Lectorale rede Veiligheid en Digitalisering

"Onze nationale welvaart zal met eigen handen opgebouwd moeten worden" Anton de Kom[1]

Door: René Westra

Geachte dames en heren,

Het is een grote eer om aan uw Hogeschool benoemd te worden als lector Veiligheid en Digitalisering. Graag neem ik u vandaag mee met mijn fascinatie voor veiligheid en digitalisering. Hopelijk herkent u deze en kunnen we de komende jaren samen zorgen voor verdieping en verbreding ten behoeve van studenten, docenten, onderzoekers van Polytechnic College, University of Applied Sciences (PTC) en alle andere belangstellenden in Suriname.

1. Inleiding

Het uitspreken van een lectorale rede is een bijzondere gebeurtenis. Het is een gelegenheid om belangstellenden kennis te laten nemen van wat het lectoraat inhoudt. Voor de lector biedt dit een unieke kans om aan te geven wat hij of zij verstaat onder het lectoraat, wat wordt beoogd te bereiken en op welke wijze dat wordt gerealiseerd.

De lectorale rede is tevens een goede gelegenheid om te benadrukken dat het lectoraat refereert aan de kennispositie van de hogeschool waar kennisontwikkeling, kennisoverdracht en kennissamenwerking centraal staan. Bij kennisontwikkeling wordt verwezen naar het doen van onderzoek waarmee nieuwe kennis of aanscherpingen van bestaande kennis kunnen worden verkregen. Kennisoverdracht verwijst naar onderzoek en advisering op basis van aanwezige en nieuw verkregen kennis en ervaring. Bewust wordt hier advisering genoemd. Het is cruciaal dat de samenleving en het openbaar bestuur, waar mogelijk en nodig, kunnen worden geholpen met de beschikbare kennis en ervaring. Dit geldt ook voor de kennissamenwerking: natuurlijk in eerste plaats met de mede-lectoren om samen de kennispositie van deze hogeschool te versterken, maar ook met overheidsorganisaties, kennisinstellingen en bedrijven.

Tot slot een laatste opmerking vooraf. Het is bijzonder om als lector met Nederlandse roots te worden aangesteld aan een Surinaamse hogeschool. Gezien de historische banden tussen

[1] Kom, A. de, Wij slaven van Suriname, Atlascontact, 2020, p. 186.

beide landen[2] zal het lectoraat -met respect voor hetgeen heeft plaatsgevonden- verder worden ingevuld. Daarnaast zal het lectoraat, waar gewenst en mogelijk, actief bruggen slaan tussen beide landen op het terrein van kennisontwikkeling, kennisoverdracht en kennissamenwerking. In de rede beoog ik de te bespreken onderwerpen ook aan beide landen te verbinden.

2. Veiligheid en Digitalisering, een duo apart?

Het aandachtsgebied van het lectoraat Veiligheid en Digitalisering is breed. Op het eerste gezicht lijkt het lectoraat uit twee gescheiden werelden te bestaan. Niets is echter minder waar. Veiligheid en digitalisering hebben in toenemende mate met elkaar van doen gekregen. Veiligheid staat hoog op de politieke agenda en kent vele verschijningsvormen[3]. Dagelijks worden we hiervan bewust door fysieke, digitale, geopolitieke medische en andere bedreigingen van onze veiligheid. Daarnaast wordt onze samenleving steeds meer afhankelijk van digitalisering. Veel van onze persoonlijke en zakelijke activiteiten worden direct en indirect ondersteund c.q. beïnvloed door digitalisering.
Belangrijk is de onderlinge relatie tussen beide: veiligheid kan met digitalisering worden versterkt en ondersteund[4], maar kan er ook door worden ondermijnd[5]. Zie bijvoorbeeld cybercriminaliteit[6], hacking[7] en witwassen met bitcoins[8]. Op nationaal niveau worden de risico's onderkend[9].
Vanuit digitalisering wordt in toenemende mate duidelijk dat er maatregelen nodig zijn om te kunnen borgen dat het gebruik van de gedigitaliseerde informatievoorziening veilig gebeurt en de gedigitaliseerde omgeving weerbaar is voor mogelijk onveilige interventies. Dat geldt ook voor de inzet van artificiële intelligentie[10], big data[10] en algoritmen[11]. Het is belangrijk dat binnen het onderwijs en onderzoek van PTC ook aandacht is voor deze ontwikkelingen.

Er zijn meerdere benaderingen om de werkelijkheid van veiligheid en digitalisering te beschouwen[12]. Dat geldt ook voor de wetenschapper die de werkelijkheid wil begrijpen. Die

[2] Zie Jaarrede 2022 president van Suriname Santokhi d.d. 1 oktober 2021 en rede premier Rutte van Nederland op 13 september 2022 in De Nationale Assemblée in Paramaribo.
[3] Zie de Bosaltlas van de veiligheid, Noordhoff, 2017. In 10 hoofdstukken wordt veiligheid in Nederland "in kaart" gebracht; van persoonlijke veiligheid via criminaliteit, waterveiligheid en milieurisico's tot nationale en internationale veiligheid.
[4] Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid, Amsterdam University Press, 2011.
[5] Voorbeeld van ondermijning: Tops, P. en J. Tromp, De achterkant van Nederland, Balans, 2017. Zie voor politieke aandacht onder meer brief Minister van Justitie en Veiligheid aan Tweede Kamer, Integrale aanpak van online fraude, 8 juli 2022.
[6] Modderkolk, H., Het is oorlog, maar niemand die het ziet, Podium, 2019.
[7] Buchanan, B., The hacker and the state, Harvard University Press, 2020.
[8] Uitspraak gerechtshof Den Haag op 1 februari 2022 (ECLI:NL:GHDHA:2022:104).
[9] NTCV, Nationale veiligheid strategie, 2019; NTCV, Rijksbrede risicoanalyse nationale veiligheid, 2022. [10] Crawford, K., Atlas of AI, Yale University Press, 2021; Passchier, R., Artificiële intelligentie en de rechtsstaat, Boomjuridisch, 2021.
[10] Mayer-Schönberger en K. Cukier, Big Data, John Murray, 2013; Westra, R.L.N. en G.J.C.M. Bakker, Big data en rechtshandhaving; hype of hoop?, BISC nr. 5, Cahiers Inlichtingenstudies (België), Maklu, 2015, p. 139 -150.
[11] Klous, S. en N. Wielaard, Vertrouwen in de slimme samenleving, Business Contact, 2017.
[12] Zie de lectorale redes van: Kolthoff, E., Integriteit, mensenrechten en veiligheidsmythe, Avans, 2010; Stol, W.,

moet zich bewust zijn van zijn/haar eigen referentiekader om de juiste analyses te maken en hiermee de werkelijkheid te begrijpen. Daarbij is het van groot belang om de verkregen inzichten te vertalen naar de praktijk. Dit lectoraat ziet de praktijkgerichtheid van onze activiteiten als een continue opdracht. De samenleving moet kunnen profiteren van de groeiende kennispositie.

In deze rede wil ik stilstaan bij een drietal onderwerpen:

a. de verschillende invalshoeken, ofwel rationaliteiten;
b. de veiligheidsdriehoek;
c. een drietal uitdagingen.

3. Rationaliteiten

Allereerst ga ik nader in op het referentiekader om de werkelijkheid te beschouwen. En wel specifiek de werkelijkheid van het handelen van de overheid. Dit kan vanuit verschillende wetenschappelijke disciplines worden beschouwd en verklaard[13].
Snellen noemt deze disciplines rationaliteiten. Een rationaliteit is volgens hem een gesloten stelsel van begrippen, uitgangspunten en criteria om de werkelijkheid te kunnen begrijpen en ontwikkelingen te kunnen duiden. Een rationaliteit vormt een betekenisvol kader voor rationeel handelen. Omdat rationaliteiten in zich gesloten stelsels zijn, trachten ze elkaar te verdringen. Wat voor de ene rationaliteit rationeel handelen is, kan voor een andere rationaliteit juist niet rationeel zijn[14].

Eerder heb ik betoogd dat voor het begrijpen van overheidshandelen vijf rationaliteiten belangrijk zijn: de juridische, de economische, de politicologische, de beleidswetenschappelijke en de sociaal-psychologische rationaliteit[15][16]. Elke rationaliteit heeft een ander aangrijpingspunt wat doorwerkt in het overheidshandelen. Wat voor de één een variabele is (bijvoorbeeld voor econoom: kosten handhavingsapparaat) is dat voor de ander een gegeven (jurist). En wat voor door de één kan worden gezien als vooruitgang (cameratoezicht) kan door de ander juist worden ervaren als een inperking c.q. bedreiging van de levenssfeer (sociaal-psycholoog).

Rationaliteit	***Mogelijke aangrijpingspunten***
Juridische rationaliteit	wet- en regelgeving, grondrechten, rechtszekerheid, rechtsgelijkheid, toezicht en normhandhaving[17]

Cybersafety overwogen, Boom, 2010; Khonraad, S., Integrale veiligheid als reflexieve praktijk, Avans, 2011; Kokkeler, B., Smart public safety, Avans, 2017; Leukfeldt, E.R., De 'human' factor in cybersecurity, De Haagse Hogeschool, 2018; Spithoven, R., Verbonden risico's, Boomcriminologie, 2020.

[13] Snellen, I.Th.M., Boeiend en geboeid, Samsom Tjeenk Willink, 1987; Westra, R.L.N., Fiscale fraudebestrijding: grenzen aan sturing, Pantheon, 2006.

[14] Snellen, I.Th.M., Boeiend en geboeid, Samsom Tjeenk Willink, 1987, p. 5.

[15] Westra, R.L.N., Fiscale fraudebestrijding: grenzen aan sturing, Pantheon, 2006.

[16] Otte laat zien dat het begrip "schuld" in het licht van straffen vanuit meerdere juridische, theologische en psychiatrische invalshoek begrepen kan worden. Otte, M., Een kleine biografie van het straffen, Boomjuridisch, 2018.

Economische rationaliteit	kosten van handhaving en opbrengsten van criminaliteitsbestrijding
Politicologische rationaliteit	macht/invloed, besluitvormingsprocessen, draagvlak en agendavorming
Beleidswetenschappelijke rationaliteit	doelbepaling en -realisatie, doelmatigheid, procedures, standaardisatie, formalisering
Sociaal-psychologische rationaliteit	subjectieve en objectieve veiligheid en de impact van veiligheid op groepsgedrag

Voor de bestuurskunde, de wetenschap die het overheidshandelen bestudeerd, is lang de psychologie als een vreemde invalshoek gezien[17]. De persoonlijke motivatie en strevingen van ambtenaren zijn lang, conform de Weberiaanse opvatting over bureaucratie[18], terzijde geschoven. Ik heb eerder laten zien dat deze discipline juist onmisbaar is om te begrijpen waarom ambtenaren, politici en bestuurders bepaald gedrag vertonen.

In dit lectoraat wordt gekozen voor de multidisciplinaire benadering. Immers, het is belangrijk vanuit dit lectoraat de werkelijkheid zo goed mogelijk te begrijpen en te kunnen inspelen op maatschappelijke vraagstukken.

4. Veiligheidsdriehoek

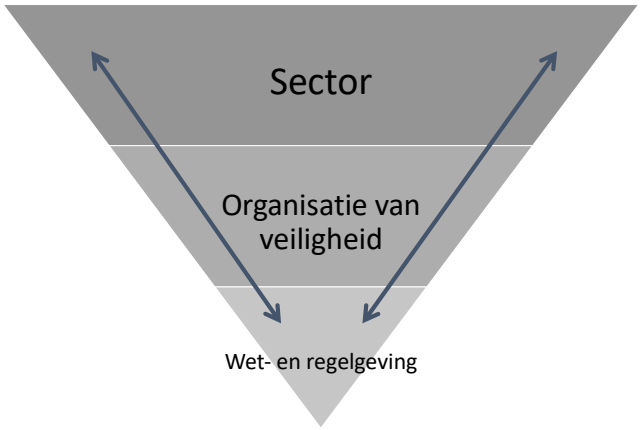
Nu we zicht hebben op de verschillende invalshoeken, komt de vraag op “welke aspecten het handelen van de overheid m.b.t. veiligheid” beïnvloeden? Om de wereld waarin het handelen van de overheid m.b.t. veiligheid plaatsvindt scherper te kunnen duiden, is het belangrijk onderscheid te maken tussen drie aandachtsgebieden:

- de *wet- en regelgeving* – het formele normen- en waardenkader dat door de overheid in wet- en regelgeving is vastgelegd;
- de *organisatie van veiligheid* – wie doet wat binnen de overheid, incl. hoe wordt wet- en regelgeving geïmplementeerd dan wel geactualiseerd door ontwikkelingen in de omgeving;
- de *sector(en)* waar het beleid en het handelen op is gericht – dat zijn de sectoren waarvoor de wet- en regelgeving is bedoeld en de rationeel[19] handelende overheid impact beoogt. Te denken valt aan sectoren als defensie, openbare orde,

[17] De multidisciplinaire studie bestuurskunde is lang gestoeld geweest op de vier kerndisciplines: rechten, economie, politicologie en sociologie. Zie de opzet van de eerste studie in Nederland aan de toenmalige TH Twente (nu: Universiteit Twente) bij de start in 1976.
[18] Weber, M., Wirtschaft und Gesellschaft, Mohr, 1985. Weber gaat in zijn beeld van een rationeel en efficiënt werkende bureaucratie uit van objectieve en trouwe ambtenaren, die zonder waardegebonden opvattingen uitvoeren wat de politiek heeft beslist.
[19] Rationeel: vanuit de betreffende rationaliteit bezien “rationeel”.

volksgezondheid, voedselproductie, verkeer en vervoer, woningbouw, watermanagement, energieproductie en mijnbouw.

Deze 3 aandachtsgebieden zijn continu in beweging, zowel intern als ten opzichte van elkaar. Visueel zou het volgende beeld kunnen worden geschetst, de veiligheidsdriehoek.



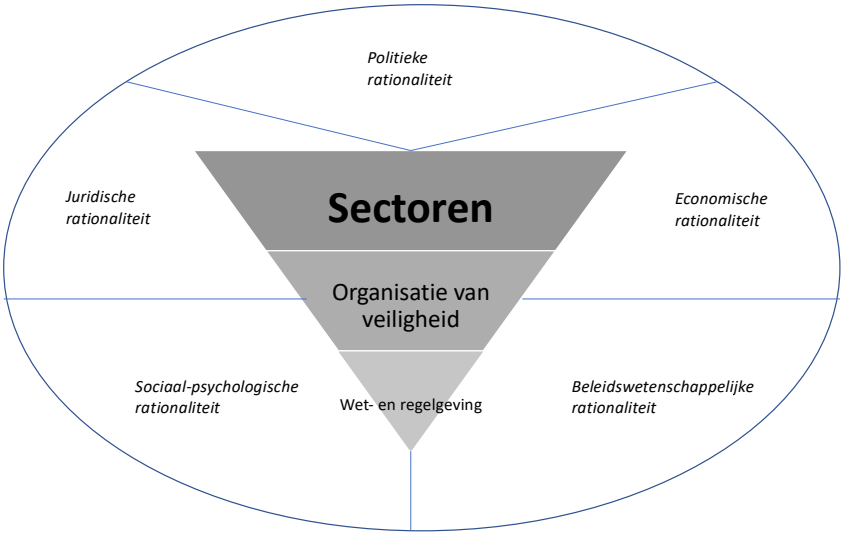
Deze veiligheidsdriehoek leidt tot twee kanttekeningen:

- consistent overheidshandelen – voor de legitimiteit van het overheidshandelen is het cruciaal dat de overheid consistent handelt binnen en tussen de sectoren. Dus op dezelfde wijze reageert op normoverschrijding en dit op een vergelijkbare manier sanctioneert. Dit stelt eisen aan wet- en regelgeving en aan de organisatie van veiligheid. Door het wetgevingsproces te formaliseren[20], te structureren en te standaardiseren kan eenduidigheid in wet- en regelgeving worden bevorderd[21]. Het is belangrijk dat burgers het rechtsstelsel[22] kunnen vertrouwen.
- Externe sensitiviteit – voor overheidsmanagers is het cruciaal oog te hebben voor de afstemming tussen de bestuurlijke, politieke en maatschappelijke ontwikkelingen[23]. Indien afstemming tussen bestuur, politiek en maatschappij niet of onvoldoende

[20] https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving
[21] Er zijn specifieke opleidingen voor wetgevingsambtenaren. Daarmee gereageerd op de constatering van de 14 wetsfamilies daar duidelijk was dat dit het functioneren van “de overheid” niet ten goede komt. Zie Hoefnagel, F.J., De veertien wetsfamilies, Bestuurswetenschappen, maart/april 1977, nr. 2 p.199 ev. De term “14 wetsfamilies” komt uit de rede van prof. dr. S.O. van Poelje tijdens het IBW-afscheidssymposium 1977. Met deze wetsfamilies wordt geduid op de verschillende wetgevingspraktijken van de (toen) 14 ministeries.
[22] Bos, K. van den en A.F.M. Brenninkmeijer, Vertrouwen in wetgeving, de overheid en de rechtspraak, NJB, nr. 21 2012, p. 1451.
[23] Westra, R.L.N. en G.J.C.M. Bakker, De overheidsmanager van de toekomst, M&O nr. 3, 2019, p. 41.

plaatsvindt, kan dit tot grote problemen leiden in de uitvoering[24]. Dit kan tevens het vertrouwen van burgers in wat er gebeurt beïnvloeden[25].

Wanneer de veiligheidsdriehoek wordt geplaatst in de context van de rationaliteiten, ontstaat een interessant beeld. De vijf voor het overheidshandelen relevante rationaliteiten beïnvloeden wet- en regelgeving, organisatie van veiligheid en sectoren alsmede de onderlinge relaties. In onderstaand figuur is dat gevisualiseerd. Dit model zal een belangrijke inspiratiebron zijn voor het lectoraat.



5. Drie uitdagingen

Aan de hand van drie uitdagingen zal het interessante terrein van veiligheid en digitalisering verder worden verkend. Deze uitdagingen zijn slechts illustraties van het brede terrein dat het lectoraat omvat.

[24] Putters, K., Veenbrand, smeulende kwesties in de welvarende samenleving, Prometheus, 2019; Tjeenk Willink, H.D., Kan de overheid crises aan? Prometheus, 2021; Hirsch Ballin, E.H.M., Waakzaam burgerschap, Vertrouwen in democratie en rechtsstaat herwinnen, Querido Facto, 2022.
[25] Wetenschappelijke Raad voor het Regeringsbeleid, Vertrouwen in burgers, 2012; Rovers, E., Nu is het aan ons, De Correspondent, 2022.

De drie uitdagingen zijn gekoppeld aan de hierboven genoemde veiligheidsdriehoek. Daarbij begin ik met het hart van het model, de organisatie van de veiligheid, om in te kunnen gaan op het dilemma van sturing via ketens i.p.v. kolommen. Vervolgens verken ik met digitale veiligheid de impact op de sectoren. Tot slot neem ik de arbeidsveiligheid om enkele opmerkingen te maken t.a.v. wet- en regelgeving. Zo komt de gehele veiligheidspiramide aan bod.
Voor het lectoraat bevatten deze beschouwingen bouwstenen voor het onderwijs- en onderzoeksprogramma. Hopelijk nodigen deze bouwstenen uit om ze met belangstellenden uit het openbaar bestuur, bedrijfsleven en kennisinstellingen op te pakken.

5.1. Eerste uitdaging: denken in ketens i.p.v. kolommen

De eerste uitdaging is het denken in ketens i.p.v. kolommen. De vertaling van wet- en regelgeving naar uitvoering lijkt -vanuit Weberiaans perspectief- eenvoudig: de regels zijn bekend, ze hoeven alleen maar bij de uitvoering te worden gevolgd. De praktijk is echter weerbarstiger: theorie en praktijk kunnen ver uit elkaar liggen. Illustratief is het verschil tussen gezaghebbende benaderingen van Hoogerwerf[26] en Coba[27] op het overheidsbeleid en de ervaringen, zoals die door Rosenthal c.s. [28] en Docters van Leeuwen[29] zijn opgetekend. De Toeslagenaffaire[30] laat ook zien hoe het fraudebeleid kan ontsporen[31], waarbij zelfs de legitimiteit van de overheid aan de orde is. Ook waar wetgevende macht en uitvoerende macht de kloof eerder groter maken dan kleiner[32] en de rechtspraak in de knel in gekomen[33]. Dat het recht de sociale cohesie kan bevestigen, is hier nadrukkelijk niet gebeurd. Vanuit de constitutionele levenscirkel[34] bezien waarschuwt Hirsch Ballin voor manipulatie van de politieke meningsvorming door geavanceerde informatietechnologie. Hoewel de democratische structuren formeel in stand blijven, is er geen sprake van een vrij keuzeproces.

[26] Hoogerwerf, A. (red), Overheidsbeleid, Samsom, 1980.
[27] Interdepartementale Commissie voor de Beleidsanalyse (COBA); in: Commissie Hoofdstructuur Rijksdienst, Bijlage bij Achtergrondstudie 6, BiZa, 1981, p. 112.
[28] Rosenthal, U., A.H.W. Docters van Leeuwen, M.J.G. van Eeten en M.J.W. van Twist, Ambtelijke vertellingen, Lemma, 2001.
[29] Docters van Leeuwen, A.W.H., Een spoor van vernieuwing, Prometheus, 2020.
[30] De fraude met toeslagen door Bulgaren leidde door een motie (Omtzigt, 2013) tot aanscherping van het fraudebeleid (zero tolerance). Hierdoor kwamen veel ouders met kinderopvangtoeslag in de problemen door onterechte fraudeverdenkingen. De Belastingdienst, Tweede Kamer en rechtspraak kwamen pas na jaren in actie.
[31] Parlementaire ondervragingscommissie Kinderopvangtoeslag, Ongekend onrecht (eindverslag), 17 december 2021.
[32] Fredrik, J. Zo hadden we het niet bedoeld, De Correspondent, 2021.
[33] Brenninkmeijer, A.F.M., De grondbeginselen van de rechtsstaat zijn ‘geschonden’ als ‘verschrikkelijk ongeluk’, NJB, nr. 1 2021, p. 6; Raad van State, Lessen uit de kinderopvangtoeslagzaken, november 2021; Beeten, J. Van de en R.H. Van de Beeten, Driemaal is (geen) scheepsrecht? NJB, nr. 10 2021, p. 3550.
[34] Hirsch Ballin, E.H.M., Waakzaam burgerschap, Vertrouwen in democratie en rechtsstaat herwinnen, Querido Facto, 2022, p. 86 resp. p.44. Hirsch Ballin verwijst naar de inzet van artificiële intelligentie door Cambridge Analytica in de Verenigde Staten (2016).

In een eerder onderzoek naar fiscale fraudebestrijding[35]is gebleken dat er grenzen aan de sturing zijn. Het feit dat uitvoering, handhaving, opsporing en vervolging niet alleen onder verschillende ministeries vallen, maar ook verschillende doelstellingen kennen, leidt ertoe dat er een spanningsveld ontstaat tussen de strafrechtelijke keten en de samenwerkende kolommen van ministeries.

Ter illustratie:
De Belastingdienst heeft tot taak de belastingopbrengst conform wet- en regelgeving te maximaliseren. Fiscale fraude is een ongewenst verlies en dient te worden gecorrigeerd (fraudebestrijding) en, waar mogelijk, tegen te gaan (controlestrategie, informatiepositie e.d.).

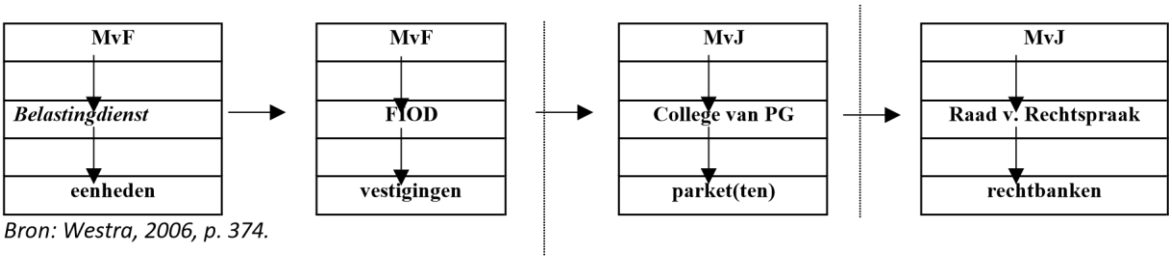
Voor de opsporingsdienst staat het signaleren van fiscale delicten en deze succesvol bij de rechter brengen voorop. De fraudeur moet, in lijn met de benadering van Bentham[36], weten dat er zeker (pakkans), snel (strafrechtelijke reactie) en stevig (strengheid) wordt opgetreden. Dit betekent sturing op aantallen zaken, verdachten en fiscale impact.

Daarentegen zal het Openbaar Ministerie vanuit het opportuniteitsbeginsel[37] kijken naar de maatschappelijke impact en zoeken naar een balans tussen de verschillende soorten zaken die zijn voorgelegd. Het Openbaar Ministerie beschikt over de mogelijkheid om bepaalde zaken (ZSM-zaken[38]) zelf af te doen.

De rechtspraak is lijdelijk: alle zaken die worden voorgelegd moeten -in beginsel- worden behandeld. De rechtspraak kan sturen op aard van de behandeling (EK/MK) en te besteden tijd per zaak[40]. Soms kunnen er capaciteitsproblemen optreden waardoor blijkt behandeling toch niet mogelijk is en gekozen wordt voor seponering[39].

In onderstaande figuur is als voorbeeld de strafrechtelijke keten in Nederland gevisualiseerd. Er is sprake van verticale en horizontale sturing. Doordat de financiering van de activiteiten in keten geschiedt via de twee betreffende ministeries (Financiën en Justitie & Veiligheid[40]), en dus de cyclus van de Rijksbegroting, heeft de verticale sturing grote invloed op de sturing in de strafrechtelijke keten (horizontale sturing). De economische rationaliteit is hier dominant ten opzichte van de juridische rationaliteit.

[35] Westra, R.L.N., Fiscale fraudebestrijding: grenzen aan sturing, Pantheon, 2006.
[36] Wetenschappelijke Raad voor het Regeringsbeleid, Doelmatigheid van rechtsvervolging, (W35), 1988.
[37] In de praktijk wordt dit opportuniteitsbeginsel genuanceerd gehanteerd, zie Van Liempt, P., Misdaad en straf in de polder, Het OM aan het woord, Prometheus, 2022, p.331.
[38] Thomas, M.S. e.a., Snel, Betekenisvol en Zorgvuldig, Een tussenevaluatie van de ZSM-werkwijze, Boomjuridisch, 2016.
[40] De rechtspraak wordt gefinancierd volgens het P x Q principe: elk type zaak krijgt een bepaalde prijs (P) toegewezen op basis van de inzet (minuten). Het aantal zaken (Q) maal de prijs levert de financiering van een gerecht op (hoofdlijn).
[39] De Gelderlander, Streep door 1500 strafzaken: te weinig rechters bij rechtbank Gelderland, 16 juni 2022.
[40] In 2006 is er sprake van het Ministerie van Justitie, nu is dit het Ministerie van Justitie en Veiligheid geworden.



Bron: Westra, 2006, p. 374.

Vanuit het besef dat de maatschappelijke impact van de strafrechtelijke keten cruciaal is voor de effectiviteit van de keten, zou juist de verticale sturing ten dienste moeten staan van de horizontale sturing. Sinds enige jaren wordt de dominantie van de economische rationaliteit (verticale sturing) getracht te corrigeren met een bestuurlijk en operationeel Ketenoverleg strafrechtketen[41]. Gevolg: in het laatste Coalitieprogramma[42] (Nederland) is nu een groot bedrag voor de versterking van de gehele keten beschikbaar gesteld. Een belangrijke stap.

Het is interessant om nu een brug te slaan naar de digitalisering. Ook hier is de oude aanpak per kolom nog duidelijk zichtbaar. De partners in de strafrechtelijke keten - Politie, Openbaar Ministerie en rechtspraak- kennen eigen informatiesystemen voor de primaire processen en de bestuurlijke informatie. Dat dit tot problemen leidt voor het functioneren van en de sturing in de keten, zal geen verrassing zijn. Zeker wanneer de systemen zelf ook niet optimaal presteren[45]. Externe ontwikkelingen als maatschappelijke onvrede over de lange doorlooptijden[43] en cybercriminaliteit[44] kunnen leiden tot de urgentie om meer fundamenteel te kijken naar de digitale infrastructuur. Een ketengerichte digitalisering kan dan de werkwijze zijn om institutionele barrières[48] in de keten te slechten. Dit vraagt leiderschap en visie[45].

Het dilemma van verticale en horizontale sturing is een kenmerk van organisaties en samenwerkingsverbanden van organisaties[46]. Dit geldt ook voor het stimuleren van

[41] Ministerie van Justitie en Veiligheid/directie strafrechtketen, Ketenplan van aanpak, 2018. Bestuurlijk Ketenberaad, Actieplan strafrechtketen, 6 november 2020.
[42] Omzien naar elkaar, vooruitkijken naar de toekomst (Coalitieakkoord 2021-2025 VVD, D66, CDA, CU), 15 december 2021. [45] Brief Raad voor de Rechtspraak aan Minister voor Rechtsbescherming, Reset digitalisering van de Rechtspraak (KEI), 10 april 2018; Stol, W., Essenties van politiewerk en digitalisering, Strafblad nr. 1, Sdu, 2019; Wetenschappelijke Raad voor het Regeringsbeleid, Politiefunctie in een veranderende omgeving, working paper WRR, 2021; Programma Digitalisering Strafrechtketen, Halfjaarrapportage, 29 juli 2021.
[43] Reiling, D., Technology for Justice, how information technology can support judicial reform, Leiden University Press, 2010.
[44] Eeden, van den, C.A.J. e.a., Opsporen, vervolgen en tegenhouden van cybercriminaliteit, WODC 2021-23, 2001. [48] Eén van die barrières is het hanteren van dezelfde gegevensdefinities tussen de organisaties. Een andere is de interne begrotingssystematiek van de kolom. Digitalisering maakt het mogelijk om bestuurlijk of politiek gegroeide patronen te doorbreken ten behoeve van het maatschappelijke belang.
[45] 't Hart, P. en M. ten Hooven, Op zoek naar leiderschap, De Balie, 2004; Horrevorts, T. en R. Pans, Presterende bestuurders, Sdu, 2010; Brink, G. Van den en Th. Jansen, Ambtelijk vakmanschap en moreel gezag, Stichting Beroepseer, 2016; Brenninkmeijer, A.F.M., Moreel leiderschap, Prometheus, 2020.
[46] Mintzberg, H., The structuring of organizations, Prentice-Hall, 1979.

innovaties en de rol van de overheid daarbij, zoals Mazzucato[47] dat treffend heeft aangetoond. Vanuit het lectoraat zullen deze inzichten worden vertaald naar onderwijs en onderzoek alsmede zijn ze beschikbaar voor advisering in Suriname.

5.2. Tweede uitdaging: digitale veiligheid

De tweede uitdaging betreft de digitale veiligheid. Dat de inzet van informatie- en communicatietechnologie grote invloed heeft op de werkprocessen binnen en tussen organisaties in het algemeen en met burgers, is helder. De "digitale revolutie"[48] heeft sinds de jaren '80 het functioneren van de overheid fors veranderd en zal dat nog veel verder gaan doen. De WRR spreekt zelfs over de kansen en nieuwe perspectieven voor de "iOverheid" [49]. De overwegende teneur is dat digitalisering kansen biedt, voor zowel de overheid als organisatie om effectiever en efficiënter te functioneren als in relatie tot de samenleving en de burger. Te denken valt aan participatie via digitale referenda, dienstverlening via een digitaal loket, online voorlichting, het gebruik van algoritmen[50], AI en big data alsmede het denken over de blockchain economie[51].

Gaandeweg wordt duidelijk dat er ook dilemma's rond de digitale veiligheid te zijn, waarvan de ernst, omvang en urgentie niet kan worden overzien. Dat er dilemma's zijn, is wel duidelijk. In 2012 verschijnt het Cybersecuritybeeld[56] van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het geschetste beeld van de kwetsbaarheden is schokkend. Echter, wanneer Modderkolk[52] in 2019 aan de hand van concrete voorbeelden laat hij zien welke impact digitale aanvallen hebben gehad op onder meer DigiNotar en KPN komt er brede aandacht. De constatering dat de bedreiging komt van met name buitenlandse mogendheden en niet van criminele organisaties, levert voor velen een paradigmawisseling in het denken op. Daarnaast wordt helder dat deze dreiging door het lucratieve karakter niet kleiner zal worden en kan door de mate van ongerichtheid ieder, organisatie of individu, raken.

[47] Mazzucato, M., De ondernemende staat, Nw Amsterdam, 2015.
[48] Snellen, I.Th.M. e.a., Technology assessment van het openbaar bestuur, Sdu, 1988.
[49] Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid (nr. 86), Amsterdam University Press, 2011.
[50] Het gebruik van algoritmen kan de besluitvormingsprocessen versnellen. Algoritmen houden keuzes in, die normatief bepaald kunnen zijn. Het binnen het openbaar bestuur cruciaal deze normatieve afweging te kennen en er, daar waar nodig, politiek en bestuurlijk expliciet over te beslissen. Dit gaat zeker op voor algoritmen die grote impact voor burgers en bedrijven kunnen hebben dan wel de rechtszekerheid en/of rechtsgelijkheid kunnen/zullen gaan beïnvloeden. Passchier, R., Artificiële intelligentie en de rechtsstaat, Boomjuridisch, 2021; Crawford, K., Atlas of AI, Yale University Press, 2022.
[51] Swan, M., Blockchain: blueprint for a new economy, O'Reilly, 2015. Ammous, S., The bitcoin standard, Wiley&Sons, 2018.
[56] NCTV, Cybersecuritybeeld 2012, juni 2012. Dit is de tweede openbaar gepubliceerde rapportage, de eerste uit 2011 is niet gepubliceerd.
[52] Modderkolk, H., Het is oorlog maar niemand die het ziet, Podium, 2019.

Ondertussen worden overheden[53], instellingen en bedrijven getroffen door hacks en andere vormen van cybercriminaliteit. De gevolgen van hacks bij de overheid zijn groot. Niet alleen een tijd onbereikbaar te zijn geweest, ook hebben bijvoorbeeld alle bewoners van een gemeente nieuwe identiteitsbewijzen gekregen omdat het systeem met persoonsgegevens was gehackt. Organisaties gaan meer en meer actief communiceren over misbruik van hun gegevens om problemen te voorkomen[54].

Vanuit het perspectief van digitale veiligheid worden in toenemende mate de dilemma's van digitalisering voor de overheid zichtbaar. Enerzijds de overheid als hoeder van de veiligheid van en in de samenleving, gebruikmakend van het geweldsmonopolie, de rechtshandhaving en informatieverstrekking[55], en anderzijds de overheid als slachtoffer of vertegenwoordiger van de samenleving als slachtoffer van cybercriminaliteit. De eerste positie vraagt een actieve opstelling waarbij het cruciaal is te weten wat de grenzen zijn alsmede hoe en door wie deze bewaakt dienen te worden. De tweede positie is eerder reactief en -voor zover mogelijk- preventief van aard.

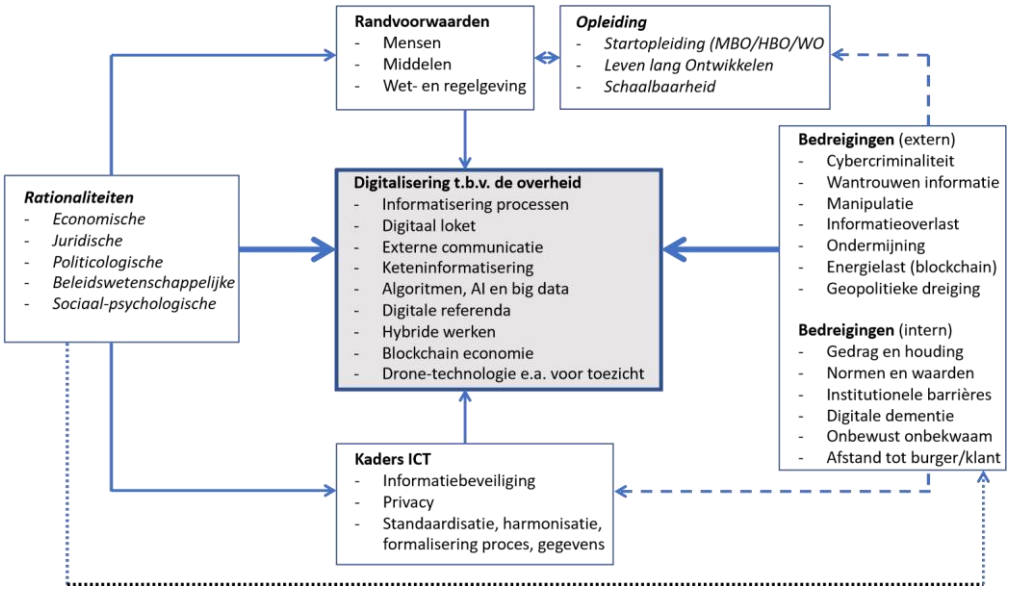
De positie van de overheid krijgt meer kleur en reliëf wanneer de vraagstukken van de overheid m.b.t. de digitalisering in het perspectief wordt geplaatst van de eerder besproken rationaliteiten, de mogelijke bedreigingen (extern en intern), de randvoorwaarden en daaruit afgeleide kaders voor de ICT. Dit geheel leidt tot een indicatief beeld van speelveld voor de overheid. Juist deze rationaliteiten kunnen invloeden en relaties blootleggen, die anders verborgen zouden blijven[56].

[53] Bijvoorbeeld Hof van Twente, Lochem en Buren en de provincie Gelderland. https://decrisismanager.nl/cyberaanvalgemeente-buren-het-was-veel-erger-dan-we-dachten; https://www.gld.nl/nieuws/7642649/privegegevens-inwonersaangeboden-op-darkweb-na-hack-in-gemeentesysteem https://www.binnenlandsbestuur.nl/digitaal/mogelijke-hackpersoneelsgegevens-provincie-gelderland

[54] Zie bijvoorbeeld Nieuwsbericht van de Raad voor de Rechtspraak op 9 augustus 2022 over misbruik van telefoonnummers, sms- en WhatsApp-berichten van rechtbanken, gerechtshoven en bijzondere colleges om geld over te maken.

[55] Zie het oprichten in 2021 van het Digital Trust Center binnen het Ministerie van Economische Zaken en Klimaat ten behoeve van de voorlichting aan bedrijven over digitale veiligheid en de (digitale) weerbaarheid van het bedrijfsleven te vergroten. "Het DTC heeft als missie om 2,0 miljoen Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen. Alles van zzp'ers tot en met het grootbedrijf." Ministerie van EZK, Terugblik Digital Trust Center 2021, 2022.

[56] Zo spreekt Spithoven over een 'black box society'. Het valt niet uit te sluiten dat het gebruik van de rationaliteiten deze black box een stuk transparanter zou maken. Spithoven, R., Verbonden risico's, Boomcriminologie, 2020, p. 127.



Ter toelichting een paar korte observaties en opmerkingen:

- Cybercriminaliteit – uit onderzoek[57] blijken bepaalde vormen van cybercriminaliteit (phishing, hacking, ID-fraude, whatsappfraude etc) bij veel burgers bekend te zijn, maar bepaalde (botnet, social engineering e.a.) slechts in beperkte mate. Door de andere verschijningsvormen heeft dit consequenties voor aanpak en organisatie van de criminaliteitsbestrijding[58];

- Informatiebeveiliging - om veilig online te kunnen werken is een geheel ander gedrag en houding t.a.v. digitale informatie-uitwisseling noodzakelijk[59];

- Privacy – het vraagstuk van de privacy is actueel door de inzet van ICT[65]. De doelbepaling is steeds scherper geformuleerd[60]. De keerzijde is dat het voor handhavings- en opsporingsinstanties steeds lastiger wordt om informatie uit te wisselen, fraudeprofielen op te stellen en trends te signaleren (informatiefunctie)[61] en daarmee de veiligheid in en van de samenleving wordt beoogd te borgen;

- Keteninformatisering – bij de organisatie van veiligheid is reeds gewezen op het belang van digitale ondersteuning van ketens i.p.v. kolommen. Door juist uit te gaan

[57] I&O research, Cybersecurity onderzoek Veilig Online 2021.
[58] Goodman, M., Cybercrime en cyberwar, Karakter, 2018; Wagen, van der, W. e.a. (red), Basisboek cybercriminaliteit, Boomcriminologie, 2020;
[59] Oostveen, R., De digitale epidemie, Haystack, 2020; Baars, H. ea, Basiskennis informatiebeveiliging, Van Haren, 2017; [65] Overkleeft-Verburg, M., De Wet persoonsregistraties, Tjeenk Willink, 1995.
[60] Autoriteit Persoonsgegevens, Jaarverslag 2021, 2022; Roosendaal, A., De informatiefuik, Businesscontact, 2013;
[61] Bantema, W., Black box van gemeentelijke online monitoring : een wankel fundament onder een stevige praktijk, Sdu, 2021; Sloot, B. van der, Deepfakes : de juridische uitdagingen van een synthetische samenleving, Tilburg University, 2021;

van de externe werking van de overheid, ligt keteninformatisering meer voor de hand dan de traditionele organisatie(kolom)gerichte digitalisering;

- Digitale dementie – door de eenduidige afspraken en procedures m.b.t. de archivering van documenten (memo's, rapporten, boeken ed) zijn deze vindbaar en toegankelijk. De snelle ontwikkeling van de digitalisering heeft geleid tot het ontbreken van eenduidige afspraken en procedures m.b.t. het archiveren van digitale producten. De door de Inspectie geuite noodkreet heeft nauwelijks gehoor gevonden[62]. Met de Wet open overheid (voorheen Wet Openbaarheid Bestuur) zal de geconstateerde problemen klemmender worden daar de verplichtingen om documenten beschikbaar te kunnen stellen scherper zijn bepaald[63]. Voor bestuurders is het een (potentieel) risico wanneer zij niet meer kunnen terugvallen op een eenduidig bestuurlijk archief en wel verantwoordelijk zijn voor het (actief) verstrekken van informatie[64];

- Capaciteit en opleiding – er is een groot tekort, kwantitatief en kwalitatief, aan ICTdeskundigen[65]. Dit vraagstuk wordt versterkt door de snel voortschrijdende ontwikkeling van de ICT. Dit vraagt om een andere benadering van medewerkers: die dienen zich continu vanuit het "leven lang ontwikkelen"-concept bij te scholen om met actuele kennis en ervaring een bijdrage aan de gezondheid en continuïteit van de organisatie te leveren.

Wat hier is geschetst, is ook herkenbaar in Suriname. Digitalisering stopt niet bij landsgrenzen en daarmee ook de effecten op veiligheid niet. Dat geldt natuurlijk ook voor de kansen van digitalisering voor de ondersteuning van veiligheid in Suriname.
Voor het lectoraat is digitalisering vooral een vraagstuk ter ondersteuning van veiligheid. Dit valt in twee delen uiteen:

a. het gevolg van digitalisering op veiligheid
b. het ondersteunen van veiligheid met digitaal functionerende producten

[62] Inspectie Overheidsinformatie en Erfgoed, Een dementerende overheod 2.0?, 2021.
[63] Per 1 mei 2022 heeft de Wet open overheid (Woo) de Wet Openbaarheid Bestuur (WOB) vervangen. In de Woo is geen opzet voor de ordening en vindplaatsen van documenten geregeld. Ook niet met terugwerkende kracht. Dit houdt in dat documenten (incl. versiebeheer) uit het zicht verdwijnen, niet meer vindbaar en toegankelijk zijn.
[64] Spitzer, M., Digitale dementie, Olympus, 2017.
[65] Recent onderzoek wijst uit dat een gebrek aan kennis en capaciteit bij de overheid tot grote problemen bij de uitvoering van wetten te leiden. AG Connect; 25 mei 2022.

Hurk, J.W. van der en S.J. de Vries, Onderzoek aan digitale gegevensdragers : een technische en juridische verkenning, Wolters Kluwer, 2021.

Op deze aandachtsgebieden zullen de activiteiten m.b.t. onderwijs, onderzoek en advisering zijn gericht. Het lectoraat kan ook bruggen slaan naar kennisposities[66] op het terrein van digitale veiligheid in Nederland[67].

5.3. Derde uitdaging: volledigheid van wet- en regelgeving m.b.t. veiligheid

Het laatste onderdeel van de piramide is de wet- en regelgeving. De vraag die opkomt is: hoe weten we of de wet- en regelgeving voldoende is?[68] Dat is de derde uitdaging die ik de revue wil laten passeren. Dit doe ik aan de hand van arbeidsveiligheid.

> *Voorbeeld: COVID-19*
> *Velen zullen bij arbeidsveiligheid snel een link leggen met de recente COVID-19 pandemie en de impact op het arbeidsproces. We hebben gezien hoe het Corona-virus heeft geleid tot een mondiale beweging om zo veel mogelijk hybride te gaan werken. In alle sectoren, ook in het onderwijs. Voor landen, die minder een traditie hebben met afstandsonderwijs, zoals Nederland, betekende dit een enorme omschakeling. Uit eigen ervaring[69] kan ik constateren dat een organisatie in uitzonderlijke situaties tot grootse prestaties in staat is: in één lang weekend gingen we over van volledig fysiek naar volledig digitaal onderwijs door 3.000 docenten aan 26.000 studenten. Voor docenten betekende dit een geweldige omschakeling: de kennisoverdracht door direct contact werd vervangen door contact via beeldschermen. De continuïteit van het onderwijs geven stond voorop.*
> *De onderliggende wet- en regelgeving verliep moeizaam[70]. Het bleek lastig te zijn om voor deze situatie wet- en regelgeving te formuleren, die op voldoende politiek draagvlak kon rekenen èn de regering voldoende ruimte bood om alert en adequaat in te kunnen grijpen. De volledigheid van de wet- en regelgeving was door de onbekendheid met de impact niet op voorhand goed te bepalen. Deze pandemie is gelukkig een uitzonderlijke situatie.*

[66] Een belangrijke ontwikkeling is de oprichting van het Centrum voor Veiligheid en Digitalisering (CVD) in Apeldoorn. Dit is een samenwerkingsverband van de Hogeschool Saxion, de Universiteit Twente, de Politieacademie en de gemeente Apeldoorn. Andere partners zijn Nederlands Instituut voor Publieke Veiligheid (NIPV, voorheen Instituut Fysieke Veiligheid (brandweer, CHOR, veiligheidsregio's)), ROC Aventus, Belastingdienst, Kmar, Achmea, Kadaster, Saab Technologies ea anderen. Het doel van het CVD is het realiseren van innovatief onderwijs, incl. nieuwe concepten voor Leven Lang Ontwikkelen op de werkplek en het doen van gezaghebbend onderzoek. De samenwerkende partijen willen door de unieke combinatie en ambitie nationale impact realiseren.

[67] Sedert enige jaren vindt er samenwerking plaats tussen PTC en Saxion. Dat is versterkt met de ondertekening van de Intentieverklaring op 19 november 2019 in Amsterdam.

[68] De Raad van State hanteert een vast toetsingskader met drie elementen: beleidsanalytische toets, juridische toets en wetstechnische toets. De derde uitdaging richt zich op het eerste element. (wat is het probleem, wordt het effectief en efficiënt opgelost en is het uitvoerbaar, handhaafbaar en voor burgers en bedrijven hanteerbaar (doenvermogen)).

[69] Academiedirecteur bij Saxion Hogeschool.

[70] Prins, C., Corona & langetermijnstrategie: afscheid van juridische lapmiddelen, NJB, 2021 nr. 44. Raad van State, Adviesaanvraag verlenging per 1 maart 2022 van de Tijdelijke wet maatregelen covid-19, 16 februari 2022.

Arbeidsveiligheid is belangrijk voor een gezonde economie. Het voorkomen van ziekte en arbeidsongevallen is goed voor werknemer en werkgever. In de toelichting van de Arbeidsomstandighedenwet, die in 2019 bij het Surinaamse parlement is ingediend, staat dit helder verwoord.

> *"Werkgevers, werknemers en overheid hebben een groot en gemeenschappelijk belang bij goede arbeidsomstandigheden. Gezond personeel draagt ook bij aan een bedrijf met hogere arbeidsproductiviteit en concurrentievermogen. Een goed arbeidsomstandighedenbeleid is een belangrijke factor bij het terugdringen van verzuim en arbeidsongeschiktheid. De veranderde opvatting is dat de primaire verantwoordelijkheid voor goede arbeidsomstandigheden ligt binnen de ondernemingen, dus een aangelegenheid is primair van de werkgevers en de werknemers."*[71]

Hoewel hierin nadrukkelijk wordt gesproken over de verantwoordelijkheid van werkgever en werknemer, is er een cruciale rol weggelegd bij de overheid voor de benodigde wet- en regelgeving t.b.v. de normstelling. Daar horen toezicht en handhaving bij[72]. Uitgangspunt is dat een werkgever[73] oog heeft voor risico's voor zijn werknemers en deze risico's wegneemt[74].

In het licht van de volledigheid van wet- en regelgeving plaats ik graag vier opmerkingen die het vraagstuk accent geven.

1. Reikwijdte: is de wet- en regelgeving zo opgezet dat deze is toegesneden op alle sectoren? Gezien de optimistische berichten over olievondsten op zee zal de sector mijnbouw incl. de offshore-bedrijven te maken krijgen met een impuls op de werkgelegenheid. De vraag is of de huidige wet- en regelgeving is ingespeeld op deze nieuwe arbeidssituatie en de daarmee samenhangende accenten m.b.t. de arbeidsveiligheid. Daarbij is het belangrijk helder te zijn welke regels er gelden indien buitenlandse maatschappijen aan de slag zullen gaan. T.a.v. de binnenlandse mijnbouw zijn er ook signalen[75] dat de arbeidsveiligheid eenduidige wet- en regelgeving kan gebruiken.

[71] Arbeidsomstandighedenwet 2019, door de Surinaamse regering ingediend op 25 april 2019 bij De Nationale Assemblée.
[72] Ruimschotel, D., Goed toezicht, Mediawerf, 2014.
[73] In de praktijk blijkt dit minder van zelfsprekend dan men zou verwachten. Er kunnen overwegingen uit de economische, technologische en/of juridische rationaliteit zijn die een werkgever weerhouden om uit eigen initiatief te komen tot maatregelen om de werksituatie zo in te richten, dat die volgens algemene maatstaven, als "gezonde" werkomgeving kan worden bestempeld.
[74] Heck, M., Arbeid en veiligheid, in: W. Stol e.a., Basisboek integrale veiligheid, Boomcriminologie, 2016. Hierin komen onder meer instrumenten als de RI&E (Risico-inventarisatie en -evaluatie), Ontruimingsplan en BHV (bedrijfshulpverleningsorganisatie) aan de orde.
[75] Heemskerk, M., Kleinschalige goudwinning in Suriname, CEDLA, 2009; Trommelen, J., Gowtu, Conserve, 2013. [82] Algemeen Bureau voor de Statistiek, Statistisch Jaarboek 2017/2018 Suriname, 2019 en Statistisch Jaarboek 2019 Suriname, 2020.

2. Dark number: wat zien we niet? Als we kijken naar de statistieken m.b.t. de ongevallen[82], dan kunnen we een eerste beeld halen over het aantal bedrijfsongevallen en het aantal verloren mandagen. Bij dergelijke cijfers is het belangrijk te realiseren dat dit het feitelijk geregistreerde aantal betreft. Datgene, dat niet is geregistreerd, kennen we niet. Veelal wordt gesproken over het "dark number", het aantal dat wel heeft plaatsgevonden, maar we niet kennen.

Jaar	**2016**	**2017**	**2018**	**2019**
Aantal ongevallen	887	780	862	751
Verloren mandagen	74.420	49.044	64.114	110.935
Aard				
- Niet ernstig	697	637	682	577
- Matig	108	81	102	98
- Ernstig	69	47	72	62
- Dodelijk	9	7	6	14

Bron: Algemeen Bureau voor de Statistiek 2019, 2020.

Dit fenomeen van het dark number is vooral interessant voor de sectoren waar dit voorkomt en de mate waarin. Daar ligt een opgave voor wet- en regelgeving om onvoldoende registratie van ongevallen tegen te gaan. Dit kan met heldere normstelling, toezicht en handhaving. (In de bijlage is een overzicht gegeven van de arbeidsplaatsen per sector).

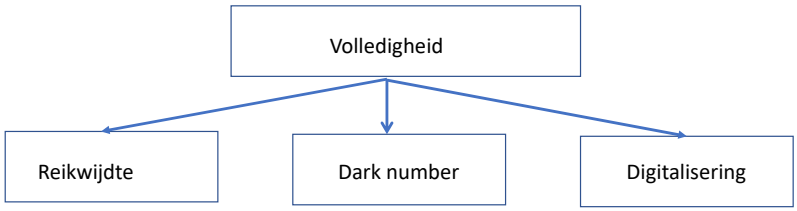
3. Digitalisering: biedt in het algemeen voor het efficiënter maken van bedrijfsprocessen. Dat kan aanleiding geven tot het actualiseren van wet- en regelgeving[76] m.b.t. de arbeidsomstandigheden. Digitalisering kan ook aanpassingen van de bestaande arbeidssituatie initiëren -al dan niet met wet- en regelgeving- indien negatieve beelden over arbeidsveiligheid online beschikbaar komen. Voor werkgevers kunnen deze beelden reputatieschade opleveren, werknemers blijven weg en kopers kunnen via hun koopgedrag[77] hun steun[78] of afkeuring kenbaar maken over de arbeidsomstandigheden.

   Een aanvullende opmerking bij digitalisering van geheel andere aard: privacy. In een recent verschenen dissertatie memoreert Chotoe[79] dat in 2017 de Wet Elektronisch Rechtsverkeer door het parlement (DNA) is aangenomen, maar dat t.a.v. de bescherming van de persoonsgegevens er wettelijk nog niets is geregeld. Terwijl de behoefte hieraan

[76] European Agency for Safety and Health at Work, Artificial Intelligence for worker management: an overview, 2022.
[77] ASN Bank, ASN Bank & Living wages in Garments: the 2020 overview, 2021.
[78] Zie bijvoorbeeld Tony's Chocolonely. Dit beeld wordt bewust als asset geframed. Smit, J. Het grote gevecht, Prometheus, 2019.
[79] Chotoe, M.M., Het recht op privacy in de arbeidsrelatie in Suriname (diss), Universiteit Utrecht, 2020. In haar dissertatie bespreekt Chotoe het concept-wetsvoorstel Bescherming Privacy en Persoonsgegevens in Suriname (2019). Interessant is de beoordeling van het maatschappelijke draagvlak en de uitvoerbaarheid van het voorstel.

door de snelle ontwikkeling van de ICT toeneemt. Het ontbreken van goede privacyspelregels kan resulteren in situaties, waarin de veiligheid van personen onder druk staat. Dit kan ook binnen organisaties plaatsvinden, waardoor het de arbeidsveiligheid raakt.

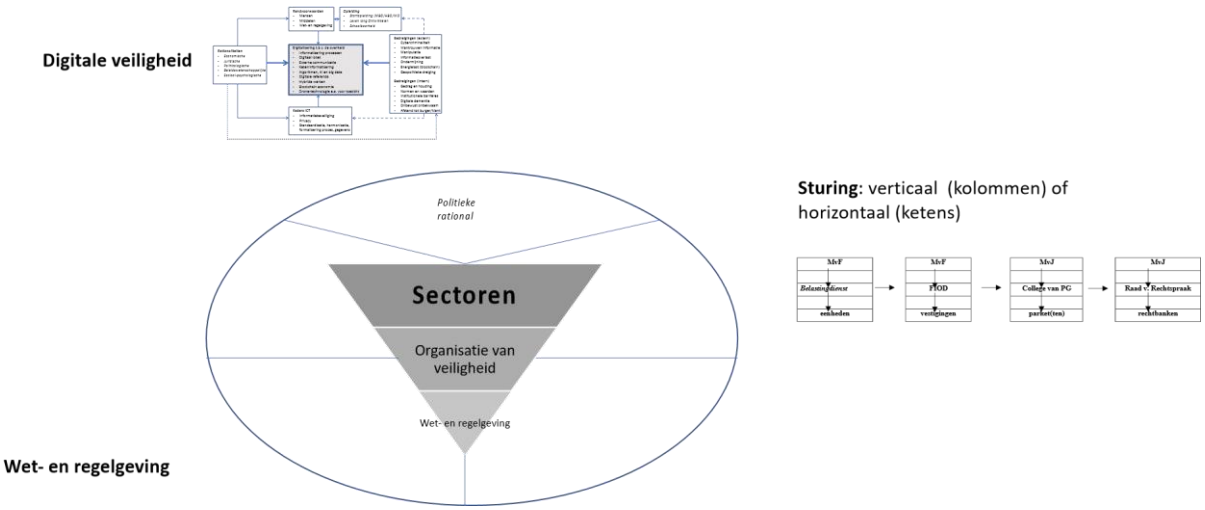
Het is duidelijk dat de volledigheid van wet- en regelgeving, gerelateerd aan bijvoorbeeld arbeidsveiligheid, een dynamisch terrein is binnen het lectoraat, dat interessant is voor onderwijs en onderzoek.



6. Slot

In het voorgaande is een beeld geschetst van het lectoraat Veiligheid en Digitalisering. Onderweg zijn diverse bouwstenen gepresenteerd. Deze bouwstenen moeten leiden tot een hecht kennis-fundament voor activiteiten ten behoeve van onderwijs en onderzoek binnen PTC en advisering vanuit PTC alsmede het aangaan van samenwerkingsverbanden binnen Suriname en, waar gewenst, met Nederlandse kennisinstellingen en andere organisaties.

De opdracht voor het lectoraat is ambitieus en uitdagend. Voor de lector, en hopelijk ook de studenten, medewerkers en externe belangstellenden. Het lectoraat kent het motto: samen kunnen we maatschappelijke vraagstukken beter begrijpen en oplossen. Hopelijk is vandaag de eerste gezamenlijke stap gezet.



Literatuur

- AG Connect; 25 mei 2022.
- Ammous, S., The bitcoin standard, Wiley&Sons, 2018.
- Algemeen Bureau voor de Statistiek, Statistisch Jaarboek 2017/2018 Suriname, 2019 en Statistisch Jaarboek 2019 Suriname, 2020.
- ASN Bank, ASN Bank & Living wages in Garments: the 2020 overview, 2021.
- Autoriteit Persoonsgegevens, Jaarverslag 2021, 2022; Roosendaal, A., De informatiefuik, Businesscontact, 2013;
- Baars, H. ea, Basiskennis informatiebeveiliging, Van Haren, 2017;
- Bantema, W., Black box van gemeentelijke online monitoring : een wankel fundament onder een stevige praktijk, Sdu, 2021.
- Beeten, J. Van de en R.H. Van de Beeten, Driemaal is (geen) scheepsrecht? NJB, nr. 10 2021.
- Binnenlands Bestuur, Mogelijke hack persoonsgegevens Gelderland, 24 augustus 2021.
- Bos, K. van den en A.F.M. Brenninkmeijer, Vertrouwen in wetgeving, de overheid en de rechtspraak, NJB, nr. 21 2012.
- Bosaltlas van de veiligheid, Noordhoff, 2017.
- Brenninkmeijer, A.F.M., Moreel leiderschap, Prometheus, 2020.
- Brenninkmeijer, A.F.M., De grondbeginselen van de rechtsstaat zijn ‘geschonden’ als ‘verschrikkelijk ongeluk’, NJB, nr. 1 2021.
- Brink, G. Van den en Th. Jansen, Ambtelijk vakmanschap en moreel gezag, Stichting Beroepseer, 2016.

- Buchanan, B., The hacker and the state, Harvard University Press, 2020.
- Chotoe, M.M., Het recht op privacy in de arbeidsrelatie in Suriname, Universiteit Utrecht, 2020.
- Coalitieakkoord 2021, Omzien naar elkaar, vooruitkijken naar de toekomst (Coalitieakkoord 2021-2025 VVD, D66, CDA, CU), 15 december 2021.
- Crawford, K., Atlas of AI, Yale University Press, 2022.
- DeCrisismanager, Cyberaanval gemeente Buren: 'Het was veel erger dan we dachten', 19 september 2022.
- Docters van Leeuwen, A.W.H., Een spoor van vernieuwing, Prometheus, 2020.
- Eeden, van den, C.A.J. e.a., Opsporen, vervolgen en tegenhouden van cybercriminaliteit, WODC 2021-23, 2001.
- European Agency for Safety and Health at Work, Artificial Intelligence for worker management: an overview, 2022.
- Fredrik, J. Zo hadden we het niet bedoeld, De Correspondent, 2021.
- Gelderlander, De, Streep door 1500 strafzaken: te weinig rechters bij rechtbank Gelderland, 16 juni 2022.
- Gerechtshof Den Haag, Uitspraak op 1 februari 2022 (ECLI:NL:GHDHA:2022:104).
- Goodman, M., Cybercrime en cyberwar, Karakter, 2018.
- 't Hart, P. en M. ten Hooven, Op zoek naar leiderschap, De Balie, 2004.
- Heck, M., Arbeid en veiligheid, in: W. Stol e.a., Basisboek integrale veiligheid, Boomcriminologie, 2016.
- Heemskerk, M., Kleinschalige goudwinning in Suriname, CEDLA, 2009.
- Hirsch Ballin, E.H.M., Waakzaam burgerschap, Vertrouwen in democratie en rechtsstaat herwinnen, Querido Facto, 2022.
- Hoefnagel, F.J., De veertien wetsfamilies, Bestuurswetenschappen, maart/april 1977, nr. 2.
- Hoogerwerf, A. (red), Overheidsbeleid, Samsom, 1980.
- Horrevorts, T. en R. Pans, Presterende bestuurders, Sdu, 2010.
- Hurk, J.W. van der en S.J. de Vries, Onderzoek aan digitale gegevensdragers: een technische en juridische verkenning, Wolters Kluwer, 2021.
- I&O research, Cybersecurity onderzoek Veilig Online 2021.
- Inspectie Overheidsinformatie en Erfgoed, Een dementerende overheid 2.0?, 2021.
- Interdepartementale Commissie voor de Beleidsanalyse (COBA); in: Commissie Hoofdstructuur Rijksdienst, Bijlage bij Achtergrondstudie 6, BiZa, 1981.
- Kenniscentrum voor beleid en regelgeving, Integraal afwegingskader voor beleid en regelgeving (website).
- Khonraad, S., Integrale veiligheid als reflexieve praktijk, Avans, 2011.
- Klous, S. en N. Wielaard, Vertrouwen in de slimme samenleving, Business Contact, 2017.
- Kokkeler, B., Smart public safety, Avans, 2017.
- Kom, A. de, Wij slaven van Suriname, Atlascontact, 2020.
- Kolthoff, E., Integriteit, mensenrechten en veiligheidsmythe, Avans, 2010.
- Leukfeldt, E.R., De 'human' factor in cybersecurity, De Haagse Hogeschool, 2018.
- Liempt, P. van, Misdaad en straf in de polder, Het OM aan het woord, Prometheus, 2022.
- Mayer-Schönberger en K. Cukier, Big Data, John Murray, 2013.
- Mazzucato, M., De ondernemende staat, Nw Amsterdam, 2015.
- Ministerie van EZK, Terugblik Digital Trust Center 2021, 2022.
- Ministerie van Justitie en Veiligheid/directie strafrechtketen, Ketenplan van aanpak, 2018.
- Ministerie van Justitie en Veiligheid, Bestuurlijk Ketenberaad, Actieplan strafrechtketen, 6 november 2020.
- Minister van Justitie en Veiligheid, Brief aan Tweede Kamer, Integrale aanpak van online fraude, 8 juli 2022.
- Mintzberg, H., The structuring of organizations, Prentice-Hall, 1979.
- Modderkolk, H., Het is oorlog maar niemand die het ziet, Podium, 2019. - NCTV, Cybersecuritybeeld 2012, juni 2012.
- NTCV, Nationale veiligheid strategie, 2019
- NTCV, Rijksbrede risicoanalyse nationale veiligheid, 2022.
- Omroep Gelderland, Privégegevens inwoners aangeboden op darkweb na hack in gemeentesysteem, 20 april 2022.
- Oostveen, R., De digitale epidemie, Haystack, 2020.
- Otte, M., Een kleine biografie van het straffen, Boomjuridisch, 2018.
- Overkleeft-Verburg, M., De Wet persoonsregistraties, Tjeenk Willink, 1995.
- Parlementaire ondervragingscommissie Kinderopvangtoeslag, Ongekend onrecht (eindverslag), 17 december 2021.
- Passchier, R., Artificiële intelligentie en de rechtsstaat, Boomjuridisch, 2021.
- Prins, C., Corona & langetermijnstrategie: afscheid van juridische lapmiddelen, NJB, 2021 nr. 44.
- Programma Digitalisering Strafrechtketen, Halfjaarrapportage, 29 juli 2021.
- Putters, K., Veenbrand, smeulende kwesties in de welvarende samenleving, Prometheus, 2019.

- Raad van State, Lessen uit de kinderopvangtoeslagzaken, november 2021.
- Raad voor de Rechtspraak, Brief aan Minister voor Rechtsbescherming, Reset digitalisering van de Rechtspraak (KEI), 10 april 2018.
- Raad voor de Rechtspraak, Nieuwsbericht, 9 augustus 2022.
- Raad van State, Adviesaanvraag verlenging per 1 maart 2022 van de Tijdelijke wet maatregelen covid-19, 16 februari 2022.
- Reiling, D., Technology for Justice, how information technology can support judicial reform, Leiden University Press, 2010.
- Rosenthal, U., A.H.W. Docters van Leeuwen, M.J.G. van Eeten en M.J.W. van Twist, Ambtelijke vertellingen, Lemma, 2001.
- Rovers, E., Nu is het aan ons, De Correspondent, 2022.
- Ruimschotel, D., Goed toezicht, Mediawerf, 2014.
- Rutte, M., Rede in De Nationale Assemblée, 13 september 2022.
- Santokhi, Ch., Jaarrede 2022 President van Suriname, 1 oktober 2021
- Sloot, B. van der, Deepfakes : de juridische uitdagingen van een synthetische samenleving, Tilburg University, 2021.
- Smit, J. Het grote gevecht, Prometheus, 2019.
- Snellen, I.Th.M. e.a., Technology assessment van het openbaar bestuur, Sdu, 1988.
- Snellen, I.Th.M., Boeiend en geboeid, Samsom Tjeenk Willink, 1987.
- Spithoven, R., Verbonden risico's, Boomcriminologie, 2020.
- Spitzer, M., Digitale dementie, Olympus, 2017.
- Swan, M., Blockchain: blueprint for a new economy, O'Reilly, 2015.
- Stol, W., Cybersafety overwogen, Boom, 2010.
- Stol, W., Essenties van politiewerk en digitalisering, Strafblad nr. 1, Sdu, 2019.
- Tjeenk Willink, H.D., Kan de overheid crises aan? Prometheus, 2021;
- Thomas, M.S. e.a., Snel, Betekenisvol en Zorgvuldig, Een tussenevaluatie van de ZSM-werkwijze, Boomjuridisch, 2016.
- Tops, P. en J. Tromp, De achterkant van Nederland, Balans, 2017.
- Trommelen, J., Gowtu, Conserve, 2013.
- Wagen, van der, W. e.a. (red), Basisboek cybercriminaliteit, Boomcriminologie, 2020.
- Weber, M., Wirtschaft und Gesellschaft, Mohr, 1985.
- Westra, R.L.N., Fiscale fraudebestrijding: grenzen aan sturing, Pantheon, 2006.
- Westra, R.L.N. en G.J.C.M. Bakker, Big data en rechtshandhaving; hype of hoop?, BISC nr. 5, Cahiers Inlichtingenstudies (België), Maklu, 2015.
- Westra, R.L.N. en G.J.C.M. Bakker, De overheidsmanager van de toekomst, M&O nr. 3, 2019.
- Wetenschappelijke Raad voor het Regeringsbeleid, Doelmatigheid van rechtsvervolging, (W35), 1988.
- Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid (nr. 86), Amsterdam University Press, 2011.
- Wetenschappelijke Raad voor het Regeringsbeleid, Vertrouwen in burgers, 2012.
- Wetenschappelijke Raad voor het Regeringsbeleid, Politiefunctie in een veranderende omgeving, 2021;

Bijlage. Arbeidsplaatsen per sector

Sector	2012	2013	2014	2015	2016	2017

Landbouw, Veeteelt en Bosbouw en Visserij	10,200	10,800	10,900	10,400	10,100	9,900
Mijnbouw + Industrie	23,700	23,100	23,800	19,500	17,800	17,600
Elektriciteit, Gas en Water	2,500	2,700	2,800	2,900	3,200	3,000
Constructie	19,900	20,900	20,400	19,600	17,600	21,500
Handel	28,200	28,700	29,300	29,100	27,000	27,100
Hotels en Restaurants	7,000	7,300	7,600	7,500	7,600	7,800
Transport en Communicatie	14,800	15,500	15,300	15,200	14,100	14,400
Financiële Instellingen	4,900	5,000	5,200	5,300	6,100	6,200
Zakelijke diensten	9,700	9,400	10,000	8,500	8,600	8,800
Onderwijs	700	800	800	900	900	1,000
Gezondheidszorg	3,700	3,700	3,900	4,100	4,000	4,500
Overige gemeenschaps- , sociale en persoonlijke diensten	17,200	17,600	16,600	17,200	15,900	17,400
Subtotaal -1	142,500	145,500	146,600	140,200	132,900	139,200
Sector Overheid COFOG Landbouw, Veeteelt en Bosbouw	1,200	1.200	1,100	1,400	1,400	1,400
Elektriciteit, Gas en Water	600	600	600	700	600	600
Constructie	400	400	400	300	400	300
Transport en Communicatie	900	900	900	1,500	1,400	1,400
Public administration	21,000	21,200	21,100	24,800	24,100	24,200
Onderwijs	16,700	17,000	17,200	17,600	18,200	17,800
Gezondheidszorg	11,800	12,000	12,200	12,800	11,200	12,100
Subtotaal -2	52,600	53,300	53,500	59,100	57,300	57,800
Totaal arbeidsplaatsen	195,100	198,800	200,100	199,300	190,200	197,000

Bron: Arbeidsstatistieken van het Statistiekbureau in Suriname (ABS) 2012-2017, 2018[80]

[80] In dit overzicht staat het aantal arbeidsplaatsen. Dit is niet hetzelfde als het aantal werknemers; één werknemer kan meerdere arbeidsplaatsen innemen.