkende bedrijven, de kern van het werk. En als IV inderdaad de kern van het werk is, dan geldt dat ook voor privacy. De laatste tijd ben ik privacy en gegevensbescherming gaan zien als een brug tussen het primaire proces en de IV. Kern van gegevensbescherming is immers het noodzaak-criterium (*need to know*, *need to share*) en die noodzaak ligt in het hart van het primaire proces. Via dit criterium vormt de gegevensbescherming de brug tussen het primaire proces en de IV.

In de jaren negentig coördineerde ik binnen het ministerie van Justitie het fraudebeleid. In die tijd verschenen er nogal wat rapporten over gegevensuitwisseling ten dienste van fraudebestrijding. Die bevatten vaak de klacht dat de privacyregelgeving de gegevensuitwisseling belemmerde. Ik stapte dan naar de verantwoordelijke wetgevingsjuristen: de makers van de Wet persoonsregistraties en (daarna) van de Wet bescherming persoonsgegevens. Hun antwoord was altijd hetzelfde: 'Het kan wél, als je het maar goed regelt.' Dat wil zeggen: als je je primaire proces goed op orde hebt, wéét wat je doet en waarom en hoe. Dat moet je goed beschrijven. Daaruit volgen dan de informatievoorziening en de antwoorden op vragen rond privacy vanzelf, voor pakweg 80%. Dan resteert er misschien nog 20% aan 'voer voor de juristen'. (Hiermee ontken ik niet dat die 20% vaak wel goed is voor 80% van de hoofdpijn.)

De laatste jaren zijn samenwerkingsverbanden een heet hangijzer uit oogpunt van privacy: welke gegevens mogen we delen, wat mag wel en wat mag niet. Daarvoor geldt: breng de processen goed in kaart, dan is het niet zo moeilijk. Voor ketensamenwerking betekent dat, dat je de analyse van product–proces–partijen uitvoert (zie par. 1.3). Daarmee maak je de taken, bevoegdheden en verantwoordelijkheden (TBV) helder. Op basis daarvan kun je de IV inrichten en de vragen rond privacy beantwoorden, al dan niet in het kader van een Data Protection Impact Assessment (DPIA; zie par. 2.5).

In dit verband moet ik nog iets meer zeggen over het begrip privacy. Dat is een containerbegrip en wordt ook te pas en te onpas ingeroepen. Het kent ten minste vier compartimenten: lichaam, huis, relaties en informatie. Dat laatste wordt wel aangeduid als de informationele privacy. Het moge duidelijk zijn dat ik het daarover heb in het kader van de IV en niet over bijvoorbeeld het huisrecht of het recht op lichamelijke integriteit (onschendbaarheid van het lichaam). Inmiddels kent het Handvest van de grondrechten van de EU (2009) naast de klassieke vrijheidsrechten een apart recht op gegevensbescherming (art. 8 van dat Handvest: 'Eenieder heeft recht op bescherming van zijn persoonsgegevens'). Hoe zich dat recht precies verhoudt tot de overige zogenoemde privacyrechten is niet zonder meer duidelijk. Maar het lijkt me inderdaad niet zo gek om dit recht centraal te stellen, los van het oeverloos geworden begrip privacy. Het Europees Hof voor de Rechten van de Mens ('Straatsburg') verbindt ze soepel aan elkaar door te zeggen dat '*the protection of personal data (…) is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention*'.[2] Daarmee is gegevensbescherming onder de paraplu van artikel 8 EVRM (bescherming van de persoonlijke levenssfeer) gebracht. Maar begripsmatig brengt dat ons niet veel verder. Een voorbeeld van iets wat niet onder de privacy valt maar wel onder gegevensbescherming, is de geheimhoudingsplicht van de arts, de notaris, de advocaat en de geestelijke, en het daarmee corresponderende verschoningsrecht van deze beroepsbeoefenaren. Die plicht en dat recht strekken namelijk niet, in elk geval niet in de eerste plaats, tot bescherming van de

persoonlijke levenssfeer van de betrokkenen, maar van de vrije en onbelemmerde toegang tot professionele hulp op de diverse gebieden.

Verder moet ik erop wijzen dat het begrip *persoonsgegevens* in de praktijk nogal eens wordt gebruikt in de betekenis van *personalia* of *identificerende persoonsgegevens*. Dat laatste betreft gegevens die ertoe dienen een betrokkene te identificeren, dat wil zeggen te onderscheiden van anderen. Er wordt dan gesproken van persoonsgegevens tegenover zaaksgegevens. Dat is misleidend. Het juridische begrip persoonsgegevens omvat namelijk ook verreweg het grootste deel van wat in de praktijk als zaaksgegevens wordt aangeduid. Persoonsgegeven is immers 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon' (art. 4, onder 1, Avg; art. 3, onder 1, Rgbs). In die betekenis gebruik ik het.

De regelgeving is gelaagd en complex. Lange tijd hebben wij de Wet bescherming persoonsgegevens (Wbp) gehad. Dat was min of meer de Nederlandse vertaling van een richtlijn van (toen nog) de EG uit 1995. Beide zijn onlangs van het toneel verdwenen. De richtlijn uit 1995 is in mei 2018 vervangen door een nieuwe verordening (de Avg) en richtlijn (de Rgbs). De verordening wordt uitgewerkt in een Uitvoeringswet, de richtlijn wordt in nationaal recht omgezet via een implementatiewet (meer hierover in par. 2.2). Daarnaast hebben we binnen het domein van veiligheid en justitie nog twee sectorale wetten: de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Ook die gaan de komende jaren op de schop (meer daarover in par. 5.1-5.3).

Het object van regulering is en blijft intussen het *gegeven*. Resteert de vraag wat dat nu eigenlijk is: een gegeven. Daarover zwijgen de wet en de wetsgeschiedenis. De wet definieert wel wat een *persoonsgegeven* is, maar niet wat een *gegeven* is; dat is een te moeilijke vraag. Is bijvoorbeeld een proces-verbaal van opsporing (art. 152 Sv) als zodanig een gegeven? Of is de verklaring van de getuige in het proces-verbaal dat? Of gaat het om elke afzonderlijke bewering van die getuige in die verklaring? Bijvoorbeeld: 'Ik zag dat de auto tegen de fiets botste.' Of om de elementen waaruit die bewering is samengesteld (ik, zag, auto, fiets, botste)? Hoe atomistischer we kijken naar het begrip gegeven,

des te meer verdampt betekenis en des te moeilijker wordt het ook om zulke elementaire deeltjes te beheren. De wet laat ons hier in de steek. Er zijn diverse opvattingen over wat *informatie* is en wat een *gegeven* is. Die liggen min of meer op het vlak van de filosofie. Dat mensen daarover van mening verschillen, is niet per se een probleem. Maar dat we het begrip gegeven ook juridisch niet kunnen definiëren, terwijl het de kern is van het rechtsgebied privacy en gegevensbescherming, is eigenlijk schandalig.

Het leidt bovendien in de praktijk tot verwarring. Dat betreft het *verstrekken* van gegevens. Dat daarvan sprake is als ik iemand een usb-stick met data geef, zal iedereen duidelijk zijn. Maar verstrek ik hem ook gegevens (of informatie) als die usb-stick beveiligd is met een wachtwoord dat ik er niet bij geef? Ik verstrek natuurlijk gegevens als ik iemand een pdf toestuur via de e-mail. Maar wát als ik iemand alleen maar een stukje tekst laat lezen zonder het uit handen te geven? Of als ik hem iets vertel? Is dat ook het *verstrekken* van gegevens? Een usb-stick is een *informatiedrager* (iets materieels), een pdf is een *informatieproduct* (in dit geval: immaterieel). Als ik iemand iets vertel of hem op afstand via een portal laat kijken in een bestand waarvan hij niets kan downloaden of kopiëren, ook niet via *printscreen*, verstrek ik geen informatieproduct, maar wel degelijk *informatie*. Informatie is per definitie iets immaterieels. Vanaf het moment dat iemand iets heeft gehoord of gelezen, zit de informatie in zijn hoofd, die krijg je er niet meer uit. Nu bestaat er over de status van informatiedragers weinig onduidelijkheid. Maar het niet goed onderscheiden tussen informatie en informatieproduct wil nog wel eens tot verwarring leiden. De regels over gegevensbescherming kunnen op alle drie de vormen van *verstrekken* van toepassing zijn.

2.2 Nieuwe regels vanuit de EU

De Wbp was, zoals gezegd, gebaseerd op een Richtlijn uit 1995 van (toen nog) de EG. Die is vervangen door de Algemene verordening gegevensbescherming (Avg). De Avg werkt rechtstreeks in de lidstaten. Zij is van toepassing met ingang van 25 mei 2018 – een cadeautje van de EU aan de schrijver van deze regels ter gelegenheid van zijn 65ste verjaardag.

De Avg is níet van toepassing op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid (art. 2, tweede lid, onder d, Avg). Voor die verwerkingen geldt de Richtlijn gegevensbescherming strafrecht (Rgbs).[3] Deze moest uiterlijk op 6 mei 2018 door de lidstaten zijn omgezet in nationale wetgeving.

Aan de basiseisen van wettelijke grondslag, doelbinding, noodzaak, proportionaliteit, dataminimalisatie, beveiliging en dergelijke hebben de verordening en richtlijn niets veranderd. In feite zijn die al sinds 1981 – het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa ('Straatsburg') – gelijk gebleven. Ook bevatten zij geen exacte regels over bewaartermijnen; dat moet nog steeds op nationaal niveau worden geregeld. De vernieuwingen betreffen vooral de rechten van geregistreerden, de administratieve verplichtingen van verwerkers en de sancties die kunnen worden opgelegd als de regels niet worden nageleefd. Vooral die laatste hebben tot een lichte paniek geleid in gegevensverwerkend Nederland.

Nieuw is dat elke verwerkingsverantwoordelijke verplicht wordt 'een register bij (te) houden van alle categorieën van onder hun verantwoordelijkheid vallende verwerkingsactiviteiten' (art. 24 Rgbs). Dit moet onder meer de volgende gegevens bevatten:
- de verwerkingsdoeleinden;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden bekendgemaakt;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- een aanwijzing betreffende de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de persoonsgegevens bestemd zijn;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens moeten worden gewist;

– indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Dat is nogal wat. Maar eigenlijk had elke organisatie dat natuurlijk al lang op orde moeten hebben, ook zonder nieuwe verordening of richtlijn vanuit de EU. Het zijn elementaire eisen van je zaken goed op orde hebben: een uitwerking van de begrippen accountability en transparantie (c.q. *good governance*). De verantwoordelijke moet duidelijk maken hoe hij met de data omgaat. Er kan in een rechtsstaat immers geen bevoegdheid zijn zonder plicht tot verantwoording.

Nieuw in de verordening en de richtlijn zijn verder de verplichting tot het toepassen van *privacy by design* en *privacy by default* (gegevensbescherming door ontwerp en door standaardinstellingen), het recht op gegevenswissing (ook wel genoemd het recht op vergetelheid) en 'het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft' ('geautomatiseerde individuele besluitvorming'). Dit laatste recht geldt echter niet 'indien het besluit is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene'. Het is een spannende vraag of de Wahv (zie par. 3.2) deze laatste toets zal kunnen doorstaan. De Mulder-beschikkingen worden immers sinds jaar en dag volledig geautomatiseerd verwerkt. De Hoge Raad heeft daar geen moeite mee (HR 16 februari 2016, *NJ* 2016, 404). Het is afwachten of dit stand houdt onder de nieuwe verordening (art. 22) en richtlijn (art. 11), want dan heeft niet de Hoge Raad meer het laatste woord, maar het Hof van Justitie van de EU. Misschien maakt dat verschil.

De bepaling van het toepassingsgebied van de beide nieuwe rechtsinstrumenten is een lastige kwestie. Waar de richtlijn ophoudt, begint de verordening; dat is scherp afgebakend. Maar waar ligt die grens precies? Dat is geformuleerd als 'verwerking van persoonsgegevens

door de bevoegde autoriteiten met het oog op (...)'. Op het eerste gezicht gaat het dus om de grenzen van *organisaties*. Maar dat alleen kan niet beslissend zijn. De meeste organisaties in de strafrechtspleging hebben immers ook taken en bevoegdheden in andere ketens of domeinen; zie paragraaf 1.5. De Rechtspraak bijvoorbeeld behandelt zaken op het gebied van het strafrecht, het bestuursrecht en het burgerlijk recht. Als het toepassingsbereik van de richtlijn alléén zou worden bepaald door de grens van de *organisatie*, zou de richtlijn ook van toepassing zijn op de civielrechtelijke en bestuursrechtelijke zaken van de Rechtspraak. Dat pretendeert de richtlijn niet. De invalshoek moet dus niet alleen zijn de *organisaties*, maar ook – en zelfs in de eerste plaats – het *proces* dat zij uitvoeren c.q. de *keten* waarin zij opereren. Dat is 'de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid'. Oftewel strafrechtstoepassing plus nog wat: 'de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid'. Wat die plus precies inhoudt, valt noch in de verordening, noch in de richtlijn te lezen. Het is in ieder geval iets anders dan de nationale veiligheid of defensie, want die worden wel uitdrukkelijk apart genoemd. De grenskwestie komt terug in de wetten die gemaakt zijn ter uitvoering van de Avg en ter implementatie van de richtlijn.

'Bevoegde autoriteit' is in de richtlijn (art. 3, onder 7) gedefinieerd als: 'a) iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; of b) ieder ander orgaan dat of iedere andere entiteit die krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid'. Volgens deze definitie valt bijvoorbeeld iemand die in een strafzaak als deskundige wordt gehoord (art. 343 Sv) of die wordt gevraagd (dan wel

opgedragen) als deskundige een verslag uit te brengen (art. 344, eerste lid, onder 4°, Sv) niet onder de richtlijn, want hij is niet gemachtigd openbaar gezag en/of openbare bevoegdheden uit te oefenen – net zo min als de getuige of de tolk. Het NFI daarentegen valt wel onder de richtlijn, omdat en voor zover het de wettelijke taak heeft de DNA-profielen en het DNA-materiaal van verdachten en veroordeelden te beheren. Hetzelfde geldt voor de reclassering (inclusief de jeugdreclassering) en voor de tientallen instellingen voor ggz die cliënten op strafrechtelijke titel binnen krijgen. Daarentegen vallen wetenschappelijke instituten, zoals het WODC (Wetenschappelijk onderzoek- en documentatiecentrum van het ministerie van Justitie en Veiligheid), het NSCR (Nederlands studiecentrum voor criminaliteit en rechtshandhaving) of andere criminologische instituten, niet onder de richtlijn, omdat zij weliswaar strafrechtelijke persoonsgegevens verwerken, maar geen openbaar gezag en/of openbare bevoegdheden uitoefenen. In dit verband moet nog bedacht worden dat het Wetboek van Strafvordering taken en bevoegdheden doorgaans toekent aan functionarissen, dus aan individuen – niet aan organisaties (vgl. par. 4.1). Maar het is zonneklaar dat het niet in de macht van die individuele functionarissen ligt om aan alle regels van de gegevensbescherming te voldoen, dat moeten de organisaties voor hen regelen.

2.3 Gegevensbescherming in een keten …

Gegevensbescherming gaat, zoals gezegd, over *persoonsgegevens*. Dat is het eerste kernbegrip in de regelgeving. De twee andere zijn *verwerken* en *verantwoordelijke*. Van *verwerken* is, simpel gezegd, sprake zodra er een toetsenbord of een muis (of enig ander schrijfgerei) aan te pas is gekomen. In de regelgeving zijn onder meer de volgende materiële principes voor de verwerking van persoonsgegevens vastgelegd:

- Persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (doelbinding).
- Persoonsgegevens mogen slechts worden verwerkt indien de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen of voor de goede vervulling van een publiekrechtelijke

taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt (*need to know*).
- Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel waarvoor zij worden verwerkt (opslagbeperking).
- Verwerking van persoonsgegevens moet tot het noodzakelijke minimum worden beperkt (dataminimalisatie).
- Verwerking van persoonsgegevens moet uiteindelijk een wettelijke grondslag hebben (zie art. 5 en 6 Avg; art. 4 en 8 Rgbs.) Een protocol of convenant kan als zodanig nooit een toereikende wettelijke grondslag opleveren (zoals in de praktijk nog wel eens schijnt te worden gedacht).
- Verwerking van 'bijzondere' en/of strafrechtelijke persoonsgegevens is verboden behoudens uitdrukkelijke wettelijke grondslag (art. 9 en 10 Avg; art. 10 Rgbs). Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over gezondheid of ras of biometrie. Een strafrechtelijk persoonsgegeven is bijvoorbeeld het criminele verleden van iemand. Het verbod geldt ook voor de verwerking van 'een nummer dat ter identificatie van een persoon bij wet is voorgeschreven' (art. 87 Avg), zoals het burgerservicenummer (BSN). Tegen die laatste regel wordt nogal eens gezondigd, zowel in het publieke als in het private domein. Zie daarover bijvoorbeeld de Richtsnoeren Identificatie en verificatie van persoonsgegevens (Gebruik van 'kopietje paspoort' in de private sector) van het toenmalige CBP (tegenwoordig: de Autoriteit Persoonsgegevens) van 12 juli 2012, *Staatscourant* nr. 14741. Een foto wordt aangemerkt als een gegeven waaruit het ras van de gefotografeerde kan worden afgeleid, dus ook foto's mogen niet zonder uitdrukkelijke wettelijke grondslag worden verwerkt (geraadpleegd, gekopieerd, opgeslagen, enz.).

Uit het beginsel van *need to know* vloeit voort dat als een overheidsfunctionaris of bestuursorgaan persoonsgegevens wenst van een andere functionaris of een ander bestuursorgaan, hij dient aan te geven welke gegevens hij nodig heeft en voor welk doel. *Nice to know* is niet voldoende, 'handig om te hebben' is geen wettelijke grondslag. We huldigen binnen de overheid en binnen het

informatiemanagement het principe dat er bij voorkeur één – en niet meer dan één – authentieke bron is van gegevens en dat de gegevens vandaaruit meervoudig worden gebruikt (principe van *single truth* c.q. *single source* c.q. hergebruik van gegevens). Dat geldt bij uitstek binnen ketens. Daaruit vloeit een *need to share* voort. Functionarissen en organisaties dienen de informatie waarover zij beschikken waar nodig te delen met andere functionarissen. Overheidsinformatie móet worden hergebruikt als zij kan worden hergebruikt. Dat roept – ook in ketenverband – een aantal lastige vragen op. Het delen van informatie kan op gespannen voet komen te staan met de geheimhoudingsverplichting die alle functionarissen ook hebben. Bovendien kan het op gespannen voet komen te staan met de eigen verantwoordelijkheid van ieder die gegevens verwerkt voor de juistheid van de gegevens waarop hij zijn beslissingen en handelingen baseert. Want hoe betrouwbaar zijn de gegevens die je bij anderen – binnen of buiten de keten – ophaalt? En in hoeverre kan en mag je vertrouwen op en moet je vervolgens ook instaan voor de juistheid en betrouwbaarheid van die informatie van anderen?

De *need to share* roept ook lastige vragen op over de *verantwoordelijkheid* voor het gegeven. Wie is er verantwoordelijk voor het beveiligen, verstrekken, bewaren en vernietigen van het informatieproduct (gegeven, document, dossier) als meer partijen tegelijk er toegang toe hebben, er gebruik van maken en erover kunnen beschikken? In de regelgeving is verantwoordelijkheid gekoppeld aan 'verwerken' en niet aan 'gegeven'. Dat maakt het mogelijk dat er meer dan één verantwoordelijke is voor een bepaald gegeven; er kunnen immers meer dan één verwerkingen na elkaar of tegelijkertijd worden uitgevoerd aan een gegeven. De vragen over verantwoordelijkheid betreffen vooral drie aspecten van verwerken: het beheren (bewaren, wijzigen c.q. muteren, beveiligen, enz.), het verstrekkingenregime (kennisnemen, raadplegen, uitwisselen, enz.) en het bewaken van de bewaartermijn (en na afloop daarvan vernietigen).

De regelgeving (dus niet de beheerder van de data) bepaalt wie welke informatie mag hebben en onder welke voorwaarden. Zij belegt ook de bevoegdheden en de verantwoordelijkheden voor de omgang met

gegevens. Onbevoegden mogen geen kennis krijgen en ook geen kennis kúnnen krijgen van gegevens waarvan zij geen kennis mógen krijgen. Dit betreft *authenticatie* (is degene die om gegevens vraagt inderdaad degene die hij claimt te zijn), *autorisatie* (de vertaling van de wettelijke bevoegdheid om gegevens te verwerken naar de kolom van de ICT), *logging* (vastleggen wat er met en aan gegevens wordt gedaan), toezicht en beveiliging. Logging en toezicht zijn onderdeel van *accountability*. Het hele verhaal wordt daarom ook wel aangeduid als 'AAA': authenticatie, autorisatie en accountability. Maar wie is er verantwoordelijk voor die AAA als een veelheid van partijen toegang heeft tot het informatieproduct (gegeven, document, dossier)? (Dat hoeft zich nog niet eens tot één keten te beperken.)

> 'Tot voor kort was de regel dat wie het papieren dossier in bezit had, er tevens over ging. Geen toekomst heeft de opvatting dat het eigenaarschap van het digitale dossier naar analogie van het werken met papier zou overgaan van instantie naar instantie. Het digitale dossier kan immers niet los worden gezien van het document management systeem waarin de processtukken van het dossier worden aangemaakt, bewaard, ontsloten en bewerkt. Het beheer van een dergelijk systeem, ofwel een stelsel van met elkaar in verbinding staande systemen, is een vanuit ketenperspectief noodzakelijk gezamenlijke aangelegenheid van ten minste politie, openbaar ministerie en rechtspraak. Ik acht het van belang dat het beheer of het eigenaarschap zo wordt georganiseerd dat het de uitoefening van strafvorderlijke bevoegdheden met betrekking tot het weigeren en toevoegen van processtukken maximaal faciliteert.' (Jos van Wetten in *Delikt en Delinkwent* 2016, p. 318-319)[4]

De regelgeving bepaalt ook de bewaartermijnen. Maar de regelgeving is op dit moment nog zodanig ingericht, dat soms op één gegeven meer dan één wettelijk regime van toepassing is en ook méér dan één bewaartermijn. Dan geldt uiteindelijk natuurlijk de langste bewaartermijn, waarbij het gebruik geblokkeerd moet worden voor degene voor wie of het doel waarvoor de bewaartermijn verstreken is. Maar

wie is er dan op ketenniveau verantwoordelijk voor het zo lang bewaren, het blokkeren en ten slotte ook vernietigen? Voor alle gegevens en documenten van de overheid geldt dat zij uiteindelijk ofwel moeten worden vernietigd ofwel moet worden overgebracht naar een archiefbewaarplaats (Archiefwet 1995). Voor gegevens en documenten die een functie hebben in een ketenverband roept dit bijzondere vragen op. Ik volsta hier met verwijzing naar het lezenswaardige rapport *Het puberbrein van de overheid* van de Raad voor het Openbaar Bestuur en de Raad voor Cultuur uit 2016.

En om het nog wat ingewikkelder te maken: een gegeven is in de digitale wereld iets immaterieels en kan zich fysiek (als *bits* en *bytes*) op meer dan één locatie tegelijk bevinden, bijvoorbeeld op verschillende computers of servers. Wie is er dan verantwoordelijk? Dit laatste geldt natuurlijk ook al in de papieren wereld, waarin naar hartenlust wordt gekopieerd en overal en nergens kopieën van documenten en dossiers rondzwerven. De vraag is of de digitalisering het ingewikkelder of juist eenvoudiger maakt op dit punt.

2.4 ... en op de kruispunten van ketens

De beginselen van gegevensbescherming zijn, zoals gezegd, niet wezenlijk veranderd bij de komst van de Avg en de Rgbs. Een hardnekkig punt in de discussie over gegevensbescherming wordt dus niet vanzelf opgelost door de nieuwe regels. Ik doel op de gegevensuitwisseling in samenwerkingsverbanden. Denk aan ZSM, Veiligheidshuizen, casusoverleggen, ketenunits, RIEC's (Regionale Informatie- en Expertisecentra), enzovoort. Want hoe belangrijk strafrecht ook is, de wereld is groter dan de strafrechtsketen. Zoals een organisatie deel kan hebben aan meer dan één keten (par. 1.5), zo kan een individu voorwerp van aandacht zijn in meer dan één keten. Iemand volgt onderwijs (of behoort dat te doen omdat hij leerplichtig is), geniet gezondheidszorg, heeft een inkomen of een inkomensvervangende uitkering, vraagt een verblijfsstatus, een verblijfsdocument of een vergunning aan, pleegt delicten, enzovoort. En dat allemaal tegelijk. Individuen kunnen dus de aandacht hebben van meer ketens tegelijkertijd (zie nader par. 5.3). Omgekeerd hebben vele instanties vanuit uiteenlopende gezichtspunten tegelijkertijd bemoeienis met hetzelfde individu. Tot op zekere

hoogte moeten die bemoeienissen op elkaar afgestemd worden, willen zij zinvol zijn. In elk moeten zij elkaar niet hinderen. Om dat te bereiken, moeten de actoren op zijn minst van elkaar weten *dat* zij bemoeienis hebben met eenzelfde individu, en onder omstandigheden ook *wat* die bemoeienis inhoudt. Er is dus in een of andere vorm informatie-uitwisseling tussen ketens nodig. Hoe regel je dat zodanig, dat het effectief is en tegelijk de gegevensbescherming in acht wordt genomen?

Kern van het vraagstuk is de doelbinding. Persoonsgegevens mogen alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art. 5, eerste lid, onder b, Avg; art. 4, eerste lid, onder b, Rgbs). Zij mogen 'verder' worden verwerkt, dat wil zeggen: voor een ander doel worden gebruikt dan waarvoor zij zijn verzameld, mits dat verdere gebruik niet onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (art. 6, vierde lid, Avg; art. 4, tweede lid, Rgbs). De verordening en de richtlijn geven een aantal aanknopingspunten om te bepalen of er voldoende verwantschap is tussen het oorspronkelijke doel en het doel van het verder gebruik. Maar de vraag die daaraan voorafgaat, is: hoe c.q. op welk niveau definieer je het doel waarvoor gegevens worden verzameld? Daarover zwijgt de regelgeving.

Theoretisch komen daarvoor drie niveaus in aanmerking. Het ene uiterste is het microniveau: de concrete casus. Alleen binnen de context van die casus, bijvoorbeeld één enkele strafzaak (*whatever that may be*, vgl. par. 4.5), mag dan informatie worden uitgewisseld. Dat beperkt de mogelijkheden voor gegevensuitwisseling sterk. Het andere uiterste is het macroniveau, oftewel zo iets als: het welzijn van Nederland, of het welzijn van de betrokkene, of de veiligheid van ons land – dat soort abstracte omschrijvingen. Maar dat trekt de grenzen veel te ruim, dan kun je wel alles met iedereen uitwisselen en dat kan ook niet de bedoeling zijn.

Mijns inziens biedt hier het ketenconcept een goed aanknopingspunt.[5] Daarmee zitten we op het mesoniveau. De keten bestaat volgens de omschrijvingen in de paragrafen 1.2-1.3 bij de gratie van een ketenproduct. Voor de strafrechtsketen is dat: de wetsovertreding wordt

bestraft (par. 3.1). Dat product kan geen enkele partij alléén realiseren, daarvoor zijn meer partijen nodig. Als dat zo is, moeten die partijen ook informatie kunnen uitwisselen. Binnen een keten moet dus in ruime mate informatie kunnen worden uitgewisseld. De verwantschap in het doel van de verwerkingen ligt dan in het gezamenlijke ketenproduct, dat door geen van de afzonderlijke ketenpartijen kan worden gerealiseerd. Dat geldt voor de strafrechtsketen en bijvoorbeeld ook voor de zorg (medische gegevens). Het netwerkconcept helpt ons hier niet.

Intussen zijn de samenwerkingsverbanden die ik aan het begin van deze paragraaf noemde geen ketens maar netwerken waarin verschillende ketens elkaar raken. Hoe gaan we daar om met gegevensuitwisseling? Er wordt wel gezegd dat samenwerkingsverbanden de ketens doorbreken. Het zou kwalijk zijn als dat waar was. Samenwerking en informatiedeling in netwerken kun je alleen goed regelen als je de afzonderlijke ketens die in het samenwerkingsverband samenkomen, scherp in het vizier houdt.

Voor het delen van strafrechtelijke informatie in publiekrechtelijke samenwerkingsverbanden gelden ruime regels (art. 33, eerste lid, onder b, Uitvoeringswet Avg). De enige eisen zijn in feite de proportionaliteit en de subsidiariteit. De vraag is hoe je daar op een nette en slimme manier gestalte aan geeft. (Voor informatie-uitwisseling in samenwerkingsverbanden met ook niet-publieke partijen komt er een aparte wet.) Zie verder paragraaf 5.3.

Ergens in de jaren negentig belandde de volgende vraag c.q. opdracht op mijn bord. Als iemand die een uitkering ontving, gedetineerd werd, moest die uitkering volgens sommige sociale wetten worden stopgezet. Hoe kwam de uitkeringverstrekkende instantie erachter dat betrokkene gedetineerd werd? Bij het verhoor van betrokkene als verdachte (niet verplicht tot antwoorden!) door de politie of de OvJ werd hem gevraagd of hij een sociale uitkering genoot; en in geval van bevestigende beantwoording, werd dat gemeld aan de uitkeringverstrek-

kende instantie. Hoe betrouwbaar was dat? Aan mij het verzoek/de opdracht om een betrouwbaardere manier te vinden.

Ik had geen idee in welke hoek ik het moest zoeken. Je kunt niet zo maar aan de (toenmalige) bedrijfsverenigingen de namen van alle gedetineerden verstrekken. En je kunt ook niet zo maar de namen van alle ontvangers van sociale uitkeringen verstrekken aan Justitie. Maar wat dan wel?

Ik ging praten met allerlei mensen die mij misschien zouden kunnen helpen. Dat bracht mij niet veel verder. Totdat ik via via belandde bij Jan Grijpink, (destijds) collega binnen het departement, maar binnen een heel andere directie en mij toen nog onbekend. Die had binnen vijf minuten het concept voor de oplossing. Er bestaat (c.q.: er bestond toen) een centrale verwijsindex voor gedetineerden (de toenmalige VIP, min of meer Grijpinks geesteskind; zie nader par. 5.4) en één voor werknemersverzekeringen. Check *real time*, dat wil zeggen op het moment van insluiting, en in een afgeschermde omgeving, of de verdachte bekend is in de verwijsindex van uitkeringsontvangers. De *hits* (signalen) die daaruit rollen, verdienen nader onderzoek. Grijpink heeft deze casus in tal van zijn publicaties geschetst onder het label 'meerketenoplossing', het uitvoerigst in zijn boek *Werken met keteninformatisering* (1999), p. 26-31. (Inmiddels is het allemaal expliciet wettelijk geregeld, zie par. 5.3.)

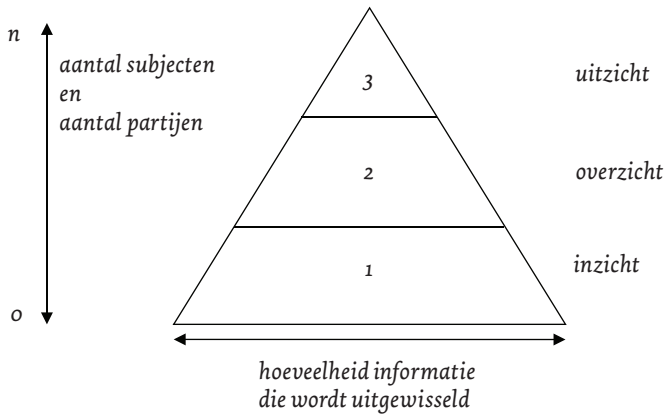
De verbindende factor in samenwerkingsverbanden is in alle gevallen de cliënt, de persoon die het voorwerp van zorg is van de samenwerkende partijen (vgl. par. 5.2). Het ligt dus voor de hand het verbindingspunt voor de informatievoorziening te zoeken in de persoon, het individu. De IV over ketens heen kan op basis van een paar eenvoudige principes worden ingericht, namelijk:
- scheiding van lagen (niveaus);
- scheiding tussen incidentgebonden en persoonsgebonden informatie;

- scheiding tussen *dat-* en *wat*-informatie;
- gegevens zo veel mogelijk halen bij de bron (in plaats van kopiëren c.q. dupliceren); en
- doelbinding op ketenniveau (zie de vorige paragraaf).

Door de toepassing van deze principes ontstaat – wat je zou kunnen noemen – een informatiepiramide. Bovenin, op ketenniveau, wordt alleen *dat*-informatie gedeeld. Er wordt een beperkte, kale set van gegevens over de persoon gedeeld met een groot aantal partijen. Onderin, op organisatieniveau c.q. in het grondvlak, wordt veel meer informatie gedeeld maar met veel minder partijen. Daar gaat het over *wat*-informatie: wat is er met de persoon aan de hand, wat is er al over hem bekend, waarom is hij in beeld (de incidentgebonden informatie), welke acties lopen rond hem, enzovoort.

Tussen deze twee niveaus kan nog een derde liggen. In casusoverleggen en Veiligheidshuizen bijvoorbeeld worden afspraken gemaakt rond personen over de op hen toe te passen interventies. Of over doelgroepen. Die afspraken moeten voor alle deelnemende partijen kenbaar en dus ook toegankelijk zijn.

Het hoogste niveau, de kale dat-informatie, biedt *uitzicht* over de grenzen van organisaties en ketens heen, het middenniveau *overzicht* binnen een samenwerkingsverband en het laagste niveau *inzicht* in de exacte situatie rond een justitiabele.



Het onderscheiden van deze lagen is van belang uit oogpunt van gegevensbescherming. Hoeveel informatie je mag delen, wordt immers (mede) bepaald door de noodzaak om die informatie te delen (*need to know*, *need to share*). Kale *dat*-informatie kun je ruimer delen dan volledige, inhoudelijke *wat*-informatie. En dat is vaak al voldoende. Op het hoogste niveau (uitzicht) kun je bijvoorbeeld heel kale *dat*-informatie uitwisselen tussen ketens; zie het voorbeeld van de uitkeringsgerechtigde die wordt gedetineerd. Zo wordt bevorderd dat je niet méér informatie deelt of uitwisselt dan nodig is (*data protection by design*).

Om over de grenzen van ketens heen meer dan deze beperkte hoeveelheid informatie te delen, is een uitdrukkelijke wettelijke grondslag nodig. Zie de paragrafen 5.2 en 5.3. Verder verwijs ik nog graag naar het informatieblad *Informatie delen in samenwerkingsverbanden* (2012) van het voormalige College bescherming persoonsgegevens (CBP).

2.5 Tips & tricks voor (D)PIA's in ketenverband

De discussie over gegevensbescherming in ketens wordt de laatste tijd vaak gevoerd in het kader van het maken van – wat tot voor kort werd genoemd – een Privacy Impact Assessment (PIA). De Avg spreekt van een Data Protection Impact Assessment (DPIA), oftewel: gegevensbeschermingseffectbeoordeling, zoals de officiële Nederlandse – of is het de Vlaamse? – vertaling het noemt. Dat is eigenlijk beter. Zo'n assessment kan betrekking hebben op nieuw beleid, nieuwe regelgeving of nieuwe systemen.

> 'Privacyregels hoeven aan weinig legitieme overheidsdoelstellingen in de weg te staan. Daarvoor is het wel van belang om er vanaf het begin rekening mee te houden. Dat geldt zowel voor het opstellen van beleid als voor het ontwerpen van organisatiestructuren, informatiesystemen en procedures', aldus de (toenmalige) voorzitter van het (toenmalige) CBP (tegenwoordig: AP), Peter Hustinx, in zijn Voorwoord bij het rapport *Elektronische overheid en privacy* (2002). 'Vanaf het begin er rekening mee houden' – daartoe dient een DPIA.

Het is een mooi instrument om op een gestructureerde manier de discussie te voeren over gegevensbescherming. Ik heb in de loop der jaren een aantal vuistregels ontwikkeld of ontdekt:

- Maak onderscheid tussen wat er 'onder' en wat er 'boven de motorkap' gebeurt. Gegevens(verzamelingen) zitten boven, informatiesystemen onder de motorkap (zie de informatiester in par. 1.1) Gegevensbescherming gaat over wát wij doen met persoonsgegevens. Hóe we dat doen, is in hoge mate een kwestie van techniek. Naarmate we dieper in de techniek duiken, verliest de regelgeving inzake de bescherming van persoonsgegevens haar greep. Dit is geen pleidooi om de techniek tot juridische vrijstaat uit te roepen, maar eenvoudigweg een erkenning van de realiteit dat de arm van het recht wel sterk is maar niet zo lang.
- Waar gegevens fysiek staan, is uit juridisch oogpunt niet relevant, dat is 'maar' techniek, iets onder de motorkap. Bij wijze van denkoefening zeg ik altijd: al zou je ze op de maan zetten. Het maakt geen verschil in de verantwoordelijkheden voor een gegeven. Of je je informatie(producten) nu in Tokio, Timboektoe of Teheran opslaat, de verantwoordelijkheden veranderen niet; maar er kunnen natuurlijk andere dan technische redenen zijn om je spullen liever in Tokio dan in Teheran of Timboektoe op te slaan. Of misschien toch maar helemaal in eigen beheer, als het waar is dat gegevensbescherming in de *cloud* niet te garanderen is.[6]
- Eigendom van gegevens bestaat niet als het gaat over het verwerken van persoonsgegevens door de overheid. De wetgeving over gegevensbescherming gaat, zoals gezegd, over 'verwerken' en 'verantwoordelijke'. Eigendom suggereert een soort van exclusieve zeggenschap. Dat is in de context van bijvoorbeeld het patiëntendossier misschien wel relevant (zeggenschap van de patiënt over zijn gegevens), maar als het gaat om de verwerking van persoonsgegevens door een overheidsorgaan is het niet aan de orde. De overheid verwerkt persoonsgegevens uitsluitend instrumenteel, doelgebonden en op wettelijke grondslag; daar is geen sprake van ermee kunnen doen wat je wilt zo lang het maar niet in strijd is met de wet. En in het strafrecht kan om voor de hand liggende redenen al helemaal geen sprake zijn van zeggenschap van de

verdachte of veroordeelde over de op hem betrekking hebbende gegevens. (Iets anders is dat met *eigenaarschap* vaak wordt bedoeld de verantwoordelijkheid voor het bestaan en het beheer van een gegeven of document als zodanig. Partijen in een samenwerkingsverband bijvoorbeeld kunnen daar best afspraken over maken. Alleen doen die niets af aan de wettelijke verantwoordelijkheid van elke verwerker afzonderlijk voor wat hij zelf met de gegevens doet.)

- Gegevensbescherming gaat over persoonsgegevens, verwerken en verantwoordelijke. Gegevens worden gecreëerd en gebruikt in processen. Die processen bepalen de noodzaak en de doelen van de gegevensverwerking. Dus het zal ook moeten gaan over de processen. En over de gegevensverzamelingen (zie par. 1.1 voor het verschil tussen gegevensverzameling en informatiesysteem). Systemen, applicaties, services of functionaliteiten daarentegen zijn stoorzenders. Ze zitten in het domein van de techniek (hóe) en zijn als zodanig uit oogpunt van gegevensbescherming niet relevant.
- Tot op zekere hoogte geldt dat ook voor de organisatie waar de gegevens zich bevinden. Het enkele feit dat bepaalde gegevens zich fysiek onder één dak bevinden, zegt op zichzelf nog niets over de vraag of ze bijvoorbeeld met elkaar in verband gebracht mogen worden Dit is vooral van belang voor de vraag of en in hoeverre personalia van subjecten uit verschillende domeinen, bijvoorbeeld strafrecht, vreemdelingenrecht, fiscaal recht, 'Mulder', gematcht mogen worden. De regels over gegevensbescherming gelden ook achter de voordeur van een organisatie of systeem.
- In een discussie in het kader van een DPIA is het dus handig om woorden als systeem, organisatie, eigenaar, te parkeren als 'verboden woorden'. Helaas beginnen veel discussies over gegevensuitwisseling aan de verkeerde kant. Zelfs in brieven van de minister aan de Tweede Kamer valt soms te lezen dat 'de politie' toegang moet krijgen tot dit of dat 'systeem' van bijvoorbeeld het openbaar ministerie. Ik noem dit het binnen-zonder-kloppen-syndroom. Dat is voor de executieve taken van de politie (opsporing, hulpverlening) onder omstandigheden wel een passende denkwijze, maar in het kader van gegevensbescherming niet. Ook is er in de

loop der jaren veel discussie geweest over de vraag of bepaalde informatiestromen nu moesten verlopen via organisatie A (bijvoorbeeld: de Justitiële Informatiedienst) of organisatie B (bijvoorbeeld: het CJIB/AICE). Ook dat is de verkeerde vraag. De juiste vraag is: welke gegevens moeten worden uitgewisseld en wat zijn de authentieke bronnen van die gegevens. (Zo'n authentieke bron is een proces, een organisatie of een gegevensverzameling, waarvan is afgesproken dat díe binnen de keten de exclusieve kenbron – *single source* – is van een gegeven.) Het moet dus gaan over de gegevensverzamelingen en pas daarna, als afgeleide daarvan, over de organisaties die die verzamelingen beheren.

- Een handig hulpmiddel is een *create-use* matrix. Daarin zet je op de ene as in welk proces een gegeven wordt gegenereerd (*create*) en op de andere in welk proces het gegeven wordt gebruikt (*use*). Als je dat overzicht hebt gemaakt, kun je dat vertalen naar de organisaties waarbinnen die processen verlopen (de actoren) en vervolgens naar de systemen die daarbij worden gebruikt (vgl. de ketenanalyse aan de hand van de drie P's, par. 1.3). Zo worden verantwoordelijkheden helder.
- Maak onderscheid tussen structurele en incidentele gegevensuitwisseling. Incidenteel is er vaak meer mogelijk dan op structurele basis. Een bepaalde verwerking kan in een incidenteel geval noodzakelijk zijn, maar niet voor een grote groep van gevallen en daarom niet op structurele basis. Zo is bijvoorbeeld in het sociale domein het samenstellen van een integraal persoonsbeeld ongeacht de hulpvraag of de noodzakelijkheidsafweging niet aan de orde. In de context van het strafrecht ligt dat anders (zie hoofdstuk 2).
- Maak onderscheid tussen regel en uitzondering. Je kunt bijvoorbeeld regelen dat functionarissen in beginsel geen toegang hebben tot bepaalde gegevens of soorten gegevens, maar in uitzonderingsgevallen er wel bij kunnen. Dit wordt wel het *breaking the glass*-principe genoemd.
- En nog een aandachtspuntje: er wordt in dit werkveld veel gewerkt met *pilots*. Dat is heel goed. Maar als iets volgens de wet niet mag, mag het ook niet in het kader van een *pilot*. Daarom worden er nu

her en der experimenteerbepalingen in de wetgeving gecreëerd, onder andere in het Wetboek van Strafvordering.
– Dat de discussie over gegevensbescherming geen exclusieve bezigheid is van de juristen, moge na en uit het voorgaande voldoende duidelijk zijn.

Noten

1 PIOFACH staat voor: Personeel, Informatievoorziening, Organisatie, Financiën, Administratieve organisatie, Communicatie en Huisvesting. De term *bedrijfsvoering* wordt soms gebruikt ter aanduiding van deze PIOFACH-aspecten, soms als aanduiding van het primaire proces. Ik zal de term daarom goeddeels vermijden. Van Dale definieert *bedrijfsvoering* heel neutraal: *(wijze van) exploitatie van een bedrijf.*
2 EHRM 25 februari 1997, *NJ* 1999, 516 (Z. v. Finland) en 29 april 2014, *NJ* 2016, 179 (L.H. v. Letland).
3 De wetgever heeft het over de Richtlijn gegevensbescherming opsporing en vervolging. Maar het toepassingsbereik van de richtlijn omspant de hele strafrechtspleging, met inbegrip van de berechting en de tenuitvoerlegging van sancties. Dat is dus veel meer dan alleen opsporing en vervolging. Sterker nog, zelfs ordehandhaving en het voorkomen van strafbare feiten (dus preventie) vallen onder de richtlijn. Maar een hanteerbare aanduiding die ook dat allemaal dekt, kan ik niet verzinnen.
4 Reactie naar aanleiding van het artikel van Martijn van Wees, Modernisering en digitalisering van het strafproces, *DD* 2015/72.
5 Vgl. M.J. Bonthuis, Dataprotectie in ketens. Zijn de huidige privacyconcepten wel geschikt voor toepassing in ketens?, *Privacy & Informatie* (P&I) 2016, p. 156-162.
6 R. Kuijpers, Zekerheid is niet te geven. Over privacy in de cloud, *Informatie*, 2013 (november), p. 17-22.

HOOFDSTUK 3

DE VERDACHTE IN DE STRAFRECHTSKETEN

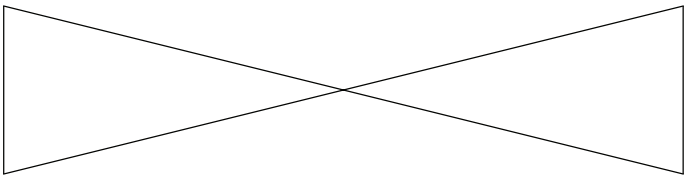
3.1 Strafrecht is de koppeling van incident, individu en interventie

Wat strafrecht is, daar heeft iedereen wel een – meer of minder vage – voorstelling bij. In deze en de volgende paragraaf probeer ik die wat aan te scherpen (voor de niet-juristen onder de lezers).

Strafrecht is het verbinden van een sanctie (straf of maatregel) aan een menselijke gedraging. De verbinding tussen beide ligt in de persoon. De gepleegde strafbare feiten worden herleid tot een persoon als verdachte respectievelijk dader.[1] Dit betreft de schuld, opheldering, waarheidsvinding, bewijs. *Jegens* die persoon worden interventies (straffen en/of maatregelen) toegepast *wegens* de door hem begane delicten.

Strafrechtspleging begint met opsporing. Alleen op basis van voldoende – en overtuigend – bewijsmateriaal kan het oordeel worden geveld dat de betrokkene schuldig is en dat hem een straf mag en moet worden opgelegd. Als het ten laste gelegde feit niet kan worden bewezen, dient de rechter te besluiten tot vrijspraak dan wel moet de officier van justitie het feit seponeren. De opgelegde straf wordt ten uitvoer gelegd. Na de tenuitvoerlegging keert (in het geval van detentie) de betrokkene terug in de samenleving.

De drie basiselementen van het strafrecht zijn dus: gedraging, persoon en sanctie; oftewel: *incident*, *individu* en *interventie*.



feit, gedraging, delict	persoon (natuurlijk persoon, rechtspersoon)	straf, maatregel, sanctie

INCIDENT ← *'wegens'* ← INDIVIDU ← *'jegens'* ← INTERVENTIE

Sancties zijn de producten, de *output*, van het strafrechtelijk systeem. De maatschappelijke waarde, de *outcome*, zoeken wij in noties als rechtvaardigheid, veiligheid, leefbaarheid. Daar draagt het strafrecht alleen indirect aan bij en dan ook nog eens in beperkte mate.

Partij in een rechtszaak zijn degenen van wie de rechten en verplichtingen inzet zijn van het geding. In een strafzaak zijn dat de verdachte (of veroordeelde), de OvJ en de benadeelde partij. Met dat laatste wordt bedoeld degene die schade heeft geleden door een strafbaar feit en zich voegt in het strafproces om schadevergoeding te claimen. Daarnaast heeft het slachtoffer in bepaalde gevallen het recht om op de terechtzitting een verklaring af te leggen over de gevolgen die het misdrijf voor hem persoonlijk heeft gehad. Zolang het slachtoffer niet als benadeelde partij een claim indient in de strafzaak, is hij geen partij, net zomin als alle andere betrokkenen (getuigen, deskundigen, tolken).

Opsporen is het werk van de politie en andere opsporingsdiensten en -ambtenaren (er lopen buiten de politie meer opsporingsambtenaren rond dan binnen de politie). Zij maken proces-verbaal (pv) op van het strafbare feit of 'van hetgeen door hen ter opsporing is verricht of bevonden' (in de honderd jaar oude bewoordingen van art. 152, eerste lid, Sv). In de lichtere gevallen leveren zij dat pv rechtstreeks aan bij het Centraal Justitieel Incassobureau (CJIB), waarna het CJIB de ten-

uitvoerlegging van de sanctie verzorgt. In de zwaardere gevallen leveren zij het pv aan bij de OvJ. De OvJ maakt deel uit van het openbaar ministerie (OM).

Het OM schrijft het proces-verbaal in onder een parketnummer. Daarmee wordt het een *zaak*. De OvJ moet beslissen of hij de zaak aan de rechter voorlegt. Het voorleggen van een zaak door een OvJ aan een rechter heet *vervolgen*. De officier kan ook een strafbeschikking uitvaardigen (= OM-afdoening). Ook dat heet volgens het huidige Wetboek van Strafvordering vervolgen.

Als de OvJ besluit tot een strafbeschikking, gaat de zaak naar het CJIB. Het CJIB heeft twee taken: ten uitvoer leggen van financiële sancties en coördineren van de tenuitvoerlegging in breedste zin van het woord. Voor dat laatste is het Administratie- en Informatiecentrum voor de Executie (AICE) als apart onderdeel van het CJIB in het leven geroepen.

Als de OvJ besluit de zaak aan de rechter voor te leggen, maakt hij een *dagvaarding*. Op basis van de dagvaarding behandelt de rechter de zaak op een openbare terechtzitting en wijst daarna *vonnis*. In geval van schuldigverklaring legt de rechter doorgaans een straf of maatregel op. Al deze documenten – proces-verbaal, dagvaarding, strafbeschikking, vonnis – zijn in het perspectief van de keten halfproducten, niet meer en niet minder (ook al klinkt dat voor een vonnis misschien een beetje oneerbiedig).

Een veroordelend vonnis moet worden ten uitvoer gelegd. Dat doet het CJIB (voor de vermogenssancties) of de Dienst Justitiële Inrichtingen (voor de vrijheidsbenemende sancties) of de reclassering (voor de taakstraffen).

Na een ten uitvoer gelegde vrijheidsstraf draagt Justitie de zorg voor de ex-gedetineerde over aan de gemeente voor de re-integratie. Deze zorg betreft de zogeheten primaire leefgebieden: huisvesting, zorg, werk/inkomen en identiteit (het hebben of krijgen van een geldig identiteitsbewijs).

De strafrechtspleging bestaat dus uit de volgende fasen of stappen:

Deze stappen staan in een *logisch* dwingende volgorde. Elke eerdere stap is een noodzakelijke voorwaarde voor elke latere. Althans, in een rechtsstaat; in totalitaire staten worden mensen ook zonder vorm van proces opgesloten.

Een stap is niet per se ook een *voldoende* voorwaarde voor de volgende. Het kan zijn dat de opsporingsdiensten geen verdachte kunnen vinden; dan gaat de zaak niet naar de OvJ. De OvJ kan een zaak om allerlei redenen seponeren en hij kan een strafbeschikking opleggen; ook dan komt er geen rechter aan te pas. Een rechter kan besluiten tot vrijspraak, ontslag van alle rechtsvervolging zonder oplegging van een maatregel, of schuldigverklaring zonder oplegging van straf; dan is tenuitvoerlegging niet aan de orde.

Volgens de definitie uit de paragrafen 1.3 en 1.4 is de strafrechtspleging dus een zuivere keten. Het *product* (P_1) van de keten is: de wetsovertreding wordt bestraft. Het *proces* (P_2) is zuiver sequentieel (op logisch niveau). En geen enkele *partij* (P_3) kan het ketenproduct in z'n eentje maken: ieder maakt een deel, ze zijn operationeel van anderen afhankelijk voor het geheel, maar bestuurlijk autonoom ten opzichte van elkaar.

3.2 Belendende percelen: 'Mulder', bestuursrecht, toezicht

Honderd jaar geleden was het nog eenvoudig: strafrecht was het enige publieke middel om wetsovertreders te bestraffen. Toen kwamen ook de meeste strafzaken nog voor de rechter. Inmiddels kennen we een veelheid van publiekrechtelijke sanctiestelsels en is berechting door de rechter uitzondering geworden. In verreweg de meeste gevallen komt er geen rechter meer aan te pas. Hoe zit het nú in elkaar? Het plaatje ziet er ruwweg als volgt uit.

Strafrecht gaat over strafbare feiten (delicten). Strafbare feiten worden onderverdeeld in misdrijven (dat zijn de ernstigere strafbare feiten) en overtredingen (de lichtere strafbare feiten). Strafrecht is alles wat in de wet als zodanig wordt aangeduid. Het is te herkennen aan de formule 'wordt gestraft met'. Het kent om zo te zeggen drie smaken.

- De harde kern is het zogenoemde commune strafrecht, de 'echte' misdrijven. Deze worden voornamelijk door de politie en de Koninklijke Marechaussee opgespoord, door de rechter berecht en veelal met vrijheidsstraf bestraft; denk aan *high impact crimes* (zoals zware geweldsmisdrijven) en ondermijning (georganiseerde criminaliteit).
- De lichtere misdrijven en de overtredingen worden in hoofdzaak met een geldboete en/of taakstraf bestraft. Dit wordt ook wel aangeduid als veelvoorkomende criminaliteit (VVC). Deze delicten worden deels door de politie, deels door Buitengewoon Opsporingsambtenaren (BOA's) opgespoord en voor het merendeel buiten de rechter om afgedaan.
- Als derde is er het ordeningsrecht. Dit betreft fiscale, economische en milieudelicten. De misdrijven in de sfeer van het ordeningsrecht worden vooral door de vier bijzondere opsporingsdiensten (BOD'en) opgespoord. Ze kunnen zowel in de lichtere als in de zwaardere categorie vallen.

De laatste decennia is sanctierecht buiten het strafrecht om sterk in opkomst.

- Sinds 1990 hebben we de Wet administratiefrechtelijke handhaving verkeersvoorschriften (Wahv), beter bekend als de Wet-Mulder, genoemd naar Albert Mulder, die als gepensioneerd secretaris-generaal van het ministerie van Justitie voorzitter was van de commissie die de wet heeft ontworpen. Dit is een soort van schaduwstrafrecht, met eigen procedures. Het is gelabeld als bestuursrecht, geen strafrecht. Daarom spreekt de wet bijvoorbeeld niet van overtreding maar van 'gedraging', niet van verdachte of dader maar van 'betrokkene', en niet van boete maar van 'administratieve sanctie'. De strafrechtelijke afkomst van de Wet-Mulder verraadt zich onder meer in de rol van de OvJ als degene bij wie de betrokkene in beroep kan gaan tegen de administratieve sanctie.

– Al veel ouder is het administratieve sanctierecht. Dit wordt ook wel genoemd het bestuursstrafrecht. Dit bestrijkt die feiten waarop het bestuur zelf, buiten de OvJ om, met een boete kan reageren. Het fiscale strafrecht dateert al uit de negentiende eeuw, het economische strafrecht kwam op in de jaren dertig van de twintigste eeuw. Sinds ongeveer 1990 is er sprake van een hausse aan bestuurlijke boetebevoegdheden. Een van de jongste loten aan de stam is de bevoegdheid van de Autoriteit Persoonsgegevens (tot 1 januari 2016: College bescherming persoonsgegevens) om bestuurlijke boetes op te leggen voor overtredingen van de regels van de Avg.

In deze gevallen wordt er wel een sanctie opgelegd, maar het is geen strafrecht. Er is géén sprake van een strafbaar feit en géén sprake van een verdachte.

'Mulder' en bestuursstrafrecht beogen net als het eigenlijke strafrecht leedtoevoeging wegens een begaan delict. Het zijn repressieve handhavingsinstrumenten, ze kijken in eerste instantie naar het verleden. Daarnaast kent het bestuursrecht preventieve sancties, zoals het opleggen van een dwangsom of het intrekken van een vergunning. Deze hebben niet tot doel als straf te dienen (leed toe te voegen wegens een begane wetsovertreding), maar een onrechtmatige situatie op te heffen. Ze zijn op de toekomst gericht. Voorbeelden zijn de bestuursdwang (bijvoorbeeld: het bestuur laat een onrechtmatig geplaatst bouwsel afbreken) en de last onder dwangsom (de toezichthouder dreigt met een financiële sanctie als een bepaalde onrechtmatige situatie niet binnen een bepaalde tijd wordt rechtgezet).

De bestuurlijke sancties zijn gebaseerd op bestuurlijk toezicht. Dat toezicht kan dus leiden tot bestuurlijk ingrijpen, maar het kan ook het voorportaal zijn van toepassing van strafrecht. In al deze gevallen van bestuurlijke handhaving is er géén sprake van een strafbaar feit en géén sprake van een verdachte. Wel is er zo langzamerhand een compleet schaduwstrafprocesrecht ontwikkeld, omdat bepaalde waarborgen van het strafrecht ook van toepassing zijn verklaard op niet-strafrechtelijke bestraffing. Dit betreft vooral het recht op een

eerlijk proces als bedoeld in artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

De trits incident-individu-interventie (par. 3.1) is op al deze sanctievormen evenzeer van toepassing als op het echte strafrecht. De niet-strafrechtelijke sanctiesystemen vertonen ook dezelfde ketenstructuur. We hebben dus te maken met verschillende ketens, die ongeveer hetzelfde beogen (namelijk rechtshandhaving c.q. criminaliteitsbeheersing), maar waarbinnen andere regels gelden. (Het modelletje is zelfs nog veel breder toepasselijk, op veel meer gebieden van overheidsoptreden. Bijvoorbeeld op het verlenen van een vergunning of andere diensten door de overheid.)

3.3 De binnenkant van de strafrechtsketen: de verdachte en de zaak

Strafrecht is, zoals gezegd, een keten. Maar niet een keten zoals alle andere. Maatschappelijke ketens kennen een *cliënt*. De cliënt is degene die centraal staat in het proces. De cliënt is degene aan wie de dienst wordt *verleend*, hij is de afnemer van de dienst waaraan de keten haar bestaansrecht ontleent, bijvoorbeeld een uitkering, een subsidie, een vergunning. In een aantal gevallen is hij tevens degene aan wie de dienst wordt *verricht*, bijvoorbeeld een medische behandeling. In het bedrijfsproces van de strafrechtsketen staat de verdachte c.q. veroordeelde centraal. De strafzaak is tegen hem gericht, *jegens* hem wordt een sanctie toegepast *wegens* iets wat hij gedaan heeft. In die zin is hij het object van de keten. Hij is echter meer degene aan wie de dienst wordt *verricht* dan degene aan wie de dienst wordt *verleend*. Straf pleegt te worden gedefinieerd als beoogde leedtoevoeging (par. 3.1). Waar in andere ketens een dienst aan de cliënt wordt *aangeboden*, impliceert straf juist dat iemand iets wordt *afgenomen*: zijn bewegingsvrijheid en/of zijn bestedingsvrijheid, althans een deel daarvan.

Een keten heeft om zo te zeggen een binnenkant en een buitenkant. De binnenkant is het proces, de buitenkant zijn de organisaties of actoren. Naar de binnenkant kunnen we twee soorten ketens onderscheiden: logistieke ketens en voortbrengingsketens.

- In een logistieke keten gaat het om het *transport* van een goed (Van Dale: logistiek = beheersingsproces van goederenbewegingen). Dat transport loopt over verschillende schijven. Het goed zelf verandert alleen maar van plaats, niet van aard, hoedanigheid of samenstelling. In een voortbrengingsketen daarentegen (productieketen, *supply chain*)[2] gaat het om de *productie* of totstandkoming van een resultaat (goed of dienst) waar uiteenlopende actoren een bijdrage aan leveren.
- In de logistiek gaat het altijd om fysieke goederen en goederenstromen; in voortbrengingsprocessen kan het ook betrekking hebben op diensten. Een goed wordt geleverd aan een *klant*, een dienst wordt verricht voor of aan een *cliënt*.
- Bij de logistieke keten past de metafoor van het buizenstelsel. Er moet iets getransporteerd worden van A naar B: het gaat er aan de ene kant (punt A) in en komt er aan de andere kant (punt B) – hopelijk ongeschonden – uit. Bij de productieketen past meer de metafoor van de fabriek: er gaat iets in, een grondstof of halffabrikaat, dat wordt in een aantal fasen bewerkt, en er komt iets uit, het eindproduct.

De strafrechtspleging is tot op zekere hoogte een logistieke keten: er worden, in elk geval in de papieren wereld, documenten en dossiers overgedragen c.q. rondgepompt. Als zo'n document is vastgesteld, bijvoorbeeld een proces-verbaal, een rapport, een vonnis, mag het wel doorgegeven maar meestal niet meer veranderd worden. Het is tegelijk ook een voortbrengingsketen: elke volgende schakel voegt waarde toe op weg naar het gezamenlijke eindproduct, het dossier verandert onderweg.

In de metafoor van het buizenstelsel is de keten vooral een managementprobleem: hoe kunnen we zo veel mogelijk zaken door het systeem pompen tegen zo laag mogelijke kosten. De metafoor van de voortbrengingsketen stelt meer de professional centraal: hoe breng ik een zaak tot een goed einde.

In de meeste gevallen zit de verdachte gewoon thuis, op zijn werk, of waar dan ook – maar in elk geval niet fysiek 'in de keten'. Slechts in een klein aantal gevallen is een verdachte fysiek in het ketenproces

betrokken, bijvoorbeeld als hij gedetineerd is, of tijdens een verhoor of op de terechtzitting. Het is dus geforceerd om te zeggen dat de verdachte door de keten stroomt. Wat feitelijk door de keten stroomt, is een hoeveelheid informatie over een bepaald feit en een bepaalde persoon. Die informatie kan belichaamd zijn in een papieren dossier of in digitale documenten, zoals de elektronische aangifte of het elektronisch proces-verbaal. Maar ook dat is niet de essentie van wat er door de keten stroomt. De relatie tussen feit en persoon ligt in het begrip zaak. Wat door de keten stroomt, is dus de zaak (meer hierover in par. 4.2 en 4.5).

In logistieke ketens kan de informatiestroom zowel in de tijd als qua te volgen pad losgekoppeld worden van de goederenstroom. Een document zit niet langer in hetzelfde schip of vliegtuig als de lading, maar wordt elektronisch verzonden. In bijvoorbeeld een ZSM-omgeving kunnen alle betrokken partijen – zoals OM, politie, reclassering, kinderbescherming, slachtofferhulp – gelijktijdig (in plaats van volgtijdelijk) werken aan dezelfde zaak en vooral ook informatie uitwisselen. Het ketenbegrip dwingt er niet toe (zoals wel eens beweerd wordt) om volgtijdelijk te werken.

Het voortbrengingsproces omvat een aantal overdrachtsmomenten. Er is verschil tussen overdracht van *informatie* en overdracht van de *zaak*. Overdracht van de zaak impliceert vrijwel per definitie ook overdracht van informatie, maar het omgekeerde hoeft niet het geval te zijn. De overdracht van de zaak tussen twee schakels (fasen, stappen) in de keten kan worden beschouwd als een order, dat wil zeggen: als een vraag om verdere bewerking c.q. waardetoevoeging. De overdracht van alleen maar informatie hoeft niet dat karakter te hebben. Omgekeerd is het mogelijk een zaak over te dragen zonder ook meteen alle bijbehorende informatie over te dragen. De ene partij kan een berichtje sturen naar de andere dat er een zaak voor hem klaar staat, de andere partij kan vervolgens de voor hem relevante informatie (het dossier) ergens ophalen. Ook zo kunnen de informatiestroom en de zaakstroom worden gescheiden en efficiënter worden ingericht.

3.4 De buitenkant van de strafrechtsketen: de organisaties

De keten is een proces over de grenzen van organisaties heen. Omgekeerd kunnen door één organisatie of netwerk verschillende ketens (productieprocessen) lopen (zie par. 1.4). De meeste organisaties in de strafrechtspleging hebben ook functies in andere ketens of domeinen. Dat maakt het lastig als zij worden geconfronteerd met uiteenlopende eisen vanuit de verschillende ketens, bijvoorbeeld met regelgeving over het verwerken van persoonsgegevens of verschillende standaarden voor berichtuitwisseling.

De meeste actoren hebben ook een rol in meer dan één fase. De OvJ bijvoorbeeld is belast met de leiding van de opsporing, is de enige die vervolging kan instellen, heeft de exclusieve toegang tot de rechter en heeft een rol bij de tenuitvoerlegging van opgelegde straffen en maatregelen. De reclassering verleent vroeghulp bij de inverzekeringstelling van verdachten, brengt rapport uit aan de OvJ en de rechter, is belast met de tenuitvoerlegging van de taakstraffen en begeleidt gedetineerden na hun detentie c.q. houdt toezicht als er een voorwaardelijke sanctie is opgelegd. De Dienst Justitiële Inrichtingen (DJI) is verantwoordelijk zowel voor de voorlopige hechtenis als voor de tenuitvoerlegging van opgelegde vrijheidsbenemende straffen of maatregelen. De rechter beslist in het vooronderzoek (de vervolging) en in het eindonderzoek (de berechting) en heeft een rol in de tenuitvoerlegging van sancties. Alleen al daarom is het gangbare beeld van 'de strafrechtsketen = politie, openbaar ministerie, rechtspraak, gevangeniswezen, reclassering' te simpel.

Er wordt wel beweerd dat digitalisering de keten radicaal overhoop kan halen. Je zou organisaties kunnen samenvoegen, opheffen, enzovoort. In het bedrijfsleven is dat ongetwijfeld het geval. En in sommige sectoren van het openbaar bestuur misschien ook. Maar in de strafrechtsketen ligt dat toch een slagje anders. Dat hangt samen met de *checks and balances* die onze rechtsstaat gestalte geven. Je wilt toch niet dat de politie ook de kinderbescherming doet of DJI de rechtspraak. Dus het strafrechtelijke landschap is weliswaar versnipperd, maar dat heeft een goede reden en zal ook (hopelijk) niet snel veranderen.

Ik heb door de jaren heen ook nogal eens opmerkingen gehoord in de trant van: ach, de partijen in de keten kennen en vertrouwen elkaar toch, waarom zou je dan (bijvoorbeeld) strenge eisen moeten stellen aan bijvoorbeeld autorisatie, authenticatie, logging, elektronische handtekeningen? Vertrouwen is goed in een contractuele context. De strafrechtspleging daarentegen moet het vertrouwen hebben van de buitenwereld: de verdachte, het slachtoffer en de hele samenleving. Zulk vertrouwen moet voortdurend waargemaakt worden. Dat vergt transparantie (controleerbaarheid) en verantwoording. De keten moet daar niet tegen heug en meug maar *con amore* aan werken.

De advocatuur heeft een eigen plek ten opzichte van de keten. De advocaat is niet belast met de toepassing van het strafrecht; hij staat systemisch bezien juist aan de andere kant. Conceptueel behoort de advocatuur daarom niet tot de strafrechtsketen (gedefinieerd als *proces*). Ze zit evident wel in het *netwerk* van de strafrecht toepassende organisaties. In de IV van de strafrechtsketen moet dus plaats worden ingeruimd voor de advocatuur, zodat de raadsman zijn rechten (c.q. die van de verdachte) geldend kan maken. De verdediging heeft immers recht op een gelijke informatiepositie als de OvJ (*equality of arms*) en de IV kan – en moet – daaraan bijdragen.

3.5 Het integraal en integer strafrechtelijk persoonsbeeld

Aan de binnenkant van de keten vinden we dus de verdachte en de zaak (par. 3.3). Dat zijn centrale begrippen in het proces en in de IV. Vele partijen zijn betrokken (of kunnen betrokken zijn) bij een en dezelfde zaak respectievelijk een en dezelfde verdachte. Die partijen moeten met elkaar communiceren, onderling informatie uitwisselen. Als zij dat doen, moeten ze wel redelijke zekerheid hebben dat ze het over dezelfde zaak respectievelijk dezelfde verdachte hebben. De identiteit van de verdachte en van de zaak is een essentieel vereiste bij werken in ketenverband. Alle partijen hebben stukjes informatie daarover; stukjes die voor anderen van belang kunnen zijn. Hoe krijgen we al die stukjes bij elkaar?

Een voorbeeld: een verdachte is aangehouden. Zijn identiteit wordt vastgesteld en hij wordt voorgeleid aan de hulpofficier van justitie. Die moet de verdachte verhoren en nagaan of de aanhouding rechtmatig was. Na het verhoor kan hij de verdachte ophouden voor onderzoek of in verzekering stellen (of direct voor de rechter-commissaris doen geleiden) of naar huis laten gaan (art. 57 en 61 Sv). Op basis waarvan beslist hij? Hij moet natuurlijk in de eerste plaats weten voor welk strafbaar feit de verdachte is aangehouden. Maar hij wil ook weten of er misschien nog meer strafzaken tegen de verdachte lopen. Is er ergens anders nog een onderzoek aan de gang? Moet de verdachte nog een straf uitzitten of een boete betalen? Is het een *first offender* of een notoire recidivist? Is het een veelpleger? Als de hulpofficier besluit de verdachte in verzekering te stellen, moet hij (c.q. de beheerder van het cellencomplex) weer een heleboel andere dingen weten, zoals: is de ingesloten verdachte agressief of misschien verslaafd, heeft hij bepaalde ziektes onder de leden, is hij geestelijk instabiel, moet hij een dieet houden of medicijnen gebruiken, mag hij bepaalde voedingsmiddelen of medicijnen per se niet gebruiken? Waar moet de politie al die informatie vandaan halen?

Hetzelfde geldt voor andere functionarissen in de strafrechtsketen: de officier van justitie, de rechter, de medewerker van de reclassering of de kinderbescherming, de directeur van de penitentiaire inrichting en vele anderen. Of ze werken in de klassieke context van ieder op zich of in de moderne setting van de ZSM-tafel of het Veiligheidshuis, maakt niet uit. Allemaal hebben ze informatie nodig over de persoon met wie ze te maken krijgen. Ongeveer de helft van alle verdachten die worden aangehouden, is recidivist. Over hen is al informatie aanwezig ergens binnen het strafrechtelijk systeem – en vaak ook elders binnen de overheid, bijvoorbeeld binnen de vreemdelingenketen, de Belastingdienst, het UWV of de Onderwijsinspectie. Alleen: die informatie is niet aanwezig bij degene die op dat moment een beslissing moet nemen of iets moet doen.

Grote bedrijven, zoals banken of verzekeringsmaatschappijen, staan voor hetzelfde probleem. Een verzekerde kan verschillende verzekeringen hebben lopen bij dezelfde maatschappij. Het kan zowel voor de verzekeringsmaatschappij als voor de cliënt interessant zijn om de informatie over die verschillende verzekeringen (polissen) niet gescheiden te houden, maar op een slimme manier bij elkaar te brengen. Hetzelfde geldt binnen de Belastingdienst. Een bedrijf moet bijvoorbeeld loonbelasting en invoerrechten en accijnzen en BTW (omzetbelasting) en vennootschapsbelasting betalen. Zowel voor het bedrijf als voor de fiscus is het nuttig als de informatie over al die belastingsoorten niet gescheiden, in silo's, wordt behandeld, maar op een intelligente manier bij elkaar wordt gebracht.

In de financiële wereld is hiervoor de term *integraal klantbeeld* bedacht. In het strafrecht is dit vertaald naar het *integraal strafrechtelijk persoonsbeeld*. In de vreemdelingenketen spreekt men van het *vreemdelingenbeeld*. Simpel gezegd: wat weten we al van hem?

Aan de vraag 'wat weten we al van hem (de verdachte)' gaat een andere vooraf: 'wie is het?' Is hij wel degene die hij beweert te zijn? Voor de banken en verzekeraars is dat al een punt van zorg. Maar nog veel meer in de strafrechtspleging, want als de gegevens aan de verkeerde persoon gekoppeld worden, kan dat leiden tot fouten. En die kunnen ernstige gevolgen hebben. Bijvoorbeeld doordat een schuldige vrijuit gaat of een onschuldige als verdachte wordt aangemerkt, of doordat een strafvonnis op naam van de verkeerde persoon komt te staan. En anders dan cliënten bij banken of patiënten in ziekenhuizen heeft de verdachte in een strafzaak er in beginsel weinig belang bij om zijn ware identiteit bekend te maken. In ieder geval mag hij daarover zwijgen. Zorgvuldige identiteitsvaststelling is dus van groot belang. In het strafrecht duiden we dit aan als het *integer strafrechtelijk persoonsbeeld*. Dat is niet een doel op zich, maar een middel om de juiste beslissingen te kunnen nemen. Het integraal persoonsbeeld gaat over de juiste sanctie tegen de persoon, het integer persoonsbeeld over de sanctie tegen de juiste persoon. Alles hangt af van de juiste informatie op het juiste moment.

3.6 Wie is het?

Identiteitsvaststelling is altijd een middel, nooit een doel op zich. Binnen de strafrechtspleging is het een middel om te zorgen dat niet alleen de juiste sanctie wordt toegepast, maar dat die sanctie ook de juiste persoon treft. Daarnaast is het een middel om te zorgen dat de informatie-uitwisseling over verdachten en veroordeelden trefzeker de persoon betreft over wie het moet gaan. En ten slotte strekt een deugdelijke identiteitsvaststelling ook tot bescherming van potentiële slachtoffers van identiteitsfraude (ID-fraude). Dat zijn wij in beginsel allemaal.

> Fouten in identificerende gegevens kunnen ontstaan door fraude, maar ook door administratieve vergissingen. Stel: er zijn 1000 mensen bezig met het invoeren en registreren van identiteiten. Allemaal zijn ze steengoed en maken ze maar één foutje per dag. Dat zijn 1000 fouten per dag. Ga eens na wat dat kost aan herstelwerk (áls de fout al aan het licht komt); allemaal verborgen kosten.

Identiteitsvaststelling heeft twee vormen: identificatie en verificatie. *Identificatie* geeft een antwoord op de vraag: wie is dit? Een identiteit (NAW-gegevens, foto, vingerafdruk) wordt vergeleken met alle reeds geregistreerde identiteiten in een bestand (1:n vergelijking). Blijkt de persoon nog niet bekend te zijn, dan wordt in het systeem een nieuwe entiteit aangemaakt. *Verificatie* geeft een antwoord op de vraag: is de persoon degene die hij beweert te zijn? Het systeem zoekt alleen of de aangeboden identiteit al bekend is, liefst met gebruikmaking van een unieke en eenduidige sleutel, bijvoorbeeld een nummer (1:1 vergelijking). Het antwoord is in principe 'ja' of 'nee': een groen vinkje of een rood kruisje. Bij 'ja' kan het systeem de reeds bekende gegevens tonen. *Identificatie* gebeurt aan het begin van een traject, als we nog niet weten met wie we precies van doen hebben. Bij alle latere contactmomenten is sprake van *verificatie*. Dan is al bekend wie er dan en daar moet verschijnen, bijvoorbeeld op een zitting, of voor het uitvoeren van een taakstraf, of in een penitentiaire inrichting (in geval van een zelfmelder). Zijn strafrechtsketennummer (SKN) en zijn overige

identificerende gegevens zijn al bekend. Aan de hand daarvan kan via bijvoorbeeld de scan van een of twee vingers worden vastgesteld of de juiste persoon is verschenen.

De *identificatie* van een verdachte gebeurt aan het begin van een traject (voor het onderscheid tussen keten en traject zie par. 1.3) door de opsporingsambtenaren en werkt door in heel de keten voor de *verificatie* van de identiteit van betrokkene. Politie, marechaussee, bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren werken dus voor de keten als geheel als zij een verdachte identificeren. Verificaties later in het traject berusten op het werk dat de opsporingsambtenaren aan het begin hebben gedaan. Het resultaat van dat werk, de vastgestelde identiteit van de verdachte, wordt opgehangen aan het SKN. Dat nummer is een soort satéprikker door heel de keten heen:

Het SKN reist heel de keten door *downstream* met de verdachte mee. Inclusief, helaas, de eventuele fouten in die gegevens, want '*problems and errors have a tendency to travel downstream*'. Daarom is afgesproken dat organisaties aan de beheerder van de SKDB melden[3] wanneer zij menen dat de gegevens in de SKDB niet juist of niet volledig zijn en dat die beheerder dat ook weer meldt aan andere belanghebbenden in de keten. Het beeld maakt tegelijk duidelijk dat het corrigeren van fouten in identiteitsgegevens een *upstream* proces is, het is werken tegen de stroom in. Dat maakt het extra lastig (zie par. 3.8).

Identificatie betekent dat een setje identificerende persoonsgegevens wordt verzameld. Voor de lichtere strafzaken is dat – afgezien van de gegevens die de verdachte opgeeft tijdens het verhoor – alleen de kopie van het ID-bewijs. Voor de zwaardere zaken komen daar een gelaatsfoto en tien vingerafdrukken bij (art. 55c Sv). Dat geheel van gegevens wordt gehangen aan een uniek identificerend nummer, het strafrechtsketennummer (SKN). De wet schrijft voor dat alle functionarissen in de strafrechtsketen bij het onderling uitwisselen van gegevens over de verdachte of veroordeelde, dat SKN gebruiken (art. 27b Sv).

Met deze systematiek is het *integer* persoonsbeeld, dat wil zeggen de uniciteit van de informatie over een verdachte of veroordeelde door heel de keten heen, optimaal geborgd. Dit integer persoonsbeeld – opgehangen aan een uniek ketennummer – heeft binnen de keten te gelden als de *single truth*. Niet omdat het de absolute waarheid is, maar omdat zonder dit stelsel de keten geen keten is, maar los zand.

Intussen was de centrale vraag nog steeds: hoe komt de functionaris vervolgens aan alle relevante informatie over die verdachte of veroordeelde (het *integraal* persoonsbeeld)? Daarover in de volgende paragraaf.

3.7 Wat weten we al van hem?

'Ik hoef niet van iedereen alles te weten, maar voor criminelen maak ik graag een uitzondering', aldus Dato Steenhuis in enkele interviews rond zijn afscheid als procureur-generaal.[4] Alles – dat is heel veel. Om dat te vatten, hebben we wat ordening nodig.

Voor de operationele strafrechtstoepassing zijn twee soorten informatie nodig: over het incident en over het individu (vgl. par. 3.1). De eerste soort is de zaaks-, feit- of incidentgebonden informatie, de tweede is de persoonsgebonden informatie.

Veel van de *persoonsgebonden* informatie is al ergens aanwezig binnen de keten of binnen de overheid. Bijvoorbeeld de identificerende persoonsgegevens: naam, adres, woonplaats, geslacht, geboortedatum en -plaats, enzovoort. Informatie die er al is, móet zo veel mogelijk

worden hergebruikt. Dat geldt speciaal voor gegevens in de basisregistraties, zoals de BRP (Basisregistratie Personen; de opvolger van de Gemeentelijke basisadministratie, GBA). De *incidentgebonden* informatie zal vaak nog niet aanwezig zijn binnen de overheid en moet dus worden verzameld. Daarover gaat het Wetboek van Strafvordering.

De *incidentgebonden* informatie ziet altijd op een gebeurtenis die zich in het verleden heeft afgespeeld. Die informatie is dus in beginsel onveranderlijk. Het vergaren daarvan gebeurt grotendeels in één schakel van de keten: de opsporing. Is dat eenmaal 'rond', dan verandert er (alweer: in beginsel) niets meer aan. En na de fase van de berechting speelt de informatie over het incident geen rol meer, behalve bij de rapportages van de psychiater en de reclassering.

Persoonsgebonden informatie daarentegen is door heel de keten heen telkens opnieuw van belang, bij elke te nemen beslissing, en is vaak ook aan verandering onderhevig: een persoon kan verhuizen, er kunnen nieuwe zaken, antecedenten of rapporten toegevoegd worden aan zijn documentatie, enzovoort.

Het integraal persoonsbeeld gaat over de persoonsgebonden informatie die al in de keten of elders binnen de overheid aanwezig is. Welke gegevens een functionaris nodig heeft voor zijn taakuitoefening, wordt bepaald door de beslissing die hij moet nemen of de handeling die hij moet verrichten; zie de voorbeelden in paragraaf 3.5. Hieruit volgt dat vorm en inhoud van het *integraal (strafrechtelijk) persoonsbeeld* moeten worden bepaald per beslismoment of contactmoment in de keten. Het is dus niet een vooraf gedefinieerd pakketje gegevens dat ergens op een plank ligt en uit voorraad leverbaar is. Het integraal persoonsbeeld wordt naar behoefte geassembleerd vanuit de beschikbare bronnen. Dat is waar de digitalisering van de strafrechtsketen grotendeels over gaat.[5]

Het *integraal* persoonsbeeld is als concept eenvoudig. Die eenvoud moet ons geen zand in de ogen strooien. Informatie is macht, alleen vaak niet direct als zodanig waarneembaar.[6] Het *integer* persoonsbeeld confronteert ons op een veel zichtbaardere manier met het gewelds-

monopolie van de overheid. Identiteitsvaststelling is uiteindelijk een dwangmiddel. Over het integraal persoonsbeeld is in de wet vrijwel niets te vinden (ik laat in het midden of dit terecht is). De identiteitsvaststelling daarentegen is uitvoerig in de wet geregeld.

3.8 De achterkant van overheidsdigitalisering

> Mw. A wil als zijinstromer in het onderwijs gaan werken. Zij volgt de PABO, behaalt haar diploma en solliciteert hoopvol. Hoewel het basisonderwijs schreeuwt om personeel, wordt zij afgewezen. De reden? Er staan delicten op haar strafblad die het onwenselijk maken dat zij in het basisonderwijs gaat werken. Hoogst verbaasd wendt zij zich tot de Justitiële Informatiedienst (Justid), die de justitiële documentatie beheert. Volgens haar zeggen heeft zij helemaal geen strafblad. De Afdeling Matching van Justid verdiept zich in de zaak en stelt na anderhalf jaar vast – mede op basis van biometrie (vingerafdrukken) – dat de strafbare feiten op naam van mw. A in werkelijkheid door haar zus zijn begaan in Frankrijk.

Volgens alle wetten over gegevensverwerking en gegevensbescherming hebben verwerkingsverantwoordelijken een inspanningsverplichting om alleen juiste en actuele gegevens te verwerken en hebben de geregistreerden het recht fouten te laten corrigeren of foutieve gegevens te laten verwijderen. Die regels zijn goed en terecht, maar de praktijk is weerbarstig. In zijn rapport *iOverheid* (2011) wees de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) er al op dat bestanden (gegevensverzamelingen) tegenwoordig zozeer verbonden zijn in ketens en netwerken, dat wij nauwelijks meer weten welke informatie over welke personen in welke bestanden zit. Voor elke koppeling die wordt gelegd tussen twee bestanden is altijd wel een goede reden (een *business case*). Maar de verknoping van systemen leidt ertoe dat fouten in het ene bestand of systeem (zie par. 1.1 voor het onderscheid tussen gegevensverzameling en informatiesysteem) gemakkelijk worden verspreid naar andere, daarmee gekoppelde systemen. In ketens geldt nu eenmaal de ketenwet: *problems and errors have a tendency to travel*

downstream.[7] De ervaring leert vervolgens dat met correcties of het verwijderen van gegevens niet automatisch hetzelfde gebeurt als met de onjuiste gegevens zelf: dat een onjuist gegeven in het ene systeem wordt gecorrigeerd of eruit wordt verwijderd, leidt er niet automatisch toe dat het ook in de gekoppelde systemen wordt gecorrigeerd of eruit wordt verwijderd.

Op een of andere manier zit er in veel systemen een bepaalde resistentie tegen correctie ingebakken. Ook daar kunnen goede redenen voor zijn: het moet immers niet té gemakkelijk zijn voor mensen om gegevens uit een bestand te wissen of te wijzigen, dat zou de deur openzetten voor allerlei misbruik en oneigenlijk gebruik. Bovendien: zeker in ketens is het van groot belang dat over zoiets fundamenteels als de identiteit van de cliënt geen verschil van mening bestaat; zie de paragrafen 2.3 en 3.6 over het principe van *single truth | single source*. Alleen: het risico daarvan is dat er ook een *single point of failure* ontstaat. Resistentie zit trouwens niet alleen in systemen, maar ook in mensen. Hirsch Ballin waarschuwde al in 1986 voor '*het risico dat de door een computer verschafte informatie, meer dan de langs andere weg verkregen inlichtingen, de reputatie van exactheid en objectiviteit verwerft*'.[8] Wat de computer zegt, wordt gemakkelijk voor waar aangenomen. En een laatste reden waarom het lastig is onjuiste gegevens te corrigeren, is, zoals Jan Grijpink, de goeroe van keteninformatisering, ons steeds heeft voorgehouden: de sporen wijzen altijd in de richting van het slachtoffer van de identiteitsfouten of -fraude: hij of zij moet aannemelijk maken dat de gegevens onjuist zijn, dus dat hij het misdrijf níet heeft gepleegd, de koop níet heeft gesloten, de bestelling níet heeft geplaatst, enzovoort.[9] Maar bewijzen dat iets *niet* is gebeurd of dat je iets *niet* hebt gedaan, is altijd lastig. Kortom, digitalisering en bureaucratie hebben ons veel goeds gebracht, maar als het fout gaat, gaat het ook goed fout. De Kafkabrigade wordt niet moe ons daarop te wijzen.

In zijn jaarverslag over 2008, getiteld 'De burger in de ketens', heeft de Nationale Ombudsman al de problemen geschetst die de burger kan ondervinden als het in ketens fout gaat. In een *Ongevraagd advies over*

de effecten van de digitalisering voor de rechtsstatelijke verhoudingen van 31 augustus 2018 heeft ook de Raad van State nog eens met klem aandacht gevraagd voor deze achterkant van de digitalisering. Want de aantallen slachtoffers van identiteitsfouten en -fraude mogen misschien niet heel groot zijn, de gevolgen voor die slachtoffers zijn vaak wel heel ernstig. Wat valt eraan te doen? Preventief zou er veel meer aandacht voor fouten en fraude moeten komen in de fase van het ontwerpen en ontwikkelen van systemen. Gangbaar is dat die worden ontwikkeld vanuit de *happy flow*: zo lang het goed gaat, gaat het goed. Gegevensbeschermingstests (*data protection impact assessments*, zie par. 2.5), gebruikerstests en veiligheidstests zijn tegenwoordig gangbaar. Daar zou een fraudetest aan moeten worden toegevoegd: hoe kan het systeem worden omzeild, misleid, misbruikt. Jan Grijpink heeft er steeds op gewezen dat daarbij moet worden gedacht vanuit de crimineel, degene die het systeem wil oplichten. Ook moet er in de ontwerpfase meer aandacht komen voor *bypasses*, noodzakelijke nooduitgangen – die overigens ook weer niet té gemakkelijk te openen moeten zijn. Aan de curatieve kant moeten de organisaties die worden geconfronteerd met een geval van beweerde persoonsverwisseling in goede harmonie het slachtoffer tegemoet treden en niet naar elkaar verwijzen. In zijn rapport 2017/114 van 11 oktober 2017, getiteld *Verdwaald in een digitaal doolhof*, heeft de Nationale ombudsman daar heldere aanwijzingen voor gegeven. Een van de aangesproken organisaties moet de regie nemen, dat wil zeggen: aanspreekpunt zijn voor de klager en ervoor instaan dat de klacht wordt afgehandeld. Ik zie niet in waarom die aanwijzingen niet ook in de strafrechtsketen van toepassing zouden (moeten) zijn. En ten slotte moet het herstellen van fouten door alle publieke organisaties worden erkend als te behoren tot hun kerntaken. Het is moeizaam werk, arbeidsintensief en in die zin bedrijfsmatig inefficiënt. En natuurlijk kun je erop wachten dat iemand een keer ten onrechte komt claimen slachtoffer te zijn van een persoonsverwisseling (identiteitsfouten of -fraude). Maar de publieke sector is het aan zichzelf verplicht om zich op dit punt maximaal in te zetten, in het belang van de slachtoffers en van de rechtsstaat Nederland.[10]

Noten

1 Ik spreek consequent over 'verdachten', 'daders' en/of 'veroordeelden' en tracht collega's te bewegen datzelfde te doen. Het is de enigszins onderkoelde juridische terminologie waaraan ik hecht. Woorden als 'criminelen' of 'boeven' horen daarin niet thuis.
2 In *Jegens en Wegens* heb ik de term *supply chain* – bij nader inzien – ten onrechte gekoppeld aan de logistieke keten (*Jegens en Wegens*, 2010, p. 121).
3 Deze afspraak is vastgelegd in het Protocol identiteitsvaststelling strafrechtsketen (te vinden op de site van de Justitiële Informatiedienst).
4 Onder meer in *De Gelderlander*, 27 mei 2006.
5 Uitvoeriger hierover: *Jegens en Wegens*, hoofdstukken 5 en 7. Zie ook het visiedocument *Naar een digitale strafrechtspleging* (bijlage bij brief van de minister van VenJ van 17 februari 2016, Kamerstukken II, 2016/16, 29279, nr. 298).
6 Wie wil weten hoe informatie leidt tot macht, leze het fascinerende boek van Alvin Toffler, *De nieuwe machtselite*, Amsterdam: Uitgeverij Atlas (Olympus) 1990. Het is vijfhonderd pagina's dik, zonder dat er een woord te veel in staat.
7 Zie par. 3.2.3, 7.3, 7.4.2, 7.7.2 van *Jegens en Wegens* (met verwijzingen).
8 E.M.H. Hirsch Ballin, De legitimiteit van de selectie van informatie, *Ars Aequi* 35 (1986) 11, p. 729.
9 Van de vele publicaties van Jan Grijpink noem ik hier slechts zijn boek *Informatiestrategie voor ketensamenwerking. Keteninformatisering als visie, resultaat en methode. Speciaal thema: Persoonsherkenning en identiteitscontrole*, Den Haag: Sdu Uitgevers 2002.
10 Uitvoeriger hierover mijn artikel Karl Marx en de slachtoffers van identiteitsfouten en -fraude in *Delikt en Delinkwent* 2018/43, p. 572-584 (september 2018).

HOOFDSTUK 4

IV EN STRAFRECHTSPLEGING: WERELDEN IN BOTSING

4.1 Strafrechtstoepassing is informatieverwerking

De strafrechtspleging is, net als de hele overheid, een informatieverwerkend bedrijf.

Ga maar na.

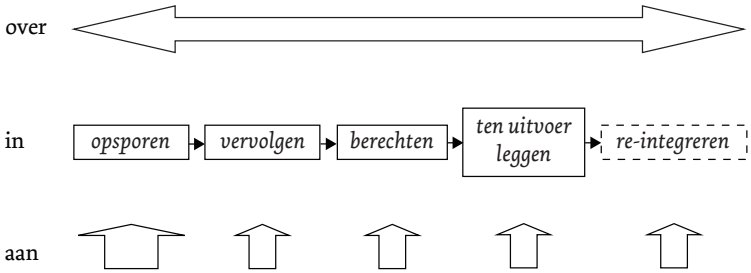
- Opsporing houdt in het verhoren van getuigen en verdachten, sporenonderzoek, inbeslagneming van voorwerpen, doorzoeking, afluisteren van telecommunicatie, enzovoort. Dit is informatievergaring en -veredeling.
- De meeste dwangmiddelen dienen voor het vergaren van informatie. Bijvoorbeeld inbeslagneming, doorzoeking, afluisteren van telecommunicatie, openen van brieven.
- De opsporingsambtenaar legt zijn bevindingen (= de informatie over het incident en de verdachte) vast in een proces-verbaal. Dat stuurt hij naar het CJIB of de OvJ.
- De OvJ besluit op basis van het proces-verbaal de zaak zelf af te doen of legt haar voor aan de rechter ter zitting. Dit laatste is weer informatieoverdracht: er gaat een dossier naar de rechter en een dagvaarding naar de verdachte. In geval van een OM-afdoening geeft het OM opdracht aan het CJIB tot tenuitvoerlegging (incasso); ook dit is overdracht van informatie.
- Reclassering, kinderbescherming, psychiaters, het Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP) en vele anderen schrijven rapporten voor de OvJ of de rechter.

- Het onderzoek op de terechtzitting bestaat uit het vergaren en toetsen van informatie.
- De rechter schrijft zijn vonnis op basis van het hem voorgelegde dossier en de behandeling ter terechtzitting.
- Het OM ontvangt het vonnis (= informatieoverdracht) en levert dat aan bij het AICE voor de tenuitvoerlegging.
- Het AICE geeft namens de minister opdrachten tot tenuitvoerlegging van het vonnis.
- De vele tientallen, om niet te zeggen honderden instanties die betrokken (kunnen) zijn bij de tenuitvoerlegging, moeten rapporteren over het verloop en de afloop van de tenuitvoerlegging.

Dit is allemaal informatieoverdracht. Pas bij de tenuitvoerlegging gaat het niet, althans niet hoofdzakelijk, meer om informatieverwerking: geld moet worden geïnd, een persoon moet een taakstraf uitvoeren of moet worden gedetineerd of behandeld.

Behalve informatie *in* en *over* de keten (par. 1.1) is er in het strafrecht nog een derde categorie: hoe komt de keten *aan* haar informatie. Denk aan het horen van verdachten en getuigen, in beslag nemen van stukken, doorzoekingen, telefoontaps, deskundigenrapporten, observaties, het zoeken in computerbestanden, het uitvoeren van bestandsvergelijkingen. Dit is waar het Wetboek van Strafvordering over gaat.

In en *aan* hebben betrekking op het microniveau: de individuele zaak en persoon. *Over* heeft betrekking op het mesoniveau: werkplanning, work-flowmanagement, procesbeheersing, sturen op zaken, en het macroniveau: beleid, begroting, financiering, politieke en maatschappelijke verantwoording.



Opsporing is over het algemeen de fase waarin de meeste informatie wordt verzameld; daarom teken ik de blokpijl op de onderste rij bij deze fase het breedst. Preventie gaat aan strafrechtstoepassing vooraf en valt dus buiten het concept van de strafrechtsketen. Re-integratie is het open einde van de strafrechtsketen: het loopt als het ware het strafrecht uit; daarom teken ik dat vakje met een stippellijn.

Strafrechtstoepassing is dus informatieverwerking. En de digitalisering rukt onstuitbaar op, ook in de strafrechtsketen. Maar dat betekent nog niet dat er geen spanningen bestaan tussen beide disciplines. Gaat de strafrechtsketen dat overleven?

Een relatief simpele kwestie om mee te beginnen. Het Wetboek van Strafvordering legt taken en bevoegdheden meestal bij functionarissen, niet bij organisaties. De rechter, de OvJ, de opsporingsambtenaar, de medewerker van de reclassering of de kinderbescherming, de directeur van de penitentiaire inrichting, zij ontlenen hun bevoegdheden niet aan de minister (mandaat), maar aan de wet (attributie). De functionaris is daarom het ijkpunt van de informatievoorziening *in* de keten. In de ICT daarentegen wordt juist vaak vanuit organisaties gedacht. Dat verschil heeft consequenties voor bijvoorbeeld de vraag hoe autorisaties (toegang tot gegevens) moeten worden geregeld. Dat is onder meer van belang vanwege de wettelijke verplichtingen om naar de geregistreerde toe te kunnen verantwoorden aan wie welke gegevens zijn verstrekt. In het domein van het strafrecht kun je autorisaties niet toekennen aan organisaties, alleen aan functionarissen. Maar hoe ga je dat praktisch beheersen in een keten waarin meer dan 100.000 mensen werkzaam zijn? Daarvoor is in de strafrechtsketen in

de afgelopen jaren het idee van de federatieve authenticatie ontwikkeld. Wissel de gegevens uit op het niveau van de organisaties en leg de verantwoordelijkheid voor de verwerking van de gegevens bij de ontvangende partij: die moet haar eigen mensen autoriseren, loggen wat zij doen en toezien op hoe zij de gegevens gebruiken. Conceptueel niet zo ingewikkeld, maar praktisch heeft het heel wat voeten in de aarde. Zo zijn er nog een paar spanningsvelden; daarover gaat de rest van dit hoofdstuk.

4.2 Het begrip 'zaak': onmisbare stoorzender in de keten

ICT heeft behoefte aan eenduidig te definiëren begrippen. Het strafrecht heeft daar moeite mee. Veel begrippen zijn niet zo eenduidig gedefinieerd, of je struikelt over de uitzonderingen. Denk bijvoorbeeld aan een begrip als 'de tenlastelegging'. Wij kennen enkelvoudige en samengestelde tenlasteleggingen. De samengestelde zijn onder te verdelen in primair/subsidiaire, cumulatieve en alternatieve. Die onderscheidingen kunnen samengaan in één tenlastelegging. En dan ook nog eens impliciet, dus zonder dat het als zodanig is aangegeven en herkenbaar is in het document. In de loop der jaren heb ik een paar keer geprobeerd dit uit te leggen aan informatiearchitecten; zij werden er wanhopig van.

Een beruchte complicatie waar de IV van de strafrechtsketen mee heeft te kampen, betreft de zogeheten breukvlakken.

- In de fase van de opsporing gaat het om het feit, de gebeurtenis, het *incident*. Dat is ook wat er wordt geregistreerd.
- Het ingezonden proces-verbaal wordt bij het openbaar ministerie ingeschreven (geregistreerd) als een *zaak*.
- Sancties (vrijheidsstraffen, geldboetes, werkstraffen) worden ten uitvoer gelegd ten aanzien van *personen* en geregistreerd (geteld) in aantallen celdagen, detentiejaren, taakstraffen, euro's, enzovoort.

Door deze breukvlakken kun je niet goed volgen wat er van begin tot eind van het ketenproces met een incident gebeurt. Een zaak is daardoor lastig door de keten heen te sturen. Bovendien kun je incidenten, zaken en personen niet over en weer optellen. Dat geeft problemen voor de statistiek, de beleidsinformatie en de sturingsinformatie. Valt dit op te lossen?

In paragraaf 3.1 heb ik betoogd dat incident (gebeurtenis), individu (persoon, dader) en interventie (sanctie) de basisingrediënten zijn van de strafrechtspleging. Zaak daarentegen is niet meer dan een administratieve hulpconstructie. Die dient om de verbinding tussen delict en sanctie tot stand te brengen. Het begrip zaak heeft verschillende betekenissen. Bij de politie betekent het: een gebeurtenis (delict) waarnaar onderzoek wordt gedaan en waarbij één of meer verdachten betrokken kunnen zijn. Bij het openbaar ministerie en de Rechtspraak betekent het: een specifieke feit-dadercombinatie zoals die door het OM wordt geconstrueerd door het toekennen van een parketnummer. Dit lijkt ook de betekenis die het begrip zaak heeft in het Wetboek van Strafvordering.

Eén zaak (parketnummer) heeft in de Nederlandse praktijk altijd betrekking op één verdachte (individu), maar kan meer dan één feit (incident) betreffen. Omgekeerd kan één feit (incident, gedraging, gebeurtenis) leiden tot meer dan één zaak, met name als er meer verdachten bij betrokken zijn. Eén persoon kan meer feiten gepleegd hebben en er kunnen meer zaken tegelijk tegen hem lopen. De sanctie wordt altijd opgelegd in één zaak tegen één dader (veroordeelde), ter zake van één of meer feiten. Omgekeerd kan één dader (veroordeelde) ter zake van één of meer feiten (delicten) meer sancties tegelijk opgelegd krijgen (cumulatie van straffen). In informatiekundige termen ritselt het hier van de 1:n- en n:m-relaties.[1] De zaak is dus op administratief niveau een voertuig om van A naar B te komen, maar tegelijk op conceptueel niveau een stoorzender. En een fragmentatiebom in de IV.

Om de genoemde problemen op te lossen, zouden we het begrip zaak moeten elimineren. We moeten dus een manier verzinnen om vanuit

het allereerste begin van een strafrechtelijk traject te identificeren om welk feitelijk substraat (welk incident) het gaat, op zo'n manier dat we dat tot en met het einde van het traject, de afdoening (de interventie), kunnen volgen. Dat is nog een mooie uitdaging voor de digitalisering van de strafrechtsketen.

4.3 Document en dossier als digisaurussen

Wie het Wetboek van Strafvordering doorleest, struikelt over de papierstapels.

> Rechters moeten hun beslissingen op schrift stellen. Officieren van justitie geven schriftelijke bevelen aan opsporingsambtenaren en dienen schriftelijk hun vorderingen in bij de rechter. De verdachte kan allerlei verzoeken indienen en moet dat vaak schriftelijk doen. Opsporingsambtenaren moeten proces-verbaal opmaken. Hoger beroep of cassatie wordt ingesteld door het opmaken van een akte. Een gerechtelijk schrijven, bijvoorbeeld een dagvaarding, wordt betekend door middel van uitreiking, waarvan een akte wordt opgemaakt: de akte van uitreiking (binnenkort opent de wet de mogelijkheid om dat digitaal te doen). Deskundigen brengen schriftelijk verslag uit aan de OvJ of aan de rechter (alleen op de terechtzitting kunnen zij een mondelinge verklaring afleggen). De documenten die worden opgemaakt in de zaak worden door de OvJ als processtukken in het dossier gevoegd. De verdachte en diens raadsman hebben recht op kennisneming (inzage) en/of afschrift van de processtukken.

Strafvordering draait om *documenten*. In de wereld van ICT daarentegen draait alles, zwart-wit gesteld, om gegevens (*data*). In die wereld wordt een document beschouwd als een verzameling gegevens. Zo'n atomistische zienswijze is in de context van ICT misschien begrijpelijk, maar overgezet naar de wereld van het strafrecht schiet zij tekort. Een document is méér dan een verzameling gegevens, zoals een boek of een gedicht meer is dan een verzameling woorden en een

muziekstuk meer dan een verzameling noten. Een document is zelfs meer dan een aantal zinnen en een muziekstuk meer dan een reeks akkoorden. Het is een compositie, waarbij de betekenis en klank van de afzonderlijke noten en akkoorden mede bepaald wordt door de context, ofwel door de overige inhoud van het stuk. Het geheel is meer dan de som der delen. De elementen in een document, de woorden en de zinnen, zijn samengevoegd in een specifieke vorm en deze vorm (ordening, structuur, samenhang) bepaalt mede de betekenis van de afzonderlijke elementen. Als in een document, bijvoorbeeld een onderzoeksrapport of een beleidsnota, die structuur en samenhang ontbreken, wordt het lastig de betekenis ervan te bepalen. Wij zeggen dan dat het los zand is. Het geheel gaat dus in zekere zin zelfs aan de samenstellende delen vooraf. Nauwkeuriger gezegd: het geheel kan slechts worden verstaan via een begrip van de delen en omgekeerd.

> In de filosofie staat dit bekend als 'de hermeneutische cirkel'. De eenvoudigste omschrijving daarvan die ik ken, is dat men eerst het geheel moet begrijpen voor men de delen kan begrijpen, maar eerst weer de delen moet kennen voor men het geheel kan begrijpen.[2] Kijk maar eens hoe dat werkt als iemand een tekst vanuit een vreemde taal wil vertalen. Als hij een bepaald woord in een zin niet snapt, ontspoort vaak de vertaling van de hele zin. Maar juist omdat hij het geheel van de zin niet snapt, kan hij dat ene woord niet goed vertalen!

Bovendien bestaat de inhoud van strafrechtelijke documenten voor pakweg 80% uit beweringen van mensen (getuigen, verdachten, verbalisanten, enz.), waarvan de inhoud niet zonder meer als vaststaande feiten kan worden beschouwd. Zelfs het schijnbaar vaststaande feit dat een bepaalde verklaring op een bepaald moment door een bepaalde persoon is afgelegd, is nader beschouwd niet meer dan een bewering van die persoon zelf of van een ander, bijvoorbeeld de opsporingsambtenaar die in zijn proces-verbaal de inhoud van een voor hem afgelegde getuigenverklaring heeft opgenomen.

'Het koffiekopje waaruit u 's ochtends drinkt is een houder van vocht. Het kopje is ook een cilindrische vorm, aan één kant dicht. Het is een industrieel ontwerp uit, zeg, het eind van de twintigste eeuw. Het is úw kopje. Het is het cadeau van tante Esther voor uw verjaardag van afgelopen jaar.
Hier kun je oneindig mee doorgaan. Het zijn allemaal werkelijkheden die tegelijk bestaan en die in principe waar zijn. Ze ontmoeten elkaar weliswaar in het kopje, maar in principe raken die werkelijkheden elkaar nauwelijks. Wat voor tante Esther haar cadeau is, is voor een wiskundige een cilindrische vorm, aan één kant gesloten. Dat uw kopje in een boekwerk over industrieel ontwerpen staat, zegt u, als u 's ochtends met een slaperig hoofd nog eens bijschenkt, niets. Als het de koffie maar warm en bij elkaar houdt.
De wereld bestaat uit oneindig veel werkelijkheden, die allemaal vrolijk – en soms helaas wat minder vrolijk – naast elkaar bestaan. En aangezien wij de hele dag vrijwel niets anders doen dan met andere mensen samenwerken en communiceren, kan dit verschijnsel nogal wat misverstanden opleveren.'[3]

Je kunt een document dus niet uiteenrafelen in losse elementen (gegevens) die min of meer naar believen beschikbaar zijn voor hergebruik. Een document is een selectieve en gestructureerde verzameling van gegevens op een bepaald moment voor een bepaald doel. Elke bewering is onderdeel van een verhaal.

'Een verhaal is meer dan een reeks woorden achter elkaar; in een verhaal krijgen woorden via zinnen ritme en betekenis. In een verhaal worden woorden (letterlijk en figuurlijk) van con-tekst voorzien en in een bepaald tijdsverloop geplaatst, onderling verbonden door een thema. Een verhaal beschrijft een ontwikkeling in de tijd. (...) Soms loopt een verhaal via het midden, van het einde naar het begin. Het verhaal krijgt op die manier een tijdsverloop dat logischerwijs niet voorspeld had kunnen worden. Dit maakt duidelijk dat een verhaal, net als overigens een model of theorie, de (tijd in de) wereld niet beschrijft, maar herschrijft.'[4]

De verhouding tussen data en document is één verdieping hoger terug te vinden in de verhouding tussen document en dossier. Een dossier is niet maar een willekeurige stapel documenten. Het is een geordende eenheid; geordend op een bepaald moment door en/of voor een bepaalde beslisser met het oog op een bepaalde beslissing. Een processtuk dat in het dossier in zaak A zit, mag daarom nog niet zonder meer worden gebruikt in zaak B. De begrippen dossier en zaak zijn nauw met elkaar verweven. Het dossier is vaak de papieren belichaming van de zaak. Informatiekundig bezien is het dossier een elastiekje (van rubber of digitaal) om een stapel informatieproducten.

> Van 1986 tot 1989 werkte ik bij de Hoge Raad op het Wetenschappelijk Bureau. Alles draaide daar om het elastiekje. Dát definieerde de eenheid van het dossier en daarmee van de zaak. En de stukken in het dossier waren strikt chronologisch geordend: het oudste onderop, het recentste bovenop. Het ergste wat je kon doen, was die volgorde schenden. Zo orden ik dertig jaar later nog steeds al mijn dossiers, op het werk of thuis, ongeacht waar het over gaat. En wee degene die dat overhoop haalt …

De grenzen tussen data, document en dossier vervagen in een digitale omgeving. Uit documenten en dossiers kun je data halen en die hergebruiken. Bijvoorbeeld: persoon (identiteit), object, plaats (locatie), vervoermiddel, incident, strafbaar feit, gedraging. Je kunt die elementen bijvoorbeeld checken (verifiëren) op andere databases, bijvoorbeeld de basisregistraties, of op andere documenten. Je kunt ze ook gebruiken in het kader van big data-onderzoek. Allemaal onder omstandigheden erg nuttig en nodig. Als je maar voor ogen houdt dat het geen abstracte, absolute waarheden zijn, maar beweringen met een principieel beperkte waarheidsaanspraak. De wettelijke eis dat de getuige 'de gehele waarheid en niets dan de waarheid' moet vertellen, is uit moreel oogpunt terecht, maar kennistheoretisch onhoudbaar. En hier geldt ook de waarschuwing van de WRR over het decontextualiseren en hercontextualiseren van gegevens (par. 1.5). Iemand staande houden als verdachte heeft een andere lading dan iemand staande

houden als getuige. En in het strafrecht betekent staande houden iets anders dan in het vreemdelingentoezicht. De woonplaats zoals die door de verdachte is opgegeven bij het verhoor is iets anders dan de woonplaats in de zin van de Basisregistratie Personen. Zulke verschillen kun je niet met ICT oplossen.

4.4 Authenticiteit en integriteit: digitale anachronismen?

ICT eist nogal vanzelfsprekend dat alle informatie (data, documenten, dossiers) authentiek en integer moet zijn. *Authentiek* wil zeggen dat kan worden vastgesteld wie de informatie oorspronkelijk heeft gecreeerd en/of vastgelegd. *Integer* wil zeggen dat (kan worden vastgesteld dat) de informatie naderhand nog steeds compleet en vanaf het moment van vaststelling of ondertekening niet gewijzigd is.[5]

Strafrechtelijk ligt dit wat genuanceerder. In ketenperspectief moeten we onderscheid maken tussen informatie die ín de keten wordt geproduceerd, zoals processen-verbaal of rapporten van deskundigen, en informatie die van buitenaf naar binnen wordt gehaald als bewijsmiddel, bijvoorbeeld een vervalste boekhouding. Voor de informatie die ín de keten wordt geproduceerd, is de dubbele eis van authenticiteit en integriteit inderdaad vanzelfsprekend. Voor de informatie die van buiten naar binnen wordt gehaald, is dat minder vanzelfsprekend. Ieder vodje of krabbeltje, hoe vunzig of obscuur ook, kan potentieel als bewijsmiddel gelden. Ik licht dat toe.

Voor bewijs gelden drie vereisten:
1. Wat is toelaatbaar als bewijsmiddel in een strafzaak?
2. Is het bewijsmiddel betrouwbaar?
3. Is het bewijsmiddel bruikbaar?

Deze vereisten corresponderen in feite met verschillende stadia in het ketenproces. Wat *toelaatbaar* is, is in de wet gedefinieerd (art. 340-344a Sv). Het betreft de resultaten van het werk in de opsporingsfase. Opsporingsambtenaren moeten zorgen dat die producten, bijvoorbeeld hun processen-verbaal, daaraan voldoen, anders zijn ze waardeloos.

Het oordeel over de *betrouwbaarheid* en *bruikbaarheid* is aan de rechter (of aan de OvJ als het niet tot een zitting komt, maar bijvoorbeeld tot een strafbeschikking). Hiermee zitten we dus in de fase van de oordeelsvorming (de *context of discovery*). Alleen wat de rechter voldoende betrouwbaar acht, kan en mag hij gebruiken voor zijn beslissing. Een verklaring van een getuige kan vervolgens als zodanig wel betrouwbaar zijn, maar gezien haar inhoud toch van geen nut (niet redengevend) voor een bewezenverklaring; dan is die verklaring toch niet bruikbaar.

In de beslissing ten slotte promoveert de beslisser (rechter of OvJ) het bruikbare bewijsmiddel tot *gebruikt* (in het juristenjargon: gebezigd) bewijsmiddel. Dan gaan we via het vonnis en de redengeving daarvan (de *context of justification*) al over naar de volgende fase in het ketenproces: de uitspraak (vonnis, strafbeschikking) ligt er, nu moet hij ten uitvoer gelegd worden.

In de praktijk wordt nogal eens gesproken over de bewijskracht van een informatieproduct. Die term is niet erg handig zolang de spreker niet specificeert welk aspect hij bedoelt: de toelaatbaarheid, de betrouwbaarheid, de bruikbaarheid of het feitelijke gebruik van een bewijsmiddel.

Voor zover de wet geen eisen stelt aan de toelaatbaarheid, de betrouwbaarheid of de bruikbaarheid van een bewijsmiddel, moet de ICT dat ook niet willen doen. Dat geldt niet alleen voor de in het vonnis *gebezigde* (gebruikte) bewijsmiddelen, maar ook voor de in het dossier aanwezige *beschikbare* bewijsmiddelen. De eisen die ICT stelt (c.q. ICT'ers stellen) aan informatieproducten betreffen de integriteit en de authenticiteit van die producten. De *integriteit* van informatieproducten (documenten, data, tekst, beeld, geluid of wat dan ook) betreft de eis dat er niets meer aan veranderd mag worden als ze eenmaal als beschikbaar bewijsmateriaal aan het dossier zijn toegevoegd. Dat kan iets zijn dat in beslag is genomen of iets dat een functionaris zelf heeft vervaardigd. Die eis is zo vanzelfsprekend dat de wet daar tot dusver niets over zei. Althans, niet in positieve zin: wat er moet of hoe het moet. Wel in negatieve zin: vervalsen is strafbaar (art. 225 e.v. Wetboek van Strafrecht). De bepalingen in het Wetboek van Strafrecht moet je in spiegelbeeld lezen om erachter te komen wat er wél moet

of mag. Het enige positieve voorschrift tot dusver is te vinden in de Wet digitale processtukken strafvordering, die sinds 1 december 2016 voorschrijft dat 'van een processtuk in elektronische vorm de integriteit (kan) worden nagegaan doordat iedere wijziging daarvan kan worden vastgesteld' (art. 149a, derde lid, Sv). Dat is heel nieuw.[6]

Voor het waarborgen van de *authenticiteit* van een informatieproduct wordt in de papieren omgeving vaak de handtekening gebruikt. In de strafrechtspleging is die handtekening de grondslag van het vertrouwen van de verdachte en van de samenleving in de waarde en de betrouwbaarheid van het informatieproduct (zie par. 3.4). Er zijn in een digitale omgeving verschillende mogelijkheden om dat vertrouwen te borgen. En een digitale handtekening kan zelfs meer dan een papieren (zgn. natte) handtekening: zij kan ook de *integriteit* waarborgen, dus dat het informatieproduct niet na de ondertekening is gewijzigd. Hier kan ICT dus helpen de rechtsstatelijke kwaliteit van het werk in de strafrechtsketen te verhogen.

Af en toe beluister je het idee dat we misschien strengere eisen moeten stellen aan stukken (en/of aan de handtekening daarop) die naar de rechter gaan dan aan stukken die de rechter niet bereiken. Dat idee is in ketenperspectief onjuist. Want in dat perspectief is de functie van het stuk dezelfde, ongeacht of de zaak bij de rechter komt of niet, namelijk: dienen als grondslag voor een strafrechtelijke interventie. Dáárom stelt de wet (en stellen rechters) eisen aan stukken. En bovendien: er zijn wel veel strafzaken die de rechter niet bereiken, maar er zijn geen strafzaken die de rechter niet kúnnen bereiken. Of een zaak uiteindelijk bij de rechter komt, weet je meestal niet van tevoren.

Het ketenperspectief staat er ook aan in de weg dat de rechter naar believen informatie van internet haalt en die als feit van algemene bekendheid (art. 339, tweede lid, Sv) in zijn vonnis ten bezware van de verdachte gebruikt.[7] Feiten van algemene bekendheid zijn in de regel gegevens die geen specialistische kennis veronderstellen en waarvan de juistheid redelijkerwijs niet voor betwisting vatbaar is. Dat geldt niet per se voor alles wat op internet staat. En dan moet het op de zitting, dus vóórdat de rechter vonnis wijst aan de orde gesteld worden, zodat partijen (verdachte, OvJ) zich erover kunnen uitlaten (art. 301,

vierde lid, Sv). Dat is een noodzakelijke – maar niet per se ook voldoende – voorwaarde om het als bewijsmiddel te mogen gebruiken, dus om de sprong te maken van de *context of discovery* naar de *context of justification*.

4.5 'De' zaak bestaat niet (in ketenperspectief), 'het' dossier evenmin

In paragraaf 4.2 voerde ik 'de zaak' al op als onmisbare stoorzender in de keten c.q. de keten-IV. Wat is dat eigenlijk: een zaak? De dikke Van Dale geeft veertien betekenissen. Die helpen ons niet verder. De ArchiefWiki wél (een beetje). Daar lezen we: 'Een zaak wordt meestal gedefinieerd als een in de tijd begrensd complex handelingen betreffende een bepaald geval' (https://archiefwiki.org/wiki/Zaak, geraadpleegd 30 november 2017). Het is dus een bepaalde combinatie van één of meer *handelingen* en een *geval*. Ik heb de keten gedefinieerd als een reeks van handelingen naar aanleiding van een incident (c.q. geval) met als doel het realiseren van een gemeenschappelijk resultaat. Daarmee is het begrip *zaak* dus het belangrijkste wat de partijen in de keten verbindt. (Waar ketens elkaar kruisen, is de *persoon* veel meer het verbindende element, zie par. 5.3.) *Handelingen* verwijzen naar actoren en hun bevoegdheden, *geval* naar het object van hun bemoeienis. In hoofdstuk 3 heb ik dat strafrechtelijk ingevuld.

Nog een stapje verder komen we als we er informatiekundig naar kijken. Een 'zaak' is informatiekundig bezien een hoeveelheid informatie die moet dienen als grondslag voor een te nemen beslissing. Als er bijvoorbeeld te weinig gegevens zijn voor een redelijke verdenking, zeggen we dat we 'geen zaak hebben' tegen deze persoon. Voor elke beslissing heeft het zaaksbegrip dus een andere inhoud. Het is verschillend voor de politie, voor de OvJ, voor de rechter, voor de kinderbescherming, voor de reclassering. 'De' zaak bestaat niet in ketenperspectief. In de papieren wereld is die hoeveelheid informatie belichaamd in een stapeltje stukken. Vandaar dat de zaak vaak wordt geïdentificeerd met het dossier. Een dossier is, zo bezien, een elastiekje om een stapel informatieproducten (par. 4.3). Dat elastiekje kan, net als documenten, fysiek of virtueel (digitaal) zijn. En zoals 'de' zaak niet bestaat, zo bestaat evenmin 'het' dossier (in

ketenperspectief). Juristen worden in hun studie geprogrammeerd om te denken vanuit het perspectief van de rechter, niet vanuit de keten. Als ze het hebben over het dossier, bedoelen ze daarmee dan ook meestal het dossier dat aan de rechter wordt voorgelegd – en denken dat dát 'het' dossier is. Niet, dus.

In de papieren wereld bleef de schade van de spraakverwarring nog tamelijk beperkt. Er werd (en wordt nog steeds) veel papier in de keten heen en weer geschoven en doorgegeven en dat was (c.q. is) dan *het* dossier. In de digitale wereld daarentegen kunnen allerlei mensen overal vandaan toegang krijgen tot informatie (data, documenten, dossiers), ongeacht waar die informatie zich fysiek bevindt. Van papier doorgeven gaan we naar informatie delen. Zo krijgt het begrip dossier een heel nieuwe betekenis. Het is een hoeveelheid informatie die op een bepaald moment ten behoeve van een bepaalde beslissing of handeling door een bepaalde functionaris tot een geheel wordt geassembleerd en vervolgens ook als zodanig vastgelegd ten behoeve van de interne openbaarheid (d.w.z.: naar de partijen toe) en de verantwoording. In de wereld van ICT wordt in dit verband vaak gesproken van een bevroren informatieproduct. Daarmee wordt bedoeld dat er aan die data, documenten of dossiers, niets meer mag worden veranderd. Voor een latere beslissing in dezelfde zaak kan andere, al dan niet nieuwere informatie nodig zijn, waarvoor dan weer hetzelfde geldt. *De* zaak bestond al nooit vanuit het perspectief van de keten, *het* dossier verdampt (in de digitale wereld) terwijl je ernaar kijkt.

Informatici hebben het ook vaak over kunnen tijdreizen door een ketendossier. Achteraf moet kunnen worden vastgesteld welke informatie beschikbaar was voor (en op het moment van) een beslissing en hoe die informatie is gebruikt en gewaardeerd door de beslisser. De beslissing moet kunnen worden gereconstrueerd. Het recht was hier de ICT al lang vóór. Van oudsher eist de wet dat rechterlijke beslissingen de gronden moeten bevatten waarop zij rusten. Die regel is tegenwoordig onder meer te vinden in artikel 121 Grondwet en artikel 359 Sv. De rechter bepaalt zelf welke informatie hij relevant acht en bruikbaar voor zijn beslissing (vgl. par. 4.4 over beschikbaar en gebruikt bewijsmiddel). In de bewoordingen van de Hoge Raad:

de rechter is vrij in de selectie en waardering van de bewijsmiddelen en die beslissing hoeft niet te worden gemotiveerd. (De uitzonderingen op deze regel laat ik hier voor wat ze zijn.) Dankzij moderne ICT krijgen beslissers tegenwoordig steeds vaker voor de voeten geworpen dat ze dit of dat hadden kunnen weten op het moment dat zij hun (achteraf bezien foute of ongelukkige) beslissing namen. De spannende – en voor mij nog open – vraag is of dit ook gaat doordringen in de strafrechtspleging en met name of dit gevolgen gaat hebben voor de toetsing van rechterlijke beslissingen. Gaan we rechters achteraf confronteren met bewijsmateriaal dat er al was en dat de rechter bewust of onbewust terzijde heeft gelaten? Komt de tot dusver onwrikbare jurisprudentie van de Hoge Raad over de vrijheid van de rechter onder druk te staan? Gaan er dingen veranderen in het stelsel van rechtsmiddelen en met name op het punt van de herziening? Of maken we misschien nu het begin van deze kentering al mee? Over tien jaar kan ik u het antwoord op deze vragen geven …

4.6 Feiten of fouten

Strafrechtstoepassing is gegevensverwerking. Maar wat ís dat: een *gegeven*? De wet geeft – zoals gezegd (par. 2.1) – op die vraag geen antwoord. In de ICT worden gegevens vaak gedefinieerd als een symbolische weergave van de werkelijkheid. En daarmee gemakkelijk gelijkgesteld aan feiten. Informatie ontstaat in die visie wanneer een persoon betekenis toekent aan de gegevens. Maar zo'n weergave van een stukje werkelijkheid is niets anders dan wat de menselijke waarneming of een door mensen gemaakte en ingestelde sensor daarover aangeeft. Daar zit dus al betekenisgeving in. Gegevens zijn als zodanig niet betekenisloos. *There are no pure facts* (Popper). Daarom gaat de huidige wetgeving niet meer over *registers*, zoals de voormalige Wet persoonsregistraties, Wet politieregisters, Wet justitiële documentatie, maar over *gegevens*: Wet bescherming persoonsgegevens, Wet politiegegevens, Wet justitiële en strafvorderlijke gegevens.

Gemakkelijk wordt echter een model als de werkelijkheid beschouwd en de relatie met de realiteit uit het oog verloren: het systeem gaat de werkelijkheid over-rulen. Dat laatste doet zich bijvoorbeeld voor als een verdachte verklaart dat hij in 1980 in Kazachstan is geboren en het

systeem dat corrigeert, want Kazachstan bestond in 1980 nog niet als zelfstandige staat, het was toen onderdeel van de Sovjet-Unie, dus dat past niet in de tabellen waarmee de automatisering werkt. Zó moet het dus niet.

Ander voorbeeld: de regelgeving over de identiteitsvaststelling van verdachten en veroordeelden. Volgens de wet kunnen voor de identiteitsvaststelling verschillende middelen worden ingezet, variërend van onofficiële documenten en verklaringen via officiële documenten tot foto's en vingerafdrukken. Een eenmaal vastgestelde identiteit geldt voor heel de keten. Het is duidelijk dat het voor de hardheid van de identiteitsvaststelling nogal verschil maakt waarop deze vaststelling is gebaseerd. Dat moet daarom worden vastgelegd in het proces-verbaal van de opsporingsambtenaar. Het dient ook te worden vastgelegd in de strafrechtsketendatabank (SKDB). Want als de context van de identiteitsvaststelling uit het oog wordt verloren, kunnen de eenmaal in het systeem vastgelegde identiteitsgegevens een eigen leven gaan leiden. *Single truth* c.q. *single source* is een belangrijk principe in ketenperspectief. Heel de keten moet dan óók kunnen zien wat de waarde van die *truth* is en eventueel correcties daarop kunnen aandragen.

De keerzijde hiervan is dat ook onware (of onwaar lijkende) verklaringen van verdachten of getuigen geregistreerd moeten worden. Die onware verklaring is als zodanig een historisch – en te registreren – feit. Bovendien kan zij van groot belang zijn in bijvoorbeeld een opsporingsonderzoek. Computers hebben de neiging fout (b)lijkende gegevens te (willen) overschrijven door de correct geachte gegevens; zo zijn ze geprogrammeerd. Bovendien schrijft het stelsel van authentieke basisregistraties dat op het eerste gezicht ook voor. Alle overheidsinstanties moeten bijvoorbeeld de gegevens uit de Basisregistratie personen (BRP) gebruiken. In de strafrechtsketen kan het consequent volgen van dat principe rampzalige effecten hebben. Foutieve adres- of naamgegevens kunnen de keten op het verkeerde spoor zetten, maar kunnen soms ook juist belangrijke sleutels zijn tot opheldering van een misdrijf.

Er kan dan ook geen sprake van zijn dat verdachten of veroordeelden een beroep kunnen doen op hun recht op correctie van onjuiste gegevens om naderhand hun 'onware' verklaringen te laten corrigeren. Anders zouden wij de leugen belonen en de geschiedenis vervalsen – en de keten van belangrijke informatie beroven. De Rgbs (Richtlijn 2016/680 van de EU over gegevensbescherming bij de opsporing, vervolging en berechting van strafbare feiten en de tenuitvoerlegging van straffen) geeft dit in overweging nr. 30 helder weer: 'Het beginsel van juistheid van gegevens moet worden toegepast met inachtneming van de aard en het doel van de verwerking in kwestie. In het bijzonder bij gerechtelijke procedures zijn verklaringen die persoonsgegevens bevatten, gebaseerd op de subjectieve perceptie van natuurlijke personen en niet altijd te controleren. Het vereiste van juistheid dient derhalve geen betrekking te hebben op de juistheid van een verklaring, maar alleen op het feit dat een specifieke verklaring is afgelegd.' En zo mogelijk nog puntiger in overweging nr. 47: 'Een natuurlijke persoon dient het recht te hebben onjuiste hem betreffende persoonsgegevens te laten rectificeren, vooral wanneer het gaat om feiten, en deze te laten wissen indien de verwerking van die gegevens inbreuk maakt op deze richtlijn. Het recht op rectificatie mag echter geen invloed hebben op, bijvoorbeeld, de inhoud van een getuigenverklaring.' Hier stelt de eigen aard van de keten dus specifieke eisen aan de informatieverwerking.

Dat de aard van de keten ook consequenties moet hebben voor het corrigeren van fouten in identiteits- (en eventueel ook andere) gegevens betoogde ik al in par. 3.8 (over 'de achterkant van digitalisering').

Noten

1 In par. 2.4 van *Jegens en Wegens* heb ik deze informatierelaties uitvoerig geanalyseerd.
2 Ik vond deze omschrijving bij H. van den Brink, *Bijbels recht. Oefeningen in exegese*, Kampen: Uitgeverij Kok 1995, p. 19.
3 Vrijwel deze hele passage is een citaat uit het boekje van Jeroen Busscher, *Pimp je afdeling! Voor wie meer uit zijn afdeling wil halen*, Den Haag: Academic Service 2007, p. 7. Uitvoeriger hierover: *Jegens en Wegens*, par. 2.2.3 ('There are no pure data'). Het 'subjectief en intersubjectief karakter van waar-

nemingsuitspraken' is mij als eerstejaars rechtenstudent in Rotterdam (1971-1972) al met de paplepel ingegoten via het verplichte vak wetenschapsleer en het daarbij behorende boekje van de docent, J.P.M. Geurts, *Feit en theorie*, Assen: Koninklijke Van Gorcum 1978.

4 Ook dit mooie citaat komt uit een boekje over veranderkunde, in dit geval het boekje van Peter Terlouw en Mark van Twist, *Hoe ruikt verandering? Het verstaan van veranderaars*. Den Haag: Boom Lemma uitgevers 2014, p. 74. Over beide onderwerpen (uit deze en de vorige noot) zijn natuurlijk bibliotheken vol geschreven aan wetenschappelijke werken.

5 Ik gebruik de termen *authentiek* en *integer* (met betrekking tot informatie) overeenkomstig de brief van de staatssecretaris van Onderwijs, Cultuur en Wetenschap en de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties van 29 juni 2006, Kamerstukken II, 2005/06, 29362 nr. 101 (*Kabinetsvisie informatie op orde*), p. 2.

6 Graag verwijs ik hier naar het artikel van Martijn van Wees, raadsheer in het Hof Arnhem-Leeuwarden en lid van Rechtspraak-projectteams digitalisering, Modernisering en digitalisering van het strafproces, *Delikt en Delinkwent* 2015/72, p. 801-812 en de discussie daarover met Jos van Wetten, *Delikt en Delinkwent* 2016/27 en 28, p. 318-323.

7 Zie HR 29 maart 2016, *NJ* 2016, 249; HR 5 juli 2016, *NJ* 2016, 333. Zie ook: L. Stevens, Het onderbouwen van een veroordeling met behulp van internet, *Ars Aequi* 2016, p. 753-757 (commentaar op het arrest van 29 maart 2016); en Carla Klaassen, De rechter gaat digitaal… nou en?, *Ars Aequi* 2015, p. 448-452.

HOOFDSTUK 5

INFORMATIE DELEN IN EN MET DE STRAFRECHTSKETEN

5.1 In de doolhof van Wjsg en Wpg – en er ook weer uit

De justitiële ketens worden van A tot Z beheerst door regelgeving, stelde ik in paragraaf 1.5. Dat geldt ook voor de informatieverwerking in die ketens – en helemaal in de strafrechtsketen. De wetten die daarover gaan, zijn in het voorgaande al een paar keer genoemd. Het zijn de Avg, de Rgbs, de Wjsg en ten dele ook de Wpg. (De politietaak is breder dan alleen opsporing; dus gaat de Wpg over meer dan alleen strafrechtstoepassing.) Over die regelgeving – zo kort mogelijk – het volgende.

De Avg en de Rgbs sluiten elkaar uit (zie par. 2.2). Voor zover de verordening spreekt over verwerken van strafrechtelijke persoonsgegevens, gaat het dus over verwerkingen die buiten het toepassingsbereik van de richtlijn vallen, oftewel, als we het even plat slaan: buiten de strafrechtstoepassing.

Op nationaal niveau hebben we te maken met de Wjsg en de Wpg. Dan gaat het in de eerste plaats om het delen van informatie tussen *tweeden*. Daarmee bedoel ik instanties die zijn belast met de toepassing van het strafrecht. Die instanties móeten wel samenwerken en informatie uitwisselen om het ketenresultaat te bereiken. Tussen hen mogen strafrechtelijke persoonsgegevens in ruime mate worden uitgewisseld. De Wjsg bevatte al twee categorieën van gegevens, de justitiële en de strafvorderlijke, maar is bij gelegenheid van de implementatie van de richtlijn uitgebreid met nog eens twee categorieën: de gerechtelijke gegevens en de tenuitvoerleggingsgegevens. Of daarmee inderdaad het hele terrein van de strafrechtstoepassing is gedekt

(zoals de wetgever beoogde), is voor mij nog twijfelachtig. De wet is er in elk geval nóg ingewikkelder op geworden dan ze al was.

De Wpg en de Wjsg regelen onder andere onderwerpen als de bewaartermijnen en het verstrekkingenregime. Bovendien vestigt de Wjsg een aantal specifieke verplichtingen tot het verstrekken van gegevens; dat doen de Avg en de Rgbs in beginsel niet.

Daarnaast bevatten beide wetten regels over de uitwisseling met *derden*, dat wil zeggen: partijen buiten de strafrechtsketen.

Gegevensbescherming is in de grond van de zaak niet zo moeilijk, zei ik in paragraaf 2.1. De Wpg en de Wjsg zijn niettemin ingewikkelde wetten, vooral in hun onderlinge verhouding. De toepasselijkheid van die wetten wordt (mede) bepaald door de plaats waar de gegevens zich bevinden.

Voor de politiegegevens is dat – onder de huidige regelgeving – het *domein*, dat wil zeggen: de politie plus enkele belendende percelen, want bijvoorbeeld de Koninklijke Marechaussee voert ook een aantal politietaken uit. Het begrip politiegegeven is gekoppeld aan de uitvoering van de politietaak.

Voor de strafvorderlijke en de gerechtelijke gegevens is die plaats de *organisatie*. Strafvorderlijke gegevens zijn de data en dossiers bij het openbaar ministerie, gerechtelijke gegevens en de data en dossiers bij de gerechten.

Voor de justitiële gegevens is die plaats de *gegevensverzameling*. Het begrip justitiële gegevens is in de wet gekoppeld aan het begrip 'justitiële documentatie' (de JD). Dat was tot halverwege de jaren negentig een papieren kaartenbak, tegenwoordig een geautomatiseerd systeem, het Justitieel Documentatiesysteem (JDS; zie par. 5.3).

Alleen de tenuitvoerleggingsgegevens zijn niet gedefinieerd naar de plaats waar ze zich bevinden, maar naar het *object* van de gegevens: de tenuitvoerlegging van strafrechtelijke beslissingen.

Maar in het digitale tijdperk zijn gegevens niet meer aan een fysieke plaats gebonden. De verschillende wettelijke regelingen kunnen dus tegelijkertijd op eenzelfde gegeven van toepassing zijn. En gegevens kunnen om zo te zeggen van kleur verschieten als ze van het ene domein (organisatie, systeem) in het andere komen. Overigens gold dat in het papieren tijdperk tot op zekere hoogte ook al.

Dit geeft vooral problemen bij de bewaartermijnen. Die moeten over systemen heen worden bewaakt. Maar zo zijn de systemen niet gebouwd. Documenten en vooral zaken kunnen niet, of in elk geval niet gemakkelijk, over systemen heen worden gekoppeld. Dus als bijvoorbeeld de politie te horen krijgt dat een bepaalde zaak heeft geleid tot een vrijspraak, weet zij daarmee nog niet welke informatieproducten (data, documenten) nu precies moeten worden vernietigd. Daar komt bij dat de politie ook lang niet altijd weet in welke van de vele honderden systemen in haar domein zich gegevens of documenten in relatie tot een bepaalde zaak bevinden. Dat zou in het digitale tijdperk beter moeten.

Verder sporen de Wpg en de Wjsg al helemaal moeizaam met de algemene beginselen van gegevensbescherming en met het Wetboek van Strafvordering. Privacybescherming bestond nog niet toen het Wetboek van Strafvordering werd ontworpen. Het eerste complete ontwerp voor dat wetboek dateert van 1913 (het ontwerp van de commissie-Ort), de eerste ideeën over privacy ontstonden in ons land in de jaren zeventig van de vorige eeuw. Beide takken van sport zijn in hoge mate onafhankelijk van elkaar ontwikkeld, het gedachtegoed van de privacywetgeving begint nog maar net in strafvorderingsland door te dringen. Dat leidt tot een erfenis (*legacy*) waarmee moeizaam valt te werken. Een complicatie is bovendien dat de Wet politiegegevens, zoals gezegd, niet alleen gaat over strafrechtelijke persoonsgegevens. Zij omvat de hele politietaak en dat is veel breder dan alleen opsporing en strafrechtelijke handhaving (vgl. par. 1.4).

Tot aan de implementatie van de Rgbs gold de Wjsg wel voor het openbaar ministerie, maar niet voor de Rechtspraak. Dit leidde tot het wonderlijke verschil dat als een zaak door de officier van justitie

was afgedaan, de termijnen van de Wjsg golden, die konden oplopen tot tachtig jaar. Werd een zaak daarentegen door de rechter afgedaan, dan gold voor de bewaartermijn alleen de algemene regel dat gegevens niet langer mogen worden bewaard dan nodig is voor het doel van de verwerking (en voorts de Archiefwet 1995). Dat verschil was niet te rechtvaardigen. Bij de implementatie van de Rgbs zijn de gerechtelijke gegevens wel als nieuwe categorie ingevoegd in de Wjsg, maar de bewaartermijnen zijn niet gelijk getrokken. Dat zal in een volgende wetgevingsoperatie alsnog moeten gebeuren.[1]

Justitiële en strafvorderlijke gegevens mógen niet alleen, maar móeten ook worden bewaard zo lang als de Wjsg voorschrijft. De regels van de Wpg en de Wjsg zien op het operationele gebruik van de gegevens, dat wil zeggen het gebruik voor het doel waarvoor zij zijn verzameld. Zijn de termijnen van die wetten verstreken, dan komt eventueel overbrenging naar een archiefbewaarplaats volgens de Archiefwet 1995 in beeld. Zo'n 10 tot 15% van wat de overheid aan informatie produceert, belandt uiteindelijk bij een openbare archiefinstelling.[2] Of dat percentage ook geldt voor de strafrechtelijke informatie weet ik niet, maar in elk geval kan de Archiefwet de bewaartermijnen zoals die gelden volgens de Wbp, de Wjsg en/of de Wpg wel verlengen, maar niet verkorten. Alleen mag die langer bewaarde informatie dan dus niet meer voor operationele doelen worden gebruikt. (Vgl. art. 17, derde lid, Avg.)

Of de Wjsg inmiddels de hele verwerking van strafrechtelijke persoonsgegevens dekt, is voor mij, zoals gezegd, twijfelachtig. Zo staat er bijvoorbeeld volgens mij nog steeds nergens in de wet – noch in de Wjsg noch in het Wetboek van Strafvordering – dat de officier van justitie voor de zitting een dossier naar de rechtbank moet sturen…[3] De Wjsg bouwt voort op de Wet justitiële documentatie en de verklaringen omtrent het gedrag (Wet JD) van 1955. Die regelde precies wat de titel aangaf, niet meer en niet minder. In de loop der jaren is er van alles aangebouwd aan de Wjsg. Met als jongste loot aan de stam de gerechtelijke en de tenuitvoerleggingsgegevens. De Wjsg is daardoor in haar huidige vorm te groot voor servet en te klein voor tafellaken. Dat leidt tot veel onduidelijkheid. De minister van Veiligheid en

Justitie heeft in 2014 aangekondigd dat de Wpg en de Wjsg in onderlinge samenhang grondig zullen worden herzien.[4] Maar eerst moet – aldus de minister – de modernisering van het Wetboek van Strafvordering worden afgemaakt. Dat kan dus nog even gaan duren.

5.2 Informatie delen tussen handhavingsstelsels

De strafrechtsketen staat centraal in dit boekje, maar die staat natuurlijk niet op zichzelf. Rechtshandhaving kent tegenwoordig vele smaken (zie par. 3.2). Het gaat hier niet, zoals in paragraaf 2.4, om kruisende ketens, domeinen van verschillende aard, maar om concentrische cirkels, verwante domeinen. *High Impact Crimes*, ondermijning, veelvoorkomende criminaliteit (VVC) en ordeningsstrafrecht behoren tot het domein van het strafrecht. De overige, te weten 'Mulder', het bestuurlijke sanctierecht en bestuurlijke handhaving en toezicht, zijn wel handhaving, maar geen strafrecht. Buiten het domein van handhaving is er ten slotte nog het reguliere bestuur, bijvoorbeeld de vergunningverlening. Zij liggen als het ware als schillen om een kern heen.

In al deze schillen van de handhaving kan het intussen wel gaan over dezelfde subjecten (natuurlijke personen, rechtspersonen) of fenomenen. Sterker nog: via handhaving van (zogenoemde) kleine normen, worden soms 'grote vissen' gevangen. Waar nodig zal daarom informatie over die subjecten moeten kunnen worden uitgewisseld tussen instanties in de diverse schillen. Dat kan – alweer – alleen als die informatie is geordend naar de subjecten waarop zij betrekking heeft. Waar bínnen een keten vooral de zaak het verbindende element is (vgl. par. 4.5), is dat over ketens heen vooral de persoon (cliënt).

De juistheid van de informatie behoeft dan wel extra aandacht. Immers, hoe meer schillen er worden gekoppeld, des te langer wordt de keten. En des te groter de gevolgen als er ergens aan het begin fouten insluipen (*problems and errors have a tendency to travel downstream*). Dus fouten die al in de fase van de vergunningverlening in bijvoorbeeld de identificerende persoonsgegevens zijn geslopen, worden ongemerkt doorgegeven aan de strafrechtsketen. (In gedigitaliseerde netwerken kunnen fouten overigens ook met de snelheid van het licht worden verspreid.) Daarnaast moeten er nogal eens de nodige

juridische horden worden genomen om informatie vanuit een schil te kunnen delen met actoren in een andere schil.

Voor de Verklaring omtrent het gedrag (VOG) bijvoorbeeld, inmiddels uitgegroeid tot een waterhoofd van de Wjsg, zijn de schotten tussen de domeinen steeds moeilijker te handhaven.[5] Steeds vaker wordt sollicitanten om een VOG gevraagd. De beslissing over de VOG leunt sterk op de JD – en daarmee op strafrechtelijk gelabelde gedragingen (daarnaast kan de minister ook kijken naar politiegegevens). Maar waarom zou niet de aard van het gedrag, maar het juridische etiket dat erop wordt geplakt, namelijk strafrecht dan wel bestuursrecht, beslissend moeten zijn voor het kunnen krijgen van een VOG? Het politiek correcte antwoord op de opgeworpen vraag is dat de keuze voor het ene of het andere sanctiestelsel mede bepaald wordt door de aard en ernst van de gedraging. Maar de diversiteit leidt in de praktijk wel eens tot verrassingen. Er vindt bovendien geregeld grensverkeer plaats tussen het ene en het andere domein. Een feit kan zomaar van het eigenlijke strafrecht worden weggedefinieerd naar het bestuursrecht (worden 'vermulderd' in het beleidsjargon). Daarmee eindigt van de ene op de andere dag de opneming van die feiten in de JD. Het omgekeerde kan ook. En als klap op de vuurpijl: sommige feiten kunnen zowel langs strafrechtelijke als langs bestuursrechtelijke weg worden gesanctioneerd. Dat laatste komt vaak voor in het ordeningsrecht. Er moet op het casusniveau wel een keuze worden gemaakt. Beleidsregels bepalen of een feit strafrechtelijk of bestuursrechtelijk wordt 'afgedaan'. Van de keuze uit die twee smaken hangt het af of het feit in de JD komt of niet. Hoe logisch is dat? Voor Bibob (de Wet bevordering integriteitsbeoordelingen openbaar bestuur) is de reikwijdte al ruimer: onder strafbaar feit wordt mede verstaan een overtreding waarvoor een bestuurlijke boete kan worden opgelegd (art. 3, achtste lid, Wet Bibob).

Omgekeerd is er een steeds sterkere neiging om de documentatie uit te willen breiden naar feiten die niet strafrechtelijk maar tuchtrechtelijk worden afgedaan. Díe afdoeningen kunnen, in tegenstelling tot strafrechtelijke en bestuursrechtelijke sanctionering, overigens wél samenlopen: een en hetzelfde feit kan zonder bezwaar zowel tuchtrechtelijk

als strafrechtelijk worden gesanctioneerd. Maar ook hier zal de keuze voor de ene of de andere route doorgaans niet worden bepaald door de vraag of de afdoening wel of niet in de documentatie belandt.

Hoe dan ook, het lijkt mij archaïsch en niet meer te verdedigen dat de bestaande schotten tussen de verschillende handhavingsketens zich automatisch vertalen naar schotten tussen de informatiedomeinen. Van oudsher kennen wij in het strafrecht het leerstuk van de sfeerovergang. Dat betrof de overgang van de toezichts- naar de opsporingsfase. Opsporing is strafrecht, toezicht niet. De kernvraag was altijd in hoeverre dwangmiddelen uit de beide sferen kunnen samengaan. De Straatsburgse jurisprudentie die is begonnen met het Saunders-arrest (EHRM 17 december 1996, *NJ* 1997, 699), heeft daar de dimensie aan toegevoegd van het gebruik van informatie uit de ene sfeer (toezicht) in de andere (opsporing). Deze jurisprudentie biedt, onder de vlag van de clausule 'noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt' (vgl. art. 6, eerste lid, onder c en e, Avg; art. 8 en 9 Rgbs), voldoende grondslag voor de uitwisseling van de nodige informatie tussen beide sferen.

5.3 Informatie delen tussen ketens

In paragraaf 2.4 introduceerde ik het concept van kruisende ketens. Dan gaat het over strafrechtsketen en bijvoorbeeld zorg, welzijn, werk & inkomen, scholing, huisvesting. Deze en/of andere takken van sport komen bijvoorbeeld in een Veiligheidshuis bij elkaar. In de genoemde paragraaf schetste ik een soort van architectuur voor informatie delen tussen ketens vanuit het perspectief van gegevensbescherming. Daaraan valt vanuit het perspectief van het delen van strafrechtelijke persoonsinformatie nog het volgende toe te voegen (zonder te veel in details te treden).

Ik noemde in paragraaf 2.4 al de uitzonderingsgrond van artikel art. 33, eerste lid, onder b, Uitvoeringswet Avg, die ziet op publiekrechtelijke samenwerkingsverbanden. Deze uitzondering is opmerkelijk open geformuleerd. Er worden maar twee eisen gesteld: de

verwerking moet noodzakelijk zijn voor de uitvoering van de taak van de deelnemende partijen en bij de uitvoering is voorzien in waarborgen voor de persoonlijke levenssfeer van de betrokkene (= de geregistreerde). De eerste voorwaarde voegt niets toe aan de algemene eisen van *need to know* en *need to share*. En de tweede is ook nogal vanzelfsprekend (en van elastiek). De wet zegt niets over hoe dit artikel zich verhoudt tot allerlei geheimhoudingsverplichtingen die professionals doorgaans hebben. Dáár begint meestal de hoofdpijn als het gaat om gegevensuitwisseling in samenwerkingsverbanden.

Meer en meer wordt dat ondervangen in allerlei bijzondere wetten. Ik doel op een aantal wetten buiten de Wpg en de Wjsg, die regels bevatten over de uitwisseling van strafrechtelijke persoonsgegevens met *derden* (partijen buiten de keten, die zich bezighouden met dezelfde justitiabele) voor specifieke situaties of domeinen. Zo bevatten de SUWI-wet, de Participatiewet, de Jeugdwet, de Wajong en de Zorgverzekeringswet verplichtingen tot het verstrekken van gegevens vanuit het justitiële domein aan de uitvoerders van die wetten. DJI moet bijvoorbeeld informatie verstrekken aan het UWV over het feit dat iemand gedetineerd is. Dat gaat dus over strafrechtelijke persoonsgegevens. Ook het wetsvoorstel verplichte geestelijke gezondheidszorg (Wvggz), dat de Wet bijzondere opnemingen in psychiatrische ziekenhuizen (Wet Bopz) moet vervangen, gaat verplichtingen bevatten tot het verstrekken van strafrechtelijke persoonsgegevens aan de commissie die onder meer de rechter moet adviseren over de afgifte van een zorgmachtiging en tevens die machtiging ten uitvoer moet leggen. De algemene eisen van proportionaliteit, subsidiariteit, dataminimalisatie, beveiliging en dergelijke blijven gelden.

De zojuist genoemde regels betreffen het verstrekken van strafrechtelijke informatie aan partijen en voor doeleinden buiten de strafrechtsketen. Er is ook een behoefte de andere kant op: strafrechtstoepassing heeft behoefte aan gegevens uit andere domeinen en sectoren. Voor zover het gaat om informatie op incidentele basis is in het Wetboek van Strafvordering het vorderen van gegevens geregeld. Daarnaast bevatten bijzondere wetten soms specifieke regelingen voor het ver-

strekken van informatie aan strafrechtstoepassers. Een voorbeeld is het – in 2009 in het *Staatsblad* gepubliceerde, maar nog altijd niet in werking getreden – artikel 4b van de Paspoortwet, dat voorziet in de verstrekking van gegevens uit de reisdocumentenadministratie met het oog op de opsporing en vervolging van strafbare feiten. Een ander voorbeeld is de Wet basisregistratie personen (Wbrp), die regels bevat over het verstrekken van gegevens uit de Wbrp aan overheidsorganen. Als zulke bijzondere wettelijke regels bestaan, is geen vordering op grond van het Wetboek van Strafvordering nodig.

Ik noemde – tot slot – in paragraaf 2.4 ook al het wetsvoorstel dat regels gaat bevatten voor informatie-uitwisseling in samenwerkingsverbanden met ook niet-publieke partijen.

5.4 Ketenvoorzieningen

Digitalisering brengt kansen en bedreigingen mee. Hoofdstuk 4 stond helemaal in het teken van de spanningen tussen ICT en de *business* van het strafrecht. Dat kun je duiden als bedreigingen. Dat ICT ook kansen meebrengt voor de strafrechtsketen, wordt onder meer zichtbaar in de explosieve toename van het aantal ketenvoorzieningen in de laatste paar jaar.

Onder 'ketenvoorzieningen' versta ik: voorzieningen voor de keten als geheel, die door alle partijen gebruikt (moeten) worden omwille van het goed functioneren van de keten als geheel, dat wil zeggen voor het realiseren van het gezamenlijke resultaat, ongeacht of individuele organisaties er behoefte aan of voordeel van hebben. Zo'n ketenvoorziening kan een gegevensverzameling zijn of een informatiesysteem (vgl. par. 1.1).

Een decennium geleden waren er nog maar twee van zulke voorzieningen: de JD en VIP. Inmiddels zijn er al een stuk of vijftien. Deels zijn dat gegevensverzamelingen waar gebruikers in het primaire proces rechtstreeks uit putten, deels technische hulpmiddelen voor het ontwerp en de realisatie van de keten-IV.

- De JD vindt haar wettelijke grondslag in de Wjsg, speciaal artikel 2, eerste lid: 'Onze Minister verwerkt in de justitiële documentatie justitiële gegevens ten behoeve van een goede strafrechtspleging.' De JD omvat twee gegevensverzamelingen: de justitiële gegevens en de persoonsdossiers.
- VIP staat voor 'Verwijsindex Personen'. Deze ontstond in 1994 als VIPS: Verwijsindex personen strafrecht. Ook dit systeem omvat twee gegevensverzamelingen: personalia en verwijzingen. Aanvankelijk betrof dat alleen OM en DJI. De verwijsindex was een succes. Daarom sloten steeds meer partijen en systemen aan. De S van strafrecht werd in 1999 geschrapt. VIP bevatte gegevens van onder meer verdachten, veroordeelden, gedetineerden (zowel op basis van strafrecht als op basis van vreemdelingenrecht, jeugdbescherming, 'Mulder', civiel recht) en 'Mulder-klanten' in de fase van verhaal en dwang (dus niet alle tien miljoen op jaarbasis). In 2010 werd de categorie strafrechtelijke subjecten (verdachten en veroordeelden) er wettelijk uitgelicht en ondergebracht in de strafrechtsketendatabank (SKDB).
- De SKDB heeft, net als de JD, een expliciete wettelijke grondslag, namelijk artikel 27b, vierde lid, Sv ('Het strafrechtsketennummer en de andere gegevens die noodzakelijk zijn voor de vaststelling van de identiteit van verdachten en veroordeelden en die bij algemene maatregel van bestuur zijn aangewezen, worden in de strafrechtsketendatabank verwerkt. Onze Minister van Veiligheid en Justitie is verantwoordelijke voor deze databank.'). En ook de SKDB omvat twee gegevensverzamelingen: de identificerende persoonsgegevens van verdachten en veroordeelden (administratieve gegevens, kopie ID-bewijs, foto's, vingerafdrukken) en de verwijzingen naar andere systemen in de strafrechtsketen waarin gegevens over de verdachte of veroordeelde zijn verwerkt.
  Centrale gegevensverzamelingen behoeven expliciete rechtvaardiging. Dat is nog iets anders dan een expliciete wettelijke grondslag. Niet elk systeem of elke dataverzameling hoeft met naam en toenaam in de wet te worden genoemd. Het gaat in het gegevensbeschermingsrecht om de *gegevens* en wat je er operationeel mee mag en moet doen, niet om de *systemen* die je daarvoor gebruikt (zie par. 1.1). De wettelijke regeling van de JD en de SKDB is dus

vanuit dat gezichtspunt niet noodzakelijk. Wel kan zij worden opgevat als een vingerwijzing van de wetgever dat de gegevens die in die centrale, wettelijk geregelde verzamelingen worden bewaard, niet ook nog eens op andere plaatsen moeten worden opgeslagen (*single truth, single source*). Dat zou in strijd zijn met de strekking van de wet en afbreuk doen aan het regime dat zorgvuldig rond deze gegevens is opgebouwd. Maar het zou wel handig zijn als de wetgever dat dan ook uitdrukkelijk zou zeggen.
- In verband met de SKDB kan ook het SKN als ketenvoorziening worden aangemerkt. Het is het relatienummer dat geldt voor heel de keten (zie par. 3.6). En in het verlengde daarvan kan de Afdeling Matching van de Justitiële Informatiedienst een ketenvoorziening worden genoemd. Zij is de instantie die de SKDB operationeel beheert en de SKN's toekent.

De overige ketenvoorzieningen zijn vooral technische hulpmiddelen en in elk geval geen gegevensverzamelingen. De gebruiker in het primaire proces komt ze in zijn dagelijks werk niet tegen, ze zitten voor hem 'onder de motorkap'.

- EBV (elektronisch berichtenverkeer) is in 2003 gestart als programma (toen nog geheten EPV: elektronisch proces-verbaal) van een aantal partijen, met name OM en politie. Doel was tot gezamenlijke standaarden en gegevenswoordenboeken voor de strafrechtsketen te komen ten behoeve van de uitwisseling van elektronische berichten. Sinds 2007 is dit structureel ondergebracht bij Justid.
- Het identificeren van een verdachte op een politiebureau gebeurt met de zogenoemde identificatiezuil. Dit is een geïntegreerde opstelling van apparatuur voor het maken van foto's, het nemen van vingerafdrukken en het uitlezen en maken van een digitale kopie van een paspoort of ander identiteitsbewijs. De Basisvoorziening identiteitsvaststelling (BVID) is de software die de verwerking van de verzamelde gegevens voor zowel de strafrechtsketen als de vreemdelingenketen faciliteert. Omdat ID-vaststelling een ketenaangelegenheid is, merk ik de BVID als ketenvoorziening aan.

- De Spelverdeler ontvangt de gegevens die worden verzameld aan de zuilen bij de identificatie van verdachten en vreemdelingen, distribueert die naar de achterliggende systemen, onder andere SKDB, VVI (de vingerafdrukkenverzameling voor de verificatie in de keten), HAVANK (de vingerafdrukkenverzameling van de Nederlandse politie), BVV (de centrale databank van de vreemdelingenketen) en stuurt de antwoordberichten vandaaruit terug naar de zuil.
- De Verificatiemodule (Vmod) is de software waarmee ketenorganisaties de identiteit van een verdachte of veroordeelde verifiëren.
- Het Canoniek datamodel (CDM) beschrijft de belangrijkste gegevenssoorten in de strafrechtsketen en de relaties tussen die gegevenssoorten. Het model dient als uitgangspunt voor het Gegevenswoordenboek voor de strafrechtsketen.
- De Referentie-architectuur en het Bestemmingsplan beschrijven de principes voor de inrichting van de informatievoorziening van de strafrechtsketen.
- De wet en het protocol identiteitsvaststelling geven de regels voor de identificatie van verdachten aan de voorkant van de keten en de verificatie van de identiteit van verdachten en veroordeelden in het vervolg van het strafrechtelijke traject. De identiteitsvaststelling is uitdrukkelijk in de wet geregeld, zie paragraaf 3.6.
- Daarnaast zijn er nog diverse ketenstandaarden, onder meer over de kwaliteit van gegevens, en ketenwerkprocessen, onder meer over de toepassing van de wet en het protocol identiteitsvaststelling.
- In ontwikkeling zijn momenteel (2018) een advocatenportaal en een slachtofferportaal. Dat zijn voorzieningen waar advocaten respectievelijk slachtoffers van delicten informatie over hun zaken kunnen ophalen (downloaden) en in de toekomst ook kunnen inbrengen (uploaden). Als die voorzieningen eenmaal tot volle wasdom zullen zijn gekomen, dat wil zeggen: de hele keten omspannen, kunnen zij ook als ketenvoorzieningen worden aangemerkt.
- Nog ter discussie staat of ook de regeling van de toegang tot gegevens (AAA: authenticatie, autorisatie en accountability; met dit laatste wordt gedoeld op onder meer logging c.q. de *access control*

rules en toezicht) een ketenvoorziening moet zijn of dat je dat aan de individuele ketenorganisaties kunt of moet overlaten. Ik ben vooralsnog geneigd te denken dat ook dit iets is dat wel degelijk de keten als geheel aangaat en dus het belang van de afzonderlijke partijen overstijgt. Daarmee is nog niet gezegd dat je dan ook per se een centrale voorziening moet creëren. Misschien kunnen we volstaan met het formuleren van een aantal functionele eisen waaraan de AAA moet voldoen, ook als de voorzieningen technisch gesproken door de ketenorganisaties zelf zouden worden gerealiseerd en beheerd.

– Iets dergelijks geldt voor het assembleren van het integraal persoonsbeeld. Eist het belang van de keten zoiets als een generieke informatie-assembleur? Functionarissen moeten gemakkelijk en snel, met een *single search*, toegang krijgen tot de voor hen relevante informatie over een verdachte of veroordeelde. Ze zouden zich niet moeten hoeven bekreunen om de vraag of een bepaald gegeven dat ze nodig hebben in systeem A, B of C zit. En het zou al helemaal niet nodig moeten zijn dat ze bij drie of vier verschillende systemen telkens opnieuw moeten inloggen om aan hun informatie te komen. Maar vergt dat een centrale voorziening? Binnen de politie is men al een heel eind op weg met de zogeheten integrale bevraging. Moeten we daar een ketenvoorziening van maken? Gaan we dat regelen via portalen? Of nog anders?

En dan zijn er nog voorzieningen die weliswaar een grote rol spelen in het strafrecht, maar een veel breder bereik hebben dan alleen de strafrechtsketen.

– De laatste tien jaar heeft het Centraal Digitaal Depot (CDD) een hoge vlucht genomen. Hierin kunnen zowel *digital born* als gedigitaliseerde (*digitized*) papieren documenten worden opgeslagen. Dit bespaart organisaties kilometers papieren archief. Door de documenten digitaal op te slaan, kunnen ze ook veel beter toegankelijk worden gemaakt. En dat niet alleen achteraf als historisch archief, maar ook al in en voor het primaire proces. Het CDD is in feite een vorm van opslag in de *cloud*, dus strikt genomen geen ketenvoorziening van de strafrechtsketen. De strafrechtelijke organisaties

zijn vrij om hun documenten (of breder: hun informatieproducten) digitaal bij het CDD dan wel elders op te slaan c.q. in bewaring te geven.[6]

– Ook Justid, de beheerder van veel van de genoemde ketenvoorzieningen, is zelf meer dan een ketenvoorziening voor de strafrechtsketen. De dienst is begin 2006 ontstaan uit de fusie van de Centrale Justitiële Documentatie (CJD) in Almelo en het Bureau VIP bij het CJIB in Leeuwarden. Met het beheer van deze twee systemen, JD en VIP, lagen de kerntaken op het gebied van het strafrecht. Maar in Almelo was ook toen al een belangrijke niet-strafrechtelijke taak belegd, namelijk het 'onder substitutie' digitaliseren van de dubbelen van de burgerlijke stand (waaruit CDD+ is ontstaan). En VIP was, sinds de S van strafrecht er (in 1999) vanaf was gehaald, al niet meer beperkt tot strafrechtelijke subjecten (verdachten, veroordeelden). In de afgelopen tien jaar zijn tal van al dan niet strafrechtelijke taken naar Justid geschoven. Daarmee heeft Justid zich in feite ontwikkeld tot een ICT Service Provider voor het hele JenV-domein en is hij als zodanig dus geen ketenvoorziening (meer) voor de strafrechtsketen.

5.5 Digitalisering van de strafrechtsketen: uitleidende overpeinzingen

Teksten en documenten worden vandaag de dag overal op de computer gemaakt. Bijvoorbeeld het proces-verbaal van opsporing. De opsporingsambtenaar tikt het uit (klopt het in) op zijn computer. Vervolgens print hij het stuk, ondertekent het met de pen (de zogenoemde natte handtekening), stopt het in een enveloppe en stuurt het naar het parket van de OvJ. Daar wordt het uit de enveloppe gehaald en onder een scanner gelegd. Er wordt een pdf van gemaakt, die vervolgens digitaal de administratieve molen in gaat. Natuurlijk moeten de noodzakelijke metagegevens nog wel even handmatig worden toegevoegd. Bijvoorbeeld de naam van de verdachte en andere gegevens die nodig zijn om de zaak en het document te identificeren.

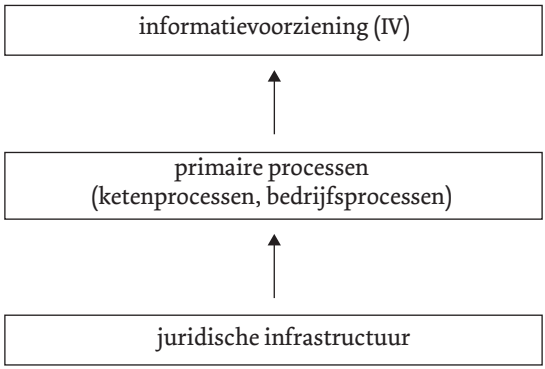
Documenten ontstaan dus al wel digitaal (*digital born*), maar van een echte digitale verwerking is nog geen sprake. Het is alleen nog maar digitaliseren in de betekenis van '*digitization: the conversion of*

analogue data (esp. in later use images, video, and text) into digital form'. Tel uit je verlies aan menskracht, foutenkans, correcties, enzovoort. De samenleving is al veel verder. Die digitaliseert in de betekenis van '*digitalization: the adoption or increase in use of digital or computer technology by an organization, industry, country, etc*'.[7] Die ontwikkeling houdt niet halt bij de poorten van de strafrechtspleging. Het is ongeveer als met de vervanging van de trekschuit en de paardentram door de auto en het vliegtuig. Er is geen sprake van een ambitie, iets wat je wel of niet kunt wíllen; het gebéurt gewoon en alles en iedereen wordt erin meegezogen. Het enige wat je kunt doen, is proberen het binnen je eigen domein zo goed mogelijk te absorberen. Voor de (straf)rechtspleging betekent dat: met behoud (op zijn minst; het mag ook leiden tot versterking) van alle rechtsstatelijke waarden en waarborgen die ons dierbaar zijn.[8]

Of je met digitalisering ook concrete verbeterdoelen kunt realiseren, zoals besparingen, het verkorten van doorlooptijden of het verminderen van ongewenste uitval, is niet zonder meer vanzelfsprekend. Doorlooptijd bijvoorbeeld, een ketenaangelegenheid bij uitstek, is de optelsom van bewerkingstijd, transporttijd en wachttijd. Stel dat de gemiddelde doorlooptijd van een gemiddelde strafzaak negen maanden bedraagt. Slechts een fractie daarvan wordt ingenomen door de bewerkingstijd en de transporttijd; laten we zeggen: twee weken. De rest is wachttijd. Automatisering of digitalisering kan dat wel beter zichtbaar maken, maar kan er weinig aan veranderen. Dat vergt verandering van werkwijzen en processen. Hoe ver gaat dat of kan en mag dat gaan?

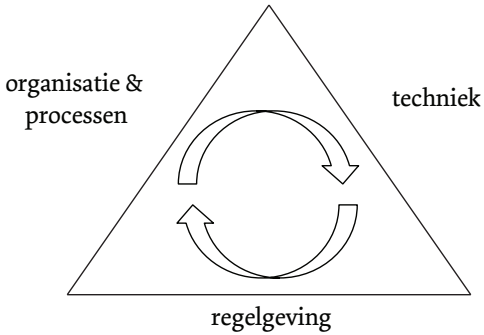
Regelmatig komt de vraag op waar je nu eigenlijk moet beginnen: bij de IV of bij de processen. Kun je wel de IV goed inrichten zo lang de processen nog niet op orde zijn? De processen zijn toch primair, die bepalen toch de inrichting van de IV? 'De gewenste informatievoorziening wordt bepaald door de planning, beheersing en uitvoering van de bedrijfsprocessen' en 'de bedrijfsprocesstructuur dient als basis voor de bepaling van de informatiebehoefte', aldus de theorie.[9] Ik denk dat dit uitgangspunt in de strafrechtsketen wat genuanceerd moet worden. Ik licht dat toe.

Strafrechtspleging is in hoge mate juridisch gereglementeerd via wetgeving en jurisprudentie. Onder de dagelijkse praktijk ligt een heel stelsel van regels, waarden en beginselen: een juridische infrastructuur (*infra* is Latijn voor: *onder*). Recht, praktijk en IV vormen als het ware drie lagen:[10]



(Dit plaatje is een variatie op het lagenmodel van Kumar et al. dat ik weergaf in par. 1.4.) In de juridisch gereglementeerde omgeving van het strafrecht (en de andere Justitieketens) zitten we in een krachtenveld van regelgeving, organisatie (i.e.: processen, cultuur, structuren) en techniek (ICT). In de rechtsstaat is de regelgeving uiteindelijk het fundament. De informatievoorziening moet sporen met de juridische infrastructuur, bijvoorbeeld als het gaat om de definities, de gegevenssoorten en -stromen, de autorisaties, de toedeling van verantwoordelijkheden. En dan is er naast het straf- en strafprocesrecht ook nog het privacy- en gegevensbeschermingsrecht (zie hoofdstuk 2). Ook dat is inmiddels, net als de IV, een onderdeel van het primaire proces. Het informatiseren van de strafrechtsketen is dus, afgezien van het noodzakelijke verandermanagement, een kwestie van schaken op drie borden: straf- en strafprocesrecht, privacy- en gegevensbeschermingsrecht en informatiekunde c.q. informatiemanagement.[11]

Ik geef de drie lagen ook wel eens weer als de drie zijden van een driehoek:

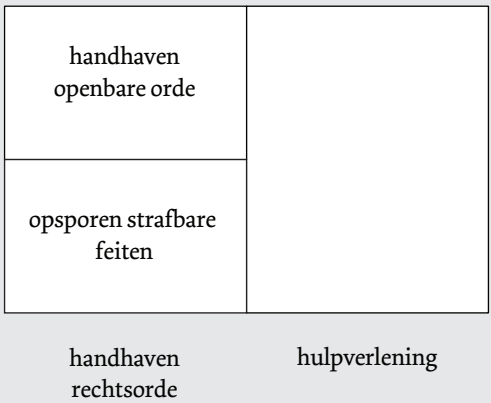


Het rechtsstatelijke primaat van de regelgeving betekent intussen níet dat er sprake is of zou moeten zijn van eenrichtingsverkeer. Juristen zullen al gauw roepen dat de informatiesystemen moeten worden aangepast, ICT'ers dat de regelgeving moet worden gewijzigd. Maar de drie componenten bepalen elkaar wederzijds. Organisatie en processen bepalen in feite de visie en de strategie. Die moet worden vertaald in regelgeving en techniek. De regelgeving op haar beurt bepaalt uiteindelijk hoe het primaire proces eruit moet komen te zien en hoe met gegevens wordt omgegaan. Omgekeerd kan de techniek eisen stellen aan de regelgeving of helpen regelgeving handiger, efficiënter, slimmer, transparanter in te richten. Enerzijds is dus de vraag met welke regels de techniek rekening moet houden. Anderzijds is er ook de vraag wat er vanuit het perspectief van de IT moet of (beter dan nu) kan worden geregeld. Regelgeving kan een hefboom zijn voor het verbeteren van processen en IV. En omgekeerd: processen en IV kunnen fouten, lacunes, onduidelijkheden, tegenstrijdigheden in de regelgeving aan het licht brengen. Ook is het zo dat IT genadeloos alle zwakke plekken in je organisatie en je processen vindt. Positief gezegd, kan IT dus helpen je organisatie en je processen te verbeteren.

Wat ik met het drielagenplaatje ook wil signaleren, is dat de taal van de werkvloer nog wel eens afwijkt van de juridische taal.

> Een voorbeeld: het gebruik van de termen *handhaving* en *opsporing* in politieland. Ik hanteer, als eenvoudig jurist, de term opsporing in de betekenis van 'onderzoek om een gepleegd

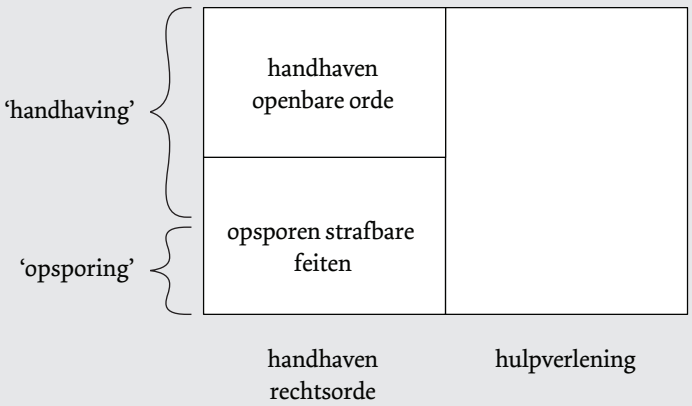
strafbaar feit op te helderen'. Deze omschrijving leunt losjes aan tegen de definitie in artikel 132a Sv: 'het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen'. (Ik ga in dit verband voorbij aan allerlei juridische discussies over de precieze reikwijdte van het opsporingsbegrip.) 'Opsporing' in deze betekenis staat tegenover 'handhaving van de openbare orde'; samen vallen ze onder het begrip 'daadwerkelijke handhaving van de rechtsorde' in artikel 3 van de Politiewet 2012. Die 'daadwerkelijke handhaving van de rechtsorde' staat in dat artikel naast 'het verlenen van hulp aan hen die deze behoeven'. (Zo stond het van oudsher ook al in de voorgaande Politiewetten, in elk geval in die van 1993 en 1957.) Het juridische plaatje ziet er dus zo uit:



Voor de ordehandhaving staat de politie onder het gezag van de burgemeester, voor het opsporen van strafbare feiten onder dat van de officier van justitie. Dit beeld is generaties juristen met de paplepel ingegoten – mij ook.

Maar de politie zelf benoemt het anders. Zij vat (of vatte?) haar taken samen in de formule 'H2O': handhaving, hulpverlening, opsporing. 'Handhaving' omvat alles wat 'blauw' is, wat 'op straat' gebeurt; onder 'opsporing' verstaat men het recherchewerk ('grijs'). Dat betekent dat 'opsporing' in de

juridische betekenis zowel binnen 'handhaving' als binnen 'opsporing' valt, want op straat, door de geüniformeerde dienst ('blauw') wordt er net zo goed 'opgespoord' (in juridische zin) als door de recherche. De Basisvoorziening handhaving (BVH) is zelfs dé proces-verbaalmachine van de politie (behalve voor de zwaarste zaken, waarvoor SummIT wordt gebruikt). 'Handhaven' is in het politiële spraakgebruik dus ruimer en 'opsporen' beperkter dan in het juridische. Het plaatje komt er dan ongeveer zo uit te zien:



Ik probeer altijd de alledaagse taal van de werkvloer te vertalen naar de formele juridische taal. Want uiteindelijk ontleent alles wat er op de werkvloer van de strafrechtsketen gebeurt, zijn betekenis aan die juridische infrastructuur, dat wil zeggen de regelgeving en de jurisprudentie. Iets wat niet te vertalen valt, is om zo te zeggen verdacht. En als het wél te vertalen valt, dan is voor mij de vraag: waarom gebruik je dan niet de juridische taal? Door in plaats daarvan andere termen te bezigen, verlies je aan scherpte en maak je het alleen maar ingewikkelder en vager. En als je de dingen niet goed juridisch kunt duiden, kun je ze ook niet goed verantwoorden. Daarmee eindigen we waar dit boekje begon: bij de rechtsstaat.

Noten

1 Zie de brief van de minister van VenJ van 23 juni 2014, Kamerstukken II, 2013/14, 33842, nr. 2 (*beleidsreactie evaluatie Wpg en Wjsg*).
2 Brief van de minister van BZK van 30 juni 2011 aan de Tweede Kamer, Kamerstukken II, 2010/11, 26643, nr. 187 (*Archiefvisie*), p. 1.
3 De wet biedt de ruimte om een zaak op zitting te brengen zonder dossier. Immers, de mondelinge verklaringen van verdachte(n), getuige(n) en deskundige(n) op de terechtzitting kunnen als bewijsmiddel volstaan. Maar iedereen zou toch raar opkijken als een officier van justitie een zaak zou aanbrengen met alleen maar een dagvaarding, zonder dossier.
4 Brief van de minister van VenJ van 23 juni 2014, Kamerstukken II, 2013/14, 33842, nr. 2 (*beleidsreactie evaluatie Wpg en Wjsg*).
5 Zie de *beleidsvisie op integriteit en screening*, brief van de staatssecretaris van VenJ van 11 februari 2016, Kamerstukken II, 2015/16, 34300 VI, nr. 78.
6 Aldus het visiedocument van 17 februari 2016 (Kamerstukken II, 2015/16, 29279, nr. 298, p. 7): '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).'
7 Ontleend aan Scott Brennen en Daniel Kreiss, Digitalization and Digitization, September 8, 2014 (bron: http://culturedigitally.org/2014/09/digitalization-and-digitization, geraadpleegd 19 november 2015).
8 Aldus het visiedocument *Naar digitaal werken in de strafrechtsketen. Perspectief en richting*; brief (met bijlage) van de minister van VenJ van 17 februari 2016, Kamerstukken II, 2015/16, 29279, nr. 298.
9 Eleanor Pascoe-Samson, *Organisatie, besturing en informatie* (tweede druk), Deventer: Kluwer Bedrijfsinformatie 1998, p. 227 en 229.
10 Uitvoeriger over het drielagenmodel: *Jegens en Wegens*, par. 3.3 en 2.8.
11 Voor enkele in mijn ogen fundamentele beschouwingen over informatisering in ketens en netwerken verwijs ik graag naar de volgende drie studies: Reza Torabkhani, Martin Smits en Gert van der Pijl, *Improving the Performance of Business Networks in E-Government*, 20th Bled eConference eMergence: Merging and Emerging Technologies, Processes, and Institutions, June 4-6, 2007, Bled, Slovenia; Pieter Wisse, *Interoperabiliteit voor informatieverkeer in publiek domein*, PrimaVera Working Paper 2008-08 (alleen digitaal gepubliceerd: zie www.informationdynamics.nl/pwisse/pdf/pv-2008-08.pdf); NOREA (de beroepsorganisatie van IT-auditors), *Audit Alert Keteninformatisering*, 2013.

TREFWOORDENREGISTER

Verwezen wordt naar paragrafen.

Rechtshandhaving is tegenwoordig vaak een kwestie van multi-disciplinaire samenwerking, waarbij het openbaar bestuur, Justitie en private partijen zijn betrokken. Zij werken samen in ketens en netwerken. Drie disciplines zijn in vrijwel elk samenwerkingsverband aan de orde: straf- en sanctierecht (omdat dat de harde kern is van handhaving), keteninformatisering (omdat informatie moet worden uitgewisseld in en tussen ketens) en gegevensbescherming (privacy). Het unieke van dit boek is dat het een kennismaking biedt met deze drie perspectieven in hun onderlinge samenhang. Op een laagdrempelige manier brengt het theorie en praktijk bij elkaar.

Het boek helpt adviseurs, bestuurders, enterprise architecten, informatici, managers, professionals, programmamanagers en projectleiders om meer grip te krijgen op de keteninformatisering waaraan of waarmee zij werken.

Wim Borst studeerde rechten aan de Erasmus Universiteit Rotterdam en (dertig jaar later) informatiemanagement aan de Universiteit van Amsterdam. Hij werkte als docent en onderzoeker aan de Universiteit Leiden, waar hij promoveerde op een proefschrift over 'De bewijsmiddelen in strafzaken' (1985), en als gerechtsauditeur bij het Wetenschappelijk Bureau van de Hoge Raad. Tegenwoordig werkt hij als beleidsadviseur bij het ministerie van Justitie en Veiligheid. De laatste vijftien jaar richt zijn werk zich op de keteninformatisering in het strafrecht.

'inspirerend, rijk en uiterst verhelderend'
– **Corien Prins**, voorzitter Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en hoogleraar recht en informatisering, TILT/Universiteit Tilburg

'Een fantastisch boek: heel toegankelijk en wat mij betreft verplichte kost voor iedereen in de strafrechtketen.'
– **Hugo Hillenaar**, Directeur Strafrechtketen

ISBN 978-94-6236-892-7

Boombestuurskunde