Het recht van de toekomst: Technologieontwikkeling bezien vanuit het recht & Het recht bezien vanuit technologieontwikkeling

Custers, B.H.M.

Prof.mr.dr.ir. Bart H.M. Custers

Prof. mr. dr. ir. B.H.M. (Bart) Custers is hoogleraar Law and Data Science en directeur van eLaw, het centrum voor recht en digitale technologie aan de Faculteit der Rechtsgeleerdheid van de Universiteit Leiden. Hij heeft een achtergrond in rechten en technische natuurkunde en is expert op het gebied van recht en digitale technologie, onder meer op onderwerpen als profiling, big data, privacy, discriminatie, cybercrime, opsporingsbevoegdheden en kunstmatige intelligentie. Hij is een ervaren onderzoeker en projectleider die in opdracht van de Europese Commissie, NWO en verschillende ministeries en bedrijven contractonderzoek uitvoerde. Tot 2016 was hij hoofd van de onderzoeksafdeling Criminaliteit, Rechtshandhaving en Sancties van het Wetenschappelijk Onderzoekscentrum (WODC) van het ministerie van Veiligheid en Justitie. Daarvoor was hij werkzaam voor de rijksoverheid als senior beleidsadviseur voor opeenvolgende ministers van justitie (2009-2013) en in het bedrijfsleven als senior management consultant voor informatiestrategieën (2005-2009).

Bart Custers heeft tot dusver zeven boeken op zijn naam staan: vier boeken over profiling, privacy, discriminatie en big data, twee boeken over het gebruik van drones en een boek over het gebruik van bitcoins bij het witwassen van cybercrime. Regelmatig verzorgt hij lezingen over onder meer profiling en privacy bij nieuwe technologische ontwikkelingen. Hij presenteert zijn werk op internationale congressen in de Verenigde Staten, Canada, China, Japan, Korea, Afrika, het Midden-Oosten en Europa. Hij publiceert zijn werk, inmiddels meer dan honderd publicaties, in wetenschappelijke tijdschriften, vakbladen en kranten. Privé is hij een fervent reiziger en heeft hij meer dan honderd landen bezocht. Hij woont in Gouda met zijn vrouw en hun vier kinderen.

Universiteit Leiden

Prof.mr.dr.ir. Bart H.M. Custers

Het recht van de toekomst

Technologieontwikkeling bezien vanuit het recht

&

Het recht bezien vanuit technologieontwikkeling

Universiteit Leiden

Bij ons leer je de wereld kennen

Het recht van de toekomst

Technologieontwikkeling bezien vanuit het recht

&

Het recht bezien vanuit technologieontwikkeling

Oratie in verkorte vorm uitgesproken door

prof.mr.dr.ir. Bart H.M. Custers

Bij de aanvaarding van het ambt van hoogleraar Law and Data Science

aan de Universiteit Leiden

op 21 mei 2021

Universiteit
Leiden

Inhoud

1. Inleiding

Mevrouw de rector magnificus, geacht faculteitsbestuur, zeer gewaardeerde toehoorders,

Het doen van voorspellingen is buitengewoon lastig, vooral als het de toekomst betreft. Deze uitspraak wordt toegeschreven aan de beroemde natuurkundige Niels Bohr.[1] Toch proberen we steeds weer in te schatten wat de toekomst ons zal brengen, zodat we ons daarop kunnen voorbereiden. Door steeds grotere hoeveelheden beschikbare gegevens en de toenemende kracht van datagedreven analysemethodes kunnen we steeds beter voorspellen hoe de toekomst eruit zal zien. Uiteraard geven resultaten uit het verleden geen absolute garanties voor de toekomst, maar met de hulp van technologie worden we er steeds beter in.

Maar er is ook een andere reden waarom we meer over de toekomst na zouden moeten denken dan we soms doen. Een van de beste manieren om de toekomst te voorspellen is namelijk het zelf vormgeven van die toekomst. Via de huidige technologische ontwikkelingen zijn we daar hard mee op weg: technologie is tegenwoordig alom aanwezig, in onze telefoons, huizen, auto's en op straat.

Een paar decennia geleden hadden we nog geen internet, smartphones, gps-navigatie en sociale media. Nu kunnen we altijd en overal online zijn. Wie had een paar decennia geleden kunnen voorspellen dat we nu over al deze technologie zouden kunnen beschikken? Alleen als je veel naar Science Fiction films zou kijken, zou je misschien een idee hebben gehad. Dat roept de vraag op over welke nieuwe technologie we de komende decennia kunnen beschikken.

Ik ben geen futuroloog en het is misschien gewaagd om hier en nu te voorspellen hoe de toekomst eruit zal zien, maar een paar zaken zijn wel met grote waarschijnlijkheid te voorspellen. Zo zal ons vervoer de komende decennia enorm veranderen. De meeste volwassenen hebben nu nog een rijbewijs en naar verwachting zullen onze kinderen ook nog wel hun rijbewijs halen. Maar onze kleinkinderen zullen zeer waarschijnlijk nooit meer een rijbewijs hoeven behalen, omdat zij zullen leven in een tijdperk van zelfrijdende auto's. Sterker nog, zij zullen waarschijnlijk niet eens een rijbewijs mogen halen, omdat menselijke chauffeurs een gevaar op de weg zijn in vergelijking met zelfrijdende auto's.

Een andere, iets gewaagdere[2] voorspelling is dat over een paar generaties het onderwijs in vreemde talen er heel anders uit komt te zien. Het vertalen van teksten is nu al goed mogelijk met allerlei software. Het vertalen van gesprekken is nog wat lastiger, maar zal over niet al te lange tijd ook goed mogelijk zijn. Dit kan vervolgens worden ingebouwd in telecommunicatie en in hoorapparaatjes, zodat alles simultaan vertaald kan worden. In hetzelfde gesprek kan de een dan zijn eigen taal spreken en de ander zijn eigen taal luisteren. Waar een menselijke tolk slechts tussen een paar talen kan vertalen, kan deze software tussen honderden talen vertalen.

Andere ontwikkelingen die we tegemoet kunnen zien, zijn oprolbare schermen voor telefoons, kranten en tv's, het verbeteren van het menselijk lichaam met mechanische technologie en cognitieve vaardigheden, het gebruik van drones voor het vervoer van cargo en passagiers,[3] deepfakes die de publieke opinie vergaand manipuleren[4] en het steeds verder personaliseren van de geneeskunde. En dat zijn slechts enkele voorbeelden. We weten dat technologische groei exponentieel gaat, dus in zekere zin staan we pas aan het begin.[5]

Als we over een paar decennia terugkijken op technologische ontwikkelingen, is de kans groot dat we twee typen technologie kunnen onderscheiden.[6] Enerzijds is dat technologie die eeuwenoude problemen van mensen adresseert, zoals ziekte, armoede en conflict. Dit noem ik probleemoplossende of *retrospectieve technologieontwikkeling*, waarbij het gaat om gedeelde problemen van mensen, menszijn en de mensheid. Deze aan-

pak is in zekere zin retrospectief, want gericht op bestaande, bekende problemen. Anderzijds zal er steeds meer aandacht komen voor technologie die invulling geeft aan (soms excentrieke) wensen die mensen hebben om boven hun menszijn uit te stijgen, waardoor ze mooier, sneller en slimmer worden. Dit noem ik toekomstgerichte, *prospectieve technologieontwikkeling*. Daarbij kan gedacht worden aan genetische manipulatie, cognitieve implantaten, het vervangen van lichaamsdelen door robotica[7] of manipulatietechnologie. In een multipolaire, multiculturele wereld zal deze vorm van technologieontwikkeling afhankelijk zijn van uiteenlopende normatieve kaders voor wat 'verbetering' is. Deze aanpak is prospectief, want gericht op beelden en verwachtingen van de toekomst. Naarmate meer bestaande problemen van de mensheid worden opgelost, zal prospectieve technologieontwikkeling aan belang winnen. Daarbij moeten we ons realiseren dat zulke technologie mogelijk alleen exclusief beschikbaar zal zijn voor degenen die het zich kunnen veroorloven.[8] Bovendien is retrospectieve technologieontwikkeling beter te voorspellen dan prospectieve technologieontwikkeling die immers alle kanten op kan gaan.

Veel van deze technologie is gebaseerd op twee zaken: enerzijds grote hoeveelheden beschikbare gegevens en anderzijds de enorm geavanceerde analysemethoden. De grote hoeveelheden gegevens, ook wel big data genoemd, zijn afkomstige van onszelf, bijvoorbeeld door wat we online zetten of met elkaar communiceren via telefoons en sociale media, en van allerlei sensoren, zoals online trackers en sensoren in onze smartphones. Deze gegevens zijn zeer omvangrijk, komen doorgaans in verschillende formaten, zoals tekst, audio en video, en zijn vaak ook nog real-time.

De hoeveelheden gegevens zijn enorm en niet goed door mensen te overzien en doorzien, vandaar dat geavanceerde analysemethoden nodig zijn. Hier komen we in het domein van data mining, machine learning en kunstmatige intelligentie. Deze technologie wordt onderzocht en ontwikkeld in het vakgebied dat we data science noemen.[9]

In deze lezing zal ik ingaan op het snijvlak van recht en data science, de opdracht van mijn leerstoel. De keuzes die we nu maken op het vlak van technologieontwikkeling bepalen hoe onze samenleving, onze toekomst, er straks uit zal zien. Dat zijn normatieve keuzes, waarin normatieve disciplines zoals recht en ethiek een belangrijke rol kunnen en zouden moeten spelen. Ik zal laten zien hoe deze ontwikkelingen vrijwel alle belangrijke rechtsgebieden raken en ook de rechtspraktijk en juridisch onderzoek beïnvloeden. Ik zal laten zien dat het recht op veel onderdelen nog niet klaar is voor deze ontwikkelingen, maar dat we tegelijkertijd het recht hard nodig zullen hebben.

Eerst zal ik ingaan op de regulering van deze technologische ontwikkelingen in data science die mogelijk nodig is om alles in goede banen te leiden. Hiertoe zal ik verschillende rechtsgebieden uit zowel het publiekrecht als het privaatrecht bespreken. Daarna zal ik ingaan op de vraag in hoeverre ontwikkelingen in data science ook kunnen worden ingezet als onderzoeksmethoden voor juridisch onderzoek en de rechtspraktijk.

2. Regulering van data science

Bij de bespreking van het reguleren van data science zal ik de belangrijkste rechtsgebieden een voor een nalopen en onderzoeken welke uitdagingen er zoal zijn. Daarbij zal ik het klassieke rechtsencyclopedische onderscheid in verschillende rechtsgebieden volgen. Enerzijds is er het publiekrecht, dat de verhoudingen tussen overheid en burgers regelt en anderzijds is er het privaatrecht dat de verhoudingen tussen burgers onderling regelt.

2.1 Publiekrecht

In het publiekrecht zijn voor data science de belangrijkste rechtsgebieden het staatsrecht (waarbij ik vooral zal ingaan op grondrechten),[10] het bestuursrecht en het strafrecht.

2.1.1 Grondrechten[11]

Staatsrechtelijk is het van belang de grondrechten van burgers te bezien in het licht van de ontwikkelingen op het gebied van data science. In Nederland is een recht op briefgeheim en telefoon- en telegraafgeheim geregeld in de grondwet. Deze grondwet dateert van 1814 en is het laatst gewijzigd in 1983. Als gevolg daarvan zijn veel bepalingen geschreven in een tijd ruim vóór het internettijdperk. Dat roept de vraag op of en hoe deze grondrechten kunnen worden toegepast op nieuwe technologie. Bijvoorbeeld e-mail en Whatsapp hebben grotendeels brieven vervangen en Skype, Zoom en Teams zijn alternatieven voor bellen. Bij een grammaticale interpretatie ('de letter van de wet') zouden het brief- en telefoongeheim niet van toepassing zijn, maar bij een teleologische interpretatie ('de geest van de wet') mogelijk wel. Dit is ambigu, vandaar dat de wetgever de grondwet wilde aanpassen en het brief-, telefoon- en telegraafgeheim wilde vervangen door een brief- en telecommunicatiegeheim. Dit voorstel werd in 2017 in eerste lezing door het parlement geloodst, maar voor een grondwetswijziging is ook een tweede lezing nodig en die heeft tot op heden nog niet plaatsgevonden. Kortom, tot op heden is de grondwettelijke bescherming van e-mail, Whatsapp, Skype, Zoom en Teams in Nederland niet helder geregeld.

Het bij de tijd brengen van grondrechten blijkt dus al een moeilijke klus. Doordat de discussie zich vooral richt op de vraag hoe we huidige grondrechten moeten aanpassen, is er weinig ruimte voor discussie over welke grondrechten we überhaupt zouden moeten hebben in het digitale tijdperk. Voor sommige digitale rechten bestaat immers geen echt equivalent uit het pre-digitale tijdperk.

Zouden we bijvoorbeeld niet het recht moeten hebben om af en toe offline te zijn, zodat we het alom aanwezige internet, met alle bijbehorende prikkels en sociale druk, af en toe uit kunnen zetten? En omgekeerd, zou iedereen in dit land niet een grondrecht moeten hebben op internettoegang? Het lijkt mij een verdedigbare stelling dat internettoegang langzamerhand een conditio-sine-qua-non is geworden om goed te kunnen functioneren in deze maatschappij. Belastingaangifte, vergunningaanvragen, boodschappen doen en het vinden van een baan, een huis of zelfs een nieuwe partner gaat steeds vaker via internet. Offline alternatieven verdwijnen steeds meer of worden lastiger of duurder gemaakt.

Met elke nieuwe generatie communicatie- en netwerktechnologie wordt het Internet weer sneller en kunnen er grotere hoeveelheden gegevens worden verstuurd.[12] Deze ontwikkelingen kunnen echter ook leiden tot hogere kosten voor gebruikers, die steeds nieuwe versies of updates van technologie moeten aanschaffen, en tot hogere eisen aan kennis en vaardigheden van gebruikers als het gaat om digitale technologie.[13] Wanneer kosten of kennis en vaardigheden een hindernis zijn voor bepaalde groepen gebruikers om mee te kunnen met technologische ontwikkelingen, kan dit leiden tot sociale polarisatie en manipulatie. Als sommige groepen wel en andere niet toegang hebben tot (snel en functioneel) internet, kan dat leiden tot maatschappelijke segregatie. Groepen die moeilijk meekunnen

met technologische ontwikkelingen, kunnen relatief eenvoudig worden gemanipuleerd, zowel wat betreft de inhoud van informatie als wat betreft communicatiekanalen.[14]

De huidige wetgeving staat vol met informatieverplichtingen. Bijvoorbeeld de Wet Openbaarheid van Bestuur (WOB) verplicht overheden burgers op verzoek informatie te verschaffen. Voor bedrijven en overheden bevat de Algemene Verordening Gegevensbescherming (AVG) allerlei informatieverplichtingen, zoals de verplichting om (op verzoek van betrokkene) te vertellen welke informatie over de betrokkene is verzameld en wordt verwerkt, voor welke doeleinden en op welke wijze. Kortom, het recht om geïnformeerd te worden, hoewel dit actief moet worden ingeroepen, is goed geregeld. Al zijn er wel openstaande vragen over hoe het zit met afgeleide gegevens ('inferred data'), bijvoorbeeld kredietscores, levensverwachtingen, gezondheidsrisico's of andere risicoanalyses.[15]

Maar voor de tegenhanger van informatieplichten, namelijk het recht om iets niet te weten,[16] is niets geregeld. Stel dat burgers niet willen weten wat hun individuele levensverwachting is, gewoon omdat ze hun leven willen leiden zonder dat er een uitdrukkelijke termijn aan dat leven vastzit. Dan kan het zijn dat ze hiermee toch worden geconfronteerd, bijvoorbeeld wanneer ze een levensverzekering aanvragen. Iemand uit een familie met een erfelijke aandoening kan aanzienlijk nadeel ondervinden bij het aanvragen van zo'n levensverzekering. Immers, het risico op weigering of een hogere premie kan toenemen door die erfelijke aandoening. Iemand die een levensverzekering aanvraagt, is verplicht hiervan melding te maken (en zichzelf te benadelen), terwijl iemand die geen weet heeft van de erfelijke aandoening dit niet hoeft te melden. In gevallen die betrekking hebben op zeer persoonlijke en gevoelige informatie over jezelf, zou een recht om iets niet te weten welkom kunnen zijn voor bepaalde mensen.[17]

Wanneer iemand via online zoekgedrag bepaalde voorkeuren etaleert, zullen allerlei algoritmen proberen informatie aan te bieden die is toegesneden op die voorkeuren. Bijvoorbeeld, iemand die (op basis van clickgedrag) vooral geïnteresseerd blijkt in sport en economisch nieuws, zal daarover meer informatie gevoed krijgen dan bijvoorbeeld over onderwerpen zoals politiek en muziek, waar weinig op wordt geklikt. Het gevolg is dat mensen in zogeheten filterbubbels terechtkomen, waarin ze eenzijdig van informatie worden voorzien.[18]

Soms wordt informatie ook teruggekoppeld in inhoud en vorm die opvattingen van mensen steevast bevestigt, hetgeen echokamers worden genoemd. Vanuit de psychologie is bekend dat mensen liever informatie tot zich nemen over iets dat bevestigt wat ze al dachten te weten, dan informatie die dit bekritiseert of tegenspreekt (zogeheten cognitieve dissonantie).[19] Door dit mechanisme kunnen mensen klem komen te zitten in feedback lussen van informatie.

Maar wat als mensen van gedachten veranderen? Stel dat iemand die altijd geïnteresseerd was in voetbal opeens meer wil weten over tennis of iemand die voorheen veel met politiek bezig was zich meer wil gaan toeleggen op cultuur? In een vrije samenleving moet het uiteraard kunnen dat iemand wisselt van interesse of perspectief. Echter, de manieren waarop via het Internet informatie wordt aangeboden aan mensen laat zulke veranderingen maar lastig toe. Mensen kunnen daardoor vast komen te zitten in filterbubbels en echokamers op basis van interesses en voorkeuren uit het verleden. Als ze van gedachten veranderen, werken de huidige mechanismen van informatievoorziening daarin niet mee, ze verhinderen dit juist. Een recht om van gedachten te veranderen kan mogelijk worden ingelezen in het grondrecht van vrijheid van gedachten en/of het recht op vrijheid van meningsuiting, maar misschien vragen deze technologische ontwikkelingen om een hernieuwd en verstevigd recht om van gedachten te mogen veranderen.

Als iemand van gedachten verandert, moet het ook mogelijk zijn om eerder gegeven toestemming in te trekken. Juridisch gezien is dit weliswaar mogelijk, bijvoorbeeld voor het gebruik

van persoonsgegevens. Maar feitelijk geven mensen vaak eenmalig toestemming, namelijk wanneer ze registreren voor een online dienst. Vooraf is door een gebruiker echter lastig vast te stellen of deze toestemming een goede beslissing is.[20] Daarna wordt deze toestemming in de praktijk zelden hernieuwd, terwijl mensen wel van gedachten kunnen veranderen. Het zou misschien logischer zijn als aan elke vorm van toestemming een verlengbare tijdslimiet van bijvoorbeeld drie of vijf jaar zou worden meegegeven. Daarna vervalt de toestemming, tenzij deze wordt herbevestigd.[21]

Veel online producten en diensten, zoals zoekmachines en sociale media, zijn gratis. In feite betekent gratis dan vooral dat er geen euro's betaald hoeven worden, maar dat wordt 'betaald' met gegevens die de aanbieders van zulke producten en diensten over iemand mogen verzamelen en verwerken. Maar hoewel de meeste mensen wel weten dat gratis niet echt gratis is en dat hun gegevens worden verwerkt, is het zelden transparant wat er achter de schermen gebeurt. Vanuit een financieel-economisch perspectief is echter ook onduidelijk welke transactie iemand daadwerkelijk aangaat. Een recht om de waarde van je gegevens te weten zou dan kunnen helpen.[22]

Het recht om af en toe offline te zijn, het recht om iets niet te weten en andere voorbeelden die ik hier heb beschreven, zijn slechts enkele voorbeelden van nieuwe grondrechten die ter discussie zouden moeten staan. Sommige van deze ideeën zijn realistischer dan andere, maar mijn punt is hier vooral dat we wel wat meer discussie zouden mogen voeren over hoe mensen goed beschermd zijn in het digitale tijdperk. Het debat hierover is grotendeels stilgevallen en als al hierover wordt gesproken, is het vooral over het oppoetsen van bestaande grondrechten, terwijl we waarschijnlijk wel meer nodig hebben dan dat.

Als we kijken naar de verschillende catalogi van grondrechten, dan zien we dat bij de eerste ronde technologieontwikkeling vooral het recht op privacy centraal stond.[23] Echter, al snel werd duidelijk dat dit recht niet alle problemen afdekte.[24] Bij de opkomst van data science konden patronen aan gevoelige attributen worden gekoppeld en kwam ook non-discriminatie in beeld. Individualiteit en autonomie komen in het gedrang wanneer mensen vooral worden gezien als onderdeel van (soms kunstmatig gecreëerde) groepen.[25] De vrijheid van gedachten komt in het gedrang nu gedachten steeds beter kunnen worden voorspeld. Met de opkomst van kunstmatige intelligentie in de rechtspraak, waarover later meer, komt het recht op toegang tot een rechter in een heel nieuw daglicht te staan.[26] In plaats van deze grondrechten elk afzonderlijk te beschouwen, kan het ook zinvol zijn om het concept menselijke waardigheid (human dignity) dat ten grondslag ligt aan mensenrechten nader te beschouwen.[27] Hoewel de Nederlandse grondwet geen grondrecht op menselijke waardigheid bevat, heeft de Duitse grondwet dat wel en ook in de EU is dit een grondrecht. Wellicht kunnen we in de toekomst grondrechten eenvoudiger technologie-onafhankelijk[28] formuleren en interpreteren als we ze bezien vanuit het perspectief van menselijke waardigheid.

2.1.2 Bestuursrecht

Het bestuursrecht stelt regels voor beslissingen die het openbaar bestuur mag nemen. Daarbij valt te denken aan verkeershandhaving, ruimtelijke ordening, het verstrekken van bouw- en milieuvergunningen en subsidies en het heffen van belastingen. Bij al deze processen speelt het gelijkheidsbeginsel een belangrijke rol, want in gelijke gevallen kan niet sprake zijn van een verschillende behandeling. Tegelijkertijd is enige beslisruimte en maatwerk belangrijk, zodat overheden rechtvaardige beslissingen kunnen nemen.

Deze afweging tussen gelijkheid en maatwerk past precies in het domein van data science, waar goed kan worden geanalyseerd wanneer factoren tot eenzelfde of een verschillende uitkomst leiden. Bovendien zijn in veel domeinen van het bestuursrecht grote hoeveelheden gegevens beschikbaar. Volgens sommigen worden in het bestuursrecht inmiddels meer geautomatiseerde dan niet-geautomatiseerde besluiten genomen.[29]

Een eerste voorbeeld zijn WOZ-beschikkingen, waarmee elke huiseigenaar in Nederland te maken heeft. Om de waarde van uw woning te bepalen, komt er geen expert meer langs om eens goed te kijken.[30] In plaats daarvan wordt op basis van beschikbare gegevens met behulp van slimme software geanalyseerd welke andere woningen het meest op uw woning lijken en aan de hand daarvan wordt de waarde bepaald.

Een tweede voorbeeld zijn verkeersboetes. Wanneer u te hard rijdt, loopt u het risico te worden geflitst. De gegevens over deze overtreding worden doorgestuurd naar het CJIB in Leeuwarden en daar wordt een brief gegenereerd die u enige tijd later op de deurmat krijgt. Dit hele proces vindt plaats zonder menselijke tussenkomst.[31]

Een derde voorbeeld betreft de belastingdienst, die een van de grootste databanken van Nederland heeft. Met behulp van geavanceerde gegevensanalyses is het mogelijk om profielen op te stellen van personen die mogelijk frauderen met hun aangifte of van personen die mogelijk in aanmerking komen voor toeslagen.[32] De douane, onderdeel van de belastingdienst, gebruikt zulke risicoprofielen om te selecteren welke zeecontainers in de haven van Rotterdam en vliegtuigladingen op Schiphol aan een nader onderzoek moeten onderworpen.[33]

Het gebruik van deze geautomatiseerde processen in het openbaar bestuur zorgt ervoor dat de overheid enerzijds doeltreffender en anderzijds doelmatiger kan opereren. Immers, op deze manier kunnen zaken zoals verkeersovertredingen en belastingfraude beter worden aangepakt en tegelijkertijd kost het ook nog eens minder mankracht en middelen. Dat is goed, maar we moeten ons ook realiseren dat hier enkele risico's aan zitten, die we soms onvoldoende doordacht hebben.[34]

Zo kennen de gebruikte inschattingsmodellen en risicoprofielen foutmarges.[35] Er zullen mensen ten onrechte als fraudeurs kunnen worden aangemerkt (zogeheten false positives)[36] en er zullen fraudeurs buiten beeld blijven (false negatives). Bij de false positives komt bovendien het onschuldbeginsel onder druk te staan. Immers, het systeem beschuldigt mensen van iets, terwijl de vraag is of de gegevens voldoende basis voor een dergelijke beschuldiging vormen. Gegevens kunnen immers onjuist zijn, de analyse kan gebreken vertonen of er kunnen onjuiste conclusies worden verbonden aan analyseresultaten. Het is dan aan betrokkene om te bewijzen dat het anders zit. Dat kan onder meer een privacyparadox[37] oproepen, waarbij iemand een privacyprobleem (de onjuiste verwerking van gegevens) alleen maar kan oplossen door meer en meer gegevens over zichzelf prijs te geven, hetgeen uiteindelijk een nog groter privacyprobleem kan zijn.

Bestuursrechtelijk is het ook een probleem hoe uitspraken gebaseerd op algoritmische besluitvorming betwist kunnen worden.[38] Betrokkenen hebben wel het recht van bezwaar en beroep tegen een beslissing van de overheid, maar hoe toon je aan dat het onderliggende algoritme onjuist of onrechtvaardig is? De meeste mensen zullen niet weten dat een algoritme is toegepast. Bovendien zijn dergelijke algoritmen niet altijd transparant.[39] Een bestuursrechtelijk besluit wordt lastiger te betwisten als het onderliggende algoritme lastig te betwisten is.[40] Daardoor kunnen Kafkaëske situaties ontstaan, waarbij onduidelijk is op basis van welke gegevens en analyses besluiten tot stand komen en burgers zich moeilijk kunnen verweren tegen een krachtig en ondoorzichtig overheidsapparaat.[41]

2.1.3 Strafrecht

Ontwikkelingen op het terrein van digitale technologie bieden zowel voor criminelen als voor opsporingsdiensten nieuwe kansen en bedreigingen. Hieronder zal ik op beide ingaan.

Cybercrime

Wanneer digitale technologie wordt gebruikt door de *bad guys* wordt daar al snel de term cybercrime op geplakt. Hoewel de criminaliteitscijfers in westerse landen al jaren dalen,[42] is cybercrime de laatste jaren aan een flinke opmars bezig.[43] Er zijn veel verschillende vormen van cybercrime, in het Neder-

lands ook wel aangeduid als computercriminaliteit, waaraan verschillende drijfveren van criminelen ten grondslag liggen. Er kan bijvoorbeeld sprake zijn van terroristisch bedoelingen (cyberterrorisme), geopolitieke en militaire bedoelingen (cyberwarfare en cyberspionage) of activistische doelstellingen (cyberactivisme).[44] Maar in veel gevallen gaat het cybercriminelen gewoon om geld verdienen via financiële cybercrime. Op deze categorie zal ik me hier vooral richten, omdat dit binnen het domein van het klassieke strafrecht en van organisaties als politie en justitie ligt

Cybercrime wordt doorgaans onderscheiden in criminaliteit die is *gericht op* technologie, bijvoorbeeld op kritieke infrastructuur en het hacken van systemen zoals zelfrijdende auto's, en criminaliteit die gepleegd wordt *door middel van* technologie, zoals phishing of witwassen met behulp van cryptocurrencies zoals Bitcoins.[45] Soms wordt nog een derde categorie onderscheiden, waarbij technologie een omgevingsfactor is, bijvoorbeeld wanneer drugs worden verhandeld op online marktplaatsen op het darkweb.[46] Dan is sprake van 'traditionele' criminaliteit in een technologische context. Het verschil tussen technologie als middel en als context is dat de ene vorm van cybercrime niet mogelijk is zonder technologie en de andere wel.

Volgens Europol is ransomware de belangrijkste dreiging op het gebied van (financiële) cybercrime.[47] Ransomware is een vorm van kwaadaardige software (malware) waarbij een computer of computersysteem of bestanden daarop worden gegijzeld, doorgaans door ze te versleutelen met sterke encryptie, waarna een losgeldbedrag wordt opgeëist.[48] Voorheen waren vooral particulieren slachtoffer hiervan, maar in toenemende mate richt deze criminaliteit zich nu op bedrijven en organisaties. De losgeldbedragen zijn dan flink hoger. Particulieren betalen doorgaans een paar honderd euro.[49] Maar tegenwoordig richten cybercriminelen zich steeds meer op bedrijven en organisaties en is de hoogte van het losgeld maatwerk. Er kan zelfs onderhandeld worden over het bedrag. De losgeldbedragen schieten de afgelopen jaren fors omhoog: inmiddels moeten bedrijven tienduizenden of zelfs honderdduizenden euro's betalen.[50] Onlangs betaalde de Universiteit Maastricht een kwart miljoen euro nadat deze instelling slachtoffer was geworden van een ransomware aanval.[51]

Met ransomware is dus (heel) veel geld te verdienen, soms een veelvoud van wat er met andere vormen van criminaliteit kan worden verdiend. Daar komt nog bij dat het geld door opschaling snel te verdienen is en dat de risico's voor criminelen aantrekkelijk laag kunnen zijn, want fysiek zit men vaak op een veilige afstand, soms buiten de jurisdicties waar de criminaliteit plaatsvindt en is het ook mogelijk 'schone handen' te houden en weg te blijven van het geweld dat bij andere vormen van criminaliteit kan komen kijken.[52] Al kunnen de daders ook heel dicht bij zitten, zo bleek toen de cybercriminelen achter de ransomware van Coinvault en Bitcryptor werden opgepakt: het bleken twee jongens van 18 en 22 jaar achter hun computer in Amersfoort te zijn.

Door de enorme schade die ransomware aanricht, staat het volop in de aandacht. Wat veel minder aandacht heeft, is het witwassen van het losgeld.[53] Het losgeld dient meestal betaald te worden in cryptocurrencies zoals Bitcoins. Dat is handig voor de criminelen, want dat geld kunnen ze eenvoudig wegsluizen over landsgrenzen heen en vervolgens witwassen via lange ketens van transacties.[54] Omdat Bitcoins op steeds meer plekken als betaalmiddel worden gebruikt, vinden sommige criminelen de vlucht naar contant geld niet altijd meer nodig.[55]

Opsporing en vervolging van witwassen van cryptocurrencies verloopt in veel landen maar moeizaam, want het vergt een combinatie van kennis van zowel witwassen als cybercrime. Afzonderlijk zijn dat al schaarse expertises, laat staan in combinatie met elkaar. Uit eerder onderzoek dat we hiernaar deden, bleek dat de geldstromen in lange ketens van transacties via tal van landen en organisaties lopen.[56] Deze internationale dimensie en het gebrek aan transparantie maken dat het criminele

geld ontraceerbaar en ongrijpbaar wordt. Hier is dus nog een wereld te winnen, ook voor juridisch-empirisch onderzoek naar hoe dit werkt.

Naar verwachting zullen criminelen in de toekomst ook technologie steeds meer gaan inzetten voor andere doelen dan financieel gewin. Om iemand uit de weg te ruimen kunnen in de toekomst zelfrijdende auto's worden gehackt of kan de besturing van drones worden overgenomen om op mensen en objecten in te vliegen. Enkele staatshoofden werden afgelopen jaren al aangevallen met behulp van drones.[57] Andere voorbeelden van cybercrime bedoeld om personen of objecten te beschadigen, zijn het overnemen van de besturing van kerncentrales,[58] waterzuiveringsinstallaties of medische apparatuur.

Dit zijn slechts enkele mogelijkheden van hoe criminaliteit er in de toekomst uit zal kunnen zien. Tegen de problemen die we kunnen voorzien, kunnen we proberen ons vooraf te wapenen, maar sommige problemen zullen we mogelijk niet voorzien en andere problemen zijn mogelijk niet op te lossen. Het intensieve gebruik van technologie kan ons immers zeer kwetsbaar maken.

De huidige wetgeving is niet altijd toegerust op nieuwe vormen van criminaliteit. Daarom is het nodig om steeds op nieuw te kijken of bepaald gedrag strafbaar gesteld is en/of zou moeten zijn. De afgelopen decennia zijn er talloze nieuwe strafbepalingen toegevoegd aan het Wetboek van Strafrecht, meest recent nog in 2019. Maar omdat cybercrime zich voortdurend ontwikkelt, valt niet uit te sluiten dat in de toekomst opnieuw aanvullingen of aanpassingen nodig zijn.[59]

Opsporingstechnologie

Tegenover het gebruik van technologie door criminelen staat het gebruik van technologie door politie en justitie, de *good guys*. De autoriteiten voor opsporing en vervolging kunnen ook in toenemende mate gebruik maken van de mogelijkheden van nieuwe technologie.[60] Dit kan nuttig zijn bij het voorspellen van criminaliteit (*predictive policing*), en ook in de opsporing, de vervolging en uiteindelijk de berechting van misdrijven. Het gebruik van opsporingstechnologie, zoals cameratoezicht, aftappen, automatische kentekenherkenning, vingerafdrukken, DNA-onderzoek,[61] gezichtsherkenning, netwerkanalyses,[62] kunstmatige intelligentie[63] en de inzet van drones, kan allerlei aanwijzingen geven die van belang zijn voor de waarheidsvinding en het identificeren van verdachten. Dit kan bovendien informatie opleveren die in een later stadium als bewijsmateriaal kan worden gebruikt.

In de strijd tegen criminaliteit roepen politie en justitie regelmatig om meer bevoegdheden. Het beeld is dat de inzet van nieuwe technologie betere, snellere en goedkopere resultaten kan opleveren. Hoewel dat vermoeden best zou kunnen kloppen, gebiedt de eerlijkheid te zeggen dat er maar weinig bekend is over de meerwaarde die opsporingstechnologie kan bieden. Uit onderzoek dat we hiernaar deden in binnen-[64] en buitenland,[65] bleek dat er aanzienlijke misverstanden en overspannen verwachtingen zijn binnen politiekorpsen. Hoewel er al veel en vaak technologie wordt gebruikt, bestaat niet overal tevredenheid over. Met name technologie als cameratoezicht en aftappen leveren zoveel data op, dat men snel het overzicht kwijtraakt.[66] Niettemin blijken er allerlei wensenlijsten voor nog meer en nieuwere technologie te zijn. Tegelijkertijd is men niet altijd op de hoogte van de nieuwste technologie en de mogelijkheden die er zijn.

Een ander belangrijk punt is dat succesverhalen en evaluaties vaak niet beschikbaar zijn. Vaak wordt het gebrek aan succes toegeschreven aan onvoldoende juridische ruimte of gebrek aan expertise, mankracht of financiële middelen. Ondertussen is echter niet duidelijk wat de effectiviteit van verschillende opsporingstechnologieën is. Daarom zou het goed zijn bij elke nieuwe technologie die men wil inzetten vooraf een duidelijk plan, inclusief kritische succesfactoren, op te stellen alvorens met een pilot te starten. Als er na een half of een heel jaar aantoonbare successen zijn, kan men overgaan tot implementatie. Zijn er geen aantoonbare successen, dan is het waarschijnlijk

beter om tijd, geld en mankracht op een andere technologie in te zetten. Het realiseren van een juridische basis zou pas in beeld moeten komen als een technologie aantoonbaar resultaten oplevert en daarnaast (net als bij andere opsporingsbevoegdheden) voldoet aan de eisen van proportionaliteit en subsidiariteit als het gaat om de mogelijke inbreuk op burgerrechten, zoals privacy, non-discriminatie en integriteit.

De juridische kaders voor opsporingsbevoegdheden en het gebruik van bewijsmiddelen zijn gesteld in het Wetboek van Strafvordering.[67] De opeenvolgende wetten computercriminaliteit hebben de strafvordering inmiddels aardig veel ruimte geboden, waaronder de mogelijkheid voor de politie om, onder omstandigheden computersystemen van verdachten te mogen hacken.[68] In toenemende mate begint ook het gegevensbeschermingsrecht (waarover later meer) hierin een rol te spelen. Via Europese richtlijnen is inmiddels het gebruik van persoonsgegevens in het strafrecht geharmoniseerd, onder meer wat betreft het uitwisselen van gegevens tussen lidstaten en het gebruik van gegevens door politie en justitie. In Nederland heeft dat geleid tot aanpassingen in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.[69]

Deze nieuwe regelgeving beoogt betrokkenen wiens gegevens worden verwerkt in de context van het strafrecht een betere bescherming te bieden op het vlak van (informationele) privacy. We hebben het dan over verdachten en veroordeelden, maar ook over getuigen en slachtoffers. Hoewel betrokkenen op papier veel rechten en vrijheden hebben, is onduidelijk hoe de regelgeving in de praktijk zou moeten werken. Met name de regels omtrent toestemming en controle, het onderscheid tussen verdachten, slachtoffers en getuigen en het onderscheid tussen feiten en meningen kunnen in de praktijk tot uitvoeringsproblemen leiden.[70] Dat kan weer leiden tot verminderde rechtsbescherming van betrokkenen.

Als we kijken naar de fase na de opsporing, naar het gebruik van strafrechtelijke persoonsgegevens als bewijsmateriaal in de strafrechtzaal, dan valt op dat het strafrechtelijk bewijsstelsel voldoende ruimte laat hiervoor, maar dat tegelijkertijd slechts zelden consequenties worden verbonden aan onrechtmatig verkregen bewijs. Bovendien zijn de juridische kaders voor strafrecht en gegevensbeschermingsrecht niet goed geïntegreerd, hetgeen onduidelijkheden schept.

Een ander belangrijk punt is dat zowel het strafrecht als het datarecht veel aandacht hebben voor het vergaren van gegevens, maar dat er nauwelijks iets is geregeld wat betreft het analyseren van die gegevens, hetgeen de rechtszekerheid van verdachten, slachtoffers en getuigen niet ten goede komt.[71] Als de gegevens maar rechtmatig zijn verkregen, mag er daarna van alles. Maar bijvoorbeeld het opstellen van risicoprofielen kan ertoe leiden dat het onschuldbeginsel onder druk komt te staan, omdat verdachten dan moeten bewijzen dat de profielen niet juist zijn of niet op hen van toepassing zijn.[72]

Naar verwachting gaat technologie de komende jaren een steeds belangrijkere rol spelen in de opsporing en in de rechtszaal. In dat licht is het essentieel dat zowel opsporingsambtenaren als rechters verder kennis en expertise opbouwen hoe hiermee om te gaan. Als deze technologie niet zorgvuldig wordt ingezet, zal het enerzijds niets opleveren in de strijd tegen criminaliteit terwijl anderzijds de kans bestaat dat burgers in hun rechten worden geschonden.

2.2 Privaatrecht

Na deze bespreking van verschillende onderdelen van het publiekrecht ga ik nu verder met het privaatrecht, dat de verhoudingen tussen burgers onderling regelt. In het privaatrecht zijn voor data science de meest relevante rechtsgebieden het aansprakelijkheidsrecht, het consumentenrecht, het mededingingsrecht, het gegevensbeschermingsrecht en het nondiscriminatierecht.

2.2.1 Aansprakelijkheidsrecht[73]

In mei 2017 kreeg een zwangere vrouw tijdens haar werk in een bakkerij in Zeeland een hartstilstand. Drie ambulanceteams en de traumahelikopter werden opgeroepen om hulp te verlenen. Eenmaal ter plaatse kon de traumahelikopter aanvankelijk echter niet landen, omdat er een drone in de weg vloog. De baby werd daarna via een spoedprocedure ter plekke ter wereld gebracht en per helikopter naar het ziekenhuis vervoerd. De moeder volgde per ambulance. Korte tijd later overleed de moeder en later overleed ook de baby.[74]

Eerder dit jaar stortte een drone neer in de Amerikaanse staat Arizona. Dit was waarschijnlijk de oorzaak van een grote bosbrand die daarna ontstond, als gevolg van kortsluiting in de accu van de drone. In totaal ging zo'n 80 hectare bos in vlammen op, maar de brand kon binnen een dag worden geblust en er vielen geen slachtoffers.[75]

Zomaar een greep uit de risico's en gevaren die het gebruik van drones met zich kan brengen. Het gebruik van drones wordt steeds populairder. Drones worden al lang niet meer uitsluitend gebruikt door defensie – er zijn tegenwoordig tal van civiele toepassingen. Drones worden onder meer gebruikt door de politie, de brandweer, door makelaars, in de bouw en in de landbouw.[76] Er liggen tal van kansen om drones te gebruiken voor saaie, vervelende of gevaarlijke klusjes. Bovengenoemde voorbeelden hadden ook vervangen kunnen worden door veel positievere toepassingen van drones, zoals drones die medicijnen bezorgen in lastig toegankelijke gebieden of drones die worden ingezet om bosbranden te blussen.

Niettegenstaande alle kansen brengt het gebruik van drones onmiskenbaar risico's met zich, bijvoorbeeld op het terrein van veiligheid en privacy. Immers, drones kunnen botsen of neerstorten, hetgeen kan resulteren in onder meer zaakschade en letselschade. Drones kunnen ook vliegen en filmen op plekken waar men ze niet verwacht, hetgeen kan resulteren in immateriële schade. Als het gebruik van drones schade veroorzaakt, rijst uiteraard de vraag wie aansprakelijk is.

Het Nederlandse aansprakelijkheidsrecht is een mooi voorbeeld van technologie-neutraal geformuleerde wetgeving: het gaat om de schade die iemand aan een ander toebrengt, ongeacht door middel van welke technologie.[77] Als die schade verwijtbaar en toerekenbaar is, is vergoeding gepast. Schade kan ontstaan wanneer vliegtuigen of auto's botsen of neerstorten. Ook gevaarzetting, hinder en privacy-inbreuken kunnen een vorm van schade zijn.[78] Het aansprakelijkheidsrecht is hierover helder: 'wie het potje breekt, zal het potje betalen'. Als een vliegtuig of auto neerstort, is de piloot of bestuurder aansprakelijk. Als vervolgens blijkt dat de technologie heeft gefaald, zijn de verkoper respectievelijk de fabrikant aansprakelijk.

Maar dat duidelijke verhaal wordt ingewikkeld wanneer we het hebben over autonome drones of zelfrijdende auto's.[79] Deze worden namelijk bestuurd door kunstmatige intelligentie en daarmee komen we terug in het domein van data science. Bijvoorbeeld wanneer een drone zelfstandig handelt, maar met een bestuurder op de achtergrond die kan ingrijpen als iets misgaat, is de vraag waar de aansprakelijkheid ligt als er iets misgaat. Het risico kan immers samenhangen met het gebruikersgedrag, maar ook met een gebrekkige mens-machine interactie.[80] De producent van drones zou dan tenminste via waarschuwingen en instructies ervoor moeten zorgen een zo realistisch mogelijk beeld te geven van de mogelijkheden en beperkingen van de autonome drones.[81] De geboden informatie moet voldoende begrijpelijk en niet te technisch zijn.[82] Overigens dient de producent er rekening mee te houden dat gebruikers niet altijd de gewenste voorzichtigheid in acht nemen.[83] Hier zit iets paradoxaals in: enerzijds maken deze autonome systemen besturing makkelijker en anderzijds wordt van de bestuurder verlangd dat hij continu zijn aandacht bij het besturen houdt.[84]

Bij volledig autonoom handelende drones lijkt er wellicht minder discussie mogelijk over de verdeling van aansprakelijkheid (de bestuurder heeft er immers geen invloed op), maar doemt juist de vraag op of er überhaupt iemand aansprakelijk kan worden gesteld. Stel dat een drone zelf beslist om een passagiersvliegtuig te ontwijken, maar daarbij wel neerstort op een voetganger die letselschade oploopt. Het lijkt dan voor de hand te liggen dat het slachtoffer niet zelf opdraait voor de schade – het gaat hier niet om natuurschade zoals een vallende tak in het bos, maar om door mensen gecreëerde risico's en schade. Tegelijkertijd vertoont de drone als zodanig geen gebrek op grond waarvan productaansprakelijkheid kan worden ingeroepen (het apparaat deed wat het geacht werd te doen). Aansprakelijkheid richting de bestuurder of bezitter kan ook lastig liggen, want die deed waarschijnlijk niets onrechtmatigs en had mogelijk geen of nauwelijks invloed op de gedraging van de drone (en/of kon die niet voorzien). Mogelijk is er dan een lacune in het aansprakelijkheidsrecht als het gaat om een bevredigende oplossing betreffende wie van de betrokken partijen uiteindelijk de schade zou moeten dragen.

Oplossingen hiervoor zouden kunnen worden geboden door een systemische (risico)aansprakelijkheid te creëren, waarbij een actor die de schade redelijkerwijs niet kon voorzien of afwenden toch wettelijk aansprakelijk is.[85] Hiervoor lijkt het minder zinvol om te kijken naar de invloed van de verschillende actoren en hun mogelijkheden om risico's te voorkomen, omdat deze mogelijkheden voor alle genoemde actoren gering kunnen zijn. Als het gevaarzettingsbeginsel als uitgangspunt wordt genomen, lijkt het voor de hand te liggen te kijken naar de fabrikant, omdat die uiteindelijk kan worden aangemerkt als 'bron van verhoogd gevaar', in elk geval meer dan de bestuurder die geen invloed heeft op de gedraging van de drone. Als het profijtbeginsel als uitgangspunt wordt genomen, zou ook een risicoaansprakelijkheid van de bezitter of bestuurder van de drone denkbaar zijn, omdat deze profiteert van het rondvliegen van de drone (bijvoorbeeld om pakketjes te bezorgen of luchtopnames te maken). Als wordt gekeken naar de wens om schaderisico's zoveel mogelijk te voorkomen, komt opnieuw de fabrikant als eerste in beeld voor mogelijke risicoaansprakelijkheid. Immers, de fabrikant kan via risicoaansprakelijkheid worden aangemoedigd zijn producten nog verder te verbeteren vanuit onder meer privacy- en veiligheidsperspectieven. Dit kan uiteraard ook averechts werken, als een te ruime productaansprakelijkheid voor de producent leidt tot *chilling effects* op het gebied van innovatie.[86] De dreiging voor aansprakelijkheid zou dan belemmerend kunnen werken op fabrikanten om producten als drones überhaupt verder te ontwikkelen en op de markt te brengen.[87]

Vanuit dit perspectief zou ook geredeneerd kunnen worden dat het gebruik van nieuwe technologie zodanige maatschappelijke voordelen oplevert, dat risicoaansprakelijkheid beperkt zou moeten zijn. Ter vergelijking: bij autonome auto's kan bijvoorbeeld worden geredeneerd dat het gebruik ervan weliswaar dodelijke slachtoffers kan opleveren, maar dat het gebruik van gewone auto's veel meer verkeersongevallen met dodelijke afloop met zich meebrengt.[88] Door beperkte risicoaansprakelijkheid blijft de schade eerder liggen bij slachtoffers, maar dat zou mogelijk gerechtvaardigd kunnen worden door het feit dat de kans slachtoffer te worden van een dodelijk verkeersongeval aanzienlijk afneemt. Op vergelijkbare wijze kan dat ook voor drones gelden, afhankelijk van de balans tussen allerlei (maatschappelijke) belangen die drones dienen en de mogelijke schade die ze kunnen veroorzaken.

In deze context is ook interessant het debat dat binnen de EU aan het ontstaan is over rechtspersoonlijkheid van robots.[89] De EU overweegt deze optie serieus en lijkt zich daarbij vooral te richten op humanoïde uitziende robots voorzien van kunstmatige intelligentie.[90] Het is niet duidelijk of het zou moeten gaan om een volledige rechtspersoonlijkheid (deels vergelijkbaar met die voor ondernemingen) of een bijzondere juridische status (met een beperkt aantal rechten en plichten). In beide gevallen ontstaat echter ruimte voor het toekennen van rechten en plichten aan autonome systemen (waar autonome drones

ook toe zouden kunnen behoren). In dat geval kunnen autonome drones zelfstandige dragers van rechten en plichten worden die ook aansprakelijk kunnen zijn voor schade. Dit zal echter niet altijd tot bevredigende oplossingen leiden in gevallen van schade, bijvoorbeeld omdat het lastig kan blijken schadevergoeding te bewerkstelligen. Ook retributie en, in gevallen van grove nalatigheid, strafrechtelijke aansprakelijkheid kunnen ingewikkeld zijn.[91]

Als kunstmatige intelligentie en robots in de toekomst dragers van rechten en plichten kunnen zijn, roept dat vragen op over welke rechten en plichten hen toegekend zullen worden. Hierbij is de vergelijking met dierenrechten interessant. Nu stellen mensen vast welke rechten dieren hebben en dieren hebben minder rechten dan mensen. Hieruit komt een duidelijke hiërarchie naar voren over de rolverdeling. Als in de toekomst aan bepaalde vormen van (geavanceerde) AI rechten worden toegekend door mensen, gaan we nog ook uit van zo'n hiërarchische rolverdeling tussen mensen en AI. Maar krijgt de AI dan evenveel rechten als dieren? Of minder? En op grond waarvan?

Daar komt nog bij dat het zeer wel denkbaar is dat AI mensen voorbij zal streven in zowel fysieke als cognitieve capaciteiten. Heel lang zal dat waarschijnlijk niet eens duren. In dat geval is de vraag of de AI wel zal accepteren minder rechten te hebben dan mensen. Als de feitelijke machtsbalans omgekeerd zal zijn, zal het de AI zijn die aan mensen rechten toekent (of niet).[92] Mensen zullen dan in een afhankelijke positie zijn, zoals dieren nu, en maar moeten afwachten wat hun rechten zullen zijn.

2.2.2 Consumentenrecht

Gegevens over consumenten kunnen worden gebruikt om in te schatten aan welke producten en diensten ze behoefte hebben en welke prijs ze bereid zijn hiervoor te betalen. Met behulp van klantprofielen en kredietwaardigheidsscores is het mogelijk nieuwe klantgroepen aan te boren en wanbetalers te vermijden.[93] Maar wanneer bedrijven heel veel weten van hun klanten, kunnen ze die klanten of zelfs hele markten manipuleren. Hieronder zal ik ingaan op het consumentenrecht wat betreft het manipuleren van klanten en in de volgende paragraaf zal ik ingaan op het mededingingsrecht wat betreft het manipuleren van markten.

Algoritmen worden in toenemende mate gebruikt door bedrijven voor verschillende doeleinden. Door het opstellen van klantprofielen kan worden ingeschat op welke manieren mensen kunnen worden verleid tot (meer) aankopen. Door middel van nudging kunnen consumenten worden verleid zonder dat hen keuzevrijheid wordt ontnomen.[94] Met de term *nudging* wordt gedoeld op vormen van subtiele gedragsbeïnvloeding, waarbij het doel is mensen zich te laten gedragen op een bepaalde, gewenste manier.[95] Door keuze op een bepaalde manier te framen en door de wijze van informatie aanbieden, kan gedrag worden beïnvloed. Nudging is daarmee in feite een duwtje geven in de goede richting door het gewenste gedrag aantrekkelijk te maken, zonder mensen daarbij in hun vrijheden te beperken. Het doel is gedrag (licht) bij te sturen via een keuzearchitectuur. Typische kenmerken daarbij zijn dat mensen altijd keuzevrijheid wordt geboden (afwijken van het gewenste gedrag is mogelijk) en dat het gewenste gedrag aantrekkelijk wordt gemaakt. Nudging is vaak mogelijk omdat mensen zich (doorgaans) gedragen volgens bepaalde automatismen (zoals "volg de massa") of bepaalde vooronderstellingen hebben (zoals "duurder zal wel betere kwaliteit betekenen") en/of over gebrekkige informatie beschikken ("kennelijk zijn dit mijn keuzemogelijkheden").

Typische voorbeelden van nudging zijn te vinden in de supermarkt, waarbij doorgaans groente en fruit vlak bij de ingang liggen, omdat dit uitnodigend (want vers, gezond, kleurrijk) uitziet. Daarnaast liggen A-merken doorgaans op ooghoogte, terwijl goedkopere producten vaak helemaal onder- of bovenin de schappen liggen. Ook online wordt nudging vaak toegepast, bijvoorbeeld door meerdere opties aan te bieden, maar een van de opties extra aan te prijzen als 'meest gekozen', 'nieuw', of 'nu in de aanbieding'. Veel mensen kiezen uit een reeks opties niet

de goedkoopste of de duurste variant, maar bijvoorbeeld de op-een-na goedkoopste optie. In alle gevallen blijft er ruimte voor het maken van keuzes, maar wordt de gewenste gedraging aantrekkelijk gemaakt, bijvoorbeeld visueel of fysiek (niet hoeven bukken of reiken voor producten in de schappen).[96]

Nudging kan aantrekkelijk zijn als vorm van gedragsbeïnvloeding, maar stuit ook op bezwaren. Soms worden mensen enigszins ongemerkt gemanipuleerd, hetgeen spanning kan opleveren met autonomie[97] en transparantie.[98] Ook kan nudging overgaan in manipulatie en paternalisme. Van manipulatie kan sprake zijn wanneer bepaalde vormen van nudging niet transparant zijn.[99] Immers, zowel het gedrag als het keuzeaanbod kan worden gemanipuleerd.[100] Zulke vormen van manipulatie druisen in tegen de gedachte dat consumenten vrij moeten kunnen zijn in het maken van hun keuzes.

Van paternalisme kan sprake zijn zodra bedrijven of overheden gaan bepalen wat wenselijk gedrag is en daarop actief gaan sturen. Dat kan invloed hebben op de vrijheden van burgers. Bij nudging zijn er weliswaar altijd keuzemogelijkheden, maar degenen die nudging toepassen, bepalen veelal uit welke opties kan worden gekozen. Verder is de vraag of nudging alleen aanzet tot korte termijn gedragsveranderingen of ook tot lange termijn mentaliteitsveranderingen.

Consumenten kunnen bovendien geconfronteerd worden met uiteenlopende prijzen wanneer onderliggende gegevens worden gebruikt voor het vaststellen van prijzen.[101] Dat kan ertoe leiden dat hetzelfde product voor de ene consument duurder is dan voor de andere. Voor bijvoorbeeld vliegtickets, die goedkoper zijn wanneer ze ruim van tevoren worden geboekt, wordt dat best geaccepteerd door consumenten.[102] Maar duurdere paraplu's wanneer het regent of duurdere coca cola wanneer het erg warm is, ligt al lastiger. Bezorgdiensten voor maaltijden die tot 50% hogere prijzen rekenen voor klanten in rijke wijken ligt nog ingewikkelder.[103] Een ander voorbeeld is het taxiplatform Uber, dat informatie gebruikt over een bijna lege batterij van iemands telefoon als indicatie dat klanten waarschijnlijk een hogere prijs willen betalen voor een rit.[104]

Wanneer prijzen gepersonaliseerd worden vastgesteld met behulp van algoritmen, wordt doorgaans gesproken van online prijsdiscriminatie in de economische betekenis van deze term. Maar wanneer de personalisatie plaatsvindt aan de hand van bepaalde sensitieve persoonskenmerken zoals geslacht, etniciteit of religie, kan ook sprake zijn van discriminatie in de juridisch betekenis van het woord. Op dergelijke vormen van discriminatie zal ik verderop ingaan.

Het consumentenrecht is bedoeld om de autonomie en keuzevrijheid van consumenten te bevorderen en consumenten te beschermen.[105] Bovengenoemde voorbeelden van dynamische en gepersonaliseerde prijsstelling worden echter niet of nauwelijks geadresseerd in het consumentenrecht. Toch zetten bovengenoemde vormen van manipulatie de autonomie en keuzevrijheid van consumenten onder druk. De autonomie van consumenten staat ook onder druk in fenomenen als A/B testing, waarbij consumenten ongewild en ongevraagd als proefkonijnen dienen.

Bij *A/B-testing*[106] krijgen sommige gebruikers scherm A aangeboden en andere gebruikers scherm B. Scherm A en B hebben slechts één verschil, soms is dat een heel subtiel verschil. Het verschil kan bijvoorbeeld zijn een lichtgele of een lichtblauwe achtergrondkleur, een logo in zwarte letters of donkerblauwe letters, of al dan niet een lijntje onder de kopteksten. Bij zowel variant A als variant B wordt gemonitord hoe lang mensen op de website blijven, reclame aanklikken of iets bestellen. Als blijkt dat variant A betere resultaten oplevert dan variant B, wordt die laatste verworpen en verdergegaan met variant A. Door dit herhaaldelijk en op grote aantallen gebruikers toe te passen, wordt een optimaal resultaat bereikt, namelijk de voor gebruikers meest verleidelijke manier van informatie aanbieden. In feite zijn alle gebruikers dus onderdeel van een grootschalig experiment en worden ze als proefkonijn gebruikt.

Omdat dit doorgaans ongewild en ongevraagd plaatsvindt, is de vraag of dit niet een laakbare vorm van inperking van de autonomie van consumenten is.

Een ander punt waartegen consumenten mogelijk beschermd zouden moeten worden in een online context is de gebrekkige transparantie van betalingen. Zoals eerder aangegeven, zijn veel online diensten gratis in de zin dat er geen geld voor hoeft te worden betaald. Maar door het gebruik van de diensten gaat een consument er wel mee akkoord dat zijn of haar gegevens mogen worden gebruikt en/of doorverkocht. Wanneer geheel of gedeeltelijk met gegevens wordt betaald, wordt een transactie voor consumenten onduidelijker. Zoals ik eerder heb betoogd, zouden consumenten meer moeten weten over de waarde van hun gegevens om goed te kunnen inschatten wat een transactie waarbij wordt betaald met gegevens voor hen betekent.[107]

2.2.3 Mededingingsrecht

Op individueel niveau behoeven consumenten bescherming, maar op een hoger niveau behoeven ook markten bescherming, namelijk tegen verstoring. Goed functionerende markten kunnen in een data-economie worden verstoord op verschillende manieren. Hier zal ik ingaan op verschillende risico's voor marktwerking:[108] afstemming van prijzen en kartelvorming en misbruik van economische machtsposities en data als bron van (markt)macht, hetgeen markttoegang kan verstoren en innovatie kan belemmeren.[109]

Als algoritmische besluitvorming wordt gebruikt voor prijsstellingen, kan dit leiden tot (nieuwe typen van) mededingingsbeperkende overeenkomsten. Er kan bijvoorbeeld sprake zijn van verboden prijsafstemming. Hierbij kunnen vier verschillende situaties worden onderscheiden.[110] Ten eerste kunnen algoritmen worden gebruikt als instrument om kartelvorming te faciliteren. Ten tweede kunnen algoritmen worden ingezet voor het vaststellen van prijzen.[111] Ten derde kunnen algoritmen worden geprogrammeerd om te reageren op veranderende marktomstandigheden, bijvoorbeeld via dynamische prijsstelling.[112] Ten vierde kunnen algoritmen in het domein van de kunstmatige intelligentie worden geprogrammeerd om een bepaald doel te bereiken, bijvoorbeeld winstmaximalisatie.

De algoritmen kunnen niet alleen vooraf afgesproken transacties ('kopen als de prijs zakt beneden een bepaald bedrag') automatisch uitvoeren, maar ook handelen naar omstandigheden ('als de concurrentie prijzen verlaagt, verlaag dan de eigen prijzen navenant'). De werking van algoritmische besluitvorming kan daardoor zeer verschillende effecten hebben. Enerzijds kan het zeer efficiëntieverhogend zijn en anderzijds kunnen consumenten worden uitgebuit. Bij het beoordelen van hoe algoritmische besluitvorming uitpakt, is ook van belang in hoeverre de algoritmen autonoom zijn. Eenvoudige algoritmen, zoals beslisbomen, hebben een heldere input-output structuur, waarbij dezelfde input steeds tot dezelfde output leidt. Echter, meer geavanceerder technologieën, zoals machine learning en neurale netwerken, kunnen ook zelflerend zijn. Daarbij leidt dezelfde input dus niet per se tot dezelfde output: als het algoritme heeft geleerd dat bepaalde input op een andere manier moet worden gecombineerd dan voorheen, zal dat leiden tot andere output. Als de algoritmen werken op basis van patroonherkenning, kunnen uiteraard ook veranderingen in grote datasets (bijvoorbeeld doordat er steeds nieuwe gegevens bijkomen) leiden tot het herkennen van nieuwe patronen, die vervolgens zullen leiden tot gewijzigde algoritmische besluitvorming.

Een typisch voorbeeld van hoe prijzen uit de hand kunnen lopen, betreft Amazon. In de verkoop van een boek (*The Making of a Fly* van Peter Lawrence) werd de prijs steeds verder verhoogd, uiteindelijk tot boven 23 miljoen dollar.[113] De oorzaak hiervan was dat twee verkopers van hetzelfde boek beide een algoritme gebruikten om de prijs te bepalen. De ene verkoper paste elke dag de prijs aan op 99% van de prijs van concurrent. De andere verkoper paste elke dag de prijs aan op 127% van de concurrent.[114] Dat liep al snel uit de hand met omhoog spira-

liserende prijzen, maar er was nergens een stop ingebouwd, hetgeen tot bovengenoemde absurde prijsstellingen leidde. Na ontdekking werden de prijzen handmatig teruggezet – het boek is uiteraard nooit voor die hoge prijzen verkocht.

Een ander mededingingsrechtelijk aspect vloeit voort uit het feit dat datamarkten anders werken dan reguliere markten voor producten en diensten.[115] Dit heeft onder andere te maken met de unieke eigenschap van gegevens dat ze in beginsel kosteloos kunnen worden vermenigvuldigd en verspreid. Zodoende kunnen gegevens steeds worden hergebruikt.[116] Daarnaast spelen er allerlei schaaleffecten een rol. Grote dataverzamelingen kunnen waardevolle verbanden opleveren, terwijl kleinere dataverzamelingen in dat opzicht vrijwel waardeloos kunnen zijn.[117]

Om mee te kunnen doen op het wereldtoneel heeft de Europese Commissie al in 2014 een strategie opgesteld voor een transitie van de Europese economie richting een datagedreven economie.[118] Naast de vier klassieke vrijheden van de EU (vrij verkeer van personen, goederen, diensten en kapitaal), moet er een vijfde vrijheid komen: vrij verkeer van gegevens. Dat moet een Digital Single Market (DSM) opleveren, met versnelde economische groei en innovatie en verhoogde productiviteit en concurrentie.

Dat klinkt allemaal mooi, maar in de praktijk zijn het vooral de grote ondernemingen die in de gelegenheid zijn enorme dataverzamelingen op te bouwen en waarde te creëren.[119] Er is immers veel expertise en technologie voor nodig. Het gevolg is dat de dataeconomie daardoor niet goed van de grond komt, omdat kleinere bedrijven en organisaties niet mee kunnen doen. Het MKB en bedrijven buiten de IT-sector staan grotendeels buitenspel, ondanks dat gegevens eenvoudig herbruikbaar zijn.[120]

Al die eigenschappen van gegevens maken dat data een bron van (markt)macht is. Grote bedrijven kunnen bepalen wie toegang krijgen tot deze waardevolle grondstoffen en onder welke condities. Zo heeft marktleider Google in Nederland en de rest van de EU meer dan 90% van de zoekmachinemarkt in handen en kan vervolgens bepalen welke zoekresultaten consumenten te zien krijgen. Het bedrijf gebruikte de zoekmachine om een ander product, het eigen Google shopping te bevoordelen. Dat leverde in 2017 een boete op van 2,4 miljard euro, opgelegd door de Europese Commissie voor het schenden van Europees mededingingsrecht.[121]

Het voorbeeld van Google shopping ziet vooral op uitsluiting van andere aanbieders. Een ander voorbeeld van misbruik van machtspositie dat vooral ziet op uitbuiting van gebruikers, komt uit Duitsland, waar het Bundeskartellamt stelde dat Facebook de gebruikersvoorwaarden zodanig ruim en onduidelijk heeft opgesteld, dat gebruikers geen overzicht of controle hebben over de gegevens die ze delen. Facebook misbruikt hiermee haar machtspositie volgens de Duitse toezichthouder, die stelt dat marktpartijen met een dominante machtspositie een speciale verantwoordelijkheid hebben.[122]

Een derde voorbeeld ziet vooral op het wegduwen van concurrentie door spelers met een dominante marktpositie: marktuitsluiting. Wanneer bijvoorbeeld innovatieve start-up bedrijven een markt willen betreden, dan is er steeds een kans dat ze worden overgenomen door grote bedrijven. Vaak worden ze daarna ook ingekapseld in de grotere bedrijfsstructuren. Het is begrijpelijk dat grote spelers via fusies en overnames proberen marktaandeel te winnen, maar een risico is dat nieuwe spelers nauwelijks kunnen toetreden tot diezelfde markten. Dat kan zowel innovatie in de kiem smoren als concurrentie belemmeren.

Ook voor handhavingsautoriteiten liggen er grote uitdagingen. In de eerste plaats gaat het om grote spelers, met budgetten die hoger zijn dan waarover sommige landen kunnen beschikken. Dat maakt hen lastige tegenspelers, met veel macht, ook in een rechtszaal. Een andere grote uitdaging is transparantie,

want veel van de gebruikte algoritmen en marktstrategieën zijn bedrijfsgeheimen. Toezichthouders kunnen uiteraard wel toegang krijgen tot zulke informatie als het erop aankomt, maar ook dan blijft soms nog onduidelijk hoe combinaties van datasets en algoritmen tot bepaalde uitkomsten leiden. Een derde uitdaging is dat in de dataeconomie niet alleen gehandeld wordt tegen geld, maar ook tegen data. De data worden soms als product, maar soms ook als valuta gezien. Wanneer iemand betaalt met zijn gegevens, is echter lastig vast te stellen of er ook een rechtvaardige prijs is betaald.

2.2.4 Gegevensbeschermingsrecht

Het verwerken van grote hoeveelheden gegevens kan leiden tot situaties waarin gegevensbeheerders heel veel weten over eigenschappen, gedragingen en verblijfplaatsen van mensen.[123] Om die reden wordt privacy doorgaans het eerste genoemd als probleem of punt van zorg in de context van big data.[124] Vanuit een grondrechtenperspectief hangen schendingen van privacy voor een groot deel af van de (redelijke) verwachtingen die mensen mogen hebben omtrent hun privacy.[125] Tot op zekere hoogte zijn die verwachtingen subjectief en kan dit afhangen van de situatie, de persoon en culturele omstandigheden.[126] De een maakt zich niet druk 's avonds de gordijnen te sluiten, terwijl de ander dat zorgvuldig doet. Sommige mensen zetten tot in detail hun persoonlijk leven op sociale media, terwijl anderen niet eens een account aanmaken.[127] Verwachtingen van privacy kunnen wel worden geobjectiveerd, door na te gaan wat een gemiddeld persoon zou verwachten in een bepaalde situatie en context. Dit wordt aangeduid met 'redelijke verwachtingen van privacy'.[128]

In de context van big data en data science ligt de nadruk vaak op zogeheten informationele privacy, een term die gericht is op de vraag welke persoonsgegevens worden verzameld en gebruikt en voor welke doelen. In wezen gaan verwachtingen omtrent informationele privacy vooral over het delen, onthullen en gebruiken van gegevens op manieren die de personen die het betreft (de data subjecten/betrokkenen) niet op prijs stellen. Zulk gebruik van persoonsgegevens is soms gerelateerd aan informatiebeveiligingsproblemen, bijvoorbeeld wanneer gegevens worden gehackt (zie het voorbeeld van de datingsite voor vreemdgangers Ashley Madison)[129] of wanneer gegevens lekken (soms opzettelijk, soms door onoplettendheid). Het ongewenst gebruik van gegevens kan onder andere het gevolg zijn van een gebrek aan transparantie en van *function creep*, waarbij gegevens worden gebruikt voor nieuwe doelen en/of in een nieuwe context.

Ongewenste onthullingen kunnen echter niet alleen het gevolg zijn van datalekken. Zelfs wanneer betrokkenen hun gegevens met niemand anders delen, kunnen deze toch worden blootgelegd in een big data context. Dat is omdat big data de mogelijkheid biedt om op basis van grote hoeveelheden beschikbare gegevens ontbrekende gegevens te voorspellen. Dit kan ook voor gevoelige gegevens die mensen doorgaans (liever) niet delen met anderen, zoals gegevens over hun gezondheid, etnische afkomst, strafblad en seksuele voorkeuren. Gegevensbeheerders kunnen deze ontbrekende gegevens overigens betrekkelijk eenvoudig voorspellen.[130] Ook eigenschappen die door de tijd heen variëren, zoals emoties en locaties, kunnen aan de hand van big data worden voorspeld, bijvoorbeeld op basis van berichten op sociale media of op grond van videobeelden.[131] Als mensen bepaalde informatie over zichzelf niet willen delen en die informatie wordt via een omweg toch afgeleid, is duidelijk sprake van een privacyprobleem. Redelijke verwachtingen van privacy worden daarmee geschonden, hetgeen een inbreuk op het recht op privacy kan opleveren.

In bepaalde gevallen kunnen gegevensbeheerders zelfs meer weten over betrokkenen dan dat deze over zichzelf weten, waaronder levensverwachtingen, kansen op ernstige ziektes of auto-ongelukken, risico's op bepaalde verslavingen en inschattingen van welzijn en geluk. Een typisch voorbeeld is het uitdelen van zogeheten likes op Facebook. Met deze icoontjes kunnen gebruikers aangeven welke muziek, filmpjes, games, uitspraken, personen, etc. ze leuk vinden. Uit onderzoek blijkt dat op basis van enkele Facebook likes tal van gevoelige per-

soonlijke attributen zeer nauwkeurig kunnen worden voorspeld.[132] Zo konden deze onderzoekers bij Facebookgebruikers onder meer de seksuele voorkeur, etniciteit, religie, politieke voorkeur, persoonlijkheidskenmerken, intelligentie, geluk, drugsgebruik en echtscheiding van ouders voorspellen met hoge nauwkeurigheid. Zelfs als mensen zulke eigenschappen niet (willen) prijsgeven, zijn ze dus te voorspellen op grond van andere gegevens die zijzelf (of anderen) wel prijsgeven.[133] Overigens kan op dezelfde manier bijvoorbeeld ook anonimisering ongedaan worden gemaakt.[134]

Toen de EU in 2000 het Handvest van de grondrechten van de Europese Unie aannam, werd daarin ook het recht op bescherming van persoonsgegevens als grondrecht opgenomen, in artikel 8, om precies te zijn. Deze grondrechtelijke bescherming, tot dusver uniek in de wereld, is een explicitering van het feit dat bescherming van privacy in een sterk gedigitaliseerde samenleving verder gaat dan het klassieke recht op privacy. Dit grondrecht is verder uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG).

Die AVG werd in 2018 met veel tromgeroffel van kracht in de gehele EU. Deze nieuwe wetgeving zou de twintig jaar oude wetgeving op dit vlak weer bij de tijd brengen en ervoor moeten zorgen dat burgers veel beter beschermd zouden worden in de maalstroom van gegevensverwerkingen. Bij de invoering van de AVG stond inderdaad iedereen op scherp, niet in de laatste plaats vanwege de hoge boetes die opeens konden worden uitgedeeld door de toezichthouder. Tegelijkertijd kunnen we constateren dat de AVG zeer sterk lijkt op de oudere wetgeving, met dezelfde uitgangspunten en reikwijdte. Alleen de boetes zijn nieuw en een paar bepalingen rondom het recht op vergetelheid,[135] het recht op gegevensportabiliteit,[136] privacy by design[137] en data protection impact assessments.[138]

Als we goed kijken naar de nieuwe wetgeving, dan zijn er allerlei kleinere en grotere problemen. De kleinere problemen zien vooral op de open normen in de AVG, waardoor onduidelijkheden ontstaan over wat er wel en niet is toegestaan wat betreft het verwerken van gegevens. Dat is voer voor veel juristen die nu discussiëren over interpretaties en daardoor is een florerende markt ontstaan voor adviesbureaus.

Maar er zijn ook enkele zeer grote, conceptuele problemen. Het belangrijkste probleem is waarschijnlijk dat de AVG voornamelijk gericht is op procedurele rechtvaardigheid: als gegevens netjes worden verwerkt, bijvoorbeeld door toestemming, transparantie en beveiliging goed te regelen, dan zal het wel ok zijn. Maar over materiële rechtvaardigheid is maar weinig terug te vinden in de tekst van de AVG. Er wordt niet duidelijk welke soorten gegevensverwerkingen en beslissingen niet acceptabel zijn. Nergens wordt gesproken over de schadelijke effecten die grootschalige gegevensverwerkingen kunnen opleveren voor burgers en waar een grens wordt getrokken van tot hier en niet verder. Daarmee kan worden gesteld dat de AVG niet de gewenste bescherming biedt: bedrijven kunnen uitstekend de wetgeving naleven terwijl burgers tegelijkertijd daarvan grote nadelen kunnen ondervinden. Dat klinkt als operatie geslaagd, maar patiënt overleden.[139]

Daarenboven is de procedurele rechtvaardigheid op papier weliswaar goed geregeld, maar in de praktijk niet goed uitgewerkt. Bijvoorbeeld een concept als toestemming is problematisch, want burgers worden overladen met toestemmingsverzoeken en hebben helemaal geen tijd om alles te lezen.[140] Tegelijkertijd kan worden gesteld dat als iemand alles zou lezen, de kans groot is dat hij of zij de technische en juridische teksten vaak niet helemaal kan doorgronden en de consequenties van toestemming goed kan overzien.[141] En zelfs als dat wel het geval is, dan is het doorgaans onmogelijk om je voorkeuren aan te kruisen: meestal is het een alles-of-niets beslissing, waarbij je onderaan een lange lijst met voorwaarden een vinkje kunt zetten – iets dat vrijwel iedereen blindelings doet.

In feite kan zelfs gesteld worden dat alle beginselen waarop de AVG is gestoeld, op gespannen voet staan met de ontwikkelin-

gen rondom big data en data science.[142] De technologie is immers gericht op meer en meer gegevens, terwijl de wetgeving daaraan juist paal en perk probeert te stellen. Op zichzelf niet verkeerd, maar de vraag is wel of dat haalbaar is, wanneer gegevens met een druk op de knop kunnen worden gekopieerd en met nog een druk op de knop kunnen worden verspreid naar heel veel andere plekken. De entropiewetten uit de informatietheorie lijken ons te zeggen dat dit onhoudbaar is.[143]

Daarmee is de handhaving van deze wetgeving knap ingewikkeld. Hoewel de wetgeving nu voor de gehele Europese Unie geharmoniseerd is, blijken er grote verschillen te zijn in de implementatie, beleidsinvulling en handhaving.[144] Sommige lidstaten volstaan met het overnemen van de Europese regels, terwijl andere lidstaten veel gedetailleerdere wetgeving en aanvullend beleid hebben ingevoerd, bijvoorbeeld op sectoraal niveau. In het ene land hebben toezichthouders nauwelijks budget, terwijl in het andere land fors wordt ingezet op handhaving.[145] Ook zijn er grote culturele verschillen als het gaat om de vraag in hoeverre de letter van de wet of de geest van de wet moet worden nageleefd.[146]

De AVG kent burgers veel rechten en zeggenschap toe als het gaat om hun eigen gegevens. Onderzoek laat echter zien dat veel burgers niet weten wat er allemaal gebeurt, niet op de hoogte zijn van hun rechten en niet weten waar ze zouden moeten aankloppen.[147] In de praktijk zijn veel van deze rechten daarom niet eenvoudig uit te oefenen voor individuele burgers. Daar komt nog bij dat in veel gevallen 'de kool het sop niet waard is': het gaat doorgaans om relatief kleine onrechtvaardigheden, waarvoor burgers niet bereid zijn een rechtszaak aan te spannen. Als gevolg daarvan bestaat er weinig jurisprudentie en blijven er veel onduidelijkheden in de interpretatie van de AVG bestaan. Dat draagt niet bij aan het vergroten van het bewustzijn van burgers op dit vlak, waarmee het geheel in een vicieuze cirkel lijkt te zitten.

Een ander groot probleem is dat de AVG rechten en zeggenschap aan individuen toekent, terwijl de gegevensverwerkingsprocessen (met name de analyses) in de context van big data en data science juist op geaggregeerd niveau plaatsvinden. Het opstellen van risicoprofielen en voorspelmodellen werkt alleen als gegevens op geaggregeerd niveau worden geanalyseerd.[148] Een voorbeeld van groepsgegevens betreft het opstellen van risicoprofielen voor criminaliteit.[149] Hiervoor moeten determinanten worden onderzocht die het verschil maken tussen crimineel gedrag en niet-crimineel gedrag of tussen criminelen en onschuldige burgers. Om dit onderscheid in risicoprofielen te kunnen vatten, zijn dus ook gegevens van onschuldige burgers nodig. Burgers hebben alleen zeggenschap over hun eigen gegevens en (uiteraard) niet over de gegevens van anderen, maar in de context van big data en data science doen zich problemen voor waarvoor de AVG eigenlijk geen oplossing biedt.[150]

Het eerste probleem is dat met behulp van big data en data science voorspellingen mogelijk worden die een betrokkene niet kan *verifiëren*. Sommige voorspellingen kunnen eenvoudig worden gecontroleerd door de persoon die het betreft. Bijvoorbeeld, wanneer op basis van beschikbare gegevens eigenschappen als geslacht, etniciteit, nationaliteit, inkomen of opleidingsniveau worden voorspeld, kan iemand eenvoudig nagaan hoe goed het algoritme klopt voor hem of haar. Wanneer eigenschappen als intelligentie of geluk worden voorspeld, is dit al iets lastiger, want hoewel iemand bij zichzelf te rade kan gaan of een aantal testen kan doen om dit op individueel niveau vast te stellen, zijn het doorgaans geen eigenschappen die men onmiddellijk kan kwantificeren zoals een algoritme dat kan doen. Nog lastiger wordt het wanneer het algoritme gaat voorspellen wat iemands levensverwachting of kredietwaardigheid is. Of andere voorspellingen die toekomstige gebeurtenissen voorspellen, zoals de kans op echtscheiding of een hartaanval binnen nu en vijf jaar. Op individueel niveau heeft een burger nauwelijks mogelijkheden ter beschikking dit voor zichzelf vast te stellen.

Het tweede probleem is dat een betrokkene zulke voorspellingen bovendien niet goed kan *beïnvloeden*. Stel dat de algoritmen uitspugen dat iemand een beroerde kredietwaardigheid heeft. Op grond van de AVG kan die persoon dan uitvragen welke gegevens van hem of haar hieraan ten grondslag lagen. Maar uiteraard mag niet worden uitgevraagd welke gegevens van anderen ook zijn meegenomen in de analysis, want dat betreft persoonsgegevens van derden die uiteraard privacybescherming behoeven. Maar die gegevens van derden zijn wel van invloed op de scores die uit de algoritmen komen rollen en die beroerd kunnen uitpakken voor een individu. Daardoor krijgt een betrokkene geen zicht op hoe dergelijke scores tot stand komen en dus ook slechts beperkte mogelijkheden om iets te veranderen in eigenschappen of gedragingen die kunnen leiden tot betere scores.[151]

Een argument dat nogal eens wordt tegengeworpen door mensen die graag buiten deze voorspelmodellen willen blijven, is dat je beter geen (input)gegevens kunt verstrekken, want dan kunnen privacygevoelige eigenschappen ook niet worden voorspeld. Helaas is dat niet helemaal waar. Als iemand weinig online is en tevens weinig gegevens online verstrekt, zegt dat ook iets over die persoon. Scores met betrekking tot iemands privacygevoeligheid, introversie en digibetisme kunnen dan bijvoorbeeld toenemen. Met andere woorden, ook als je hieraan niet wilt meedoen, doe je toch mee. Iemand die weinig of niets aan gegevens prijsgeeft, wordt gewoon in een andere categorie geplaatst. Omdat zoveel mensen meedoen, zijn er niet echt mogelijkheden je hieraan te onttrekken, zeker niet op grond van gegevensbeschermingswetgeving zoals de AVG.

2.2.5 Gelijke behandeling/non-discriminatie

Wanneer de hierboven beschreven voorspellingen gevoelige gegevens (zoals etniciteit, politieke voorkeuren, seksuele voorkeuren, leeftijd en geslacht) blootleggen en deze vervolgens worden gebruikt om beslissingen over mensen te nemen, kan ook sprake zijn van discriminatie. Discriminatie kan op verschillende niveaus voorkomen in big data analyses.[152] Zo kunnen de gegevens zelf vooroordelen bevatten. Een typisch voorbeeld is wanneer de politie vooral surveilleert in bepaalde achterstandswijken waar veel migranten wonen. Het waarschijnlijke resultaat van een dergelijk beleid is dat databanken van de politie dan gevuld worden met mensen met bepaalde etnische achtergronden. Dit is een typisch voorbeeld van selecte (in plaats van aselecte) steekproeven.[153]

Wanneer dezelfde politieorganisatie vervolgens op zoek zou gaan naar verbanden in de verzamelde gegevens, teneinde uit te zoeken welke groepen hogere risico's op crimineel gedrag vertonen, zal het geen verbazing wekken dat dezelfde etnische minderheden geprofileerd kunnen worden als risicogroep voor crimineel gedrag. Echter, omdat de gegevens al vooroordelen bevatten voordat de analyses werden uitgevoerd, is er slechts sprake van een selffulfilling prophecy. Als de politie vervolgens de profielen gebruikt om te bepalen waar het meest intensief moet worden gesurveilleerd, is de cirkel daarmee rond.

Het is van belang op te merken dat discriminerende patronen niet altijd duidelijk zichtbaar zijn.[154] Wanneer bijvoorbeeld gevoelige eigenschappen als etniciteit al dan niet intentioneel worden gebruikt voor profilering, is het duidelijk dat er een risico op discriminatie is. Echter, wanneer de profielen worden gebaseerd op bijvoorbeeld postcodes, kan dit ook (indirecte) discriminatie opleveren wanneer die postcodes sterk gerelateerd zijn aan etniciteit. In zulke gevallen zijn postcodes slechts een proxy, een benaderingsvariabele, voor etniciteit. In Nederland is ook indirecte discriminatie overigens verboden doordat in art. 1 Algemene wet gelijke behandeling (waarin het discriminatieverbod in art. 1 van de Grondwet is uitgewerkt) direct en indirect onderscheid gelijk worden gesteld.[155] Feit blijft wel dat indirect onderscheid nog veel lastiger is te bewijzen dan direct onderscheid. Er zijn wel technieken om discriminatie in big data op te sporen.[156] Een typisch voorbeeld is een onderzoek waarin discriminatie op basis van etniciteit bij Airbnb aan het licht kwam: blanke verhuurders vragen ongeveer 3% hogere prijzen voor vergelijkbare accommodatie ten opzichte

van niet-blanke verhuurders (doorsnede van 24 steden in 14 landen).[157] In de Verenigde Staten loopt dit verschil zelfs op tot 7% voor Afro-Amerikaanse verhuurders en 6% voor Aziatische verhuurders. De prijsverschillen zijn bovendien groter bij accommodaties die gasten en verhuurders delen, met andere woorden wanneer klanten verwachten meer direct contact met de verhuurder te hebben.

Uit onderzoek blijkt overigens dat het weglaten van gevoelige karakteristieken uit databanken niet verhindert dat er toch patronen worden gevonden die leiden tot indirecte discriminatie.[158] Los van het feit dat ontbrekende variabelen kunnen worden voorspeld (zie hierboven), blijkt dat veel patronen die worden blootgelegd ook te vinden zijn in andere variabelen dan de gevoelige variabelen waarop een discriminatieverbod rust.[159] Bijvoorbeeld het gebruik van geografische gegevens voor profiling wordt aangeduid als redlining en is doorgaans verboden.[160] Verder moet worden opgemerkt dat de indirecte discriminatie ook non-intentioneel kan plaatsvinden en gebruikers van profielen zich mogelijk van geen kwaad bewust zijn. Indien daarentegen de profielen juist worden gebruikt om discriminatie te verhullen, wordt ook wel van 'masking' gesproken.

Er worden technologische oplossingen ontwikkeld om algoritmen zodanig te ontwerpen dat ze niet discriminerend zijn.[161] Een voorbeeld hiervan is zogeheten *discrimination-aware data mining*.[162] De achterliggende gedachte is dat niet de gegevensinput moet worden beperkt (dus het verhinderen dat discriminatiegevoelige gegevens worden verzameld en/of verwerkt), maar dat de algoritmes niet mogen leiden tot discriminerende verbanden. De nadruk op het weren van gevoelige gegevens verhindert immers niet dat deze gegevens alsnog kunnen worden voorspeld[163] en ook indirecte discriminatie (*discrimination by proxy*) is nog steeds mogelijk. De nadruk op het ontwerp van algoritmen kan dit wel verhinderen. Kort gezegd komt dit erop neer dat wanneer bijvoorbeeld een algoritme moet worden ontworpen dat gegarandeerd niet discrimineert op bijvoorbeeld etniciteit, deze gevoelige etniciteitsgegevens moeten worden gebruikt bij het bouwen van de modellen.[164] Uiteraard mogen de etnische gegevens vervolgens, als het model eenmaal is gebouwd, niet worden gebruikt als inputvariabelen voor beslissingen. Non-discriminatiewetgeving zal dat (terecht) verbieden. Een groot nadeel is echter dat voor deze aanpak het gebruik van gevoelige gegevens nodig is in de ontwerpfase, hetgeen door wetgeving als de AVG (mijns inziens onterecht) wordt bemoeilijkt.

Als het gaat om de wetgeving die discriminatie op grond van specifieke eigenschappen verbiedt, gaat het enerzijds om lijsten met eigenschappen die niet mogen worden gebruikt voor beslissingen (zoals etniciteit, politieke voorkeur, vakbondslidmaatschap, seksuele geaardheid, etc.) en anderzijds om bepaalde typen beslissingen die verboden zijn (zoals het aannemen en ontslaan van personeel, het aanbieden van producten en diensten, etc.).[165] Niet alle beslissingen op grond van de opgesomde gevoelige karakteristieken zijn verboden. Bijvoorbeeld, het is een persoonlijke keuze met wie iemand bevriend wil zijn. Niettemin kunnen zich ook dan 'zwakkere' vormen van discriminatie voordoen, bijvoorbeeld in de vorm van stigmatisering van bepaalde bevolkingsgroepen.[166] Op grotere schaal kan dat leiden tot sociale polarisatie en maatschappelijke segregatie.

Alles bij elkaar lijkt de wetgeving op het terrein van gelijke behandeling onvoldoende toegerust op de ontwikkelingen in data science. Er zijn vormen van onderscheid mogelijk die niet denkbaar waren toen de wetgeving werd opgesteld en tegen het licht moeten worden gehouden wat betreft wenselijkheid. Bovendien is indirect onderscheid dat wel verboden is, vaak zeer lastig te herkennen en dat maakt onder meer handhaving buitengewoon gecompliceerd.

3. Data science in juridisch onderzoek en de rechtspraktijk[167]

Tot dusver heb ik gesproken over verschillende ontwikkelingen op het gebied van data science, welke kansen en uitdagingen die bieden en hoe deze ontwikkelingen gereguleerd kunnen worden. Wellicht lag de nadruk daarbij vooral op mogelijke problemen. Daarom wil ik nu ook ingaan op mogelijke kansen. We zien dat big data (grote volumes, verschillende formats en vaak real-time) in allerlei sectoren ongekende mogelijkheden biedt:

- Op medisch terrein is de Google griepanalyse bekend: door zoekgedrag van burgers te analyseren kon sneller dan via de verzameling van epidemiologische gegevens de loop van een griepepidemie voorspeld worden.[168]
- Met behulp van stappentellers ingebouwd in smartphones vonden onderzoekers patronen in obesitas.[169] Ze gebruikten gegevens van ruim 700.000 mensen uit 111 landen in een onderzoek naar fysieke activiteiten van mensen. Het ondervragen van dergelijke aantallen mensen is niet alleen een schier onmogelijke opgave en zeer kostbaar, maar kent ook fikse meetproblemen, waaronder gebrekkige antwoorden (weet iemand wel hoeveel hij loopt) en wenselijke antwoorden.
- De Global Database of Events, Language and Tone (GDELT)[170] is een open databank met gegevens van nieuwsmedia en sociale media in meer dan honderd talen. Hiermee werd onder meer getracht het verloop van de Arabische lente te voorspellen.[171]
- Op basis van zoekgedrag bleek het mogelijk trends in faillissementen in Nederland te voorspellen die bijna volledig in overeenstemming waren de 'echte' faillissementscijfers van het CBS.[172]
- Met behulp van databanken over wijn, konden computermodellen beter voorspellen welke wijn goed zou worden dan vinologen en oenologen dat konden.[173]

Als in al deze verschillende domeinen zoveel mogelijk is met grote hoeveelheden data, waarom zou dit dan niet ook toegepast kunnen worden in het recht?[174] Het recht, zowel rechtswetenschappelijk onderzoek als de rechtspraktijk, beschikt immers ook over grote hoeveelheden gegevens. Juridische documenten als wetgeving, jurisprudentie, beleidsstukken en wetenschappelijke artikelen kunnen worden gekarakteriseerd als *legal big data*: het zijn grote hoeveelheden (datatechnisch gezien) ongestructureerde gegevens. Door recente technologische ontwikkelingen worden deze documenten steeds beter toegankelijk en doorzoekbaar. Hierdoor ontstaan verschillende mogelijkheden om de rechtspraktijk en juridisch onderzoek anders in te richten.

Ik zal nu ingaan op verschillende toepassingen van legal big data voor de rechtspraktijk en juridisch onderzoek. In het bijzonder zal ik ingaan op kwantitatieve juridische voorspelmodellen, het versnellen van juridisch onderzoek en het verbeteren van wet- en regelgeving. Daarna zal ik ook de gevolgen van deze ontwikkelingen voor juristen en hun werkzaamheden kort bespreken.

3.1 Juridische voorspelmodellen

Met behulp van legal big data is het mogelijk om de uitkomsten van rechtszaken te kunnen voorspellen.[175] In de Verenigde Staten worden rechters van het Amerikaanse Hooggerechtshof voorgedragen en benoemd door de president, waardoor ze een politieke kleur hebben. Wanneer er belangrijke uitspraken worden verwacht, is er veel speculatie in de media en door experts of de rechters uitspraak doen in lijn met hun politieke kleur of juist met een verrassende uitspraak komen. De uitspraken kunnen betrekking hebben op allerlei verschillende onderwerpen, zoals belastingrecht, milieurecht, discriminatie, patenten, vrijheid van meningsuiting of strafrecht. Het Hooggerechtshof bestaat uit negen rechters en de uitkomst van een rechtszaak worden door een gewone meerderheid bepaald.

In 2004 organiseerde de Amerikaanse hoogleraar Theodore Ruger een wedstrijd om te kijken wie de uitspraken van het Amerikaanse Hooggerechtshof het beste kon voorspellen: een computer of een team van experts.[176] De computer kreeg als input alle uitkomsten van alle rechtszaken die behandeld waren in het voorgaande jaar. Op basis van ruim 600 zaken werd een model gemaakt dat de uitkomst van nieuwe uitspraken moest voorspellen. Het team van experts bestond uit 83 gerenommeerde rechtenprofessoren en ervaren advocaten. Zowel de computer als de experts moesten voorspellen wat elke individuele hoge rechter zou beslissen en welke meerderheid er zou ontstaan.

Het resultaat was verbluffend. Als het aankwam op het stemgedrag van de individuele rechters voorspellen, deden de computer en de experts het ongeveer even goed (68% resp. 67% juiste voorspellingen), maar bij het voorspellen van de uitkomst van een rechtszaak versloeg de computer de experts met gemak. De computer haalde 75% juiste voorspellingen, terwijl de experts bleven steken op 59%, hetgeen nauwelijks beter is dan een muntje opgooien. Het voorspellen van wat negen rechters samen doen, bleek zo lastig voor de experts dat ze nauwelijks in staat waren de uitkomst correct te voorspellen, terwijl de computer met gemak behoorlijk goede voorspellingen kon doen. Bij de rechters met een uitgesproken ideologie herkenden de experts snel welke kant het uit ging, maar bij gematigde rechters hadden experts moeite de juiste uitkomst te voorspellen, terwijl de computer toch patronen wist te ontdekken.

In 2014 kwamen professor Daniel Katz en zijn team met een sterk verbeterd model waarvoor bijna 8000 rechtszaken van de afgelopen 60 jaar als input werden gebruikt.[177] Dit model haalde 70% juiste voorspellingen voor de zaken en 71% voor de individuele rechters. Dit model was onafhankelijk van de politieke en economische factoren van het moment. Ook was rekening gehouden met het feit dat rechters soms worden vervangen door andere rechters en met het punt dat sommige rechters in de loop der tijd ideologisch opschuiven. In 2016 publiceerden Britse en Amerikaanse wetenschappers ook een accuraat voorspelmodel (79% juiste voorspellingen) voor het Europese Hof voor de Rechten van de Mens.[178] Over enige tijd zullen er ook modellen zijn voor Nederlandse rechterlijke instanties en misschien zelfs wel voor individuele rechters.

Het voorspellen van de uitkomsten van rechtszaken kan zeer nuttig zijn voor de rechtspraktijk, onder meer om in te schatten of het zinvol is om te procederen. Als de kansen op succes gering zijn, kan een raadsman bijvoorbeeld beter aansturen op een schikking voor zijn cliënt. Voorspelmodellen kunnen voor rechtswetenschappers ook een instrument zijn om vast te stellen wat het vigerend positieve recht is en hoe dit moet worden geïnterpreteerd in bepaalde casuïstiek. Voor rechtssociologen kunnen voorspelmodellen interessant zijn om bijvoorbeeld bloot te leggen welke niet-juridische factoren een rol spelen in vonnissen (als in: "Justice is what the judge had for breakfast").[179] Als wordt gekeken naar voorspellingen op terreinen waar nog geen of weinig rechtstheorie aanwezig is, kunnen de middels legal big data blootgelegde verbanden helpen theorieën (verder) te ontwikkelen.

3.2 Versnelling van juridisch onderzoek

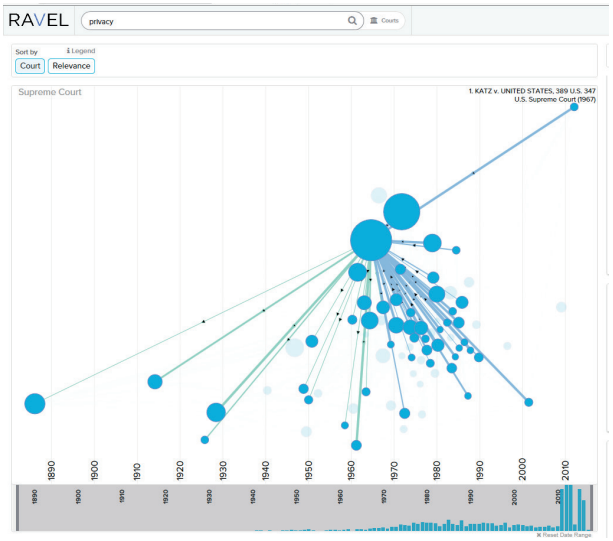
Het voorspellen van uitkomsten van rechtszaken kan in de Verenigde Staten op meer belangstelling rekenen dan in Europa. Hier te lande zullen betrekkelijk weinig juristen hun werk zien zoals de voormalige Amerikaanse opperrechter Oliver Wendell Holmes het zag: "prophesies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law".[180] Een heel ander domein waarin legal big data een bijdrage kan leveren aan de rechtspraktijk en juridisch onderzoek is middels het faciliteren van onderzoek. Daarbij wordt enerzijds gedoeld op voorbereidend juridisch onderzoek dat voorafgaat aan een rechtszaak (zoals het opzoeken van relevante bepalingen en jurisprudentie) en anderzijds juridisch wetenschappelijk onderzoek (zoals dat aan rechtenfaculteiten wordt bedreven). Legal big data kan beide vormen van juridisch onderzoek aanzienlijk verbeteren en versnellen.[181]

Technologiebedrijf IBM ontwikkelde de supercomputer Watson, die in spreektaal gestelde vragen kan interpreteren en het antwoord kan geven na het raadplegen van een verzameling encyclopedieën, boeken, tijdschriften, wetenschappelijke artikelen en websites. In 2011 mocht Watson deelnemen aan de tv-quiz *Jeopardy*, waarin deelnemers het antwoord krijgen en daarbij zelf de correcte vraag moeten stellen. Watson mocht spelen tegen de twee beste spelers uit de geschiedenis van het programma. Een van hen wist is de eerste ronde nog gelijk te spelen tegen Watson, maar daarna werden alle rondes door de computer gewonnen. Watson lijkt erg op de boordcomputer van het ruimteschip Enterprise in *Star Trek*: als de bemanningsleden aan de computer een vraag stellen, kan de computer de vraag begrijpen en een antwoord geven. Dat was ooit sciencefiction, maar bestaat dus al.

Watson is een voorbeeld van kunstmatige intelligentie. De computer wordt gevoed met grote hoeveelheden gegevens en voorzien van software die patronen kan herkennen. Momenteel wordt ROSS, een variant op Watson die specifiek gericht is op het beantwoorden van juridische vragen, ontwikkeld door IBM. Soms wordt wel gedacht dat wetboeken veel exacter moeten worden gespecificeerd in axioma's en definities wil het voor computers mogelijk zijn om ze te interpreteren, maar dat is niet nodig als er grote hoeveelheden gegevens beschikbaar zijn: de computer kan dan zelf op basis van context zulke definities en interpretaties onderscheiden. Overigens is dat bij rechters en rechtswetenschappers niet anders – ook zij geven voortdurend nadere duiding aan allerlei juridische begrippen en wetsartikelen.[182]

Een ander typisch (eveneens Amerikaans) voorbeeld van het faciliteren van juridisch onderzoek middels legal big data is Ravellaw, een innovatief bedrijf dat toegang biedt tot legal big data voor juridisch onderzoek.[183] Ravellaw kan via internet worden geraadpleegd. Een typisch voorbeeld is het zoeken naar jurisprudentie, via het invoeren van zoektermen. Anders dan bijvoorbeeld het Nederlandse rechtspraak.nl wordt niet een lijst met zoekresultaten weergegeven, maar worden ook onderlinge verbanden tussen de uitspraken getoond. In Figuur 1 is een scherm weergegeven waarbij in Ravellaw is gezocht op privacy. Ravellaw toont alle uitspraken (in dit geval van het hooggerechtshof) waarin privacy een rol speelt. Ook de relevantie van elk zaak is weergegeven: grotere bollen naarmate een zaak relevanter is – *landmark cases* zijn de zaken *Katz vs United States* en *Roe vs Wade*. Onderaan in Figuur 1 is ook de frequentie van zaken weergegeven voor elk jaar. Hier komt een onverwacht (en niet nader verklaard) verband uit, namelijk een forse toename van uitspraken in 2010.

Het gebruik van legal big data voor juridisch onderzoek heeft als voordeel dat de kans op het missen van belangrijke informatie (zoals een belangrijke rechtszaak) aanzienlijk afneemt.[184] Doordat grotere hoeveelheden jurisprudentie en andere juridische documentatie kunnen worden verwerkt (hetgeen iemand dagen of weken tijd zou kosten om door te nemen), kan de nauwkeurigheid en de betrouwbaarheid van juridisch onderzoek aanzienlijk worden vergroot. Verder kunnen, zoals hierboven aangegeven, nieuwe, onverwachte verbanden worden gevonden. Ook deze toepassing van legal big data kan een instrument zijn om vast te stellen wat het vigerend positieve recht is en hoe dit moet worden geïnterpreteerd in bepaalde casuïstiek. Bovendien kan deze toepassing worden ingezet om onderliggende rechtssociologische verbanden bloot te leggen, om rechtstheorieën verder te ontwikkelen en om wet- en regelgeving te ontwikkelen en/of verbeteren. Op dit laatste wordt hieronder verder ingegaan.



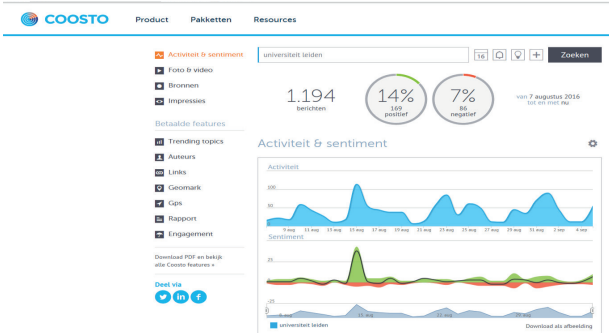
Figuur 1: Visuele weergave van gerechtelijke uitspraken (US Supreme Court) over privacy in Ravellaw.

3.3 Beter naleefbare regelgeving

Een derde toepassing van legal big data is op het terrein van verbeterde wet- en regelgeving. Onderdeel van bepaald juridisch werk (bijvoorbeeld van rechters, rechtswetenschappers, beleidsjuristen en wetgevingsjuristen) is immers ook rechtsvorming. Ook hier kan legal big data van toegevoegde waarde zijn, bijvoorbeeld wanneer legal big data wordt gecombineerd met big data afkomstig van sociale media. Gegevens op sociale media zijn ook big data, omdat het grote hoeveelheden (miljoenen gebruikers), ongestructureerde (tekst, foto's, filmpjes), snelle (real-time berichtgeving) gegevens betreft. Deze gegevens kunnen worden gebruikt om te onderzoeken hoe grote hoeveelheden mensen over bepaalde zaken denken.

Een typisch voorbeeld is Coosto, een softwarebedrijf uit Eindhoven, dat zogeheten sentimentanalyses uitvoert op basis van gegevens op sociale media. Daarbij worden berichten op sociale media als Twitter en Facebook geanalyseerd met text mining (geautomatiseerd naar patronen zoeken in teksten).

Aan de hand van deze analyses wordt vastgesteld of de berichten positief of negatief zijn over een bepaald onderwerp. In Figuur 2 is een scherm weergegeven waarbij in Coosto is gezocht op Universiteit Leiden. In de voorgaande periode waren er 1194 berichten op sociale media, waarvan 14% positief en 7% negatief. Dergelijke sentimentanalyses zijn voor rechtsvormers interessant om na te gaan welke voorstellen voor beleid, regelgeving en wetgeving kunnen rekenen op maatschappelijke acceptatie. Omdat publieke steun ook kan variëren door de tijd heen, kunnen sentimentanalyses ook worden gebruikt om de juiste timing te kiezen voor het lanceren van nieuwe plannen, zoals wetsvoorstellen of nieuw beleid.[185] Dat er sprake is van real-time gegevens kan bijdragen aan het vergroten van de inzichten.



Figuur 2: visuele weergave van sentimentanalyses op sociale media door Coosto (zoekterm: Universiteit Leiden).

Legal big data kan niet alleen helpen bij het inschatten van maatschappelijke acceptatie, maar ook bij het verbeteren van de inhoud van rechtsvormend juridisch werk. Door juridische data te combineren met data over het gedrag van mensen wordt het mogelijk na te gaan welke regels (of welke typen regels) beter nageleefd worden en/of beter te handhaven zijn. Een mooi voorbeeld is het lopen over het gras in plaats van het betegelde pad in een stadspark.[186] Als de paden te veel een omweg zijn, zijn mensen geneigd om hun route af te korten en een stukje over het gras te lopen. Na verloop van tijd slijt in

het gras een nieuw pad uit en zijn mensen steeds meer geneigd deze nieuwe route te gebruiken. De uitgesleten paden laten een heel nieuw routenetwerk zien ten opzichte van het initiële geplaveide netwerk. Het nieuwe routenetwerk zou eenvoudig het oude netwerk kunnen vervangen en zal veel beter 'nageleefd' worden door de wandelaars.

Sociale media data kunnen tal van gedragspatronen blootleggen van mensen, waaronder hun reisbewegingen, hun aankoopgedrag, hun eetgedrag en hun lichaamsbeweging. In combinatie met legal big data kan dit inzichten opleveren over hoe mensen gedragsmatig zullen reageren op voorgestelde wet- en regelgeving. Die gegevens kunnen ook worden gebruikt om achteraf beleid en wetgeving te evalueren.[187] Een typisch voorbeeld kan zijn het evalueren van een justitiële interventie, bijvoorbeeld het instellen van cameratoezicht in de binnenstad of het opleggen van een taakstraf aan winkeldieven. Net als bij het evalueren van medische interventies worden idealiter een testgroep en een controlegroep vergeleken, waarbij alleen de factor die wordt onderzocht, verschillend is. Een zogeheten *randomized controlled trial* kan in veel gevallen te kostbaar blijken of niet worden ingezet om ethische of praktische redenen. Niettemin kunnen met behulp van big data wel steeds beter achteraf controlegroepen worden samengesteld voor een quasi-experimenteel design. Naarmate de omvang van datasets toeneemt, kunnen er bijvoorbeeld meer 'twins' (individuen of groepen die in alles op elkaar lijken behalve het attribuut dat wordt onderzocht) worden gevonden. Ook doordat interventies gefaseerd worden ingevoerd, kunnen groepen ontstaan die met elkaar vergeleken kunnen worden. Daarmee wordt de zeggingskracht van evaluaties aanzienlijk sterker en dat kan weer bijdragen aan beleid of wetgeving dat evidence-based is. Verder kunnen er door de toename in de hoeveelheden beschikbare gegevens steeds fijnmazigere inzichten ontstaan, bijvoorbeeld dat een taakstraf voor winkeldieven alleen goed werkt bij jongeren van wie de ouders niet gescheiden zijn.

Het gebruik van legal big data voor het verbeteren van wet- en regelgeving kan bijdragen aan het werk van rechtssociologen, aan het ontwikkelen van rechtstheorieën en aan evidence-based rechtsvorming. Een typisch voorbeeld is het gebruik van online zoekgedrag om kennis te verkrijgen over de bijdrage van een (Amerikaanse) beleidsinterventie op het aanpakken van digitale piraterij.[188] Naast het evalueren van interventies en maatregelen kan legal big data ook bruikbaar zijn bij het evalueren van wetgeving.[189] Denk daarbij bijvoorbeeld aan het in kaart brengen van de aard en omvang van rechtszaken, gedragsveranderingen bij groepen burgers en/of kostenbesparingen die verband houden met bepaalde wetgeving.

Niet ondenkbaar is dat de ontwikkelingen rondom "Quantified Self", waarbij mensen met behulp van apps, sensoren en 'injectables' van alles over zichzelf vastleggen, hierin een belangrijke rol gaan spelen. Fawcett zegt het zo: "The last several years have seen an explosion of interest in wearable computing, personal tracking devices, and the so-called Quantified Self (QS) movement. Quantified self involves ordinary people recording and analyzing numerous aspects of their lives to understand and improve themselves".[190] In de medische wereld wordt dit soort gegevens al gebruikt om te komen tot 'personalized medicine'. Het is niet ondenkbaar dat iets dergelijks ook gebeurt bij het ontwerpen en invoeren van gedragsinterventies in de wereld van veiligheid en justitie.[191]

3.4 Een nieuwe generatie juristen

Veel juristen zijn niet snel geneigd te zeggen dat ze met data werken of gegevens analyseren – dat is vaak iets voor mensen in andere disciplines. Dat beeld komt ook naar voren uit de resultaten van een uitgebreide landelijke enquête onder Nederlandse rechtswetenschappers van enkele jaren geleden.[192] Daaruit blijkt dat rechtswetenschappers hun onderzoek nauwelijks associëren met exacte wetenschappen, al is wel een duidelijke toenadering tot de sociale wetenschappen te bespeuren.

Kortom, veel juristen zien zichzelf niet als een beroepsgroep die werkt met data. Toch is niets minder waar. Het juridische werk impliceert nagenoeg het werken met big data: het gaat om grote hoeveelheden gegevens over vele jaren, soms uit meerdere landen (volume – omvangrijke teksten), die vaak (in technologisch opzicht)[193] ongestructureerd zijn (variety – verschillende formaten). Juridische documenten, waaronder wetgeving, jurisprudentie, beleidsstukken en wetenschappelijke artikelen, kunnen om die reden niet alleen worden beschouwd als data, maar zelfs als big data. Deze nieuwe kansen vragen om een nieuwe generatie juristen die hiermee goed om kan gaan en de vruchten van kan plukken.

In de Verenigde Staten is het gebruik van legal big data al aanzienlijk verder doorgedrongen in de rechtspraktijk en de rechtswetenschappen. Inmiddels zijn de resultaten van deze ontwikkelingen ook al zichtbaar. De werkgelegenheid voor afgestudeerde rechtenstudenten is afgenomen, deels veroorzaakt doordat bedrijfsmodellen voor juridische dienstverlening aanzienlijk zijn veranderd. Door zowel toegenomen technologische mogelijkheden als de opkomst van deze nieuwe, innovatieve bedrijfsmodellen is de traditionele juridische dienstverlening onder druk komen te staan. Er zijn drie belangrijke veranderingen in de markt voor juridische dienstverlening, waarvan de eerste twee mogelijk worden gemaakt door legal big data en technologische ontwikkelingen:[194]

1. Er worden meer betaalbare, gestandaardiseerde, veralgemeniseerde diensten aangeboden, soms zelfs online.
2. Juristen zijn productiever geworden, waardoor dezelfde hoeveelheid werk door minder mensen kan worden gedaan.
3. Juristen hebben niet langer een alleenrecht op het aanbieden van juridische dienstverlening.

De arbeidsmarkt voor juristen wordt hierdoor op twee manieren minder aantrekkelijk. Ten eerste is er minder werkgelegenheid en ten tweede zijn salarissen minder aanlokkelijk, omdat werkgevers door een overschot aan werkzoekenden minder hoeven te betalen voor hun personeel. Er worden in de VS jaarlijks bijna twee keer zoveel juristen opgeleid als er banen zijn.[195] Hierdoor kunnen werkgevers de beste studenten selecteren na hun studie zonder diep in de buidel te hoeven tasten. Het gevolg is dat het steeds minder aantrekkelijk is geworden voor aankomende studenten om rechten te gaan studeren. Het aantal aanmeldingen van rechtenstudenten is in de periode 2005-2015 gedaald met maar liefst 40%.[196]

In Nederland lijkt de arbeidsmarkt voor juristen nog steeds prima. Sterker nog, het aantal juridische vacatures blijft stijgen.[197] Niettemin lijkt het goed voor juristen (en hun opleiders) om deze ontwikkelingen nauwgezet te volgen. De toekomstige manier van werken zal in toenemende mate gekarakteriseerd worden door lagere loonkosten, grootschalig maatwerk, recyclebare juridische kennis en alom aanwezige informatietechnologie.[198] Daardoor zal een deel van het werk kunnen worden uitbesteed aan andere beroepsgroepen, vergelijkbaar met een arts die bepaalde zaken uitbesteedt aan de verpleging of de assistent. Bij de griffie staan vele arbeidsplaatsen op het spel, met name omdat meer zaken digitaal zullen worden afgehandeld.[199] Juridisch werk zal (ook op lange termijn) zeker niet overbodig of vervangbaar worden, maar zal wel van karakter veranderen door legal big data. Daardoor wordt enige basale technologische kennis steeds belangrijker voor juristen. Volgens sommigen blijft deze kennis nu achter.[200] Dit houdt niet in dat juristen moeten kunnen programmeren, maar wel dat ze enig zicht hebben op technologische ontwikkelingen en de (on)mogelijkheden die daarbij horen.[201]

Gaan deze ontwikkelingen juristen en juridisch werk overbodig maken? Nee, de zeer grote hoeveelheden gegevens die beschikbaar komen, ook real-time, zullen niet per ommegaande alle vragen naar oorzakelijke verbanden beantwoorden, zonder zelfs maar behoefte te hebben aan verklarende theorieën. Ook in de gedigitaliseerde, gedataficeerde samenleving is meer nodig dan data om dingen te begrijpen en verklaren. Bovendien,

maar daar kom ik zo meteen op, zijn bij het ontwikkelen van nieuwe technologie juist normatieve disciplines zeer relevant.

Daarom is legal big data niet zozeer een vervangende aanpak voor de rechtspraktijk en juridisch onderzoek, maar vooral een aanvullende aanpak die kan versnellen en verdiepen. Het zou vreemd zijn als big data op tal van gebieden (waaronder geneeskunde, astronomie, sociale wetenschappen en psychologie) haar vruchten afwerpt en niet op het juridische domein. In de toekomst zal legal big data waarschijnlijk een steeds prominentere rol gaan vervullen in de rechtspraktijk en juridisch onderzoek. Onderdelen van het werk van juristen zullen daardoor mogelijk veranderen of verschuiven naar andere beroepsgroepen. Hoe dat gaat verlopen moet nog blijken, want de ontwikkelingen in big data staan allerminst stil.

4. Conclusies

Ik ben toegekomen aan enkele conclusies.

Tot dusver heb ik besproken hoe de ontwikkelingen op het terrein van digitale technologie, in het bijzonder big data en data science, relevant zijn op de belangrijkste rechtsgebieden in zowel het publiekrecht als het privaatrecht.[202] Tevens heb ik laten zien hoe deze technologische ontwikkelingen van invloed zijn op de rechtspraktijk en rechtswetenschappelijk onderzoek. De keuze om juist een veelheid aan gebieden te bespreken is een bewuste, om te tonen dat er zoveel gaande is op dit moment. Zoals ik in de inleiding al aangaf, gaat technologieontwikkeling exponentieel in de tijd. Technologie neemt in de maatschappij nu reeds een zeer prominente plek in en het is nauwelijks te voorzien hoe technologisch onze samenleving zal zijn over enkele decennia. Het toenemend belang van technologie in onze samenleving zal ertoe leiden dat ook het belang van technologie in het recht toeneemt. Ik heb geprobeerd te tonen dat dit niet exclusief beperkt is tot het vakgebied van het IT-recht, maar doordringt in alle rechtsgebieden.

Dat vraagt om samenwerking, zowel tussen rechtsgebieden als tussen disciplines. Mijn brede benadering hierboven is daarom tevens een handreiking, enerzijds naar juristen uit verschillende rechtsgebieden en anderzijds naar wetenschappers uit andere vakgebieden (zoals technologie en filosofie) om gezamenlijk de uitdagingen waarvoor we staan op te pakken. Ik ben zeer verheugd over het grote SAILS-programma dat onze universiteit heeft opgezet om kunstmatige intelligentie vanuit alle faculteiten op de kaart te zetten.[203] In plaats van een technologische aanpak is gekozen voor een interdisciplinaire aanpak, waarin technologen zoals datawetenschappers, informatici, wiskundigen en chemici samenwerken met psychologen, taalkundigen, medici, archeologen, juristen en filosofen.

Dit is precies wat we nodig hebben voor de toekomst. We zullen over de grenzen van rechtsgebieden en wetenschapsdomeinen heen moeten kijken om de uitdagingen waarvoor we staan te kunnen adresseren. Het aloude risico van multidisciplinair werk is echter dat het ten koste gaat van diepgang en dat kunnen we ons niet veroorloven. Vandaar dat we experts nodig hebben die grondig zijn opgeleid in specifieke disciplines, maar die tegelijkertijd getraind zijn op samenwerking met experts die een totaal andere achtergrond hebben.

Specifiek voor juristen is dus het goede nieuws dat er de komende jaren veel werk te doen is om dit allemaal in goede banen te leiden. Maar tegelijkertijd is de grote uitdaging om een open mindset te hebben en bereid te zijn over de grenzen van je eigen vakgebied heen te kijken. Dat is onontgonnen terrein, buiten de *comfort zone*, en kan dus onzekerheid en risico's met zich brengen.[204] De jurist van de toekomst zal steeds nieuwe verbindingen aangaan en een flexibele en open houding moeten hebben om te kunnen inspringen op nieuwe problemen en uitdagingen. Ook op juridisch onderzoek en onderwijs is dit van toepassing, opdat onderzoek daadwerkelijk vernieuwend is en onze studenten het meest actuele onderwijsprogramma krijgen aangeboden.

De onderwerpen die ik heb aangesneden, ogen mogelijk als een breed en veelkleurig palet, maar ze hebben één belangrijk ding gemeenschappelijk, namelijk dat we moeten zoeken naar wat ik noem een goede reguleringsbalans. Het is laveren tussen Scylla en Charybdis. Aan de ene kant loert het gevaar van overregulering, te veel en te gedetailleerde regelgeving, met als gevolg dat naleving en handhaving lastig zijn en, belangrijker nog, dat innovatie en technologieontwikkeling in de kiem worden gesmoord. Aan de andere kant loert het gevaar van gebrekkige spelregels, met als gevolg inadequate rechtsbescherming en rechtsonzekerheid. Ook dat kan namelijk een rem op technologieontwikkeling zijn, want zonder vertrouwen gaat niemand investeren.

Een goede reguleringsbalans zoekt uiteraard naar een optimum tussen beide valkuilen en zorgt ervoor dat we de kansen en

mogelijkheden van nieuwe technologie optimaal exploreren en benutten, terwijl we de risico's en bedreigingen zoveel mogelijk voorkomen en mitigeren. Dat klinkt logisch, maar het ingewikkelde is het eens te worden over welke ontwikkelingen we dan als kansen en welke we als bedreigingen beschouwen.

Gelukkig is dat nu juist waar juristen en ethici goed in getraind zijn. Het zijn normatieve disciplines waarin uiteenlopende instrumenten zijn ontwikkeld om zulke afwegingen te maken. In het digitale tijdperk zullen die juridische en ethische afwegingskaders regelmatig moeten worden herzien en soms moeten zelfs nieuwe instrumenten worden ontwikkeld en daar zijn we volop mee bezig.[205] Als we de spelregels voor de toekomst willen vaststellen, is het van belang niet zozeer een positiefrechtelijk perspectief in te nemen, maar vooral onderliggende waarden goed in het vizier te houden.[206] Waarden als vertrouwen,[207] welzijn, menselijke waardigheid[208] en rechtvaardigheid zijn dan onze meer tijdloze en technologie-onafhankelijke ankers.

Terug naar de toekomst. Wat de toekomst ons zal brengen is onzeker. Maar wat zich duidelijk aftekent, is een toekomst waarin technologie een steeds prominentere rol zal spelen. Waarschijnlijk niet eens op een erg zichtbare manier, maar vooral op een geïntegreerde manier, ingebouwd in onze gebouwde omgeving, onze apparaten en onze lichamen, nauwelijks zichtbaar. Welke kant het op zal gaan, hangt af van onze keuzes. Het is van belang dat we ons realiseren dat er op dit moment niemand is die in de *driver's seat* zit. Daarom is voor het recht hierin een belangrijke rol weggelegd om spelregels op te stellen over wat we wel en wat we niet ok vinden. Dit is het moment om goed na te denken over welke richting we willen inslaan. De toekomst hangt af van wat we vandaag doen.[209]

5. Dankwoord

Beste toehoorders, ik ben aangekomen bij het traditionele slotwoord dat hoort bij een oratie. Allereerst wil ik allen bedanken die hebben bijgedragen aan de totstandkoming van mijn benoeming. Daarbij noem ik graag het College van Bestuur en het Faculteitsbestuur, in het bijzonder (voormalig) rector Carel Stolker en decaan Joanne van der Leun voor het vertrouwen dat zij in mij stellen. Daarnaast dank ik graag Bert-Jaap Koops, Peter Blok, Tal Zarsky, Frans Leeuw, Afshin Ellian, Titia Loenen en Paul van Dam voor hun rol hierin. Ik ben er trots op dat deze mensen, die voor mij op uiteenlopende manieren voorbeeldrollen vervullen, hebben willen bijdragen aan mijn benoeming.

Maar de belangrijkste persoon in dit geheel was en is Simone van der Hof. Beste Simone, ik wil je heel hartelijk danken voor de fijne samenwerking van de afgelopen jaren, waarvan ik hoop dat er nog vele volgen. Het is alweer tien jaar geleden dat ik aan deze universiteit ging werken, al was dat toen nog part-time. Toen jij, niet heel veel later, ons nieuwe afdelingshoofd werd, begon je met het uitbouwen van de afdeling tot het team dat er nu staat – een bloeiende, inspirerende en plezierige werkplek. Een team waarvan ik altijd graag deel heb willen uitmaken en waarin mensen de ruimte krijgen om niet alleen te mogen zijn wie ze zijn, maar ook te worden wie ze werkelijk zijn. Dat ik inmiddels ook leiding mag geven aan dit team, had ik nooit gedacht. Gelukkig ben jij als onze Wetenschappelijk Directeur nog steeds beschikbaar voor raad en daad.

Aan deze eeuwenoude universiteit, die bol staat van tradities, is eLaw een piepjong instituut. Maar ook in de paar decennia die eLaw oud is, hebben we al verschillende tradities opgebouwd. Ik ben blij dat onder meer Jaap van den Herik, Franke van der Klaauw, Aernout Schmidt en Hans Franken mij hebben bijgepraat over deze historie van eLaw.

Officieel ben ik de eerste SAILS-hoogleraar, binnen het universiteitsbrede onderzoeksprogramma op het terrein van kunstmatige intelligentie onder leiding van Joost Batenburg en voorheen Aske Plaat. Het samenwerken over faculteitsgrenzen heen met de vele talenten die onze universiteit rijk is, vind ik buitengewoon inspirerend. Zo leer ik elke keer weer nieuwe dingen, dat is precies wat dit werk zo leuk maakt.

Ik realiseer mij heel goed dat ik niet zomaar hier gekomen ben. Ik zal hier niet mijn hele loopbaan opsommen, maar wil in elk geval mijn promotores Corien Prins, Anton Vedder en Henk van Tilborg noemen als belangrijkste leermeesters. Er waren (en zijn) nog vele anderen. Samen hebben zij de basis hebben gelegd voor het wetenschappelijk maken van mijn nieuwsgierigheid.

Beste collega's van eLaw, ik zou jullie graag allen persoonlijk toespreken, maar daarvoor is hier geen ruimte. Graag wil ik jullie bedanken voor de collegialiteit en inspirerende sfeer die jullie met zijn allen creëren. Ik ben er trots op deel te mogen uitmaken van een team met zulke enthousiaste, kundige en innovatieve mensen. Ik ben vol vertrouwen dat we in de nabije toekomst samen nog veel meer mooie resultaten gaan neerzetten.

Dat geldt ook voor de promovendi die ik mag begeleiden. Helena en Clemens hebben inmiddels hun proefschrift afgerond. Alan, Lexo, Linda, Mason, Dimitra, Andreas, Georgios, Oliver, Marc, Nikki en Kimia zijn hiermee nog volop bezig. Ik ben benieuwd waar ons gedeelde enthousiasme ons gaat brengen.

Mijn dank gaat ook uit naar de studenten waarop deze universiteit draait. Het is altijd een plezier college te mogen geven aan degenen die de toekomst gaan bepalen, of dat nu VWO-scholieren of bachelor, master of postgraduate studenten zijn.

De studenten van onze Advanced Master komen uit de hele wereld, waardoor wij veel van elkaar kunnen leren. Uit hetgeen ik vandaag heb gezegd, zal u duidelijk zijn geworden dat onze samenleving meer dan ooit behoefte heeft aan juristen met kennis van technologie en aan technologen met kennis van het recht.

Beste familie en vrienden, ik ben blij dat jullie hier en online aanwezig zijn. Ook jullie kan ik niet individueel toespreken, maar ik ben jullie zeer dankbaar voor alle steun door de jaren heen. Als mijn verhalen en theorieën jullie al te erg vermoeid hebben, hebben jullie dat nooit heel veel laten blijken.

Mijn ouders bedank ik graag voor het feit dat ze mij van jongs af aan alle vrijheid, ruimte en vertrouwen hebben gegeven. Als mij iets niet lukte, kreeg ik regelmatig het advies nog eens na te denken hoe het dan wel moest. Dat heeft me altijd veel geholpen. Het spijt me dat mijn moeder dit niet meer mag meemaken, maar ik weet zeker dat ze trots zou zijn geweest.

Lieve Merel, wat kan ik zeggen? Zonder jou was ik hier nooit gekomen. Het is buitengewoon fijn om iemand te hebben die je begrijpt en met wie je dingen kunt bespreken. Maar misschien is het belangrijker te zeggen dat hoe leuk en belangrijk ik mijn werk ook vind, het niet veel zou zijn zonder jou en de kinderen. Ik dank je wel voor al je steun en geduld. Fijn dat je bent wie je bent.

Lieve Anna, Sophie, Bram, Eva, wat ben ik trots op jullie. Met zijn vieren zorgen jullie ervoor dat elke dag weer een nieuwe ervaring is voor jullie moeder en mij. Als ik jullie nieuwsgierigheid en leergierigheid zie, herken ik daarin mezelf. Als ik jullie verstandige dingen hoor zeggen, herken ik daarin jullie moeder. Wat fijn dat jullie er zijn. Jullie zijn de toekomst.

Ik heb gezegd.

Bibliografie

Abe, N. & Kamba T. (2000) A Web Marketing System With Automatic Pricing, *Computer Networks*, Vol. 33, 775-788.

Aletras, N., Tsarapatsanis, D., Preoțiuc-Pietro, D., & Lampos, V. (2016) Predicting judicial decisions of the European Court of Human Rights, *PeerJ Computer Science,* 2:e93.

Althoff, T., Sosič, R., Hicks, J.L., King, A.C., Delp, S.L., Leskovec, J. (2017) Large-scale physical activity data reveal worldwide activity inequality. *Nature*, DOI: 10.1038/nature23018.

Amerongen, N.H. van & Schuurmans, Y.E. (2019) Advies van een deskundige of een algoritme? De toetsing van 'black box'-besluiten door de bestuursrechter. In: Huisman P.J., Neerhof A.R., Ommeren F.J. van (red.) *Verwant met verband: Ruimte, Recht en Wetenschap (vriendenbundel voor prof. mr. J. Struiksma).* ‹s-Gravenhage: IBR, p. 175-196.

Asimov, I. (1950) *Runaround. I, Robot,* New York City: Doubleday. p. 40.

Ayres, I. (2007) *Super Crunchers: How Anything Can Be Predicted*. London: John Murray Publishers.

Ball, P. (2004) *Critical Mass; How One Thing Leads to Another*, New York: Farrar, Straus and Giroux.

Bamberger, K.A., and Mulligan D.K. (2015) *Privacy on the Ground in the United States and Europe*, MIT Press.

Barberá, P., et al. (2015) Tweeting from left to right: Is online political communication more than an echo chamber? *Psychological science* 26.10 (2015), p. 1531-1542.

Barkhuysen, T. (2016) De Homo Digitalis als uitdaging voor het recht, *Nederlands Juristenblad*, Afl. 22, p. 1527.

Barocas, S. & Selbst, A. (2016) Big Data's Disparate Impact, 104 *California Law Review*, 671.

Baveye, Y., Bettinelli, J.N., Dellandrea, E., Chen, L. and Chamaret, C. (2013) A large video data base for computational models of induced emotion. In *Proceedings of Humane Association Conference on Affective Computing and Intelligent Interaction*.

Böhme, R. (2009) Valuating Privacy with Option Pricing Theory. In: Berthold, S. (ed.) Workshop on the Economics of Information Security (WEIS 2009), June 24-25. University College London, London.

Boom, W.H. van, Gestel, R.A.J. van (2015) Rechtswetenschappelijk onderzoek – een samenvatting van de uitkomsten van een landelijke enquête, *Nederlands Juristenblad*, Vol. 20, p. 1336-1347.

Borth, D., Chen, T., Ji, R.R., and Chang, S.F. (2013) Sentibank: Large-scale ontology and classifiers for detecting sentiment and emotions in visual content. In *Proceedings of ACM Multimedia*.

Bovens, L. (2009) The Ethics of 'Nudge'. In Preference Change: Theory and Decision Library. Vol. 42., edited by T. Grüne-Yanoff and S. O. Hansson, 207–219. Dordrecht: Springer.

Boyd, D., and Crawford, K. (2012) Critical questions for big data: provocations for a cultural, technological and scholarly phenomenon, *Information, communication & society*, 15(5), p. 662-679.

Buechi, M., Fosch-Villaronga, E., Lutz, C., Tamò, A., Velidi, S. & Viljoe, S. (2020) The Chilling Effects of Algorithmic Profiling: Mapping the Issues, *Computer Law & Security Review,* https://doi.org/10.1016/j.clsr.2019.105367.

Burns, E. (2016) Why haven't SMEs cashed in on big data benefits yet? *TechTarget*. http://searchbusinessanalytics.techtarget.com/feature/Why-havent-SMEs-cashed-in-on-big-data-benefits-yet.

Calders, T. & Custers, B.H.M. (2013) What is data mining and how does it work? In: Custers, B.H.M., Calders, T., Schermer, B., Zarsky, T. (red.) *Discrimination and Privacy in the Information Society.* nr. 3 Heidelberg: Springer.

Calders, T., Žliobaitė, I. (2013) Why unbiased computational processes can lead to discriminative decision procedures, in: Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) (2013) Discrimination and privacy in the information society, Heidelberg: Springer.

Cavoukian, A. (2013) Operationalising privacy by design: a guide to implementing strong privacy practices. Privacy Commissioner of Ontario, Ontario. https://www.privacybydesign.ca/con- tent/uploads/2013/01/operationalizing-pbd-guide.pdf.

Chadwick, R., Levitt, M., and Shickle, D. (1997) *The right to know and the right not to know*, Aldershot, U.K.: Avebury Ashgate Publishing Ltd.

Charney, S (1994) Computer crime: Law enforcement's shift from a corporeal environment to the intangible, electronic world of cyberspace, *Federal Bar News*, *41*(7), p. 489.

Clarke, R. (2011) An Evaluation of Privacy Impact Assessment Guidance Documents, *International Data Privacy Law*, 1, 2, March 2011, p. 111-120.

Colonna, K. (2012) Autonomous Cars and Tort Liability, *Journal of Law, Technology & The Internet*, Vol. 4, No. 4, p. 81-130.

Couts, A. (2011) Why did Amazon charge $23,698,655.93 for a textbook? *Digital Trends*, 23 April 2011.

Custers, B.H.M. (2003) *Effects of Unreliable Group Profiling by Means of Data Mining*. In: G. Grieser, Y. Tanaka and A. Yamamoto (eds.) *Lecture Notes in Artificial Intelligence, Proceedings of the 6th International Conference on Discovery Science (DS 2003)* Sapporo, Japan. Berlin, Heidelberg, New York: Springer-Verlag, Vol. 2843, p. 290-295.

Custers, B.H.M. (2004) *The Power of Knowledge; Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Tilburg: Wolf Legal Publishers, pp. 300.

Custers, B.H.M. (2008) The Exclusivity of Ultrafast Communication Networks, *Journal of International Commercial Law and Technology*, Vol. 3, Issue 4, p. 247-253.

Custers, B.H.M. (2008) Tapping and Data Retention in Ultrafast Communication Networks, *Journal of International Commercial Law and Technology*, Vol. 3, Issue 2, 2008, p. 94-100.

Custers, B., Dorbeck-Jung, B., Faber, E., Iacob, S., Koops, B.J., Leenes, R., Poot, H. de, Rip, A., Teeuw, W.B. (red), Vedder, A. (red.), Vudisa, J. (2008) *Security Applications for Converging Technologies; impact on the constitutional state and the legal order,* WODC rapport, Telematica Instituut, Enschede en Universiteit van Tilburg.

Custers, B.H.M. (2009) Whose responsibility is it anyway? Dealing with the consequences of new technologies. In: Sollie P., Duwell M. (red.) *Evaluating new technologies: Methodological problems for the ethical assessment of technology developments.* New York: Springer. 21-34.

Custers, B.H.M. (2012) Technology in Policing: Experiences, Obstacles and Police Needs, *Computer Law & Security Review*. Vol. 28, No. 1, p. 62-68.

Custers, B.H.M. (2012) Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination, *Privacy Observatory Magazine* 2012(3).

Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) (2013) *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*, Heidelberg: Springer.

Custers, B., Van der Hof, S., Schermer, B., Appleby-Arnold, S., and Brockdorff, N. (2013) Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law, *SCRIPTed, Journal of Law, Technology and Society*, Volume 10, Issue 4, p. 435-457.

Custers, B., Van der Hof, S., Schermer, B. (2014) Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, *Policy & Internet*, Vol. 6, No. 3, p. 268-295.

Custers, B.H.M., and Schermer, B.W. (2014) Responsibly Innovating Data Mining and Profiling Tools; A New Approach to Discrimination Sensitive and Privacy Sensitive Attributes, In: J. van den Hoven, B.J. Koops, H. Romijn, T. Swierstra and N. Doorn (eds.) *Responsible Innovation Volume 1: Innovative Solutions for Global Issues*. Dordrecht: Springer, p. 335-350.

Custers, B., Vergouw, B. (2015) Promising policing technologies: Experiences, obstacles and police needs regarding

law enforcement technologies, *Computer Law & Security Review*, 31, p. 518-526.
Custers, B.H.M. (2016) Click here to consent forever: Expiry dates for informed consent, *Big Data & Society*: 1-6.
Custers, B.H.M. (2016) *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*. Heidelberg: Springer.
Custers, B.H.M. (2016), Big Data in wetenschappelijk onderzoek, *Justitiële Verkenningen*, Vol. 2016, nr. 1, p. 8-21.
Custers, B.H.M., & Ursic, H. (2016) Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection, *International Data Privacy Law*, pp. 1-12. DOI: 10.1093/idpl/ipv028.
Custers, B.H.M., Oerlemans, J.J., en Pool, R.L.D. (2016) Ransomware, cryptoware en het witwassen van losgeld in Bitcoins, *Strafblad*, Jaargang 14, Nummer 2, mei 2016, p. 87-95.
Custers, B.H.M. (2017) *Cyber agent technology en de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV)*, Leiden: Universiteit Leiden, 30 september 2017, 30 pp.
Custers, B.H.M., & Leeuw, F. (2017) Legal big data, *Nederlands Juristenblad,* afl. 34, p. 2449-2456.
Custers, B.H.M. (2017) Kunnen computers het wetboek interpreteren? In: De Graaf B, Rinnooy Kan A. (red.) *Hoe zwaar is licht? Meer dan 100 dringende vragen aan de wetenschap.* Amsterdam: Balans.
Custers, B.H.M. (2018) Aansprakelijkheid voor drones: technologische ontwikkelingen en de toepasbaarheid van het aansprakelijkheidsrecht, *Maandblad voor Vermogensrecht,* nummer 7-8, p. 235-242.
Custers, B.H.M., and Bachlechner, D. (2018) Advancing the EU Data Economy; Conditions for Realizing the Full Potential of Data Reuse, *Information Polity,* Vol. 22, No. 4, p. 291-309. DOI 10.3233/IP-170419.
Custers, B., Dechesne, F., Sears, A., Tani, T., Van der Hof, S. (2018) A comparison of data protection legislation and policies across the EU, *Computer Law & Security Review,* Vol. 34, Nr. , p. 234-243, http://dx.doi.org/10.1016/j.clsr.2017.09.001.
Custers, B.H.M., Sears, A.M., Dechesne, F., Georgieva, I.N., Tani, T., and Van der Hof, S. (2019) *EU Personal Data Protection in Policy and Practice*, Heidelberg: Asser/Springer. pp. 249.
Custers, B.H.M. (2019) Nieuwe digitale (grond)rechten, *Nederlands Juristenblad*, afl. 44, p. 3288-3295.
Custers, B.H.M., Overwater, L.J. (2019) Regulating Initial Coin Offerings and Cryptocurrencies: A Comparison of Different Approaches in Nine Jurisdictions Worldwide, *European Journal of Law and Technology*, Vol. 10, Issue 3, pp. 29.
Custers, B., Pool, R., and Cornelisse, R., (2019) Banking Malware and the Laundering of its Profits, *European Journal of Criminology,* Vol. 16, nr. 6, p. 728-745. https://doi.org/10.1177/1477370818788007.
Custers, B.H.M., Ursic, H., and Friedewald, M. (2019) Assessing the Legal and Ethical Impact of Data Reuse: Developing a tool for Data Reuse Impact Assessments (DRIA), *European Data Protection Law Review*. Vol. 5, nr. 3, p. 317-337.
Custers, B.H.M. (2019) Reuse of data in smart cities: legal and ethical frameworks for big data in the public arena, in: F. Feldberg et al. (eds.) *Appropriate use of data in public space: essay collection*, Den Haag: NL Digitaal, p. 9-35.
Custers, B.H.M., Oerlemans, J.J., Pool, R. (2020) Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies, *European Journal of Crime, Criminal Law and Criminal Justice,* 28 (2020), p. 121-152.
Custers, B.H.M. en Stevens, L. (2021) The Use of Data as Evidence in Dutch Criminal Courts. *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 29, Nr. 1, p. 25-46.
Daily Wire (2018) Europe Considers Granting Robots Legal Status, *Daily Wire*, 13 April 2018. https://www.dailywire.com/news/29397/europe-considers-granting-robots-legal-status-paul-bois.

Dakers, M. (2016) Uber knows customers with dying batteries are more likely to accept surge pricing. *The Telegraph*, October 30, 2017.

Danziger, S., Levav, J., & Avnaim-Pesso, L. (2011) Extraneous factors in judicial decisions, *Proceedings of the National Academy of Sciences*, Vol. 108, nr. 17, p. 6889-6892.

Dechesne, F., Dignum, V., Zardiashvili, L. & Bieger, J. (2019) AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police. Rapport: Leiden/Delft.

Denning, D.D. & Baugh Jr., W.E. (2000) Hiding crimes in cyberspace, in: D. Thomas & B.D. Loader (eds.) *Cybercrime: Law enforcement, security and surveillance in the information age*, London: Routledge, p. 105-131.

Dijck, G. van (2016) Legal research when relying on open access, *Law and Method*, April 2016.

Dijk, J. van, Tseloni, A. & Farrell, G. (2012) *The international crime drop*, Londen: Palgrave Macmillan.

Drijber, B.J. (2017) *Big data en het mededingingsrecht*, in: P.H. Blok (red.) Big data en het recht, Den Haag: SDU.

Duijvenvoorde, G.P. van (2018) Marktregulering en digitale connectiviteit: Over onbegrensde elektronische communicatie en de prijs van geïndividualiseerde benaderingen, *Radix* 44(4): 264-274.

Duijvenvoorde, G.P. van & Knol, P.C. (2019) Een nieuw telecomkader: het Europees wetboek voor elektronische communicatie, *Nederlands Tijdschrift voor Europees Recht* 2019(1/2): 33-43.

Eck, B.M.A. van, Bovens, M. & Zouridis S. (2018) Algoritmische rechtstoepassing in de democratische rechtsstaat, *Nederlands Juristenblad* 93(40): 3008-3017.

Eck, B.M.A. van (2019) Computerbesluiten, kunstmatige intelligentie en de bestuursrechter, *Tijdschrift voor Formeel Belastingrecht* 20(2/8), p. 17-20.

Eckholm, E. (2015) Harvard Law Library Readies Trove of Decisions for Digital Age. *New York Times*, 28 October 2015.

Ettekoven, B.J. van (2018) Werken aan moderne(r) bestuursrechtspraak, *NTB* 2018/71, afl. 10, p. 462.

Etzioni, A. (1999) *The Limits of Privacy*. New York: Basic Books.

Europol (2015) *Why is cash still king?* The Hague: Europol Police Office, p. 41.

Europol (2019) *The Internet Organised Crime Threat (IOCTA)*, Den Haag: European Police Office.

Evers, G.H. (2016) In de schaduw van de rechtsstaat: profilering en nudging door de overheid, *Computerrecht* (3): 167-171.

Fawcett, T. (2015) Mining the Quantified Self: Personal Knowledge Discovery as a Challenge for Data Science, *Big Data*, Vol. 3 Nr. 4.

Ferguson, A.G. (2017) Policing Predictive Policing. *Washington University Law Review*, Vol. 94, No. 5, 2017: https://ssrn.com/abstract=2765525.

Festinger, L. (1962) Cognitive dissonance, *Scientific American*. 207 (4), p. 93–107.

Fors, K. la, Custers, B.H.M., and Keymolen, E. (2019) Reassessing values for emerging big data technologies: integrating design-based and application-based approaches, *Ethics and Information Technology*, Volume 21, Number 3, p. 209-226. https://doi.org/10.1007/s10676-019-09503-4.

Fosch-Villaronga, E., Kieseberg, P. & Li, T. (2018) Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, *Computer Law and Security Review* 34(2), p. 304-313.

Fosch-Villaronga, E. (2019) *Robots, Healthcare, and the Law: Regulating Automation in Personal Care*. Routledge Research in the Law of Emerging Technologies. London-New York: Routledge.

Fosch-Villaronga, E. & Özcan, B. (2020) The progressive intertwinement between design, human needs and the regulation of care technology: the case of lower-limb exoskeletons, *International Journal of Social Robotics*, p. 1-14.

Fosch-Villaronga, E., Poulsen, A., Søraa, R.A., Custers, B.H.M. (2021) A little bird told me your gender: Gender inferences in social media, *Information Processing and Management* 58, https://doi.org/10.1016/j.ipm.2021.102541.

Franken, H. (2008) *Rechtsgeleerdheid in de rij der wetenschappen*. Amsterdam: KNAW - KNAW press.

Friedman, B., Kahn Jr., P.H., Borning, A. (2006) Value Sensitive Design and information systems. In: Zhang, P., Galletta, D. (eds.) *Human-Computer Interaction in Management Information Systems: Foundations*, pp. 348–372. New York: M.E. Sharpe.

Frissen, V., Lammes, S., Lange, M. de, Mul, J. de, and Raessens, J. (2015) *Playful Identities: The Ludification of Digital Media Cultures*. Amsterdam: Amsterdam University Press.

Gershman, J. (2015) Law School Applicant Pool Still Shrinking, *The Wall Street Journal*, 23 April 2015.

Gijrath, S.J.H. (2017) Telecommunications networks: Towards smarter regulation and contracts? *Competition and Regulation in Network Industries* 18(3/4), p. 175-197.

Gijrath, S.J.H. & Kalis, J.P. (2018) The NIS Directive. In: Gijrath S.J.H., Hof S. van der, Lodder A.R., Zwenne G.J. (red.) *Concise European Data Protection, E-Commerce and IT Law.* Kluwer Law International: Alphen aan den Rijn. 591-675.

Ginsberg, J., Mohebbi, M.H., Patel, R.S., Brammer, L., Smolinski, M.S. and Brilliant, L. (2009) Detecting influenza epidemics using search engine query data. *Nature*. 457 (7232), p. 1012–1014.

Gless, S. & Weigend, T. (2014) Intelligente Agenten und das Strafrecht, *Zeitschrift für die gesamte Strafrechtwissenschaft*, Vol. 126, No. 3, p. 561-591.

Gless, S., Silverman, E., & Weigend, T. (2016) If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability, *New Criminal Law Review*, Vol. 19, No. 3, p. 412-436.

Goodman, M. (2015) *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, New York: Anchor Books, p. 156-158.

Goodwin, M.E.A., & Koops, B.J. (2015) *Cyberspace, the cloud and cross- border criminal investigation. The limits and possibilities of international law*, Den Haag: WODC.

Graef, I., Verschakelen, J., and Valcke, P. (2013) Putting the Right to Data Portability into a Competition Law Perspective, Journal of Higher School Economics Annual Review, 53, 63.

Grassegger, H. & Krogerys, M. (2017) The Data That Turned the World Upside Down, *Motherboard*, 28 januari 2017.

Guardian (2015) Drone 'containing radiation' lands on roof of Japanese PM's office, *The Guardian*, 22 april 2015.

Gurney, J.K. (2013) Sue my car not me: products liability and accidents involving autonomous vehicles, *Journal of Law, Technology & Policy*, Vol. 2013, p. 247-277.

Hansen, P., Jespersen, A. M. (2013) Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy. *European Journal of Risk Regulation* 4 (1), p. 3–28.

Harari, Y.N. (2017) *Homo Deus: een kleine geschiedenis van de toekomst*. Amsterdam: Uitgeverij Thomas Rap.

Harcourt, B.E. (2007) Against Prediction: Profiling, Policing and Punishing in an Actuarial Age. Chicago: University of Chicago Press.

Heine, F. (2013) Merkel buzzed by mini-drone at campaign event. *Der Spiegel*, 16 september 2013. www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone- a-922495.html.

Helberger, N. (2017) Big data en het consumentenrecht. In: P.H. Blok (red.) *Big data en het recht*. Den Haag: SDU Uitgevers, p. 151-168.

Herik, H.J. van den, Nakad Weststrate, H.W.R. (2018) Rechtspraak per computer. In: Schlössels, R.J.N., Beijen, B.A., Bots, A.M.M.M., Peters, J.A.F. (red.) *In het nu ... wat worden zal. Over toekomstig bestuursrecht.* Deventer: Wolters Kluwer, p. 235-248.

Hern, A. (2017) Give robots 'personhood' status, EU committee argues, *The Guardian*, 12 January 2017. https://www.theguardian.com/technology/2017/jan/12/give-robots-personhood-status-eu-committee-argues.

Hildebrandt, M., Gutwirth, S. (2008) *Profiling the European Citizen*. Heidelberg: Springer.

Hildebrandt, M., Thielemans, L. (2013) Data protection by design and technology neutral law. *Computer Law and Security Review*, 29:517.

Hillier, A. (2003) Spatial analysis of historical redlining: a methodological explanation. *Journal of Housing Research*, 14(1):137–168.

Hins A.W. (2018) De taak van sociale media bij het bestrijden van desinformatie, *Mediaforum* 30(6), p. 171-175.

Hirsch Ballin, E.M.H. (2015) Dynamiek in de bestuursrechtspraak, in: E.M.H. Hirsch Ballin, R. Ortlep & A. Tollenaar (red) *Rechtsontwikkeling door de bestuursrechter*, Den Haag: Boom Juridische Uitgevers.

Hof, S. van der (2016) Wraakporno op internet, Een verkenning van de (on)mogelijkheden voor een strafrechtelijke aanpak, *Ars Aequi* 65(01), p. 54-59.

Hof, S. van der (2017) I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World, *Wisconsin International Law Journal* 34(2), p. 409-445.

Hof, S. van der & Lievens E. (2018) The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR, *Communications Law* 23(1), p. 33-43.

Holmes, O.W. Jr. (1897) The Path of the Law, 10 *Harvard Law Review*, 457, 461.

Hwang, S.B. & Kim, S. (2006) Dynamic Pricing Algorithm for E-Commerce, in: *Advances in Systems, Computing Sciences and Software Engineering*, 149-155.

Jager, W. de (2018) Neergestorte drone waarschijnlijk oorzaak van bosbrand, *Dronewatch*, 6 april 2018. https://www.dronewatch.nl/2018/04/06/neergestorte-drone-waarschijnlijk-oorzaak-van-bosbrand/.

Jak, N., en Bastiaans, S. (2018) De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid, *Nederlands Juristenblad*, 23 november 2018, afl. 40, p. 3018-3025.

Kamiran, F., and Calders, T. (2009) Classification without discrimination. In IEEE international conference on computer, control & communication (IEEE-IC4), 17–19 February 2009, Karachi, Pakistan.

Kamiran, F., Calders, T., Pechenizkiy, M. (2013) Techniques for discrimination-free predictive models, in: Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) (2013) *Discrimination and privacy in the information society*, Heidelberg: Springer.

Kalis, J.P. & Duijvenvoorde, G.P. van (2018) Een nieuw kader voor netwerk- en informatiebeveiliging: een cultuuromslag?, *Nederlands Tijdschrift voor Europees Recht* 24(3/4), p. 114-124.

Katz, D., Bommarito, M., & Blackman, J. (2014) Predicting the Behavior of the Supreme Court of the United States, *PLoS ONE,* Vol. 12, nr. 4., e0174698.

Keymolen, E.L.O. (2016) *Trust on the line. A philosophical exploration of trust in the networked era*. Oisterwijk: Wolf Legal Publishers.

Keymolen, E.L.O. & Hof, S. van der (2019) Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust, *Journal of Cyber Policy* 4(2), p. 143-159.

Kindt, E.J. (2018) Having yes, using no? About the new legal regime for biometric data, *Computer Law and Security Review* 34(3), p. 523-538.

Kleinig, J. (2010) The nature of consent. In: Miller & Wertheim (eds.) *The ethics of consent: Theory and practice,* New York: Oxford University Press.

Kogel, C.H. de, & Cornet, L.J.M. (2016) Toepassingsmogelijkheden van Quantified Self-data, *Justitiële Verkenningen* 42 (2016): 79-95.

Kohavi, R., and Thomke, S. (2017) The Surprising Power of Online Experiments. *Harvard Business Review*, September 2017, p. 74-82.

Koops, B.J. (2006) Should ICT regulation be technology-neutral? In: Koops, B.J., Lips, M., Prins C., Schellekens, M. (eds) *Starting points for ICT regulation: deconstructing prevalent policy oneliners*, IT & LAW SERIES, vol 9, pp 77–108. Den Haag: Asser Press.

Koops, B. J., Newell, B., Timan, T., Skorvánek, I., Chokrevski, T. & Galič, M. (2017) A typology of privacy, *University of Pennsylvania Journal of International Law*. 38, 2, p. 483-575.

Koops, B.J., Newell, B., & Skorvánek, I. (2019) Location tracking by police: The regulation of "tireless and absolute surveillance, *UC Irvine Law Review.* 9, 3, p. 635-698.

Koops, B.J., & Oerlemans, J.J. (2019) *Strafrecht en ICT*, Den Haag: SDU.

Kosinski, M., Stillwell, D. & Graepel, T. (2012) Private traits and attributes are predictable from digital records of human behaviour, *Proceedings of the National Academy of Sciences* (PNAS), www.pnas.org/content/early/2013/03/06/1218772110.

La Fors-Owczynik, K. (2017) Profiling 'Anomalies' and the Anomalies of Profiling: Digitalized Risk Assessments of Dutch Youth and the New European Data Protection Regime. In: Adams S., Purtova N., Leenes R. (Eds.) *Under Observation: The Interplay Between eHealth and Surveillance.* Law, governance and technology series no. 35 Cham: Springer, p. 107-138.

La Fors, K., Custers, B.H.M., and Keymolen, E. (2019) Reassessing values for emerging big data technologies: integrating design-based and application-based approaches, *Ethics and Information Technology*, Volume 21, Number 3, p. 209-226. https://doi.org/10.1007/s10676-019-09503-4.

Leenes, R. (2019) Regulating new technologies in times of change. In L. Reins (Ed.) *Regulating New Technologies in Uncertain Times,* p. 3-17. (Information Technology and Law Series ; Vol. 2019, No. 32). Heidelberg: TMC Asser Press | Springer. https://doi.org/10.1007/978-94-6265-279-8_1.

Leetaru, K. (2014) Did the Arab Spring Really Spark a Wave of Global Protests? The world may look like it's roiling now, but the 1980s were far worse. *Foreign Policy*, 30 May 2014.

Leeuw, F. (2015) Wetgeving, empirisch juridisch onderzoek en legal big data, *Recht der Werkelijkheid*, Vol. 36, Nr. 2, p. 50-65.

Leeuw, F.L., & Schmeets, H. (2016) *Empirical Legal Research, A Guidance Book for Lawyers, Legislators and Regulators*, Cheltenham: Edward Elgar Publishing, Inc.

Leeuw, H.B.M. (2017) *Punish, Seduce or Persuade. An Empirical Assessment of Anti-Piracy Interventions*, The Hague: Eleven International Publishing.

Leiser, M.R. & Murray, A.D. (2016) The role of non-state actors and institutions in the governance of new and emerging digital technologies. In: Brownsford R., Scotford E., Yeung K. (Eds.) *The Oxford Handbook of Law, Regulation, and Technology.* Oxford, UK: Oxford University Press, p. 670-704.

Leiser, M.R. (2019) Regulating Computational Propaganda: Lessons from International Law, *Cambridge International Law Journal* 8(2), p. 218-240.

Leiser, M.R. & Custers, B.H.M. (2019) The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, *European Data Protection Law Review* 5(3), p. 367-378.

Lessig, L. (2006) *Code Version 2.0*, New York: Basic Books.

Loenen, M.L.P. (2009) *Gelijkheid als juridisch beginsel. Een conceptuele analyse van de norm van gelijke behandeling en non-discriminatie.* Den Haag: Boom Juridische uitgevers.

Luzak, J. & Hof, S. van der (2018) Directive 2011/83/EU - Consumer Rights Directive (Electronic Commerce Aspects). In: Gijrath S., Hof S. van der, Lodder A.R., Zwenne G.J. (Eds.) *Concise European Data Protection, E-Commerce and IT Law.* Alphen aan den Rijn: Kluwer Law International, p. 325-394.

Malgieri, G., and Custers, B. (2018) Pricing privacy: the right to know the value of your personal data, *Computer Law & Security Review*, Vol. 34, Nr. 2, p. 289-303, http://dx.doi.org/10.1016/j.clsr.2017.08.006.

Maxwell, S. & Garbarino, E. (2010) The identification of social norms of price discrimination on the internet. *Journal of Product & Brand Management*, 19(3), p. 218-224.

McArthur, R.L. (2001) Reasonable expectations of privacy, *Ethics and Information Technology*, 3:123.

McCrudden, C. (2008) Human Dignity and judicial Interpretation of Human Rights. *European Journal of International Law*, 19(4), 655-724. https://doi.org/10.1093/ejil/chn043.

Mehra, S.K. (2015) Antitrust and the Robo-Seller: Competition in the Time of Algorithms, *Minnesota Law Review*, Vol. 100.

Mencher, A.G. (1971) On the Social Deployment of Science, *Bulletin of the Atomic Scientists*, Vol. 27, Nr. 10, p. 37.

Meuwese, A. (2017) Grip op normstelling in het datatijdperk, in: W. den Ouden, *Algemene regels in het bestuursrecht*, Meppel: Boom Juridische Uitgevers.

Modderkolk, H. (2017) Dringend gezocht: rechters met kennis van cybercriminaliteit, *Volkskrant*, 3 augustus 2017.

Muravyeva, E., Janssen, J., Specht, M., Custers, B. (2020) Exploring solutions to the privacy paradox in the context of e-assessment: informed consent revisited, *Ethics and Information Technology*, https://doi.org/10.1007/s10676-020-09531-5.

NOS (2018) Ook baby van spoedkeizersnee in bakkerij Hulst overleden, 17 mei 2018. *NOS*, https://nos.nl/artikel/2232234-ook-baby-van-spoedkeizersnee-in-bakkerij-hulst-overleden.html.

NOS (2019) Universiteit Maastricht kampt met ransomware aanval. NOS, 24 december 2019, https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html

Odinot, G., Jong, D. de, Leij, J.B.J. van der, Poot, C.J. de, et al., (2012) *Het gebruik van de telefoon- en internettap in de opsporing*, Den Haag: Boom Lemma.

Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., and Cornelisse, R. (2016) *Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Meppel: Boom Criminologie.

Oerlemans, J.J. (2017) *Investigating Cybercrime*, Amsterdam: Amsterdam University Press.

Ohm, P. (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57: 1701.

Oostrom-Streep, N.C. van (2016) A wounded deer leaps highest, *Nederlands Juristenblad,* Afl. 41, p. 3028.

Parker, D.B. (1976) *Crime by computer.* New York: Scribner, p. 17-22.

Pariser, E. (May 2011) *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press. p. 17.

Passchier, R. (2021) *Artificiële intelligentie en de rechtstaat*, Den Haag: Boom Uitgevers.

Pedreschi, D., Ruggieri, S., Turini, F. (2013) The discovery of discrimination, in: Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) (2013) *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*, Heidelberg: Springer.

Pistone, M.R. & Horn, M.B. (2016) *Disrupting Law School: How disruptive innovation will revolutionize the legal world*. San Francisco: Christensen Institute.

Pool, R.L.D., and Custers, B.H.M. (2017) The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, *European Journal of Crime, Criminal Law and Criminal Justice,* 25 (2017), p. 123-144.

Poort, J. and Zuiderveen Borgesius, F.J. (2019) Does everyone have a price? Understanding people's attitude towards online and offline price discrimination. *Internet Policy Review*, 8(1).

Poorter, J. de, & Goossens, J. (2019) Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad*, afl. 44, p. 3303-3312.

Prins, J.E.J. (2015) Big data en de rechterlijke macht, *Nederlands Juristenblad*, Vol. 90, Nr. 30, p. 2087.

Prinsen, M.M. (2008) *Forensisch DNA-onderzoek: Een balans tussen opsporing en fundamentele rechten*. Nijmegen: Wolf Legal Publishers.

Radin, M. (1925) The Theory of Judicial Decision: Or How Judges Think, *American Bar Association Journal*, Vol. 11, p. 357-362.

Rebonato, R. (2012) *Taking Liberties: A Critical Examination of Libertarian Paternalism*. London: Palgrave MacMillan.

Rhoen, M. (2018) Big Data, Big Risks, Big Power Shifts: Evaluating the GDPR as an instrument of risk control and power redistribution in the context of big data. Proefschrift, Leiden.

Richardson, R., et al. (2019) Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (February 13, 2019). *New York University Law Review Online*.

Roelants, J. (2018) De taxateur verandert in een computer, *Financieel Dagblad*, 9 maart 2018. https://fd.nl/werk-en-geld/1244625/de-taxateur-verandert-in-een-computer.

Ruger, T.W., Kim, P.T., Martin, A.D., & Quinn, K.M. (2004) The Supreme Court Forecasting Project: Legal and Political Science Approaches to Predicting Supreme Court Decision-making, *Columbia Law Review*, Vol. 104, p. 1150.

Schaller, R.R. (1997) Moore's Law: Past, Present and Future, *Spectrum*, IEEE, Volume 34, June 1997, p. 52-59.

Schauer, F. (2003) *Profiles, Probabilities and Stereotypes*. Harvard University Press, Cambridge.

Schellekens, M. (2015) Self-Driving Cars and the Chilling Effect of Liability Law, *Computer Law & Security Review*, p. 506-517.

Schermer, B.W., Custers, B.H.M., and Van der Hof, S. (2014) The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection, *Ethics & Information Technology*, Vol. 16, No. 2, p. 171-182.

Schermer, B.W. (2017) Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, *Tijdschrift voor Bijzonder Strafrecht en handhaving* 2017(4).

Schermer, B.W. (2017) Dataportabiliteit: the good, the bad and the ugly, *Tijdschrift voor Internetrecht* 2017(4): 161.

Scherme,r B.W., Georgieva, I., Hof, S. van der, & Koops, B.J. (2019) Legal aspects of Sweetie 2.0. In: Hof S. van der, Georgieva I., Schermer B.W., Koops B.J. (Eds.) *Sweetie 2.0. Using artificial intelligence to fight webcam child sex tourism.* Information technology & law series no. 31 The Hague: Asser Press/Springer Press, p. 1-94.

Schrodt, P. (2011) Automated Production of High-Volume, Near-Real-Time Political Event Data. Paper presented at the New Methodologies and Their Applications in Comparative Politics and International Relations Workshop. Princeton University, 4-5 February 2011.

Shannon, C.E. (1948) The mathematical theory of communication, *Bell Systems Technology Journal*, Vol. 27, p. 379-423 and p. 623-656.

Shannon, C.E. (1949) Communications theory of secrecy systems, *Bell Systems Technology Journal*, Vol. 28, p. 656-715.

Simoiu, C., Gates, C., Bonneau, J., Goel, S. (2019) I was told to buy a software or lose my computer. I ignored it: a study of ransomware, *USENIX Symposium on Usable Privacy and Security (SOUPS)* 2019. August 11–13, 2019, Santa Clara, CA, USA.

Solove, D. (2004) *The digital person; technology and privacy in the information age*. New York: New York University Press.

Solove, D. J. (2013) Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, p. 1880–1903.

Squires, G. (2003) Racial profiling, insurance style: insurance redlining and the uneven development of metropolitan areas. *Journal of Urban Affairs*, 25(4), p. 391–410.

Stefoudi, D. (2017) Big Data from Space - Legal issues related to access and dissemination of large volumes of space-generated data. In: Blount P.J., Masson-Zwaan T., Moro-Aguilar R., Schrogl K.U. (red.) *Proceedings of the International Institute of Space Law 2016.* Proceedings of the International Institute of Space Law nr. 59 The Hague: Eleven International Publishing, p. 49-60.

Stolker, C.J.J.M. (2003) Ja, geléérd zijn jullie wel! Over de status van de rechtswetenschap, *Nederlands Juristenblad*(15), p. 766-778.

Stolker, C.J.J.M. (2004) Wat maakt een juridisch tijdschrift wetenschappelijk? *NJB-kronieken,* p. 1409-1418.

Stucke, M. & Ezrachi, A. (2015) *Artificial Intelligence & Collusion: When Computers Inhibit Competition*. Oxford Legal Studies Research Paper No. 18/2015.

Susser, D., Roessler, B., and Nissenbaum, H.F. (2019) Online Manipulation: Hidden Influences in a Digital World (December 23, 2018). 4 *Georgetown Law Technology Review* 1.

Susskind, R. (2013) *Tomorrow's Lawyers*, Oxford: Oxford University Press.
Swire, P., and Lagos, Y. (2013) Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 *Maryland Law Review* 335.
Tamanaha, B. (2012) *Failing Law Schools*, Chicago: University of Chicago Press.
Tene, O., and Polonetsky, J. (2012) Privacy in the age of big data: a time for big decisions, *Stanford Law Review Online*, 64, p. 63.
Thaler, R. H., & Sunstein, C. R. (2008) *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT, USA: Yale University Press.
Tjong Tjin Tai, T.F.E., en Boesten, S. (2016) Aansprakelijkheid, zelfrijdende auto's en andere zelfbesturende objecten, *Nederlands Juristenblad*, p. 656-664.
Tonry, M. (2014) Why Crime Rates Are Falling Throughout the Western World, 43 *Crime & Justice, 1.*
Ursic, H. & Custers, B.H.M. (2016) Legal Barriers and Enablers to Big Data Reuse - A critical Assessment of the Challenges for the EU Law, *European Data Protection Law Review* 2(2), p. 209-221.
Ursic, H. (2018) Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control, *SCRIPTed*, Vol. 15, Issue 1, August 2018.
Vedder, A.H. (1999) KDD: The challenge to individualism. *Ethics and Information Technology* 1, p. 275–281.
Vedder, A. (2005) Expert knowledge for non-experts: Inherent and contextual risks of misinformation. ICES, Journal of Information, *Communication and Ethics in Society* (2005) Volume 3, p. 113–119.
Verbrugge, A.M. (2018) Civiel gebruik van drones, *VR* 2018/13.
Wachter, S., Mittelstadt, B., and Floridi. L. (2017) Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation. *International Data Privacy Law,* 7(2): 76-99.
Warren, S.D., and Brandeis, L.D. (1890) The right to privacy; the implicit made explicit, *Harvard Law Review*, p. 193-220.
Warren, A., Bayley, R., Bennett, C., Charlesworth, A.J., Clarke, R., Oppenheim, C. (2008) Privacy Impact Assessments: International experience as a basis for UK guidance. *Computer Law and Security Report*, 2008, 24, 3 (April-June 2008), p. 233-242.
Wees, K.A.P.C. van (2018) Voertuigautomatisering en productaansprakelijkheid, *Maandblad voor Vermogensrecht*, 2018, Afl. 4, p. 112-122.
Westin, A. (1967) *Privacy and Freedom*, London: Bodley Head.
Wiggers, G., Verberne, S. & Zwenne, G.J. (2018) Exploration of Intrinsic Relevance Judgments by Legal Professionals in Information Retrieval Systems. In: Brandsen A., Dirkson A.R., Kraaij W., Lamers W., Verberne S., Vos H. de, Wiggers G. (red.) *Proceedings of the 17th Dutch-Belgian Information Retrieval workshop.* Leiden: DIR. 5-8.
Willemsen, C.H.J. (2019) *Identiteitsvaststelling van verdachten en ilegale vreemdelingen door opsporingsdiensten: Een toetsingskader voor de kwaliteit van het product, het proces en de organisatie*. Proefschrift, Universiteit van Tilburg.
Willemsen, F. & Leeuw, F. (2016) Big Data, real world events and evaluations, in: G. Petersson e.a. (red.) *Big Data and evaluation*, Piscataway NJ: Transaction Publishers.
Wright, D., and Hert, P. de (2012) *Privacy Impact Assessment*, Springer, Dordrecht, 2012.
Yacht (2015) *Trends en ontwikkelingen op de Legal arbeidsmarkt vierde kwartaal 2016.* Amsterdam: Yacht.
Zardiashvili, L., Bieger, J., Dechesne, F. & Dignum, V. (2019) AI Ethics for Law Enforcement: A Study into Requirements for Responsible Use of AI at the Dutch Police, *Delphi - Interdisciplinary Review of Emerging Technologies* 2(4), p. 179-185.
Zardiashvili, L. & Fosch-Villaronga, E. (2020) "Oh, Dignity too?" Said the Robot: Human Dignity as the Basis for the Governance of Robotics, *Minds and Machines: Journal for Artificial Intelligence, Philosophy and Cognitive Science.*

Zarsky, T. (2003) Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion. *Yale Journal of Law and Technology* 5, 57.

Zarsky, T. (2017) Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2).

Zliobaite, I. & Custers, B. (2016) Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, *Artificial Intelligence and Law* (24), p. 183-201.

Zouridis, S., Eck, B.M.A. van & Bovens, M. (2019) Automated discretion. In: Evans T., Hupe P. (eds.) *Discretion and the Quest for Controlled Freedom.* Cham: Palgrave Macmillan, p. 313-329.

Zwenne, G.J. & Schmidt, A.H.J. (2016) Wordt de homo digitalis bestuursrechtelijk beschermd? In: Moerel, E.M.L., Prins, J.E.J., Hildebrandt, M., Tjong Tjin Tai, T.F.E., Zwenne, G.J., Schmidt, A.H.J. (eds.) *Homo Digitalis: Preadviezen.* Handelingen Nederlandse Juristen Vereniging no. 146-1 Deventer: Wolters Kluwer, p. 307-385.

Zwenne, G.J. & Steenbruggen, W.A.M. (2017) Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning. In: *Big data in de zorg: Preadvies uitgebracht voor de Vereniging voor Gezondheidsrecht, jaarvergadering 31 maart 2017.* Preadvies Vereniging voor Gezondheidsrecht no. 2017 The Hague: Sdu Uitgevers. 73-99.

Zwenne, G.J. (2019) Het vergeetrecht vijf jaar later, *Ars Aequi* 68(7), p. 607-613.

Noten

1. Mencher, A.G. (1971) On the Social Deployment of Science, *Bulletin of the Atomic Scientists*, Vol. 27, Nr. 10, p. 37.
2. Wat betreft functionaliteit is deze voorspelling niet zo gewaagd, maar er zijn natuurlijk andere goede redenen voor taalonderwijs, zoals taalvaardigheid en uitdrukkingsvermogen. Een rekenmachine is op zichzelf ook geen goede reden om geen rekenonderwijs aft e schaffen, wel om het aan te passen.
3. Custers, B.H.M. (2016) *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*. Heidelberg: Springer.
4. Leiser, M.R. (2019), Regulating Computational Propaganda: Lessons from International Law, *Cambridge International Law Journal* 8(2): 218-240; Hins A.W. (2018), De taak van sociale media bij het bestrijden van desinformatie, *Mediaforum* 30(6): 171-175.
5. Technologieën uit verschillende domeinen raken ook steeds verder verknoopt, zie Custers, B., Dorbeck-Jung, B., Faber, E., Iacob, S., Koops, B.J., Leenes, R., Poot, H. de, Rip, A., Teeuw, W.B. (red), Vedder, A. (red.), Vudisa, J. (2008) *Security Applications for Converging Technologies; impact on the constitutional state and the legal order*, WODC rapport, Telematica Instituut, Enschede en Universiteit van Tilburg.
6. Zie ook Harari, Y.N. (2017) *Homo Deus, een kleine geschiedenis van de toekomst*. Amsterdam: Uitgeverij Thomas Rap.
7. Fosch-Villaronga, E. & Özcan, B. (2020) The progressive intertwinement between design, human needs and the regulation of care technology: the case of lower-limb exoskeletons, *International Journal of Social Robotics*, p. 1-14.
8. Cf. Custers, B.H.M. (2008) The Exclusivity of Ultrafast Communication Networks, *Journal of International Commercial Law and Technology*, Vol. 3, Issue 4, p. 247-253.
9. Hier is geen ruimte om in te gaan op hoe de technologie werkt, maar voor verdere literatuur, zie bijvoorbeeld: Calders, T. & Custers, B.H.M. (2013) What is data mining and how does it work? In: Custers, B.H.M., Calders, T., Schermer, B., Zarsky, T. (eds.) *Discrimination and Privacy in the Information Society*. nr. 3 Heidelberg: Springer.
10. Voor de invloed van technologie op de staatsrechtelijke verhoudingen, zie onder meer Passchier, R. (2021) *Artificiële intelligentie en de rechtstaat*, Den Haag: Boom Uitgevers.
11. Deze paragraaf is grotendeels gebaseerd op Custers, B.H.M. (2019) Nieuwe digitale (grond)rechten, *Nederlands Juristenblad*, afl. 44, p. 3288-3295.
12. Schaller, R.R. (1997) Moore's Law: Past, Present and Future, *Spectrum, IEEE*, Volume 34, June 1997, pp. 52-59.
13. Custers, B.H.M. (2008) The Exclusivity of Ultrafast Communication Networks, *Journal of International Commercial Law and Technology* 3(4), p. 247-253.
14. Vedder, A. (2005) Expert knowledge for non-experts: Inherent and contextual risks of misinformation. ICES, Journal of Information, *Communication and Ethics in Society* (2005) Volume 3, p. 113–119.
15. Wachter, S., Mittelstadt, B., and Floridi. L. (2017) Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), p. 76-99.
16. Chadwick, R., Levitt, M., and Shickle, D. (1997) *The right to know and the right not to know*, Aldershot, U.K.: Avebury Ashgate Publishing Ltd.
17. Met name in situaties waarin mensen geen handelingsmogelijkheden hebben, bijvoorbeeld een onbehandelbare ziekte, kan het de voorkeur hebben iets niet te weten.
18. Pariser, E. (May 2011) *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press. p. 17.

19. Festinger, L. (1962) Cognitive dissonance, Scientific American. 207 (4), p. 93–107.
20. Kleinig, J. (2010). *The nature of consent*, in Miller & Wertheim (eds.) *The ethics of consent: Theory and practice*, New York: Oxford University Press.
21. Custers, B.H.M. (2016) Click here to consent forever: Expiry dates for informed consent, *Big Data & Society*, p. 1-6.
22. Malgieri, G., and Custers, B. (2018) Pricing privacy: the right to know the value of your personal data, *Computer Law & Security Review*, Vol. 34, Nr. 2, p. 289-303, http://dx.doi.org/10.1016/j.clsr.2017.08.006. Zie ook Böhme, R. (2009) Valuating Privacy with Option Pricing Theory. In: Berthold, S. (ed.) Workshop on the Economics of Information Security (WEIS 2009), June 24-25. University College London, London.
23. Westin, A. (1967) *Privacy and Freedom*, London: Bodley Head.
24. Etzioni, A. (1999) *The Limits of Privacy*. New York: Basic Books.
25. Vedder, A.H. (1999) KDD: The challenge to individualism. *Ethics and Information Technology* 1, p. 275–281.
26. Herik, H.J. van den, Nakad Weststrate, H.W.R. (2018) Rechtspraak per computer. In: Schlössels, R.J.N., Beijen, B.A., Bots, A.M.M.M., Peters, J.A.F. (red.) *In het nu ... wat worden zal. Over toekomstig bestuursrecht*. Deventer: Wolters Kluwer. 235-248; Eck, B.M.A. van (2019) Computerbesluiten, kunstmatige intelligentie en de bestuursrechter, *Tijdschrift voor Formeel Belastingrecht* 20(2/8), p. 17-20.
27. Zardiashvili, L. & Fosch-Villaronga, E. (2020) "Oh, Dignity too?" Said the Robot: Human Dignity as the Basis for the Governance of Robotics, *Minds and Machines: Journal for Artificial Intelligence, Philosophy and Cognitive Science.*
28. Koops, B.J. (2006) Should ICT regulation be technology-neutral? In: Koops, B.J., Lips, M., Prins, C., Schellekens, M. (eds.) *Starting points for ICT regulation: deconstructing prevalent policy oneliners*, IT & LAW SERIES, vol 9, pp 77–108. Den Haag: Asser Press; Hildebrandt, M, Thielemans, L (2013) Data protection by design and technology neutral law. *Computer Law and Security Review*, 29:517.
29. Ettekoven, B.J. van (2018) Werken aan moderne(r) bestuursrechtspraak, *NTB* 2018/71, afl. 10, p. 462.
30. Roelants, J. (2018) De taxateur verandert in een computer, *Financieel Dagblad*, 9 maart 2018. https://fd.nl/werk-en-geld/1244625/de-taxateur-verandert-in-een-computer.
31. Jak, N., en Bastiaans, S. (2018) De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid, *Nederlands Juristenblad*, 23 november 2018, afl. 40, p. 3018-3025.
32. Zwenne, G.J. & Steenbruggen, W.A.M. (2017) Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning. In: *Big data in de zorg: Preadvies uitgebracht voor de Vereniging voor Gezondheidsrecht, jaarvergadering 31 maart 2017*. Preadvies Vereniging voor Gezondheidsrecht no. 2017 The Hague: Sdu Uitgevers, p. 73-99.
33. https://douane-inzicht.nl/article/247694775.
34. Zouridis, S., Eck, B.M.A. van, & Bovens, M. (2019) Automated discretion. In: Evans T., Hupe P. (red.) *Discretion and the Quest for Controlled Freedom.* Cham: Palgrave Macmillan. 313-329; Eck, B.M.A. van, Bovens, M. & Zouridis, S. (2018) Algoritmische rechtstoepassing in de democratische rechtsstaat, *Nederlands Juristenblad* 93(40): 3008-3017; Evers, G.H. (2016) In de schaduw van de rechtsstaat: profilering en nudging door de overheid, *Computerrecht* (3), p. 167-171.
35. Schauer, F. (2003) Profiles, Probabilities and Stereotypes. Harvard University Press, Cambridge; Custers, B.H.M. (2003) *Effects of Unreliable Group Profiling by Means of Data Mining*. In: G. Grieser, Y. Tanaka and A. Yamamoto (eds.) *Lecture Notes in Artificial Intelligence, Proceedings*

of the 6th International Conference on Discovery Science (DS 2003) Sapporo, Japan. Berlin, Heidelberg, New York: Springer-Verlag, Vol. 2843, p. 290-295.

36. Dit ging grondig mis bij de Belastingdienst in de zogeheten Toeslagenaffaire, waarin veel burgers ten onrechte als fraudeurs werden beschouwd. https://www.rtlnieuws.nl/nieuws/nederland/artikel/4955021/toeslagenaffaire-belastingdienst-menno-snel-kinderopvang-nationale.
37. Custers, B.H.M. (2004) *The Power of Knowledge; Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Tilburg: Wolf Legal Publishers, pp. 300.
38. Hirsch Ballin, E.M.H. (2015) Dynamiek in de bestuursrechtspraak, in: E.M.H. Hirsch Ballin, R. Ortlep & A. Tollenaar (red.) *Rechtsontwikkeling door de bestuursrechter*, Den Haag: Boom Juridische Uitgevers.
39. Amerongen, N.H. van & Schuurmans, Y.E. (2019) Advies van een deskundige of een algoritme? De toetsing van 'black box'-besluiten door de bestuursrechter.. In: Huisman P.J., Neerhof A.R., Ommeren F.J. van (red.) *Verwant met verband: Ruimte, Recht en Wetenschap (vriendenbundel voor prof. mr. J. Struiksma)*. 's-Gravenhage: IBR, p. 175-196.
40. Poorter, J. de, & Goossens, J. (2019) Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, *Nederlands Juristenblad*, afl. 44, p. 3303-3312.
41. Zwenne G.J. & Schmidt A.H.J. (2016) Wordt de homo digitalis bestuursrechtelijk beschermd? In: Moerel, E.M.L., Prins, J.E.J., Hildebrandt, M., Tjong Tjin Tai, T.F.E., Zwenne, G.J., Schmidt, A.H.J. (Eds.) *Homo Digitalis: Preadviezen*. Handelingen Nederlandse Juristen Vereniging no. 146-1 Deventer: Wolters Kluwer, p. 307-385; Solove, D. (2004) *The digital person; technology and privacy in the information age*. New York: New York University Press.
42. Tonry, M. (2014) Why Crime Rates Are Falling Throughout the Western World, 43 Crime & Justice, 1; Dijk, J. van, Tseloni, A. & Farrell, G. (2012) *The international crime drop*, Londen: Palgrave Macmillan.
43. Europol (2019) *The Internet Organised Crime Threat (IOCTA)*, Den Haag: European Police Office.
44. In deze contexten wordt ook de term cybersecurity regelmatig gebruikt, wanneer het gaat om de beveiliging van computers en netwerken tegen deze ontwikkelingen. Zie ook Gijrath, S.J.H. & Kalis, J.P. (2018) The NIS Directive. In: Gijrath, S.J.H., Hof, S. van der, Lodder, A.R., Zwenne, G.J. (red.) *Concise European Data Protection, E-Commerce and IT Law*. Kluwer Law International: Alphen aan den Rijn. 591-675; Kalis, J.P. & Duijvenvoorde, G.P. van (2018) Een nieuw kader voor netwerk- en informatiebeveiliging: een cultuuromslag? *Nederlands Tijdschrift voor Europees Recht* 24(3/4), p. 114-124.
45. In veel jurisdicties zijn cryptovaluta nauwelijks gereguleerd in financiële markten, zie Custers, B.H.M., Overwater, L.J. (2019) Regulating Initial Coin Offerings and Cryptocurrencies: A Comparison of Different Approaches in Nine Jurisdictions Worldwide, *European Journal of Law and Technology*, Vol. 10, Issue 3, pp. 29.
46. Charney, S (1994) Computer crime: Law enforcement's shift from a corporeal environment to the intangible, electronic world of cyberspace, Federal Bar News, 41(7), 489; Parker, D.B. (1976) *Crime by computer*. New York: Scribner, p. 17-22.
47. Dreigingen op het terrein van cybercrime kunnen snel verschuiven. Eerder was zogeheten banking malware nog een belangrijke dreiging, maar het belang hiervan neemt langzaam af. Custers, B., Pool, R., and Cornelisse, R., (2019) Banking Malware and the Laundering of its Profits, *European Journal of Criminology*, Vol. 16, nr. 6, p. 728-745. https://doi.org/10.1177/1477370818788007.

48. In geval cryptografische versleuteling wordt gebruikt, wordt ook wel de term cryptoware gehanteerd in plaats van ransomware. Taxonomisch is cryptoware een specifieke vorm van ransomware.
49. Simoiu, C., Gates, C., Bonneau, J., Goel, S. (2019) I was told to buy a software or lose my computer. I ignored it: a study of ransomware, *USENIX Symposium on Usable Privacy and Security (SOUPS)* 2019. August 11–13, 2019, Santa Clara, CA, USA.
50. https://www.bankinfosecurity.com/ransomware-average-ransom-payout-increases-to-41198-a-13333.
51. NOS (2019) Universiteit Maastricht kampt met ransomware aanval. NOS, 24 december 2019, https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html.
52. Cf. Denning, D.D. & Baugh Jr., W.E. (2000) Hiding crimes in cyberspace, in: D. Thomas & B.D. Loader (red.) *Cybercrime: Law enforcement, security and surveillance in the information age*, London: Routledge, p. 105-131; Goodwin, M.E.A., & Koops, B.J. (2015) *Cyberspace, the cloud and cross- border criminal investigation. The limits and possibilities of international law*, Den Haag: WODC.
53. Custers, B.H.M., Oerlemans, J.J., en Pool, R.L.D. (2016) Ransomware, cryptoware en het witwassen van losgeld in Bitcoins, *Strafblad*, Jaargang 14, Nummer 2, mei 2016, p. 87-95.
54. Custers, B.H.M., Oerlemans, J.J., Pool, R. (2020) Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies, *European Journal of Crime, Criminal Law and Criminal Justice*, 28 (2020), p. 121-152.
55. Europol (2015) *Why is cash still king?* The Hague: Europol Police Office, p. 41.
56. Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., and Cornelisse, R. (2016) Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware. Meppel: Boom Criminologie.
57. De Duitse Bondskanselier Angela Merkel werd 'aangevallen' door een drone door een actiegroep die aandacht wilde opeisen, zie: Heine, F. (2013) Merkel buzzed by mini-drone at campaign event. *Der Spiegel*, 16 september 2013. www.spiegel.de/ international/ germany/merkel-campaign-event-visited-by-mini-drone- a-922495.html. Het kantoor van de Japanse premier Abe werd belaagd door een drone, zie: The Guardian (2015) Drone 'containing radiation' lands on roof of Japanese PM's office, *The Guardian*, 22 april 2015.
58. Zie het voorbeeld van Stuxnet, malware die de besturing van centrifuges in het Iraanse Natanz kon beïnvloeden: Goodman, M. (2015) F*uture Crimes: Inside the Digital Underground and the Battle for Our Connected World*, New York: Anchor Books, p. 156-158.
59. Koops, B.J., & Oerlemans, J.J. (2019) Strafrecht en ICT, Den Haag: SDU. Voor de discussie over het strafbaar stellen van wraakporno, zie Hof, S. van der (2016), Wraakporno op internet, Een verkenning van de (on) mogelijkheden voor een strafrechtelijke aanpak, *Ars Aequi* 65(01), p. 54-59.
60. Zardiashvili, L., Bieger, J., Dechesne, F. & Dignum, V. (2019) AI Ethics for Law Enforcement: A Study into Requirements for Responsible Use of AI at the Dutch Police, *Delphi - Interdisciplinary Review of Emerging Technologies* 2(4): 179-185. Dechesne, F., Dignum, V., Zardiashvili, L. & Bieger, J. (2019) AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police. Rapport: Leiden/Delft.
61. Prinsen, M.M. (2008) *Forensisch DNA-onderzoek: Een balans tussen opsporing en fundamentele rechten.* Nijmegen: Wolf Legal Publishers; Kindt, E.J. (2018) Having yes, using no? About the new legal regime for biometric data, *Computer Law and Security Review* 34(3), p. 523-538.
62. Schermer, B.W. (2017), Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, *Tijdschrift voor Bijzonder Strafrecht en handhaving* 2017(4).

63. Schermer, B.W., Georgieva, I., Hof, S. van der & Koops, B.J. (2019), Legal aspects of Sweetie 2.0. In: Hof, S. van der, Georgieva, I., Schermer, B.W., Koops, B.J. (Eds.) *Sweetie 2.0. Using artificial intelligence to fight webcam child sex tourism*. Information technology & law series no. 31 The Hague: Asser Press/Springer Press, p. 1-94.
64. Custers, B.H.M. (2012) Technology in Policing: Experiences, Obstacles and Police Needs, *Computer Law & Security Review*. Vol. 28, No. 1, p. 62-68.
65. Custers, B., Vergouw, B. (2015) Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies, *Computer Law & Security Review*, 31, p. 518-526.
66. Odinot, G., Jong, D. de, Leij, J.B.J. van der, Poot, C.J. de, et al., (2012) *Het gebruik van de telefoon- en internettap in de opsporing*, Den Haag: Boom Lemma; Custers, B.H.M. (2008) Tapping and Data Retention in Ultrafast Communication Networks, *Journal of International Commercial Law and Technology*, Vol. 3, Issue 2, 2008, p. 94-100.
67. Oerlemans, J.J. (2017) *Investigating Cybercrime*, Amsterdam: Amsterdam University Press. De bevoegdheden van inlichtingen- en veiligheidsdiensten laat ik hier even buiten beschouwing. Voor meer hierover, zie: Custers, B.H.M. (2017) *Cyber agent technology en de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV)*, Leiden: Universiteit Leiden, 30 september 2017, 30 pp.
68. Pool, R.L.D., and Custers, B.H.M. (2017) The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, *European Journal of Crime, Criminal Law and Criminal Justice*, 25 (2017), p. 123-144. Over het volgen door de politie, zie ook: Koops, B.J., Newell, B., & Skorvánek, I. (2019) Location tracking by police: The regulation of "tireless and absolute surveillance, *UC Irvine Law Review*. 9, 3, p. 635-698.
69. Leiser, M.R. & Custers, B.H.M. (2019) The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, *European Data Protection Law Review* 5(3), p. 367-378.
70. Leiser, M.R. and Custers, B.H.M. (2019) The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, *European Data Protection Law Review*. Vol. 5, nr. 3, p. 367-378.
71. Custers, B.H.M. en Stevens, L. (2021) The Use of Data as Evidence in Dutch Criminal Courts. *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 29, Nr. 1, p. 25-46.
72. Custers, B.H.M. (2004) *The Power of Knowledge; Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Tilburg: Wolf Legal Publishers, pp. 300.
73. Deze paragraaf is grotendeels gebaseerd op Custers, B.H.M. (2018) Aansprakelijkheid voor drones: technologische ontwikkelingen en de toepasbaarheid van het aansprakelijkheidsrecht, *Maandblad voor Vermogensrecht*, nummer 7-8, p. 235-242.
74. NOS (2018) Ook baby van spoedkeizersnee in bakkerij Hulst overleden, 17 mei 2018. NOS, https://nos.nl/artikel/2232234-ook-baby-van-spoedkeizersnee-in-bakkerij-hulst-overleden.html.
75. De Jager, W. (2018) Neergestorte drone waarschijnlijk oorzaak van bosbrand, *Dronewatch*, 6 april 2018. https://www.dronewatch.nl/2018/04/06/neergestorte-drone-waarschijnlijk-oorzaak-van-bosbrand/.
76. Custers, B.H.M. (2016) *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*. Heidelberg: Springer.
77. Vaak staan in deze aanpak de onderliggende normen en waarden die bescherming behoeven nog wat meer centraal in plaats van de precieze gedragsomschrijving. La Fors, K., Custers, B.H.M., and Keymolen, E. (2019) Reassessing values for emerging big data technologies:

integrating design-based and application-based approaches, *Ethics and Information Technology*, Volume 21, Number 3, p. 209-226. https://doi.org/10.1007/s10676-019-09503-4.

78. Cf. Verbrugge, A.M. (2018) Civiel gebruik van drones, VR 2018/13. Zie ook Rb. Gelderland 21 december 2016, ECLI:NL:RBGEL:2016:7155 en Rb. Gelderland 10 mei 2017, ECLI:NL:RBGEL:2017:2663.
79. Van Wees, K.A.P.C. (2018) Voertuigautomatisering en productaansprakelijkheid, *Maandblad voor Vermogensrecht*, 2018, Afl. 4, p. 112-122. Tjong Tjin Tai, T.F.E., en Boesten, S. (2016) Aansprakelijkheid, zelfrijdende auto's en andere zelfbesturende objecten, *Nederlands Juristenblad*, p. 656-664; Colonna, K. (2012) Autonomous Cars and Tort Liability, *Journal of Law, Technology & The Internet*, Vol. 4, No. 4, p. 81-130. Gurney, J.K. (2013) Sue my car not me: products liability and accidents involving autonomous vehicles, *Journal of Law, Technology & Policy*, Vol. 2013, p. 247-277.
80. Van Wees, K.A.P.C. (2018) Voertuigautomatisering en productaansprakelijkheid, *Maandblad voor Vermogensrecht*, 2018, Afl. 4, p. 112-122.
81. Idem, p. 116.
82. HR 28 mei 2004, NJ 2005/105 (Jetblast).
83. HR 2 februari 1973, NJ 1973/315 (Lekkende kruik I). Hof Leeuwarden 8 februari 2011, JA 2011/87 (onoordeelkundig gebruik vuurwerk).
84. Van Wees, K.A.P.C. (2018) Voertuigautomatisering en productaansprakelijkheid, *Maandblad voor Vermogensrecht*, 2018, Afl. 4, p. 117.
85. Voor gedeelde verantwoordelijkheden in complexe technologie, zie Custers B.H.M. (2009) Whose responsibility is it anyway? Dealing with the consequences of new technologies. In: Sollie P., Duwell M. (red.) *Evaluating new technologies: Methodological problems for the ethical assessment of technology developments.* New York: Springer, p. 21-34.
86. Cf. Buechi, M., Fosch-Villaronga, E., Lutz, C., Tamò, A., Velidi, S. & Viljoe, S. (2020) The Chilling Effects of Algorithmic Profiling: Mapping the Issues, *Computer Law & Security Review*.
87. Schellekens, M. (2015) Self-Driving Cars and the Chilling Effect of Liability Law, *Computer Law & Security Review*, p. 506-517.
88. Gless, S., Silverman, E., & Weigend, T. (2016) If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability, *New Criminal Law Review*, Vol. 19, No. 3, p. 412-436.
89. Hern, A. (2017) Give robots 'personhood' status, EU committee argues, *The Guardian*, 12 January 2017. https://www.theguardian.com/technology/2017/jan/12/give-robots-personhood-status-eu-committee-argues; Daily Wire (2018) Europe Considers Granting Robots Legal Status, *Daily Wire*, 13 April 2018. https://www.dailywire.com/news/29397/europe-considers-granting-robots-legal-status-paul-bois.
90. Voor meer over regulering van robots, zie Fosch-Villaronga E. (2019) Robots, Healthcare, and the Law: Regulating Automation in Personal Care. Routledge Research in the Law of Emerging Technologies. London-New York: Routledge.
91. Gless, S. & Weigend, T. (2014) Intelligente Agenten und das Strafrecht, *Zeitschrift für die gesamte Strafrechtwissenschaft*, Vol. 126, No. 3, p. 561-591; Gless, S., Silverman, E., & Weigend, T. (2016) If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability, *New Criminal Law Review*, Vol. 19, No. 3, p. 412-436.
92. Soms wordt tegengeworpen dat bij het ontwikkelen van AI en robots de drie wetten van Asimov moeten worden betracht, die in essentie aangeven dat een robot een mens geen letsel mag toebrengen. Echter, dit zal maar lastig in het ontwerp van AI in te bouwen zijn, omdat zelfdenkende systemen eigen conclusies trekken. Asimov, I. (1950) *Runaround. I, Robot*, New York City: Doubleday. p. 40.
93. Zarsky, T. (2003) Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal

Information in the Forum of Public Opinion. *Yale Journal of Law and Technology* 5, 57.

94. Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness.* New Haven, CT, USA: Yale University Press.
95. In zekere zin is dit tegengesteld aan regularing via architectuur, die geen keuzevrijheid laat, zie Lessig, L. (2006) Code Version 2.0, New York: Basic Books. Zie ook Leiser, M.R. & Murray, A.D. (2016) The role of non-state actors and institutions in the governance of new and emerging digital technologies. In: Brownsford, R., Scotford, E., Yeung, K. (Eds.) *The Oxford Handbook of Law, Regulation, and Technology*. Oxford, UK: Oxford University Press. p. 670-704.
96. Voor meer voorbeelden, zie de special issue van de University of Chicago Law Review, Volume 86, Issue 2, April 2019, p. 217-609. http://lawreview.uchicago.edu/volume-86-issue-2-april-2019-217–609.
97. Rebonato, R. (2012) Taking Liberties: *A Critical Examination of Libertarian Paternalism*. London: Palgrave MacMillan.
98. Bovens, L. (2009) The Ethics of 'Nudge'. In Preference Change: Theory and Decision Library. Vol. 42., edited by T. Grüne-Yanoff and S. O. Hansson, 207–219. Dordrecht: Springer.
99. Susser, D., Roessler, B., and Nissenbaum, H.F. (2019) Online Manipulation: Hidden Influences in a Digital World (December 23, 2018). 4 *Georgetown Law Technology Review* 1.
100. Hansen, P., Jespersen, A. M. (2013) Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy. *European Journal of Risk Regulation* 4 (1), p. 3–28.
101. Overigens kunnen consumenten op vergelijkbare wijze ook worden geconfronteerd met uiteenlopende zoekresultaten en nieuwsberichten, hetgeen kan leiden tot filterbubbels en echokamers. Zie bijv. Pariser, E. (2011) *The Filter Bubble: What the Internet Is Hiding from You*, New York: Penguin Press; Barberá, P., et al. (2015) Tweeting from left to right: Is online political communication more than an echo chamber? *Psychological science* 26.10 (2015), p. 1531-1542.
102. Poort, J. and Zuiderveen Borgesius, F.J. (2019) Does everyone have a price? Understanding people's attitude towards online and offline price discrimination. *Internet Policy Review*, 8(1).
103. Maxwell, S. & Garbarino, E. (2010) The identification of social norms of price discrimination on the internet. *Journal of Product & Brand Management*, 19(3), p. 218-224.
104. Dakers, M. (2016) Uber knows customers with dying batteries are more likely to accept surge pricing. *The Telegraph*, October 30, 2017.
105. Helberger, N. (2017) Big data en het consumentenrecht. In: P.H. Blok (red.) *Big data en het recht*. Den Haag: SDU Uitgevers, p. 151-168. Zie ook Luzak, J. & Hof, S. van der (2018) Directive 2011/83/EU - Consumer Rights Directive (Electronic Commerce Aspects). In: Gijrath, S., Hof, S. van der, Lodder, A.R., Zwenne, G.J. (eds.) *Concise European Data Protection, E-Commerce and IT Law*. Alphen aan den Rijn: Kluwer Law International, p. 325-394.
106. Kohavi, R., and Thomke, S. (2017) The Surprising Power of Online Experiments. *Harvard Business Review*, September 2017, p. 74-82.
107. Malgieri, G., and Custers, B. (2018) Pricing privacy: the right to know the value of your personal data, *Computer Law & Security Review*, Vol. 34, Nr. 2, p. 289-303, http://dx.doi.org/10.1016/j.clsr.2017.08.006.
108. Voor meer over marktregulering, zie Duijvenvoorde, G.P. van (2018), Marktregulering en digitale connectiviteit: Over onbegrensde elektronische communicatie en de prijs van geïndividualiseerde benaderingen, Radix 44(4): 264-274; Duijvenvoorde, G.P. van & Knol, P.C. (2019) Een nieuw telecomkader:

het Europees wetboek voor elektronische communicatie, *Nederlands Tijdschrift voor Europees Recht* 2019(1/2): 33-43.

109. Voor een mooi overzicht, zie Drijber, B.J. (2017) *Big data en het mededingingsrecht*, in: P.H. Blok (red.) Big data en het recht, Den Haag: SDU.
110. Stucke, M. & Ezrachi, A. (2015) *Artificial Intelligence & Collusion: When Computers Inhibit Competition*. Oxford Legal Studies Research Paper No. 18/2015.
111. Abe, N. & Kamba T. (2000) A Web Marketing System With Automatic Pricing, *Computer Network*s, Vol. 33, 775-788.
112. Hwang, S.B. & Kim, S. (2006) Dynamic Pricing Algorithm for E-Commerce, in: Advances in Systems, Computing Sciences and Software Engineering, 149-155; Mehra, S.K. (2015) Antitrust and the Robo-Seller: Competition in the Time of Algorithms, *Minnesota Law Review*, Vol. 100.
113. Couts, A. (2011) Why did Amazon charge $23,698,655.93 for a textbook? *Digital Trends*, 23 April 2011.
114. Een hogere prijsstelling is niet bepaald concurrerend en mag vreemd lijken. Reden hiervoor kan zijn dat deze aanbieder het boek helemaal niet heeft, maar toch een breed portfolio wil presenteren. Een andere reden kan zijn dat de aanbieder een bepaalde marktpositie wil innemen: voor allerlei producten kiezen consumenten graag de op-een-na-laagste prijs.
115. Bovendien kunnen nieuwe technologieen worden ingezet voor regulering, bijvoorbeeld via smart contracts. Gijrath, S.J.H. (2017) Telecommunications networks: Towards smarter regulation and contracts? *Competition and Regulation in Network Industries* 18(3/4), p. 175-197.
116. Ursic, H. & Custers, B.H.M. (2016) Legal Barriers and Enablers to Big Data Reuse - A critical Assessment of the Challenges for the EU Law, E*uropean Data Protection Law Review* 2(2), p. 209-221; Custers, B.H.M., and Ursic, H. (2016) Big Data and Data Reuse; A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection, *International Data Privacy Law*, pp. 1-12. DOI: 10.1093/idpl/ipv028.
117. Zie ook Ball, P. (2004) *Critical Mass; How One Thing Leads to Another*, New York: Farrar, Straus and Giroux.
118. https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy.
119. Custers, B.H.M., and Bachlechner, D. (2018) Advancing the EU Data Economy; Conditions for Realizing the Full Potential of Data Reuse, *Information Polity*, Vol. 22, No. 4, p. 291-309. DOI 10.3233/IP-170419.
120. Burns, E. (2016) Why haven't SMEs cashed in on big data benefits yet? *TechTarget*. http://searchbusinessanalytics. techtarget.com/feature/Why-havent-SMEs-cashed-in-on-big-data-benefits-yet.
121. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784.
122. Uiteraard zou deze casus ook vanuit consumentenrecht kunnen worden geadresseerd.
123. Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (2013) Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Heidelberg: Springer.
124. Boyd, D., and Crawford, K. (2012) Critical questions for big data: provocations for a cultural, technological and scholarly phenomenon, *Information, communication & society*, 15(5), p. 662-679; Tene, O., and Polonetsky, J. (2012) Privacy in the age of big data: a time for big decisions, *Stanford Law Review Online*, 64, p. 63.
125. Koops, B. J., Newell, B., Timan, T., Skorvánek, I., Chokrevski, T. & Galič, M. (2017) A typology of privacy, *University of Pennsylvania Journal of International Law*. 38, 2, p. 483-575.
126. Custers, B., Van der Hof, S., Schermer, B. (2014) Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, *Policy & Internet*, Vol. 6, No. 3, p. 268-295; Custers, B., Van der Hof, S.,

Schermer, B., Appleby-Arnold, S., and Brockdorff, N. (2013) Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law, *SCRIPTed, Journal of Law, Technology and Society*, Volume 10, Issue 4, p. 435-457.

127. Hiermee creëren mensen hun eigen identiteit, zie Frissen, V., Lammes, S., Lange, M. de, Mul, J. de, and Raessens, J. (2015) Playful Identities: The Ludification of Digital Media Cultures. Amsterdam: Amsterdam University Press.
128. McArthur, R.L. (2001) Reasonable expectations of privacy, *Ethics and Information Technology*, 3:123.
129. https://www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts.
130. Custers, B.H.M. (2012) Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination, *Privacy Observatory Magazine* 2012(3).
131. Baveye, Y., Bettinelli, J.N., Dellandrea, E., Chen, L. and Chamaret, C. (2013) A large video data base for computational models of induced emotion. In *Proceedings of Humane Association Conference on Affective Computing and Intelligent Interaction*; Borth, D., Chen, T., Ji, R.R., and Chang, S.F. (2013) Sentibank: Large-scale ontology and classiers for detecting sentiment and emotions in visual content. In *Proceedings of ACM Multimedia*.
132. Kosinski, M., Stillwell, D. & Graepel, T. (2012) Private traits and attributes are predictable from digital records of human behaviour, *Proceedings of the National Academy of Sciences* (PNAS), www.pnas.org/content/early/2013/03/06/1218772110.
133. Custers, B.H.M. (2012) Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination, *Privacy Observatory Magazine*, Issue 3. See http://www.privacyobservatory.org/.
134. Ohm, P. (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57: 1701.
135. Zwenne, G.J. (2019) Het vergeetrecht vijf jaar later, *Ars Aequi* 68(7): 607-613; Fosch-Villaronga, E., Kieseberg, P. & Li, T. (2018) Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, *Computer Law and Security Review* 34(2), p. 304-313.
136. Ursic, H. (2018) Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control, SCRIPTed, Vol. 15, Issue 1, August 2018. Swire, P., and Lagos, Y. (2013) Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 *Maryland Law Review* 335; Graef, I., Verschakelen, J., and Valcke, P. (2013) Putting the Right to Data Portability into a Competition Law Perspective, Journal of Higher School Economics Annual Review, 53, 63; Schermer B.W. (2017), Dataportabiliteit: the good, the bad and the ugly, *Tijdschrift voor Internetrecht* 2017(4): 161.
137. Cavoukian, A. (2013) Operationalising privacy by design: a guide to implementing strong privacy practices. Privacy Commissioner of Ontario, Ontario. https://www.privacybydesign.ca/con- tent/uploads/2013/01/operationalizing-pbd-guide.pdf; Custers, B.H.M., and Schermer, B.W. (2014) Responsibly Innovating Data Mining and Profiling Tools; A New Approach to Discrimination Sensitive and Privacy Sensitive Attributes, In: J. van den Hoven, B.J. Koops, H. Romijn, T. Swierstra and N. Doorn (eds.) *Responsible Innovation Volume 1: Innovative Solutions for Global Issues*. Dordrecht: Springer, p. 335-350.
138. Wright, D., and Hert, P. de (2012) *Privacy Impact Assessment*, Springer, Dordrecht, 2012; Warren, A., Bayley, R., Bennett, C., Charlesworth, A.J., Clarke, R., Oppenheim, C. (2008) Privacy Impact Assessments: International experience as a basis for UK guidance. *Computer Law and Security Report*, 2008, 24, 3 (April-

June 2008), p. 233-242; Clarke, R. (2011) An Evaluation of Privacy Impact Assessment Guidance Documents, International Data Privacy Law, 1, 2, March 2011, p. 111-120; Custers, B.H.M., Ursic, H., and Friedewald, M. (2019) Assessing the Legal and Ethical Impact of Data Reuse: Developing a tool for Data Reuse Impact Assessments (DRIA), *European Data Protection Law Review*. Vol. 5, nr. 3, p. 317-337.

139. Zeker kwetsbare groepen, zoals kinderen kunnen zulke bescherming goed gebruiken, zie Hof, S. van der & Lievens, E. (2018) The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR, *Communications Law* 23(1): 33-43. Hof, S. van der (2017) I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World, *Wisconsin International Law Journal* 34(2): 409-445. La Fors-Owczynik, K. (2017) Profiling 'Anomalies' and the Anomalies of Profiling: Digitalized Risk Assessments of Dutch Youth and the New European Data Protection Regime. In: Adams S., Purtova N., Leenes R. (Eds.) *Under Observation: The Interplay Between eHealth and Surveillance*. Law, governance and technology series no. 35 Cham: Springer, p. 107-138.
140. Schermer, B.W., Custers, B.H.M., and Van der Hof, S. (2014) The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection, *Ethics & Information Technology*, Vol. 16, No. 2, p. 171-182. Muravyeva, E., Janssen, J., Specht, M., Custers, B. (2020) Exploring solutions to the privacy paradox in the context of e-assessment: informed consent revisited, Ethics and Information Technology, https://doi.org/10.1007/s10676-020-09531-5.
141. Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126, p. 1880–1903.
142. Zarsky, T. (2017) Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2).
143. Shannon, C.E. (1948) The mathematical theory of communication, *Bell Systems Technology Journal*, Vol. 27, p. 379-423 and p. 623-656; Shannon, C.E. (1949) Communications theory of secrecy systems, *Bell Systems Technology Journal*, Vol. 28, p. 656-715.
144. Custers, B., Dechesne, F., Sears, A., Tani, T., Van der Hof, S. (2018) A comparison of data protection legislation and policies across the EU, *Computer Law & Security Review*, Vol. 34, Nr. , p. 234-243, http://dx.doi.org/10.1016/j.clsr.2017.09.001.
145. Custers, B.H.M., Sears, A.M., Dechesne, F., Georgieva, I.N., Tani, T., and Van der Hof, S. (2019) EU Personal Data Protection in Policy and Practice, Heidelberg: Asser/Springer. pp. 249.
146. Bamberger, K.A., and Mulligan, D.K. (2015) *Privacy on the Ground in the United States and Europe*, MIT Press.
147. Custers, B., Van der Hof, S., Schermer, B. (2014) Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, *Policy & Internet*, Vol. 6, No. 3, p. 268-295.
148. Hildebrandt, M., Gutwirth, S. (2008) *Profiling the European Citizen*. Heidelberg: Springer.
149. Harcourt, B.E. (2007) *Against Prediction: Profiling, Policing and Punishing in an Actuarial Age*. Chicago: University of Chicago Press.
150. Vandaar dat regelmatig ook naar andere rechtsgebieden wordt gekeken. Zie bijv. de vergelijking met milieurecht in: Rhoen, M. (2018) Big Data, Big Risks, Big Power Shifts: Evaluating the GDPR as an instrument of risk control and power redistribution in the context of big data. Proefschrift, Leiden.
151. Uiteraard kan iemand gezond boerenverstand gebruiken om tot een betere kredietscore te komen, zoals bijvoorbeeld rekeningen altijd tijdig betalen, schulden weg te werken en minder uit te geven dan er maandelijks binnenkomt. Maar als het algoritme gebaseerd is op postcode, heeft dit allemaal betrekkelijk weinig zin als de andere bewoners in het postcodegebied niets veranderen.

152. Calders, T., Žliobaitė, I. (2013) Why unbiased computational processes can lead to discriminative decision procedures, in: Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) *Discrimination and privacy in the information society*, Heidelberg: Springer.
153. Voor meer over predictive policing, zie Richardson, R., et al. (2019) Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (February 13, 2019) *New York University Law Review Online*. Available at SSRN: ssrn.com/abstract=3333423; Ferguson, A.G. (2017) Policing Predictive Policing. *Washington University Law Review*, Vol. 94, No. 5, 2017. SSRN: https://ssrn.com/abstract=2765525.
154. Fosch-Villaronga, E., Poulsen, A., Søraa, R.A., Custers, B.H.M. (2021) A little bird told me your gender: Gender inferences in social media, *Information Processing and Management* 58, https://doi.org/10.1016/j.ipm.2021.102541.
155. Loenen, M.L.P. (2009) Gelijkheid als juridisch beginsel. Een conceptuele analyse van de norm van gelijke behandeling en non-discriminatie. Den Haag: Boom Juridische uitgevers.
156. Pedreschi, D., Ruggieri, S., Turini, F. (2013) The discovery of discrimination, in: Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Heidelberg: Springer.
157. Jaeger, B., & Sleegers, W. (2020) Racial discrimination in the sharing economy: Evidence from Airbnb markets across the world. https://doi.org/10.31234/osf.io/qusxf.
158. Zliobaite, I. & Custers, B. (2016) Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, *Artificial Intelligence and Law* (24), p. 183-201.
159. Kamiran, F., and Calders, T. (2009) Classification without discrimination. In IEEE international conference on computer, control & communication (IEEE-IC4), 17–19 February 2009, Karachi, Pakistan.
160. Squires, G. (2003) Racial profiling, insurance style: insurance redlining and the uneven development of metropolitan areas. *Journal of Urban Affairs*, 25(4):391–410; Hillier, A. (2003) Spatial analysis of historical redlining: a methodological explanation. *Journal of Housing Research*, 14(1), p. 137–168.
161. Kamiran, F., Calders, T., Pechenizkiy, M. (2013) Techniques for discrimination-free predictive models, in: Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) Discrimination and privacy in the information society, Heidelberg: Springer.
162. Als het meer algemeen gaat om het beschermen van normen en warden, word took wel gesproken van value sensitive design, zie Friedman, B., Kahn Jr., P.H., Borning, A. (2006) Value Sensitive Design and information systems. In: Zhang, P., Galletta, D. (eds.) *Human-Computer Interaction in Management Information Systems: Foundations*, p. 348–372. New York: M.E. Sharpe.
163. Custers, B.H.M. (2012) Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination, *Privacy Observatory Magazine*, Issue 3. See http://www.privacyobservatory.org/.
164. Zliobaite, I. & Custers, B. (2016) Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, *Artificial Intelligence and Law* (24), p. 183-201.
165. Merk op dat hier ook een discrepantie zit tussen de Awgb en de AVG. Bijvoorbeeld de AVG noemt ook het verwerken van strafrechtelijke persoonsgegevens als een categorie met extra beperkingen en waarborgen, terwijl de Awgb een strafblad niet als potentieel discriminerende factor beschouwt.
166. Barocas, S. & Selbst, A. (2016) Big Data's Disparate Impact, 104 *California Law Review*, 671.

167. Dit hoofdstuk is grotendeels gebaseerd op Custers, B.H.M., & Leeuw, F. (2017) Legal big data, *Nederlands Juristenblad*, afl. 34, p. 2449-2456.
168. Ginsberg, J., Mohebbi, M.H., Patel, R.S., Brammer, L., Smolinski, M.S. and Brilliant, L. (2009) Detecting influenza epidemics using search engine query data. *Nature*. 457 (7232), p. 1012–1014.
169. Althoff, T., Sosič, R., Hicks, J.L., King, A.C., Delp, S.L., Leskovec, J. (2017) Large-scale physical activity data reveal worldwide activity inequality. *Nature*, DOI: 10.1038/nature23018.
170. Schrodt, P. (2011) Automated Production of High-Volume, Near-Real-Time Political Event Data. Paper presented at the New Methodologies and Their Applications in Comparative Politics and International Relations Workshop. Princeton University, 4-5 February 2011.
171. Leetaru, K. (2014) Did the Arab Spring Really Spark a Wave of Global Protests? The world may look like it's roiling now, but the 1980s were far worse. *Foreign Policy*, 30 May 2014.
172. Willemsen, F. & Leeuw, F. (2016) Big Data, real world events and evaluations, in: G. Petersson e.a. (ed.) *Big Data and evaluation*, Piscataway NJ: Transaction Publishers.
173. Ayres, I. (2007) Super Crunchers: *How Anything Can Be Predicted*. London: John Murray Publishers.
174. Methodologisch gezien is er altijd discussie over de wetenschappelijkheid van het recht geweest. Cf. Franken, H. (2008) Rechtsgeleerdheid in de rij der wetenschappen. Amsterdam: KNAW - KNAW press; Stolker, C.J.J.M. (2003) Ja, geléérd zijn jullie wel! Over de status van de rechtswetenschap, *Nederlands Juristenblad*(15), p. 766-778; Stolker, C.J.J.M. (2004) Wat maakt een juridisch tijdschrift wetenschappelijk? *NJB-kronieken*, p. 1409-1418.
175. Custers, B.H.M. (2017) Kunnen computers het wetboek interpreteren? In: De Graaf B, Rinnooy Kan A. (red.) *Hoe zwaar is licht? Meer dan 100 dringende vragen aan de wetenschap*. Amsterdam: Balans.
176. Ruger, T.W., Kim, P.T., Martin, A.D., & Quinn, K.M. (2004) The Supreme Court Forecasting Project: Legal and Political Science Approaches to Predicting Supreme Court Decisionmaking, *Columbia Law Review*, Vol. 104, p. 1150.
177. Katz, D., Bommarito, M., & Blackman, J. (2014) Predicting the Behavior of the Supreme Court of the United States, *PLoS ONE*, Vol. 12, nr. 4., e0174698.
178. Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., & Lampos, V. (2016) Predicting judicial decisions of the European Court of Human Rights, *PeerJ Computer Science*, 2:e93.
179. Danziger, S., Levav, J., & Avnaim-Pesso, L. (2011) Extraneous factors in judicial decisions, *Proceedings of the National Academy of Sciences*, Vol. 108, nr. 17, p. 6889-6892. Overigens zouden op deze manier ook hypothesen van (Amerikaanse) Legal Realists (uit de jaren 30-50 van de vorige eeuw) opnieuw getoetst kunnen worden, zie Leeuw, F.L., & Schmeets, H. (2016) *Empirical Legal Research, A Guidance Book for Lawyers, Legislators and Regulators*, Cheltenham: Edward Elgar Publishing, Inc.
180. Oliver Wendell Holmes, Jr. (1897) The Path of the Law, 10 Harvard Law Review, 457, 461. Zie ook Radin, M. (1925) The Theory of Judicial Decision: Or How Judges Think, *American Bar Association Journal*, Vol. 11, p. 357-362.
181. Zie ook Wiggers, G., Verberne, S. & Zwenne, G.J. (2018) Exploration of Intrinsic Relevance Judgments by Legal Professionals in Information Retrieval Systems. In: Brandsen, A., Dirkson, A.R., Kraaij, W., Lamers, W., Verberne, S., Vos, H. de, Wiggers, G. (red.) *Proceedings of the 17th Dutch-Belgian Information Retrieval workshop*. Leiden: DIR, p.. 5-8.
182. Custers, B.H.M. (2017) Kunnen computers het wetboek interpreteren? In: De Graaf B, Rinnooy Kan A. (red.)

Hoe zwaar is licht? Meer dan 100 dringende vragen aan de wetenschap. Amsterdam: Balans.

183. Eckholm, E. (2015) Harvard Law Library Readies Trove of Decisions for Digital Age. *New York Times*, 28 Oktober 2015. Zie ook Van Dijck, G. (2016) Legal research when relying on open access, *Law and Method*, April 2016.
184. Custers, B.H.M. (2016) Big Data in wetenschappelijk onderzoek, *Justitiële Verkenningen*, Vol. 2016, nr. 1, p. 8-21.
185. Voor opportunistisch gebruik van big data tijdens de Amerikaanse presidentsverkiezingen in 2016, zie: Grassegger, H. & Krogerys, M. (2017) The Data That Turned the World Upside Down, *Motherboard*, 28 januari 2017.
186. Ball, P. (2004) *Critical Mass; How One Thing Leads to Another*, New York: Farrar, Straus and Giroux.
187. Willemsen, F. & Leeuw, F. (2016) Big Data, real world events and evaluations, in: G. Petersson e.a. (red.), *Big Data and evaluation*, Piscataway NJ: Transaction Publishers.
188. Leeuw, H.B.M. (2017) Punish, Seduce or Persuade. An Empirical Assessment of Anti-Piracy Interventions, The Hague: Eleven International Publishing.
189. Leeuw, F. (2015) Wetgeving, empirisch juridisch onderzoek en legal big data, *Recht der Werkelijkheid*, Vol. 36, Nr. 2, p. 50-65.
190. Fawcett, T. (2015) Mining the Quantified Self: Personal Knowledge Discovery as a Challenge for Data Science, *Big Data*, Vol. 3, Nr. 4.
191. Zie bijvoorbeeld: Kogel, C.H. de, & Cornet, L.J.M. (2016) Toepassingsmogelijkheden van Quantified Self-data, *Justitiële Verkenningen* 42 (2016) p. 79-95.
192. Boom, W.H. van, Gestel, & R.A.J. van (2015) Rechtswetenschappelijk onderzoek – een samenvatting van de uitkomsten van een landelijke enquête, *Nederlands Juristenblad*, Vol. 20, p. 1336-1347.
193. In juridisch of taalkundig opzicht zijn de teksten doorgaans uiteraard wel gestructureerd. Ongestructureerd betekent hier dat ze, anders dan kwantitatieve gegevens over bijvoorbeeld demografie, financiën of criminaliteit die een vast (cijfermatige) structuur hebben, in dát opzicht vormvrij zijn.
194. Pistone, M.R. & Horn, M.B. (2016) *Disrupting Law School: How disruptive innovation will revolutionize the legal world*. San Francisco: Christensen Institute.
195. Tamanaha, B. (2012) *Failing Law Schools*, Chicago: University of Chicago Press.
196. Gershman, J. (2015) Law School Applicant Pool Still Shrinking, *The Wall Street Journal*, 23 April 2015.
197. Yacht (2015) *Trends en ontwikkelingen op de Legal arbeidsmarkt vierde kwartaal 2016*. Amsterdam: Yacht.
198. Susskind, R. (2013) *Tomorrow's Lawyers*, Oxford: Oxford University Press.
199. Prins, J.E.J. (2015) Big data en de rechterlijke macht, *Nederlands Juristenblad*, Vol. 90, Nr. 30, p. 2087.
200. Zie bijvoorbeeld de noodkreet van het gerechtshof Den Haag: Modderkolk, H. (2017) Dringend gezocht: rechters met kennis van cybercriminaliteit, *Volkskrant*, 3 augustus 2017. Ook in het bestuursrecht wordt aan de bel getrokken, zie Meuwese, A. (2017) Grip op normstelling in het datatijdperk, in: W. den Ouden, *Algemene regels in het bestuursrecht*, Meppel: Boom Juridische Uitgevers.
201. Oostrom-Streep, N.C. van (2016) A wounded deer leaps highest, *Nederlands Juristenblad*, Afl. 41, p. 3028; Barkhuysen, T. (2016) De Homo Digitalis als uitdaging voor het recht, *Nederlands Juristenblad*, Afl. 22, p. 1527.
202. Er zijn nog meer rechtsgebieden waar technologieontwikkelingen relevant zijn. Bijvoorbeeld het mediarecht en de discussie rondom nepnieuws, het telecommunicatierecht en de discussie over netneutraliteit en het vermogensrecht en de discussie over eigendomsrechten met betrekking tot

persoonsgegevens zijn enkele van de rechtsgebieden en onderwerpen die niet aan bod zijn gekomen. Voor ruimte(vaart)recht, zie bijvoorbeeld ook: Stefoudi, D. (2017) Big Data from Space - Legal issues related to access and dissemination of large volumes of space-generated data. In: Blount, P.J., Masson-Zwaan, T., Moro-Aguilar, R., Schrogl, K.U. (eds.) *Proceedings of the International Institute of Space Law 2016*. Proceedings of the International Institute of Space Law nr. 59 The Hague: Eleven International Publishing. 49-60.

203. SAILS staat voor Society, Artificial Intelligence & Life Sciences. Zie https://www.universiteitleiden.nl/en/sails.
204. Leenes, R. (2019) Regulating new technologies in times of change. In L. Reins (ed.) *Regulating New Technologies in Uncertain Times*, p. 3-17. (Information Technology and Law Series, Vol. 2019, No. 32). Heidelberg: TMC Asser Press | Springer. https://doi.org/10.1007/978-94-6265-279-8_1.
205. Custers, B.H.M. (2019) Reuse of data in smart cities: legal and ethical frameworks for big data in the public arena, in: F. Feldberg et al. (eds.) Appropriate use of data in public space: essay collection, Den Haag: NL Digitaal, p. 9-35.
206. La Fors, K., Custers, B.H.M., and Keymolen, E. (2019) Reassessing values for emerging big data technologies: integrating design-based and application-based approaches, *Ethics and Information Technology*, Volume 21, Number 3, p. 209-226. https://doi.org/10.1007/s10676-019-09503-4.
207. Keymolen, E.L.O. (2016) Trust on the line. A philosophical exploration of trust in the networked era. Oisterwijk: Wolf Legal Publisher; Keymolen, E.L.O. & Hof, S. van der (2019) Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust, *Journal of Cyber Policy* 4(2), p. 143-159.
208. McCrudden, C. (2008) Human Dignity and judicial Interpretation of Human Rights. *European Journal of International Law*, 19(4), p. 655-724. https://doi.org/10.1093/ejil/chn043.
209. Citaat toegeschreven aan Mahatma Gandhi, zie https://www.goodreads.com/quotes/16418-the-future-depends-on-what-you-do-today.