Overwegingen en suggesties voor beleid

Expert bijeenkomst 29 oktober 2021

Zeggenschap, eigenaarschap en persoonsgegevens

Verslag van de expert bijeenkomst d.d. 29 oktober 2021

overwegingen en suggesties voor beleid

INHOUD

I. De expert bijeenkomst

Op 29 oktober 2021 is een panel van juridische experts bijeengekomen om van gedachten te wisselen over de vraag of er mogelijkheden zijn voor het vergroten van de zeggenschap van een individu over de eigen persoonsgegevens.

Aanleiding voor de bijeenkomst

In juli 2020 zegde Staatssecretaris Knops van Binnenlandse Zaken en Koninkrijksrelaties in een overleg met de Tweede Kamer toe, nog eens nader te onderzoeken wat de meerwaarde kan zijn van het hanteren van het eigendomsbegrip voor persoonlijke gegevens: een nadere toetsing van nut en hanteerbaarheid van een eigendomsbenadering van persoonsgegevens waarbij de Staatssecretaris aangaf daarbij het door het kamerlid Van Dam aangehaalde proefschrift van N. Purtova te betrekken.

De toezegging maakte deel uit van de beraadslagingen over dit onderwerp, nadat de Staatssecretaris op 15 juni 2020 een korte brief aan de Tweede Kamer had gezonden met een onderbouwing waarom het regelen van eigendom van persoonsgegevens naar analogie met het BW geen goed idee is. In die brief werd het standpunt van de Raad van State op deze invalshoek meegewogen.

De Staatssecretaris heeft aansluitend aan de Tweede Kamer wel toegezegd dat hij de afwegingen nog eens wil bezien, en daarbij te kijken hoe ‘toekomstbestendig’ de gekozen opstelling is. Hij wilde kortom de potentiële meerwaarde van een eigendomsbenadering voor persoonsgegevens nog eens opnieuw in overweging nemen.

Het panel van experts

Op verzoek van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft een panel van onafhankelijke experts zich gebogen over de door de staatssecretaris benoemde vraagstukken.

De deelnemers aan het panel waren: mr. dr. Theo Hooghiemstra, prof dr. mr. Peter Blok, prof. dr. mr. Lokke Moerel, dr. Peter Olsthoorn, prof. dr. Nadya Purtova, en prof dr. mr. Eric Tjong Tjin Tai.

II. Samenvatting van de bijeenkomst op hoofdlijnen

A. De vraagstelling

Twee vragen stonden bij de bijeenkomst centraal. Allereerst de vraag hoe individuen controle kunnen houden over gegevens die over hen gaan of van hen zijn, en als tweede de vraag of eigendomsrechten daarin een rol kunnen spelen.

Meer in het bijzonder is aandacht besteed aan de vraag of er door het beter benutten van bestaande wettelijke kaders, of door gebruik te maken van technologische oplossingen, aanvullende mogelijkheden zijn om de zeggenschap over de eigen gegevens te verbeteren.

Het doel daarvan is de positie van individuele burgers sterker te maken, met name in het licht van grootschalige gegevensverwerkingen. Daarbij is met name ook aandacht besteed of er vanuit de invalshoek van eigendom van persoonsgegevens nieuwe oplossingen mogelijk zijn.

Belangrijke conclusies:

- Het concept van eigendom is niet geschikt om toe te passen op persoonsgegevens;
- Er is niet één alomvattende oplossing als het gaat om de versterking van de positie van de individu rond de verwerking van zijn persoonsgegevens. Daarom verdienen meerdere paden uitwerking, waarbij het concept van eigendom wel een inspiratiebron kan zijn;
- De AVG kent in zijn toepassing en naleving inherente beperkingen. De huidige praktijk rond het vragen van toestemming biedt voor een individu geen afdoende bescherming en zeggenschap. En ook transparantie heeft maar een beperkte waarde voor het vergroten van de controle en zeggenschap van het individu over de eigen gegevens;
- Transparantie is nadrukkelijk wel van belang als middel om de legitimiteit van een gegevensverwerking te kunnen controleren, en daardoor duidelijkheid te verschaffen over, en te kunnen controleren, wat er met gegevens gebeurt en of deze legitiem worden gebruikt;
- In aanvulling op deze bestaande mogelijkheden zouden voor cruciale onderwerpen duidelijke grenzen moeten worden aangegeven wat mag en wat niet mag, waaronder het selectief opstellen van verboden;
- Individuele zelfbeschikking kan niet voorop staan in de relatie burger-overheid. De overheid heeft voor bepaalde taken gegevens nodig. Dat regelt de wetgever met algemene regels en niet met individuele toestemmingen. Bestuursorganen kunnen zelf wel meer keuze- en controleopties aanbieden voor de burger, en waar nodig in materie-regelgeving borgen;
- Anticipeer op mogelijkheden om zeggenschap over de eigen gegevens van het individu te versterken via uitwerkingen van EU Data Act, Data Governance Act, Digital Market Act, en de geamendeerde eIDAS-verordening (Directive on EU digital Identity);
- Verbeter en stimuleer de mogelijkheden voor collectieve actie, zoals de mogelijkheid voor handhaving langs privaatrechtelijke weg, of de mogelijkheid voor bedrijven om andere bedrijven ter verantwoording te roepen.

B. Samenvatting op hoofdlijnen

Het concept van eigendom is niet geschikt om toe te passen op persoonsgegevens

De deelnemers aan de expertbijeenkomst vinden het concept van eigendom om meerdere redenen niet geschikt om toe te passen op persoonsgegevens. Zo zijn in het Nederlands BW het eigendomsrecht en de daaruit voortvloeiende beschikkingsmacht over een goed vervreemdbaar. Zeggenschap over persoonsgegevens is echter naar zijn aard onvervreemdbaar. Het is ondenkbaar en onwenselijk dat een betrokkene de zeggenschap over zijn persoonsgegevens aan een ander kan overdragen en vervolgens dus niets meer te zeggen zou hebben over zijn of haar gegevens. Een ander voorbeeld waarom het concept van eigendom niet geschikt is om toe te passen op persoonsgegevens, is omdat de vraag wanneer iets een persoonsgegeven is, afhankelijk is van de context en de betekenis die aan een gegeven op een bepaald moment gegeven wordt. Hierdoor kunnen gegevens die eerst geen persoonsgegevens waren dit later alsnog worden, en andersom.

De beperkingen van de AVG

De AVG biedt weliswaar een belangwekkend grenzen formulerend kader, maar tegelijk kent de AVG in haar toepassing en naleving ook inherente beperkingen.

Beperkingen bij het vragen van toestemming

Bij het verwerken van persoonsgegevens gaat het in de praktijk in toenemende mate om het combineren van gegevens, en het toepassen van de inzichten die daaraan kunnen worden ontleend in de relatie met klanten of burgers. De huidige praktijk rond het vragen van toestemming biedt voor een individu geen afdoende bescherming en zeggenschap. Grote bedrijven grijpen elke mogelijkheid aan om twijfel te zaaien of de gegeven toestemmingen geldig zijn of niet. Burgers en consumenten zitten bovendien niet te wachten op een overmaat aan gevraagde toestemmingen. In de praktijk wordt daardoor veelal voetstoots toestemming verleend, ook uit angst om toegang tot diensten te verliezen, dan wel uit desinteresse.

Transparantie nadrukkelijk van belang, maar slecht in mindere mate voor het individu

De deelnemers benadrukken het belang van goede transparantie bij verwerken van gegevens. Dit belang is naar de mening van de deelnemers echter niet zozeer gelegen in bieden van meer regie voor het individu, maar heeft vooral een meerwaarde als verantwoording voor de legitimiteit van het gebruik van data door de partij die de gegevens verwerkt.

Bij de overheid is die legitimiteit vooral gelegen in de wettelijke grondslag voor de verwerking van de gegevens. Transparantie biedt in dat geval vooral de mogelijkheid het systeem te toetsen, veel meer nog dan de mogelijkheid van toetsing van de rechtmatigheid in het individuele geval.

In de particuliere sector biedt transparantie de mogelijkheid van toetsing van gemaakte afwegingen bij de juiste toepassing van een grondslag zoals het gerechtvaardigde belang. Aan de andere kant wordt ter nuancering opgemerkt dat niet geheel moet worden uitgevlakt dat betere transparantie wel degelijk wat doet met de ‘*empowerment*’ van het individu.

Oplossingsrichtingen

Er is niet één alomvattende oplossing waar het gaat om de versterking van de positie van de burger of consument rond de verwerking van zijn persoonsgegevens. In aanvulling op bestaande initiatieven zijn tijdens de bijeenkomst meerdere alternatieve oplossingsrichtingen benoemd die alle naast elkaar hun weg kunnen vinden.

(1) Stel duidelijke grenzen wat mag en wat niet mag

In aanvulling op deze bestaande mogelijkheden zouden voor cruciale onderwerpen duidelijke grenzen moeten worden aangegeven wat mag en wat niet mag, waaronder het selectief opstellen van verboden. Denk daarbij aan aanvullende regulering van, of verboden voor, profiling voor gepersonaliseerde advertenties, maar ook aan voorwaarden die moeten worden gesteld aan het hergebruik van persoonsgegevens uit overheidsadministraties.

(2) Collectieve acties en acties tussen bedrijven onderling

Een andere oplossingsrichting is het stimuleren en verbeteren van mogelijkheden voor collectieve actie. Naast de bestaande mogelijkheden voor collectieve claims op basis van de AVG, is een betere uitwerking en onderzoek nodig naar de mogelijkheden voor handhaving langs privaatrechtelijke weg, om via die optie een gezamenlijke claim in te kunnen dienen tegen partijen die gegevens verwerken en daarbij anderen benadelen.

Daarnaast is het waardevol om te onderzoeken hoe bedrijven elkaar op naleving van de privacyregels kunnen aanspreken. Denk aan een mogelijkheid voor bedrijven om andere bedrijven ter verantwoording te roepen rond concurrentieverstoring door onrechtmatige verwerking van persoonsgegevens. Een interessante lijn, omdat bij de veelheid aan maatschappelijke praktijken toezicht door de overheid alleen, nooit kan voldoen.

(3) Kaderstelling door de overheid bij delen van gegevens

Waar men bij regie op gegevens denkt aan het met toestemming delen van persoonsgegevens door publieke instanties aan private partijen, is een juridische benadering met kaderstelling belangrijk. In Europees verband zijn de eerste stappen gezet (zoals de *Data Governance Act*). Maar het is belangrijk dat nu al stappen worden uitgewerkt hoe dit op nationaal niveau optimaal kan worden geoperationaliseerd. Als de overheid gevalideerde overheidsgegevens gaat delen met derde partijen ligt het voor de hand dat de overheid namens ons allemaal eisen stelt aan de private partijen en intermediairs om de zeggenschap van het individu te bewaken.

(4) Lering uit bestaande initiatieven, en inspiratie naar analogie

Binnen diverse sectoren zijn initiatieven ontplooid om betrokkenen meer zeggenschap te geven over de eigen gegevens. Mogelijk zijn onderdelen hiervan te hergebruiken binnen andere sectoren.

En hoewel de invalshoek van eigendom van persoonsgegevens geen mogelijkheden biedt voor de versterking van de positie van de burger of consument ten aanzien van de eigen persoonsgegevens, kunnen vermogens- of eigendomsrechtelijke noties in specifieke situaties wel inspiratie bieden voor concrete maatregelen gericht op het anders regelen van zeggenschap voor de betrokkene.

(5) Controle door techniek

Het blijft een uitdaging om controle in technische systemen concreet te maken. Denk in dat geval aan mogelijkheden waarbij een individu zelf zijn gegevens kan wissen of *switchen* naar andere platforms of aanbieders. Er is meer aandacht nodig voor de vraag welke opties er mogelijk zijn, en hoe deze te implementeren zijn.

III. Inhoudelijke samenvatting van de bijeenkomst

De bijeenkomst bestond uit twee delen. In eerste aanleg werd aan alle deelnemers afzonderlijk de gelegenheid gegeven om vanuit de eigen professionele praktijk te reageren op de vraagstukken uit de startnotitie. Aansluitend is in gezamenlijkheid nagedacht welke nadere overwegingen en suggesties voor beleid mogelijk zijn.

A. Nadya Purtova

Purtova stelt dat er twee - onderling verbonden - kernvragen aan de orde zijn:

(1) de vraag hoe individuen controle houden over gegevens die over hen gaan of van hen zijn; en
(2) de vraag of eigendomsrechten daarin een rol kunnen spelen.

Wat de eerste vraag betreft, neemt Purtova waar dat er een brede overeenstemming aan het ontstaan is dat individuele controle over gegevens een illusie is. Dat is om meer redenen.

Er worden op dit moment zulke massa's aan gegevens verwerkt door tal van partijen en de verwerking is zo complex, dat het geen mens lukt om voor die verwerkingen overal toestemming te geven, of te onthouden, of toegang tot de gegevens te hebben, of zelf te beheren. Het ontbreekt individuen aan tijd, aandacht, maar ook cognitieve vermogens. Wie leest – en begrijpt volledig - alle gebruiks-en privacy-voorwaarden bij portalen, producten en diensten? Er zullen vast digitale hulpmiddelen zijn die hierin iets kunnen helpen, maar ook die dekken nooit de lading van het groeiende complex aan meer of minder herleidbare data.

Een tweede reden ligt in de vraag of we eigenlijk wel (resoluut en absoluut) *individuele* controle zouden moeten, en willen hebben.

Controle als individu over de eigen persoonsgegevens kan ook gevolgen (*spillover effect*) hebben voor anderen. Denk aan profilering: profielen die worden opgebouwd uit (met instemming) verwerkte persoonsgegevens die vervolgens ook worden toegepast op andere personen.

De persoonlijke levenssfeer beschermen vraagt om een zekere bescherming van, en toegang tot, bepaalde persoonsgegevens die de persoonlijke levenssfeer vormen (bijv. van gezondheidsdata of andere data die de AVG als bijzondere persoonsgegevens benoemt). Dat is niet het punt dat ter discussie staat. Maar niet alle persoonsgegevens in de zin van de AVG horen tot persoonlijke levenssfeer. Het begrip "persoonsgegevens" in de AVG is veel breder en omvat ook gegevens die inhoudelijk niet altijd *over* een persoon hoeven te gaan, maar wel *betrekking hebben op* een persoon, onder andere door de impact van het gebruik van de gegevens op de rechten en belangen.

Individuele controle over persoonsgegevens in de zin van de AVG lost veel problemen niet op. De bescherming van de AVG is meer beperkt dan waar de effecten van verwerkingen uiteindelijk toe strekken. En dat kan aanleiding zijn gegevensregulering breder aan te zetten.

De AVG-benadering van rechtsbescherming is "alles of niets". De AVG garanties gelden alleen wanneer persoonsgegevens worden verwerkt, en zijn niet van toepassing in situaties met niet-persoonlijke (bijvoorbeeld geanonimiseerde of geaggregeerde) gegevens. De verwerking van niet-persoonsgegevens kan negatieve gevolgen hebben voor mensen, terwijl de AVG-bescherming in dergelijke gevallen niet van toepassing zal zijn. Te denken is bijvoorbeeld aan de profilering die gebeurt op basis van groepsgegevens en die leidt tot gevolgen op groepsniveau.

De AVG wordt vaak gezien als een alomvattend kader voor de aanpak van bijna alle regelgevingskwesties omtrent een digitale samenleving.[1] Deels komt dit doordat een brede definitie van persoonsgegevens het mogelijk maakt de AVG toe te passen in vele contexten en diverse risico's van gegevensverwerking aan te pakken. Alhoewel het begrip persoonsgegevens door onder andere het Hof van Justitie van EU zeer ruim wordt geïnterpreteerd, zijn de verantwoordelijken voor de gegevensverwerkingen in de praktijk vaak niet op de hoogte van de juridische betekenis van het concept en passen het ook niet zo breed toe. Daarmee wordt het beschermingspotentieel van de AVG niet ten volle benut. In het 2020 verslag van het EU Grondrechtenagentschap (*European Union Agency for Fundamental Rights*) wordt daarom aangedrongen op meer richtlijnen voor AI-gebruikers over wat persoonsgegevens zijn in de context van AI.[2]

Een andere belangrijke overweging is dat verantwoordelijken verschillende strategieën toepassen om hun gegevensverwerking bewust buiten het toepassingsgebied van de AVG te houden, bijvoorbeeld door aan te voeren dat zij geen persoonsgegevens verwerken als gevolg van het toepassen van één of meer “anonimiseringstechnieken”, terwijl de gegevensverwerking nog steeds negatieve gevolgen kan hebben op mensen.

Purtova pleit daarom bij het reguleren van gegevensverwerkingen voor een bredere benadering dan alleen met, of in de AVG. Het moet niet over de controle over persoonsgegevens gaan, maar over de schadelijke praktijken en effecten, zoals *surveillance, targeted advertising*, of geautomatiseerde besluitvorming. In het werkingsgebied van de rechtsrelatie tussen overheid en burger zou de overheid bestaande wetgeving (administratief-recht) voortvarender moeten aanpassen aan de digitale praktijken van nu. Laat de databescherming niet alleen over aan regulering van regie op persoonlijke gegevens van het individu alleen.

Ten aanzien van het tweede vraag - of eigendomsrechten een rol kunnen spelen bij controle door individuen over de eigen gegevens - wijst Purtova erop dat haar proefschrift over dit onderwerp intussen 10 jaar oud is. Het moet worden gelezen tegen de achtergrond van de toenmalige dynamiek van gegevensverwerkingen, gebaseerd op vergelijkend eigendomsrecht en niet specifiek startend vanuit het Nederlandse rechtssysteem. Een kenmerk van eigendom daarin is het recht anderen van gebruik uit te kunnen sluiten.

Er kan gesproken worden over economische eigendomsrechten (met een feitelijke mogelijkheid om uit te sluiten) en wettelijke eigendomsrechten (met juridisch afdwingbare rechten om uit te sluiten). Ook als ze in wet niet formeel als "eigendom" worden benoemd, kunnen eigendomsrechten bestaan. Het gaat om de inhoud van de rechten. In dat opzicht kan de bestaande benadering van gegevensbescherming (bijvoorbeeld in de AVG) worden gezien als beperkte eigendomsrechten op persoonsgegevens. Begrepen als het recht om uit te sluiten, kunnen eigendomsrechten worden gebruikt om de individuele controle over persoonlijke gegevens te verbeteren. Voorgaande vormde destijds de kern van de stellingname in haar proefschrift.

In de 10 jaar die zijn verstreken, werd het voor Purtova echter duidelijk dat individuele controle over persoonsgegevens (a) niet mogelijk, en (b) niet wenselijk is als hoeksteen van de rechtsbescherming van mensen tegen digitale benadeling[3]. Om die reden heeft het geen zin om eigendomsrechten op persoonsgegevens in te voeren om de individuele controle op de eigen gegevens te verbeteren.

[1] Koops, B.J. (2014) ‘The Trouble with European Data Protection Law’, International Data Privacy Law, Doi: 10.1093/ *IDPL* 4(4) 257

[2] EU Fundamental Rights Agency (FRA) *Getting the future right: Artificial Intelligence and Fundamental Rights* (FRA 2020) https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

[3] Purtova, N.N. (2017) 'Do property rights in personal data make sense after the Big Data turn? Individual control and transparency', 10(2) Journal of Law and Economic Regulation November 2017, p.64-78 Tilburg Law School Research Paper No. 2017/21

Een context waarin het volgens Purtova mogelijk nog wel zinvol is om eigendomsrechten van gegevens te overwegen, is de verdeling van rijkdom. Op dit moment eisen *Big Tech* bedrijven feitelijk de eigendomsrechten op van de gegevens die via hun platforms worden gegenereerd. Deze gegevens - hoewel mede gegenereerd door gebruikers – komen nu alleen maar ten goede aan *Big Tech.* Hierdoor zijn we waar het om gebruik van data gaat met zijn allen als samenleving totaal afhankelijk geworden van *Big Tech.* Het toewijzen van eigendomsrechten van de gegevens aan platformgebruikers kan een optie zijn om dit te wijzigen. Maar vanuit de bescherming van fundamentele rechten voldoet deze optie niet.

Om van eigendom te kunnen spreken moet je bovendien scherp kunnen onderscheiden wat het object van de eigendom is. Anders kan je niet transparant zijn naar anderen, om aan te kunnen geven waar je ze geen toegang toe wil geven. Met persoonsgegevens is dit vrijwel onmogelijk. Persoonsgegevens zijn zo afhankelijk van de context, en van de betekenis die daar op een bepaald moment aan gegeven wordt, dat een gegeven een persoonsgegeven is of kan worden. Dezelfde gegevens kunnen op het ene moment niet-persoonlijk zijn en op een ander moment persoonlijk worden, bijvoorbeeld als gevolg van veranderingen in technologie of verwerkingsdoeleinden. "Persoonsgegevens" als voorwerp van rechten zijn niet stabiel genoeg om een voorwerp van eigendomsrechten te zijn. Het is daarom volgens Purtova niet goed mogelijk om vol te houden dat een gegeven eigendom kan zijn. En dat is nog los van de enorme mogelijkheden voor dupliceerbaarheid van persoonsgegevens.

De conclusie is dat we terug moeten naar de vraag waarom we gegevens willen uitsluiten van anderen. Purtova stelt dat het daarbij steeds gaat om een machtsbalans tussen personen en organen, om tekorten aan rekenschap en verantwoording. Eigendomsrechten zijn echter geen geschikt instrument om dit probleem aan te pakken. Er bestaan andere, betere instrumenten. Denk bijvoorbeeld aan de bestaande rechtsgebieden die van oudsher te maken hebben met problemen van beperkende macht en verantwoording: het staats- en bestuursrecht in de publieke sector, en het mededingings- en consumentenbeschermingsrecht in de particuliere sector. We moeten volgens Purtova nader onderzoeken hoe deze rechtsgebieden kunnen worden gebruikt om problemen in verband met de verwerking van persoonsgegevens beter aan te pakken.

Binnen het huidige regime acht Purtova het nog steeds te moeilijk om je bestaande rechten geldend te maken. In vergelijking tot 2011 heeft de AVG de situatie wel verbeterd, waarmee het recht op zeggenschap op eigen gegevens is verbreed. Maar we zijn er volgens Purtova nog niet. Een van de belangrijkste problemen is het gebrek aan handhaving. De AVG heet al "een van de meest de facto genegeerde wettelijke kaders in het kader van het EU-recht".[4] Ga je recht maar eens halen bij een toezichthouder of rechter. Deze resterende problematiek los je niet op met eigendomsrechten. De handhaving daarvan loopt steeds tegen vergelijkbare beperkingen aan. Als er behoefte bestaat om de individuele controle over persoonsgegevens te verbeteren, kan dit ook worden gedaan via een andere aanpak dan via eigendomsrecht. Purtova is van mening dat om de risico's van gegevensverwerking adequaat aan te pakken, de regelgeving zich moet gaan richten op het reguleren van digitale praktijken in plaats van op persoonsgegevens.

[4] Conclusie van advocaat-generaal Bobek van 6 oktober 2021 in de zaak C-245/20 *X,Z v* Autoriteit Persoonsgegevens (NL)

B. Eric Tjong Tjin Tai

Tjong Tjin Tai ziet vanuit de literatuur en de startnotitie dat er brede aarzeling is bij een eigendomsbenadering voor persoonsgegevens. Hij wil daar een nuance aanbrengen omdat naar zijn mening vanuit de privaatrechtelijke invalshoek wel degelijk bruikbare inspiratie te putten valt om de bescherming met technische of andere maatregelen te verbeteren.

Mensen hebben intuïtief een notie van eigendom. Daar kan je om die reden mogelijk iets van lenen. De overheid kan ook alle inbreuken op rechten niet zelf oplossen. Met het eigendomsconcept of elementen daarvan kan je personen zelf mogelijk nog meer hun kracht en macht geven. Vraag is dan alleen: hoe operationaliseer je dat?

Tjong Tjin Tai neemt daartoe een voorbeeld uit het domein van roerende zaken. Je ziet bij roerende zaken wanneer iemand ermee aan de haal gaat. Bij digitale data zie je de kopie niet meer. De houder en eigenaar blijft achter met gegevens, maar ook anderen kunnen er gebruik van maken.

Hoe kan je controle op het gebruik afdwingen? Mogelijk kan dit via techniek, maar ook dan kunnen er vragen blijven. Tjong Tjin Tai verwijst in dat verband naar een artikel uit P&I[5]. Het is en blijft enorm ondoorzichtig wat er onderwater in de apps en hun connectie platformen gebeurt.
Met cryptografische technieken zijn er wel opties. Je kan het mogelijk maken gegevens 'uit te lenen' die de gebruiker niet mag behouden, waarbij de techniek de mogelijkheid biedt om daar als uitlener controle over te houden.

Waar het om de intermediairs gaat is van belang dat we vanuit het oogpunt van transparantie ook rekening houden met het privacy risico dat er in de app op je mobiel schuilt, bijvoorbeeld wanneer iemand je ID gehacked heeft. Dat impliceert op zijn minst dat wordt nagedacht over waarborgen om dit soort situaties snel het hoofd te kunnen bieden.

Tjong Tjin Tai pleit voor opties om het individu meer macht te geven over het gebruik van (zijn) data. De AVG is met die invalshoek een knap bedacht kader. Maar gewone mensen begrijpen het niet.

Kijk bijvoorbeeld naar wat je als gebruiker in je browser doet. Daar liggen mogelijk kansen om meer te helpen. Wat als je big tech kunt verbieden met de browser (bijna) persoonlijke zaken op te halen? Je gebruikt dan eigendom als model *ter inspiratie* van wat maatregelen aanvullend in de techniek en regelgeving kunnen doen.

C. Peter Blok

Blok start het betoog vanuit drie deelvragen:

(1) Is het wenselijk om burgers meer zeggenschap te geven over eigen gegevens?

(2) Als je het wenselijk vindt: is het juridisch mogelijk, bijv door het concept van eigendom?

(3) En is het praktisch mogelijk om met technologie/organisatorisch meer zeggenschap over persoonsgegevens aan individuen te geven?

[5] Janssen H.L., Persoonlijke PIMS: Privacyfort of luchtkasteel? P&I jaargang 24, nr. 5, okt 2021 p.214-225

Wat de eerste vraag betreft: verantwoordelijken zitten niet te wachten op het uitbreiden van de zeggenschap van betrokkenen en betrokkenen in het algemeen ook niet. Het wordt de betrokkene nu al zo lastig gemaakt. Moeten we straks over van alles keuzes voorleggen aan de betrokkene (zoals de burger of consument)? Is dat de oplossing voor de problemen die we tegenkomen? Je hebt als betrokken in het algemeen niet de tijd, de kennis, of het inzicht om het allemaal goed in de gaten te houden. En bereik je met reeksen van toestemmingssituaties eigenlijk niet een situatie die de burger juist (meestal) niet wil?

Blok benadrukt daarbij dat in de relatie burger-overheid het bieden van veel keuze-opties nog minder voorstelbaar is. De overheid heeft voor bepaalde taken gegevens nodig, dat regel je met algemene regels als wetgever en niet met individuele toestemmingen. Individuele zelfbeschikking kan hier niet voorop staan.

Wat de tweede vraag over de juridische mogelijkheden betreft, benadrukt Blok dat de AVG al veel bepaalt. De Nederlandse overheid heeft zeer beperkte ruimte om daar aanvullend dingen in te ondernemen. Als je daarnaast zelf een eigendom voor persoonsgegevens gaat scheppen, dan ontstaan er spanningen met de AVG. Dat zou je dus in EU-verband moeten doen.

Meer zeggenschap is dus niet wenselijk en ook niet goed mogelijk binnen het kader van de AVG. Daar komt bij dat eigendom van gegevens niet het beste concept is om zeggenschap te realiseren. Het concept van eigendom kan eventueel wel ter inspiratie dienen, maar Blok heeft ook daar twijfels bij. In het Nederlands BW zijn het eigendomsrecht en de daaruit voortvloeiende beschikkingsmacht over een goed vervreemdbaar. Zeggenschap over persoonsgegevens is echter naar zijn aard onvervreemdbaar. Het is ondenkbaar en onwenselijk dat een betrokkene de zeggenschap over zijn persoonsgegevens aan een ander kan overdragen en vervolgens dus niets meer te zeggen heeft over zijn of haar gegevens. Het idee van eigendom van gegevens als concept voor het realiseren van meer zeggenschap van de betrokkene kan daardoor alleen maar meer verwarring wekken. Een beter concept dan het eigendomsrecht is het persoonlijkheidsrecht (het recht om het rust gelaten te worden en gevrijwaard te blijven van gegevensverwerkingen). Ook dat werkt *erga omnes* en verschaft zeggenschap over gegevensverwerkingen, maar is niet vervreemdbaar.

Tot slot de praktische derde vraag. Blok staat daar niet als technisch informaticus maar als jurist bij stil. Hij meent dat er juist in de operationalisering van de AVG nog veel winst is te behalen. Er is een wereld te winnen bij het beter naleven van verplichtingen, de inrichting van werkprocessen en het beter voorzien in transparantie.

De meeste voorstellen die worden gedaan om de zeggenschap van betrokkenen te vergroten, gaan over het bieden van inzage- en correctiemogelijkheden. De vraag is of die mogelijkheden de burger het gevoel geven dat deze daardoor meer controle heeft over de eigen gegevens. De ervaring leert dat meer transparantie meestal leidt tot meer besef van het gebrek aan zeggenschap binnen de rechtsrelatie.

Transparantie blijft echter wel een goed idee, maar niet zozeer voor de controle en zeggenschap over de eigen gegevens. Wel als middel om de legitimiteit van een gegevensverwerking te kunnen controleren, en daardoor duidelijkheid te verschaffen over, en te kunnen controleren wat er met gegevens gebeurt en of deze legitiem worden gebruikt. Vooral de samenleving als geheel heeft daardoor belang bij transparantie. Maar zie dat laatste niet te veel als regie op eigen data.

D. Peter Olsthoorn

Olsthoorn benadert het vraagstuk vanuit de mens, de betrokkene. En dan verschijnt volgens hem de AVG als moeilijk te doorgronden 'jurdisch gedrocht en verdienmodel van de advocatuur'. Wat kan en wil de burger of betrokkene in al zijn verscheidenheid, en waar hebben we het dan over?

Olsthoorn vraagt aandacht voor datagebruik in de markt. Kernwoord daar is profilering. Daar hebben individuen geen enkel inzicht in, en overzicht over, terwijl ze zelf het onderwerp vormen. Dit inzicht wel bieden, plus een vorm van technisch eigen beheer van persoonsgegevens stuit vooralsnog op praktische bezwaren. De meeste mensen kunnen nog net hun eigen bankrekeninggegevens bijhouden, maar een databoekhouding bijhouden dreigt complex te worden. Nederlandse initiatieven om deze drempel te verlagen, bijvoorbeeld vanuit Radboud Universiteit/SIDN (Irma), KPN, Rabobank, Volksbank/Schluss en Ockto, moeten zich nog in de praktijk bewijzen met grootschalig gebruik.

Wat Olsthoorn wel ziet is dat in EU verband, met de *Digital Market Act* en de voorstellen voor de *Data Governance Act*, in combinatie met recente aangekondigde *eIDAS-directive* aanpassing er, in aanvulling op de AVG, interessante raamwerken ontstaan waarin het verkeer met marktpartijen en datadienstverleners aanvullende regulering krijgt. Dat wordt de speelruimte waarin de Nederlandse overheid zou moeten acteren. Daarbinnen zullen ook nationale overheden de zeggenschap van de betrokkenen moeten zoeken.

Olsthoorn illustreert dit met intermediairs die gegevensverwerkingen voor personen doen. Daar ziet het voorstel van de *Data Governance Act* op. Genoemde bedrijven staan daarvoor in de rij. De EU tuigt nu een aantal kaders op.

Olsthoorn geeft aan dat eigendom over persoonsgegevens weliswaar juridisch onhaalbaar is, maar dat er wel juridische bescherming van persoonlijk en coöperatief beheer van persoonsgegevens mogelijk moet zijn. Ook dit is een Europese kwestie., zowel voor nationale overheden als bedrijven. Waarbij de vraag naar voren treedt in hoeverre gebruikers in de relatie tot overheden verregaand eigen beheer nodig hebben, anders dan om de AVG-rechten uit te oefenen De werkelijke 'strijd' voor eigen beheer zal ontbranden in markten voor big data, bijvoorbeeld in medisch onderzoek, verkeer en *smart cities*.

Ook kan omkering van de huidige markt ontstaan als de dominantie verschuift van bedrijven over persoonsgegevens naar individuen en collectieven die zelf de mate van profilering en toepassing van algoritmes over eigen en collectief gedrag ter hand nemen Rond zeggenschap en controle speelt Olsthoorn nog met zulke vragen. Maar hij ziet die hij niet langs een eigendomsbenadering opgelost.

E. Lokke Moerel

Moerel geeft aan dat de AVG vooral uitgaat van het informeren van het individu over gegevensverwerkingen, en dat het zwaartepunt voor de handhaving en uitoefening van rechten vooral bij de betrokkene ligt. Als we vinden dat dit systeem in het huidige tijdsgewricht van massale gegevensverwerkingen nu al tot problemen en lacunes leidt, dan gaat het bieden van nog meer inzage en nog meer 'empowerment' van het individu niet helpen dit vraagstuk op te lossen.

Verder beschouwen burgers hun persoonsgegevens nu al als 'van zichzelf', het officieel toekennen van eigendom (vanuit het perspectief dat burgers er dan beter op zullen passen) zal niet tot wezenlijk tot een gedragsverandering leiden, omdat burgers gewoon niet in staat zijn deze controle daadwerkelijk uit te oefenen. Toekenning van eigendom zal de verwachtingen alleen maar opschroeven, en tot verdergaande frustratie en onmacht bij burgers leiden.

Als voorbeeld hoe moeilijk het is om burgers daadwerkelijk 'controle' te geven, noemt Moerel het vereiste dat voorafgaande toestemming is vereist voor het plaatsen van *tracking cookies* waarmee het surfgedrag van individuen in kaart wordt gebracht voor persoonsgerichte advertentiedoeleinden (*micro-targeting*). Iedereen is het erover eens dat de wijze waarop organisaties bij bezoek van hun website of app toestemming vragen via *cookie statements* voor het plaatsen van *tracking cookies* voor *micro-targeting*, het de gebruikers te lastig maakt om hun toestemming te weigeren. Om te voorkomen dat bedrijven in feite toestemming afdwingen via de cookiestatements, is het inmiddels bij een aantal browsers mogelijk om via de browserinstellingen plaatsing van zogenaamde *third-party cookies* waarmee het surfgedrag van gebruikers kan worden gevolgd te weigeren, en waarbij zogenaamde *first-party cookies* in tijd sterk in levensduur beperkt worden (nog slechts 1 dag). Ook Google heeft aangegeven in 2022 een dergelijke blokkade in Chrome in te bouwen. De verwachting is (of beter: was) dat hiermee de bescherming tegen ongewenst hergebruik van persoonlijk surfgedrag sterk zou worden verbeterd.

Het gevolg van deze aanpassing in de browsers is dat de sitebeheerders en marketeers van bedrijven veel minder data gaan krijgen en advertenties niet meer kunnen richten. Grote bedrijven zijn daarom nu al aan het anticiperen op wat het 'cookieloos' tijdperk gaat worden. Tech bedrijven ontwikkelen daarom nu al opties om data te koppelen aan het ID-nummer van je mobile device (zoals de mobiele telefoon), hetgeen potentieel zelfs privacy gevoeliger is dan dat het ip-adres van de gebruiker als *identifier* wordt gebruikt.

Adverteerders kunnen het zich simpelweg niet permitteren 80% van hun data te missen. Dus er wordt naarstig gezocht naar alternatieven. Daarbij kan het zijn dat er andere vormen van *targeting* ontstaan, die minder problematisch zijn zoals contextuele *targeting* (waarbij advertenties niet worden afgestemd op de individuele gebruiker, maar op de context van de inhoud van de website). Echter we zien ook dat er alternatieven worden opgezet om de *brower blocking* te omzeilen, bijvoorbeeld door de data niet door te leiden naar de adverteerder (*third party*) maar eerst naar de website zelf, waardoor het verkeer first party lijkt (zogenaamde *server-side tagging).* .

Al dit soort ontwikkelingen demonstreren hoe ondoorzichtig de *data economy* is. Veel pogingen tot technische of juridische controle blijken uiteindelijk dweilen met de kraan open. Of we het nu over *consent* (individuele toestemming) hebben, of zeggenschap over de lijn van het privaatrecht via eigendom, het is vrijwel een illusie om te denken dat het geven van meer controle aan het individu gaat helpen tegen gegevensverwerkingen met, en via, *Big Tech*. Daarbij moet bovendien niet

vergeten worden dat het makkelijker is eigendom weg te contracteren (via contractuele voorwaarden van grote bedrijven), dan het weg contracteren van fundamentele rechten.

Moerel ziet in deze context meer als oplossing dat je als overheid moet nadenken over het actief begrenzen van wat mag en wat niet mag. Geef aan wat bedrijven niet meer mogen vragen. Waar is bijvoorbeeld bij het verwerken van gegevens geen sprake meer van een 'gerechtvaardigd belang' (waarvoor ook geen toestemming mag worden gevraagd). Als iets misleidende reclame wordt geacht, mag je dat ook niet oplossen door hier dan toestemming voor te vragen.

Trek een streep, en geef vooral aan wat er *NIET* mag. En laat ruimte voor de innovatie die 'in het publiek belang is ' maar zet ook daar ter bescherming de juiste grenzen eromheen. Dat speelt ook bij de eID-middelen. Hier dient de overheid controle te houden over onze digitale paspoorten en het gebruikt daarvan.

Wat betreft profiling stelt Moerel overigens niet dat er een algeheel verbod op profiling overwogen zou moeten worden. Dat is veel te breed. Het gaat haar om een meer specifieke beperking gericht op profiling voor '*personalised advertising*' . De bestaande incentive om op deze wijze data te verzamelen om daar andere dingen mee te doen, moet gaan kantelen. *Big Tech* hebben die vorm van *cross-site* profilering al niet meer nodig, die zijn zelf groot genoeg en hebben geen data van derden meer nodig. De privacy regels zijn dan juist een competitief voordeel, maar komen niet ten goede aan de gebruikers.

Moerel geeft aan dat er voor het gegevensverkeer tussen overheden altijd een wettelijke grondslag nodig is. Mogelijk kan je op een paar vlakken daar ook nog iets met toestemming van de burger/betrokkene, maar meestal is de machtsverhouding al ongelijk, en is het gebruik van persoonsgegevens voor de taak al wettelijk geregeld. Het enige dat daar aanvullend bij kan helpen, is transparantie: waar zitten je data en hoe worden ze verwerkt? Die informatie is nodig om daarover zo nodig het publiek debat te kunnen voeren. Het belang van transparantie is dus niet zozeer gelegen in het mogelijk maken van regie over gegevens voor het individu, maar wel door het benoemen van knelpunten door professionals en andere partijen die casuïstiek oprakelen. Het systeem leert daardoor. Eventuele verkeert uitgelegde rechtsgronden kunnen aangevochten worden door de consumentenbond, privacy organisaties etc. Het nut van transparantie binnen het debat is daarom vooral gelegen in de verantwoording voor de legitimiteit van het gebruik van data door de overheid.

Vooral vanuit de kant van aan overheid dient meer te worden gewerkt aan transparantie ten behoeve van de legitimiteit. Het zou bijvoorbeeld goed zijn om een 'mijn overheid.nl' dasboard te bieden, waar de burger kan zien in welke systemen mijn gegevens zitten, voor welke doeleinden. met je data gebeurt. De overheid zou ook een register moeten hebben met alle algoritmes die het gebruikt alsook de werking van de algoritmes open moeten stellen voor publieke controle. Een inspirerend voorbeeld hiervoor is dat Twitter de werking van zijn algoritme gaat openen en laat zien hoe het werkt en zich openstelt voor verbeteringen.

Moerel benadrukt dat het gebruik van persoonsgegevens in de publieke sfeer een heel ander ecosystemen is dan het ontsluiten van persoonlijke data in private context. De maatregelen binnen die twee ecosystemen moet je gescheiden van elkaar wegen. De overheid moet je vooral *'accountable'* houden. Voor hergebruik van persoonsgegevens in private sfeer is het meer een kwestie van de AGV goed interpreteren, en dan aangeven wat onder voorwaarden kan, en niet kan.

IV. Nadere overwegingen en suggesties voor beleid

Hierna volgen een aantal suggesties voor (toekomstig) beleid. De deelnemers gaven daarbij aan dat de vraagstelling en suggesties in de toekomst een bredere bespreking verdienen, in elk geval met inbreng van EZK wegens de relaties met marktordening, maar ook J&V.

(1) <u>Stel duidelijke grenzen wat mag en wat niet mag</u>

In het verlengde van het betoog van Moerel onderkennen de deelnemers dat aangeven wat NIET mag, rode strepen trekken, nodig zal zijn. De deelnemers onderkennen dat het varen op het vragen toestemmingen van de consument aan een onevenwichtigheid voorbijgaat. Grote bedrijven grijpen elke mogelijkheid aan om twijfel te zaaien of een toestemming wel of niet geldig is. Er wordt nu al met legers advocaten geprocedeerd over 'vinkjes' waarmee toestemming kan worden gegeven. Tot aan het EU-hof toe. Wat dat betreft is er bij de deelnemers meer vertrouwen in handhaving van een enkele duidelijke regel, zoals: 'je mag voor gepersonaliseerde advertenties niet profileren'. Dat is veel effectiever en beter afdwingbaar.

(2) <u>Collectieve actie</u>

De deelnemers geven aan dat een betere uitwerking van, en onderzoek naar de mogelijkheden voor collectieve acties belangrijk is. Hoe maak je het bijvoorbeeld makkelijker om via handhaving langs privaatrechtelijke weg samen een claim in te dienen tegen partijen die gegevens verwerken en daarbij anderen benadelen? Het gaat dan bijvoorbeeld om een beroep op de civiele rechter door maatschappelijke organisaties die een rechterlijke uitspraak benutten om de toelaatbaarheid van gegevensverwerkingen aan te scherpen. De vraagstelling zou ook kunnen zijn wat een claimorganisatie nodig heeft om zich effectief te kunnen ontplooien? Wat zijn de hobbels? Kan bijvoorbeeld bij handhaving langs de privaatrechtelijke weg overwogen worden om te werken met een forfaitair bedrag per inbreuk per individu wat kan oplopen bij groepsacties en kan variëren al naar gelang de ernst van de overtreding? Van dit soort claims kunnen grote partijen zenuwachtig worden. Daarnaast wordt wellicht ook voorkomen dat de claimende partij niet op voorhand het bos van bonnetjes en diffuse onderbouwing wordt ingestuurd.

In dit verband past ook de constatering van de deelnemers dat individuele acties bijna niet mogelijk zijn, en eigenlijk niet werken. Dat er opties voor collectieve actie zijn, en schade valt te claimen, is in de AVG al opgenomen. Er lopen op dit moment al meer dan 40 acties. En zelfs als de vergoeding maar 500 euro per individu is, dan telt dat bij grotere collectieven wel op. Dus zulke collectieve acties gaan in de toekomst verschil maken: schadevergoedingen kunnen zorgen voor betere handhaving van de AVG. In dat verband wordt ook gewezen op het proefschrift van Tim Walree uit 2021 over schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens, en de opmerkingen over de transactiekosten die daarmee gemoeid zijn bij het claimen daarvan.

(3) Bedrijven die elkaar te maat nemen

Volgens de deelnemers is het waardevol om mogelijkheden te onderzoeken hoe in het verlengde van het preadvies van Moerel en Prins[6], bedrijven elkaar op naleving van de privacyregels kunnen aanspreken, zoals bijvoorbeeld bij misleidende reclame het geval is. Laat bedrijven in dit verband elkaar aan de concurrentievoorwaarden houden, aan het gelijke speelveld, en bezie hoe die *checks and balances* te versterken zijn. Dit is temeer een interessante lijn, omdat bij de veelheid aan

[6] E.M.L. Moerel en J.E.J. Prins 'Privacy voor de homo digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things' in: Homo digitalis. Preadviezen (Handelingen Nederlandse Juristen Vereniging deel 2016-I), Deventer: Wolters Kluwer 2016/2, p.1-136

maatschappelijke praktijken toezicht door de overheid alleen, nooit kan voldoen. Bedrijven die elkaar aanspreken op normen kan dit verbeteren. Denk aan een mogelijkheid voor bedrijven om andere bedrijven ter verantwoording te roepen rond concurrentieverstoring door onrechtmatige verwerking van persoonsgegevens (zoals in Duitsland nu al mogelijk is).

(4) <u>Lering trekken uit bestaande sectorale oplossingen</u>

Binnen diverse sectoren zijn initiatieven ontplooid om betrokkenen meer zeggenschap te geven over de eigen gegevens. Mogelijk zijn onderdelen hiervan te hergebruiken binnen andere sectoren. Neem het stelsel van MedMij en de Persoonlijke gezondsheidsomgeving (PGO) binnen de gezondheidszorg. Ondanks dat het hier een sterk privaat stelsel betreft, is het voor de overheid leerzaam om te beoordelen welke behoeften daar zijn ingevuld, en hoe de zeggenschap over de gegevens daar in de praktijk verloopt. Een vergelijking van opties met sectoren zoals de gezondheidszorg of onderwijs is ook nuttig omdat deze sectoren een sterk hybride karakter hebben: ze zijn niet alleen privaat maar vooral ook sterk publiekrechtelijk gereguleerd. Je hebt daardoor als betrokkene/consument minder vrijheid om zeggenschap over de eigen gegevens te krijgen.

(5) Kaderstelling door de overheid bij delen van gegevens

Waar je bij regie op gegevens denkt aan het met toestemming delen van persoonsgegevens door publieke instanties aan private partijen, is een juridische benadering met kaderstelling belangrijk. In Europees verband de eerste stappen gezet (*zoals de Data Governance Act*). Maar het is belangrijk dat nu al stappen worden gezet hoe dit op nationaal niveau optimaal kan worden geoperationaliseerd. Is het bijvoorbeeld een optie dat er een instituut wordt ingesteld – zoals het CBS - dat bij activiteiten rond het delen van gegevens door de overheid een centrale rol gaat innemen?

Als de overheid gevalideerde overheidsgegevens gaat delen met derde partijen, heeft de overheid ook echt iets te bieden. In dat geval ligt het voor de hand dat de overheid namens ons allemaal eisen stelt aan de private partijen en intermediairs om de zeggenschap van het individu te bewaken. Laat de overheid nu alvast de opzet en voorwaarden uitdenken waaraan private partijen moeten voldoen, zowel vanuit de contractuele invalshoek als vanuit een privacy by design opzet. Daarbij kan de overheid ook restrictief zijn. Wanneer is delen in het kader van het collectieve belang en wanneer niet? Het blijft daarnaast prikkelen om na te denken over situaties waarin de overheid persoonsgegevens vooral in bruikleen lijkt te hebben, waar alleen iets mee mag gebeuren als de burger daarmee instemt. Deze benadering kan wellicht in specifieke situaties iets toevoegen.

(6) Controle door techniek

Het blijft afsluitend een uitdaging om controle in technische systemen concreet te maken. Vooral dat je het zelf kan doen (zoals wissen van data) in plaats van vragen aan de partij die de gegevens verwerkt om het te doen. Er kan in het verlengde daarvan meer aandacht worden besteed aan de vraag welke opties nog meer te bedenken zijn en hoe die te implementeren zijn. Dat is bijvoorbeeld het geval bij Solid (solidproject.org) waar een systeem in ontwikkeling is waarbij eigen beheer en zeggenschap via de browser werkt, data kan worden teruggetrokken, of van het één naar het andere netwerk kan worden overgebracht. Dat switchen en wissen moet technisch beter kunnen. Het AVG-concept van dataportabiliteit zou daarbij als inspiratie kunnen dienen, maar ook wachtwoordmanagers, *coockieblockers*, of *Privacy Enhancing Technologies* (PET).

Bijlage 1 Personalia deelnemers Expertpanel

Voorzitter: mr. dr. Theo Hooghiemstra, directeur Hooghiemstra & Partners

Secretaris: mr. Huib Gardeniers, directeur Net2Legal Consultants

Leden:

- prof dr. mr. Peter Blok, hoogleraar octrooirecht en privacy (CIER Utrecht), raadsheer
- prof. dr. mr. Lokke Moerel, hoogleraar global ICT law, Tilburg University; Senior of Counsel Morrison & Foerster (Brussel)
- prof. dr. Nadya Purtova hoogleraar Law, Innovation and Technology, Utrecht University
- dr. Peter Oltshoorn – (recent gepromoveerd op het onderwerp 'regie op gegevens')
- prof dr. mr. Eric Tjong Tjin Tai - Hoogleraar privaatrecht aan Tilburg University

Bijlage 2 Startnotitie eigenaarschap persoonsgegevens[7]

Ten behoeve van de bijeenkomst is een startnotitie opgesteld waarin de aanleiding tot de bijeenkomst is geschetst, inclusief een beknopte weergave van de recente parlementaire voorgeschiedenis. Daarnaast geeft de notie een eerste analyse voor de behandeling van het vraagstuk. Deze analyse en inzichten uit de startnotitie zijn gedurende de oordeelsvorming door het expertpanel meegenomen en meegewogen (Voor de volledige strekking van en inleiding in de startnotitie, zie de bijlage bij deze rapportage).
Een constatering uit die startnotitie, waarop het expertpanel heeft voortgebouwd, is deze:

> *"bij gegevensverwerking (van persoonsgegevens) is er altijd een onderliggende rechtsrelatie waar de gegevensverwerking op gebaseerd is. Daarbij kan gesteld worden dat de mate en vorm van zeggenschap over de eigen persoonsgegevens direct verbonden is met mogelijkheid om wel of geen zeggenschap uit te kunnen oefenen binnen de onderliggende (rechts)relatie."*

Als vertrekpunt voor de bijeenkomst zijn vooraf in de startnotitie twee vragen geformuleerd:

(A) zijn er bestaande mogelijkheden om de burger/consument meer zeggenschap over de eigen gegevens te geven, bijvoorbeeld door het beter benutten van bestaande mogelijkheden in de huidige dataprotectie wet- en regelgeving, of vanuit praktische oplossingen, zoals technologische oplossingen waarbij de burger zelf de mogelijkheid krijgt om eigen gegevens te delen met derden?

(B) zijn er vanuit een wettelijk eigendomsregime van persoonsgegevens nieuwe mogelijkheden mogelijk (of al voorhanden) om de zeggenschap over de eigen gegevens te verbeteren?

In de startnotie komt nadrukkelijk de relatie tussen de overheid en de burger aan de orde. Tijdens de expert bijeenkomst is expliciet ook aandacht besteed aan de relatie tussen individuele personen en bedrijven.

[7] De startnotitie Zeggenschap, eigenaarschap en persoonsgegevens uit oktober 2021

Bijlage 3 Literatuur

Blok, P. (2002), Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht, diss. Tilburg.

Dommering, E. (2012), 'Boekbespreking van Property Rights in Personal Data: A European Perspective, N. Purtova', Maandblad voor Vermogensrecht 2012, nr 1, p. 22-26.

Hooghiemstra, T. F. M. (2018), Informationele zelfbeschikking in de zorg, diss. Tilburg, SDU-uitgevers.

Koops, B.J. (2014), 'The Trouble with European Data Protection Law', International Data Privacy Law, Doi: 10.1093/ IDPL 4(4) 257

Moerel, E.M.L. en Prins J.E.J. (2016), 'Privacy voor de homo digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things' in: Homo digitalis. Preadviezen (Handelingen Nederlandse Juristen-Vereniging deel 2016-I), Deventer: Wolters Kluwer 2016/2, p.1-136

Moerel L. & Lyon C. (2020), 'Commoditization of Data is the Problem, Not the Solution – Why Placing a Price Tag on Personal Information May Harm Rather Than Protect Consumer Privacy', Future of Privacy Forum, 4 juni 2020

Olsthoorn, P. J.C. (2021), 'Baas over eigen data: Zelfbeschikking in bescherming van persoonsgegevens" diss. VU Amsterdam, Boom Juridisch, Den Haag

Purtova, N.N. (2011), Property Rights in Personal Data: A European Perspective. diss. Tilburg, Kluwer Law International.

Purtova, N.N. (2017), 'Do property rights in personal data make sense after the Big Data turn? Individual control and transparency', 10(2) Journal of Law and Economic Regulation November 2017, p.64-78 Tilburg Law School Research Paper No. 2017/21

Tjong Tjin Tai, T.F.E (2016), 'Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving' in: Homo digitalis. Preadviezen (Handelingen Nederlandse Juristen Vereniging deel 2016-I), Deventer: Wolters Kluwer 2016/2, p.241-306

Janssen H.L. (2021), Persoonlijke PIMS: Privacyfort of luchtkasteel? P&I jaargang 24, nr. 5, okt 2021 p.214-225

Walree, T.F. (2021), 'Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens' diss. Radboud University, Wolters Kluwer

EU Fundamental Rights Agency (FRA) Getting the future right: Artificial Intelligence and Fundamental Rights (FRA 2020) https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

Beleidsdocumenten

Ministerie van BZK (2017), 'Greenpaper Regie op gegevens? Durf te Doen!', Regie op Gegevens, Den Haag, 26 september 2017

Ministerie van BZK , 'Regie op Gegevens', www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/gegevens/regie-op-gegevens/ [Gezien 19 maart 2020]

Ministerie van BZK, 'Onderzoek naar digitale identificatie en verificatie', DigitaleOverheid.nl, www.digitaleoverheid.nl/actielijn/onderzoek-naar-digitale-identificatie-en-verificatie/ [Gezien 5 juli 2020]