Het recht op bescherming van persoonsgegevens is onbetaalbaar

Custers, B.H.M.; Malgieri, G.

Het recht op bescherming van persoonsgegevens is onbetaalbaar

Bart Custers & Gianclaudio Malgieri[1]

Veel gratis online dienstverleners, zoals zoekmachines en sociale media, zijn gebaseerd op de handel in persoonsgegevens van gebruikers. In de kern zijn ze gratis omdat gebruikers 'betalen met hun gegevens'. Deze bijdrage stelt dat deze bedrijfsmodellen, waarin persoonsgegevens worden gezien als valuta of als een verhandelbaar product, problematisch zijn in het licht van het recht op bescherming van persoonsgegevens. Immers, in artikel 8 van het Handvest van de grondrechten van de EU is het recht op persoonsgegevens verheven tot een onvervreemdbaar grondrecht en grondrechten kunnen niet worden verhandeld.

1. Inleiding

Online zoekmachines, sociale media, en ander onlinediensten zijn vaak gratis omdat ze persoonsgegevens van gebruikers verzamelen en verwerken. De gegevens worden verder geanalyseerd en opgewerkt of doorverkocht. In feite betalen gebruikers voor de gratis diensten met hun gegevens in plaats van met geld.[2] Hun persoonsgegevens vertegenwoordigen een bepaalde waarde, al wordt vrijwel nooit expliciet gemaakt hoeveel de gegevens waard zijn voor de betreffende bedrijven.[3] Het betalen met persoonsgegevens komt neer op het betalen met (informationele) privacy.

In deze bijdrage stellen we dat bedrijfsmodellen waarin mensen betalen met hun persoonsgegevens (en meer in het algemeen met het inleveren van privacy) problematisch zijn onder EU-gegevensbeschermingswetgeving. Zowel in het Handvest van de grondrechten van de EU ('Handvest') als in de Algemene verordening gegevensbescherming (AVG) zijn de rechten op gegevensbescherming onvervreemdbaar, hetgeen aan eigendom in de weg staat. In feite kunnen mensen niet met hun persoonsgegevens betalen, omdat ze er geen eigenaar van zijn. En je kunt iets waarvan je geen eigenaar bent niet weggeven.

Omdat mensen wel rechten hebben met betrekking tot hun persoonsgegevens, kan worden geredeneerd dat de 'betaling' weliswaar geen eigendomsoverdracht inhoudt, maar dan toch het verlenen van een recht tot het verzamelen en verwerken van persoonsgegevens.[4] Echter, ook vanuit dit perspectief behouden mensen hun onvervreemdbare rechten om de verwerking van de gegevens tegen te houden of te beperken. Omdat de juridische basis voor het verwerken van persoonsgegevens vaak toestemming is, kunnen mensen te allen tijde en naar willekeur hun toestemming intrekken en daarmee hun 'betaling', ook nadat ze gebruik hebben gemaakt van de onlinediensten. Dit zorgt voor aanzienlijke rechtsonzekerheid voor actoren in de data-economie.

Om misverstanden te voorkomen: in deze bijdrage pleiten we niet voor of tegen eigendom van persoonsgegevens. Hierover is veel discussie, met goede argumenten aan beide kanten. Hier betogen we slechts dat *als* de wetgever (zoals in de EU) ervoor kiest om het recht op gegevensbescherming tot een onvervreemdbaar grondrecht te verheffen, *dan* kunnen eigendom van persoonsgegevens en een data-economie gebaseerd op handel van persoonsgegevens problematisch zijn. We concluderen dat het EU-grondrecht op bescherming van persoonsgegevens onverenigbaar is met de handel in persoonsgegevens. Op zichzelf is dat geen probleem, maar het wordt wel een probleem nu we onze data-economie bouwen op de handel in persoonsgegevens.

Deze bijdrage is als volgt gestructureerd. Paragraaf 2 gaat in op de werking van bedrijfsmodellen waarin mensen met persoonsgegevens betalen en legt uit waarom in de EU geen eigendom van persoonsgegevens bestaat (in tegenstelling tot bijvoorbeeld de Verenigde Staten en China). Paragraaf 3 bespreekt de onvervreemdbaarheid van persoonsgegevens en het recht op bescherming van persoonsgegevens vanuit grondrechtenperspectief (primaire wetgeving) onder het Handvest. Paragraaf 4 bespreekt de onvervreemdbaarheid van persoonsgegevens en rechten van data-subjecten vanuit het

perspectief van de AVG (secundaire wetgeving). Paragraaf 5 rondt af met conclusies.

2. Betalen met je gegevens

2.1. Bedrijfsmodellen

Er zijn grosso modo twee scenario's waarop bedrijfsmodellen met handel in persoonsgegevens zijn gebaseerd. Het eerste scenario is dat een bedrijf persoonsgegevens vraagt aan een gebruiker in ruil voor geld of een product of dienst. Dit noemen we primaire handel in persoonsgegevens. Het tweede scenario is dat een bedrijf persoonsgegevens uitwisselt met een derde (een ander bedrijf) in ruil voor geld. Dit noemen we secundaire handel in persoonsgegevens.[5]

Het eerste scenario is duidelijk voor mensen. Veel mensen weten wel dat gratis online diensten zoals zoekmachines (Google, Yahoo, etc.) en sociale media (Facebook, X, LinkedIn, etc.) zijn gebaseerd op bedrijfsmodellen die winst genereren via advertenties die gebruikers online te zien krijgen. Steeds meer mensen weten ook dat winst wordt gemaakt met handel in gebruikersgegevens. Die gegevens worden dan weer gebruikt voor advertenties door derden, op dezelfde of andere websites, maar ook voor andere doelen, zoals risicoprofilering, voorspellingen en geautomatiseerde besluitvorming. Hoe dit achter de schermen werkt is onduidelijk voor veel mensen.[6] Hoewel mensen zich zorgen maken over hun privacy, blijven ze echter diensten gebruiken die hun persoonsgegevens verzamelen en verwerken (de zogeheten *privacy paradox*).[7]

Hoewel mensen zich zorgen maken over hun privacy, blijven ze diensten gebruiken die hun persoonsgegevens verzamelen en verwerken

Het tweede scenario komt pas in beeld nadat mensen hun persoonsgegevens hebben afgestaan. Bedrijven kunnen op verschillende manieren winst genereren uit grote datasets. De belangrijkste strategieën zijn het verkopen van (kopieën van) de gegevens, het leasen van gegevens en verdere kennis uit de data abstraheren. Het verkopen van gegevens is het meest eenvoudig. Datasets met ruwe data worden tegen zeer lage prijzen doorverkocht.[8] Omdat data eenvoudig kunnen worden gekopieerd, kan dezelfde dataset meerdere keren worden verkocht aan verschillende kopers. Om meer munt te slaan uit de gegevens, is het vaak interessant om datasets te leasen, bijvoorbeeld via een abonnement. In plaats van een eenmalige transactie levert dit maandelijkse betalingen op. Aanbieders moeten de data dan wel actueel houden en bijvoorbeeld een helpdesk inrichten. Nog meer waarde kan uit de gegevens worden gehaald door kennis te destilleren uit de datasets, bijvoorbeeld middels datamining, machine learning en AI.[9] De nieuwe inzichten, bijvoorbeeld trends, profielen en andere patronen, kunnen dan weer worden gebruikt voor het personaliseren van de dienstverlening of het identificeren van nieuwe klantgroepen.

2.2. Eigendom van persoonsgegevens

De discussie over eigendom van persoonsgegevens bestaat al geruime tijd. Persoonsgegevens vertegenwoordigen in toenemende mate waarde en worden in de praktijk als handelswaar gezien en gebruikt. Maar klassieke privaatrechtelijke kaders sluiten niet altijd goed aan bij deze praktijk. Goederenrechtelijke termen als eigendom, bezit, gebruik, overdracht en onrechtmatige daad komen in een ander licht te staan wanneer het persoonsgegevens betreft, die immers niet-stoffelijk zijn en eenvoudig overdraagbaar en kopieerbaar.

Een van de eersten die in Nederland problemen rondom eigendom van persoonsgegevens bespreekt, is Colette Cuijpers in haar proefschrift uit 2004.[10] Zij stelt dat eigendom van persoonsgegevens mogelijk is, maar dat daarvoor het Burgerlijk Wetboek zou moeten worden aangepast.[11] Om beter uitdrukking te geven aan de dematerialisering

Auteurs

1. Prof. mr. dr. ir. B.H.M. Custers is hoogleraar Law and Data Science aan de Universiteit Leiden. Dr. G. Malgieri is universitair hoofddocent aan de Universiteit Leiden. Deze bijdrage is een bewerking van een eerder verschenen artikel: B.H.M Custers & G. Malgieri, 'Priceless data: why the EU fundamental right to data protection makes data ownership unsustainable', *Computer Law & Security Review* 2022, vol. 45, p. 1-13, doi.org/10.1016/j.clsr.2022.105683.

Noten

2. Ook recente EU-wetgeving erkent dat het gebruik van persoonsgegevens feitelijk de tegenprestatie is voor toegang tot digitale content en onlinediensten, zie bijvoorbeeld art. 3 lid 1 EU-Richtlijn 2019/770.

3. G. Malgieri & B. Custers, 'Pricing privacy: the right to know the value of your personal data', *Computer Law & Security Review* 2018, vol. 34, nr. 2, p. 289-303.

4. Zie ook G. Malgieri & V. Janeček, 'Data Extra Commercium', in: S. Lohsse, R. Schulze & D. Staudenmayer (eds.), *Data as Counter-Performance – Contract Law 2.0?*, Hart Publishing/Nomos, 2020.

5. In economische termen gaat het hier respectievelijk om business-to-consumer (B2C) en business-to-business (B2B).

6. B. Custers, S. Van der Hof & B. Schermer, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies', *Policy & Internet* 2014, vol. 6, nr.. 3, p. 268-295.

7. P.A. Norberg, D.R. Horne & D.A. Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors', *Journal of Consumer Affairs* 2007, vol. 41, nr. 1, p. 100-126.

8. E. Steel, C. Locke, E. Cadman & B. Freese, 'How much is your personal data worth?', *Financial Times* 12 juni 2013, ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz2z2agBB6R; zie ook E. Steele, 'Financial worth of data comes in at under a penny a piece', *Financial Times* 12 juni 2013.

9. T. Calders, B.H.M. Custers, 'What is data mining and how does it work?', in: B.H.M. Custers, T. Calders, B. Schermer & T. Zarsky (red.), *Discrimination and Privacy in the Information Society*, nr. 3 Heidelberg: Springer 2013.

10. C.M.K.C. Cuijpers, *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn*, Sdu, 2004.

11. In het bijzonder art. 3:2 BW dat zaken definieert als voor menselijke beheersing vatbare stoffelijke objecten. Cuijpers geeft terecht aan dat de stoffelijkheid ook bij elektriciteit en software in de praktijk geen beperking is.

© Shutterstock

van het eigendomsbegrip stelt zij een wijziging van het Burgerlijk Wetboek voor waarbij het eigendomsbegrip ook (persoons)gegevens omvat. In zijn uitgebreide preadvies van 2016 beschrijft Eric Tjong Tjin Tai gedetailleerd in hoeverre privaatrechtelijke begrippen met betrekking tot bezit en gebruik kunnen worden toegepast op digitale informatie.[12] Hij stelt dat eigendom van informatie of gegevens weliswaar niet nodig is, maar wel dat een eigendomsrechtelijke benadering, in termen van bevoegdheden en rechten, van gedigitaliseerde informatie nodig is.

Eigendom en bezit zijn overdraagbaar, terwijl grondrechten onvervreemdbaar zijn

In de EU bestaat geen eigendom van persoonsgegevens.[13] Personen en bedrijven kunnen wel eigenaar zijn van ICT-hardware waarop persoonsgegevens staan, maar niet van de persoonsgegevens zelf. Voor de duidelijkheid: eigendom van gegevens bestaat wel, maar niet eigendom van *persoonsgegevens*. Eigendom van gegevens bestaat bijvoorbeeld op het gebied van intellectueel eigendom en er bestaat ook een *sui generis* eigendom voor databanken die niet onder ander copyright vallen.[14] Hoewel eigendom van persoonsgegevens niet bestaat in de EU, kan dit wel samengaan met bescherming van persoonsgegevens, zoals ook het geval is in de Verenigde Staten[15] en China.[16] Sommigen[17] stellen voor dat eigendom van persoonsgegevens ook in de EU zou moeten worden geïntroduceerd, maar anderen zijn daarop tegen.[18]

Vaak wordt gedacht dat er in de EU geen eigendom van persoonsgegevens bestaat omdat dit zich slecht verhoudt tot de mensenrechtelijke benadering van privacy

die we in de EU kennen. Immers, eigendom en bezit zijn overdraagbaar, terwijl grondrechten onvervreemdbaar zijn. In een uitgebreid overzicht van de voors en tegens van een eigendomsrechtelijke benadering van persoonsgegevens laat Corien Prins zien dat dit een misverstand is: een eigendomsrechtelijke benadering van persoonsgegevens zou wel degelijk mogelijk zijn binnen de Europese juridische kaders.[19] De nadruk zou dan meer moeten liggen op controle en zichtbaarheid dan op eigendom.[20] Controle over persoonsgegevens is dan niet zozeer geregeld via eigendom, maar via controle over de gegevens en de mogelijkheden je te verzetten tegen bepaalde gevolgen of vormen van gebruik.[21] Of eigendom mogelijk is, is tot op heden echter onduidelijk; de Hoge Raad heeft hier nog geen uitspraak over willen doen.

Hoewel een eigendomsrechtelijke benadering van persoonsgegevens in beginsel goed kan samengaan met een grondrechtelijke bescherming van persoonsgegevens, bestaat die echter niet in de EU-wetgeving. Bovendien zijn er ondertussen twee belangrijke veranderingen geweest in de Europese wettelijke kaders.

Sinds 2009 is het Handvest van de grondrechten van de EU van kracht. Artikel 8 Handvest beschermt persoonsgegevens in algemene bewoordingen: 'Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.' Hoewel veel landen een grondrecht op privacy hebben opgenomen in hun grondwet, heeft de EU een separaat grondrecht op de bescherming van persoonsgegevens geformuleerd. Dit is uniek in de wereld. Het feit dat dit recht in de grondrechtencatalogus van de EU is opgenomen maakt het tot een onvervreemdbaar recht.[22] De onvervreemdbaarheid van de bescherming die grondrechten bieden, maakt dat mensen er geen afstand van kunnen doen, zelfs niet als ze dat zouden willen.[23]

'Betalen met je gegevens' voor gratis online producten en diensten is geen goede formulering, omdat je niet kunt betalen met iets dat niet je eigendom is of met iets dat je niet kunt overdragen of afstaan

Sinds 2018 heeft de AVG de regels voor het verzamelen en verwerken van persoonsgegevens verder verankerd.[24] Er moet te allen tijde een wettelijke basis zijn, zoals toestemming of een contract. De AVG kent geen eigendomsrechten toe aan actoren, maar betrokkenen (degenen wier persoonsgegevens het betreft) hebben wel bepaalde rechten ten aanzien van de gegevens. Dit betreft onder meer het recht op informatie (artikel 12-14 AVG), het recht op toegang (artikel 15 AVG), het recht op rectificatie (artikel 16 AVG), het recht op verwijdering (artikel 17 AVG) en het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming (artikel 22 AVG). Ook deze rechten zijn onvervreemdbaar: betrokkenen kunnen er geen afstand van doen en ze niet overdragen aan anderen. Ze kunnen zelfs niet worden gemandateerd aan anderen.[25]

Het grondrecht op bescherming van persoonsgegevens in het Handvest en de rechten van betrokkenen in de AVG laten zien dat (a) eigendom van persoonsgegevens niet bestaat in de EU en (b) dat rechten met betrekking tot persoonsgegevens onvervreemdbaar zijn.[26] Het gevolg is dat 'betalen met je gegevens' voor gratis online produc-

12. E. Tjong Tjin Tai, 'Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving', in: *NJV Preadviezen 2016,* vol. 146, p. 241-306.

13. N. Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency', *Journal of Law and Economic Regulation* november 2017, vol. 10, nr. 2; N. Purtova, 'Default entitlements in personal data in the Proposed Regulation: Informational Self-Determination Off the Table ... and Back on Again?', *Computer Law and Security Review,*2017, vol. 30, nr. 1, 6; M. Dorner, 'Big Data und "Dateneigentum"', *Computer und Recht* 2014, 9, 617; M. Grützmacher, 'Dateneigentum – ein Flickenteppich', *Computer und Recht* 2016, 8, 485; T. Hören, 'Big Data and the Ownership in Data: Recent Developments in Europe', *European Intellectual Property Review* 2014, vol. 36, nr. 12, 751.

14. EU-Richtlijn 96/9/EC.

15. P. Schwartz, 'Privacy, property and personal data', 117 *Harvard Law Review* 2004, 2056; E.J. Janger, 'Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy', *William & Mary Law Review* 2003, 44, 1801.

16. T. Fu, China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent. *Global Media and Communication*, 2019, vol. 15, nr. 2, p. 195213.

17. Zie N. Purtova, *Property Rights in Personal Data: A European Perspective*, Kluwer Law Intl 2011; N. Purtova, 'Property Rights in Personal Data: Learning from the American Discourse', 25 *Computer Law & Security Review* 507; N. Purtova, *Illusion of Personal Data as No One's P*roperty, 2013papers.ssrn.com/abstract=2346693; H. Zech, 'Information as Property', *JIPITEC* 2015, 6, 192.

18. A. Wiebe, 'Protection of Industrial Data – A New Property Right for the Digital Economy?', *Journal of Intellectual Property Law & Practice* 2017, 62, vol. 12, iss. 1; B. Hugenholtz, 'Against Data Property', in: H.Ullrich, P. Drahos & G. Ghidini (eds.), *Kritika: Essays on Intellectual Property*, vol. 3, Edward Elgar Publishing Limited, 2018; J. Drexl, 'Designing Competitive Markets for Industrial Data in Europe – Between Propertisation and Access', *JIPITEC* 2017, 8, 257.

19. Merk op deze literatuur dateert van de tijd voordat het Handvest en de AVG van kracht werden.

20. J.E.J. Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', in: L. Guibault & P.B. Hugenholtz (eds.) *The Future of the Public Domain, Identifying the Commons in Information Law*, Alphen: Kluwer 2006.

21. Tjong Tjin Tai 2016.

22. In tegenstelling tot de Universele Verklaring van de Rechten van de Mens is het Handvest niet expliciet over de onvervreemdbaarheid van grondrechten. Niettemin wordt algemeen aangenomen dat onvervreemdbaarheid tot de essentie van grondrechten hoort. Zie P. Malanczuk, (1997) *Akehurst's Modern Introduction to International Law*, Londen: Routledge 1997. Zie ook de preambule Universele Verklaring van de Rechten van de Mens (1948): 'recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world'.

23. D. Groome, 'Chapter 1: Overview of Human Rights Law', in: *Handbook of Human Rights Investigation*, Penn State University, 2011.

24. Merk op dat de meeste bepalingen in de AVG ook reeds bestonden in EU-databeschermingsrichtlijn 95/46/EC die in Nederland was omgezet in de Wet bescherming persoonsgegevens, van kracht tussen 2001-2018.

25. Art. 80 AVG biedt betrokkenen het recht om privacy-organisaties namens hen een klacht te laten indienen. Maar dit betreft alleen het recht om een klacht in te dienen en het recht op een voorziening in rechte, niet op de rechten van betrokkenen in hoofdstuk 3 van de AVG.

26. Zie ook Malgieri & Janeček, 2020.

ten en diensten geen goede formulering is, omdat je niet kunt betalen met iets dat niet je eigendom is of met iets dat je niet kunt overdragen of afstaan. Juridisch gezien kan worden beredeneerd dat 'betalen met je gegevens' neerkomt op het verlenen van een recht op toegang tot de gegevens of een recht om de gegevens te mogen verwerken. Zoals we hieronder zullen betogen, staat ook dat op gespannen voet met de onvervreemdbaarheid van de rechten van betrokkenen.

3. Onvervreemdbaarheid in het Handvest

3.1. Het grondrecht op bescherming van persoonsgegevens

Historisch gezien is het recht op bescherming van persoonsgegevens een aspect van het recht op privacy dat is opgekomen in de tweede helft van de vorige eeuw. Het wordt ook wel aangeduid als informationele privacy[27] en is meestal herleidbaar naar artikel 8 EVRM.[28] In de EU leunt het Hof van Justitie doorgaans stevig op het EVRM als het om mensenrechten gaat. Pas toen het Handvest, opgesteld in 2000, van kracht werd in 2009 kwam een extra bron ter beschikking. In artikel 8 Handvest is het recht op bescherming van persoonsgegevens als apart recht opgenomen, naast het recht op privacy (artikel 7 Handvest).[29]

Hoewel het lang geduurd heeft voordat het recht op bescherming van persoonsgegevens daadwerkelijk is gecodificeerd, bestond het al veel langer in de jurisprudentie. Het EU Hof van Justitie erkende het recht op bescherming van persoonsgegevens al als een algemeen beginsel in het EU-recht in 1969, in de zaak *Stauder/the City of Ulm* (C-29/69).[30]

Artikel 8 Handvest is bindend. In beginsel betekent het verheffen van het recht op bescherming van persoonsgegevens tot een grondrecht een versteviging van de bescherming die wordt geboden aan personen binnen de EU.[31] Echter, er wordt ook wel betoogd dat het recht op bescherming van persoonsgegevens in het Handvest niet voldoet aan de criteria van een grondrecht en moet worden gezien als een gewoon consumentenrecht.[32]

3.2. De onvervreemdbaarheid van grondrechten

Of het recht op bescherming van persoonsgegevens een grondrecht zou moeten zijn en wat de reikwijdte ervan zou moeten zijn, zijn legitieme vragen. Maar doordat dit recht is opgenomen in het Handvest is het zonder twijfel een grondrecht. Aan deze constatering kunnen enkele conclusies worden verbonden. Grondrechten zijn typisch inherent (ze behoren aan mensen toe eenvoudigweg om ze mensen zijn, ze hoeven niet te worden gekocht, verdiend of geërfd), basaal (ze bieden een minimumniveau aan menselijke waardigheid), onvervreemdbaar (ze kunnen niet worden afgestaan of afgepakt), blijvend (ze kunnen niet verlopen of verloren gaan, ook niet na lange tijd), ondeelbaar (ze kunnen niet verdwijnen wanneer andere rechten al zijn ingezet), universeel (ze zijn onafhankelijk van iemands afkomst, status, geslacht, etc.) en onderling afhankelijk (het uitoefenen van een recht is verbonden met andere rechten).[33]

Hier zullen we vooral ingaan on de onvervreemdbaarheid van grondrechten. De onvervreemdbaarheid heeft twee kanten: enerzijds kunnen grondrechten niet rechtmatig worden afgenomen van iemand en anderzijds kunnen ze niet worden afgestaan, doorgegeven of verbeurd. Omdat het recht op gegevensbescherming ook een grondrecht is, kan het niet afgenomen worden, zelfs als anderen (zoals sociale media, gegevensmakelaars, etc.) dit recht bedoeld of onbedoeld schenden. Dit recht kan ook niet worden weggegeven, zelfs niet als mensen zeer slordig met hun persoonsgegevens omgaan en toestemming geven voor het gebruik van hun gegevens voor van alles en nog wat (zoals in ruil voor gratis online diensten).

Merk op dat er een verschil zit tussen de onvervreemdbaarheid van het recht op bescherming van persoonsgegevens en de onvervreemdbaarheid van de persoonsgegevens zelf. Dat laatste is van belang voor de vraag of persoonsgegevens verhandelbaar zijn. Juridisch gezien is het recht op bescherming van persoonsgegevens onvervreemdbaar, maar strikt genomen hoeft dat niet het geval te zijn voor de persoonsgegevens zelf. Toch lijkt het verhandelbaar maken van persoonsgegevens onverenigbaar met de onvervreemdbaarheid van het recht op bescherming van persoonsgegevens.[34] Een nog sterker argument hiervoor wordt gevonden in de onvervreemdbaarheid van datasubject-rechten, zie paragraaf 4.

Er zit een verschil zit tussen de onvervreemdbaarheid van het recht op bescherming van persoonsgegevens en de onvervreemdbaarheid van de persoonsgegevens zelf

Het grondrecht op bescherming van persoonsgegevens heeft een sterke relatie met menselijke waardigheid.[35] Bij menselijke waardigheid staan zelfbeschikking en persoonlijke ontwikkeling voorop, beginselen die doorgaans ook worden beschouwd als onderliggende rationale voor bescherming van privacy.[36] Ook binnen de doctrine voor een algemeen recht op privacy die het Duitse constitutionele hof heeft ontwikkeld, is een relatie tussen persoonlijkheid, menselijke waardigheid en privacy te zien.[37] Datzelfde hof heeft al voorgesteld dat de bescherming van persoonsgegevens valt onder het recht op menselijke waardigheid van artikel 1.1 van de Duitse grondwet, gelezen in samenhang met artikel 2.1 over de vrije ontwikkeling van persoonlijkheid.[38] In meer recente grondwetten van enkele Oost-Europese landen zijn de concepten waardigheid en privacy en gegevensbescherming vaker aan elkaar gekoppeld.[39] En artikel 1 van de Italiaanse wet op bescherming van persoonsgegevens van 1996 (gemoderniseerd in 2003) stelt dat het beschermen van waardigheid het doel is van gegevensbeschermingswetgeving. De sterke koppeling tussen bescherming van persoonsgegevens en waardigheid impliceert de onvervreemdbaarheid van

deze bescherming[40] en, zoals we in paragraaf 4 betogen, de onvervreemdbaarheid van rechten van betrokkenen.

4. Onvervreemdbaarheid onder de AVG

4.1 Beperkingen voor gegevensverwerking in de AVG

Onder de AVG moeten degenen die persoonsgegevens commercieel willen verhandelen of uitruilen daarvoor een juridische grondslag hebben. Deze grondslagen zijn limitatief opgesomd in artikel 6 AVG.[41] Omdat wettelijke verplichting, vitaal belang of publieke taak (artikel 6 lid 1 onder c, d en e AVG) niet erg voor de hand liggen als grondslag voor handel in persoonsgegevens, kijken we hier vooral naar toestemming, contract en gerechtvaardigd belang (artikel 6 lid 1 onder a, b en f AVG).

Toestemming kan een juridische grondslag zijn voor het verzamelen van gegevens om ze te gelde te maken.[42] Artikel 7 AVG stelt dat die toestemming ondubbelzinnig, geïnformeerd (over de commerciële doelen van de gegevensverwerking), herroepbaar en vrij moet zijn. Dit betekent dat bedrijven die persoonsgegevens willen verhandelen moeten controleren of de toestemming aan deze eisen voldoet. Toestemming is geldig als die vrij is gegeven (er moeten gelijkwaardige alternatieven beschikbaar zijn voor de geboden dienstverlening, anders heeft betrokkene niet echt een keuze) en niet is herroepen door betrokkene.

Als het verwerken van persoonsgegevens berust op toestemming, dan kunnen betrokkenen die toestemming te allen tijde en naar believen intrekken, zonder verdere toelichting. Het verlies van toestemming van een enkele gebruiker is doorgaans geen probleem voor grote bedrijven. Maar als grote groepen gebruikers tegelijkertijd hun toestemming intrekken, kan dat wel problematisch zijn voor bedrijven die hun bedrijfsmodellen hebben gebaseerd op persoonsgegevens. In de praktijk trekken mensen zelden hun toestemming in, laat staan tegelijkertijd in grote groepen.[43] Juridisch gezien is dit echter wel mogelijk, hetgeen rechtsonzekerheid kan creëren voor deze bedrijven.[44]

Als het verwerken van persoonsgegevens berust op toestemming, dan kunnen betrokkenen die toestemming te allen tijde en naar believen intrekken

Als alternatief voor toestemming kan gekeken worden naar contract als juridische basis voor het verhandelen van persoonsgegevens (artikel 6 lid 1 onder b AVG). Experts zijn het erover eens dat dit niet kan.[45] Ook de Arti-

27. Voor een gedetailleerde analyse van de opkomst van gegevensbescherming als een grondrecht, zie G. Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer International Publishing 2014, springer.com/gp/book/9783319050225.

28. Zie bijvoorbeeld de zaak *Z/Finland* (1997, 25, E.H.R.R. 371).

29. B. van der Sloot, 'Legal fundamentalism: is data protection really a fundamental right?', in: R. Leenes, R. van Brakel, S. Gutwirth & P. de Hert (eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures.* Heidelberg: Springer 2017.

30. eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:61969CJ0029.

31. G. González Fuster & R. Gellert, (2012) 'The fundamental right of data protection in the European Union: in search of an uncharted right', *International Review of Law, Computers & Technology* 2012, vol. 26, nr. 1, p. 73-82.

32. B. van der Sloot, 'Legal fundamentalism: is data protection really a fundamental right?', in: R. Leenes, R. van Brakel, S. Gutwirth, & P. de Hert (eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures.* Heidelberg: Springer 2017.

33. Cf. E.L. Rubin, 'Rethinking Human Rights', *International Legal Theory* 2003, 9(1); Ph. Alston, *The EU and Human Rights*, Oxford: Oxford University Press 1999.

34. De analogie tussen slavernij en gegevensbescherming komt vaker voor in de literatuur, onder de term 'data slavery', cf. M. Hildebrandt, 'Slaves to Big Data. Or Are We?', 17 *IPD Revista de Internet, Derecho y Politica* 2013, p. 7-44; D. Damanhouri, 'Data Slavery: You're Actually Selling Your Information For Free', *Medium.com* 3 november 2017; M. Pirkowski, 'Data Slavery and Decentralized Emancipation: Facebook, Google and the Future of Data Ownership', *Medium.com* 21 juni 2018.

35. L.A. Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, *Computer Law & Security Review* 2001, 17, 18; E.J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', *New York Law Review* 1964, 39, 962; Fuster 2014; L. Floridi, 'On Human Dignity as a Foundation for the Right to Privacy', *Philosophy & Technology* 2016, 29, 307; J.Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty', *The Yale Law Journal* 2004, 113, 72.18; Edward J Bloustein, \\uc0\\u8216{}Privacy as an Aspect of Human Dignity\\uc0\\u8239{}: An Answer to Dean Prosser\\uc0\\u8217{} (1964

36. B. van der Sloot, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data', *JIPITEC* 2014, 5, jipitec.eu/issues/jipitec-5-3-2014/4097; A.E. Pérez Luño, *Derechos humanos, Estado de Derecho y Constitución,* Edición, Tecnos, 2010, 324.

37. Fuster 2014, p. 26.

38. Mikrozensus-Urteil, 16 juli 1969 (1 BVerfGE 27, Rn. 20). P. de Hert & S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in: E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the Criminal Law,* Intersentia, p. 80; Zie ook Fuster 2014, p.176.

39. Zie: Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic, No. 2/1993 Coll. In dit Charter erkent art. 19 een recht op menselijke waardigheid en een recht op bescherming van privéleven tegen het ongewenst verzamelen, openbaar maken en ander gebruik van persoonsgegevens. Art. 19 lid 1-3 van de Slowaakse grondwet werkt op dezelfde manier.

40. Zie bijvoorbeeld J. Waldron, *Dignity, Rank, and Rights,* Oxford University Press, 2012, p. 140-141.

41. Voor gevoelige gegevens gelden striktere eisen, zie art. 9 AVG. Zie ook G. González Fuster & P. de Hert, *Understanding the legal provisions that allow processing and profiling of personal data – an analysis of GDPR provisions and principles*, 20 ERA Forum 2019, 1-25.

42. Zie WP29, 2014, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* 2014, WP 217, p. 18. Zie ook F. Borgesius, Personal Data Processing for Behavioural Targeting: Which Legal Basis? 5 *International Data Privacy* 2015, p. 176.

43. B.H.M. Custers, 'Click here to consent forever; Expiry dates for informed consent', *Big Data and Society* 2016, p. 1-6, doi.org.10.1177/2053951715624935.

44. De bedrijfsmodellen zijn vaak gemengd, met gratis basisdienstverlening en betaalde aanvullende dienstverlening ('premium service'). Hoewel het aantal betalende gebruikers doorgaans veel lager ligt, kan dit voldoende continuïteit bieden voor bedrijven als niet-betalende gebruikers massaal hun toestemming zouden intrekken.

45. Chr. Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 2nd ed., Oxford: Oxford University Press 2007, p. 234-235; Borgesius 2015, p. 170.

kel 29 Werkgroep (WP29) heeft gesteld dat deze bepaling strikt geïnterpreteerd moet worden en niet ziet op situaties waar het verwerken van persoonsgegevens niet strikt noodzakelijk is of eenzijdig wordt opgelegd door een bedrijf.[46]

Dan blijft nog over de mogelijkheid van een gerechtvaardigd belang dat de gegevensverantwoordelijke heeft (artikel 6 lid 1 onder f AVG). Deze grondslag vereist dat moet zijn voldaan aan een drietal toetsingen: (1) de noodzakelijkheidstoets, (2) de legitimiteitstoets en (3) de proportionaliteitstoets gezien de belangen van betrokkenen.

Het gebruik van gerechtvaardigd belang als grondslag is problematisch,[47] in het bijzonder vanwege de noodzakelijkheidstoets. WP29 heeft in het verleden al aangegeven dat gegevensbeheerders altijd moeten bekijken of er minder invasieve manieren zijn om de doelen van hun gegevensverwerking te bereiken.[48] Bij de handel in persoonsgegevens kan het doel zijn economisch voordeel te halen uit de persoonsgegevens, maar in dat geval is het doel wel erg algemeen en vaag.[49] Het doel van economisch voordeel zou bovendien bereikt kunnen worden op minder invasieve manieren, bijvoorbeeld wanneer 'premium' diensten tegen betaling worden aangeboden.

De legitimiteitstoets kan ruim worden geïnterpreteerd,[50] maar het belang moet altijd wettig, duidelijk, reëel en actueel zijn.[51] In de proportionaliteitstoets[52] moeten worden meegenomen het gerechtvaardigd belang van de gegevensbeheerder, de impact op betrokkenen, de voorlopige afweging en extra waarborgen om onnodige impact op de betrokkenen te voorkomen.[53]

Al deze afwegingen kunnen het gebruik van gerechtvaardigd belang als juridische grondslag voor de handel in persoonsgegevens zeer lastig of onmogelijk maken

Al deze afwegingen kunnen het gebruik van gerechtvaardigd belang als juridische grondslag voor de handel in persoonsgegevens zeer lastig of onmogelijk maken. Per situatie zal moeten worden geëvalueerd of sprake is van onder meer invasieve profilering, onduidelijke informatievoorziening, etc. Een betrokkene kan zich in dat geval op elk moment verzetten tegen het verwerken van de gegevens en dit een halt toeroepen (zie artikel 21 lid 2 en 3 AVG). Dus zelfs als een gerechtvaardigd belang de juridische grondslag vormt voor handel in persoonsgegevens, heeft betrokkene een direct recht zich hiertegen te verzetten. Dat lijkt sterk op het recht om toestemming in te trekken ingeval de handel in persoonsgegevens is gebaseerd op toestemming.

Als het de handel in 'gevoelige' persoonsgegevens betreft (bijzondere categorieën persoonsgegevens genoemd in artikel 9 AVG), kan gerechtvaardigd belang nooit als juridische grondslag dienen. Alleen toestemming kan dan de juridische grondslag zijn, tenzij de gegevens al door betrokkene zelf openbaar zijn gemaakt. Als gegevens al openbaar zijn, is de commerciële waarde van deze gegevens voor bedrijven mogelijk minimaal (deze gegevens hoeven immers niet gekocht te worden, ze zijn eenvoudig te verzamelen uit open bronnen).

Samengevat lijkt toestemming de meest voor de hand liggende juridische grondslag voor de handel in persoonsgegevens en om mensen te laten betalen met hun gegevens. Maar tegelijkertijd is toestemming onzeker en vluchtig. Zelfs als toestemming expliciet en vrij is gegeven, kan deze in de toekomst te allen tijde weer worden ingetrokken, naar believen.[54] Gerechtvaardigd belang als grondslag is zeer lastig: zelfs als de drie toetsen van noodzakelijkheid, legitimiteit en proportionaliteit worden doorstaan, kan een betrokkene zich eenvoudig verzetten tegen de verwerking van de persoonsgegevens (artikel 21 AVG) en daarmee de verwerking blokkeren. Contract als juridische grondslag lijkt voor de hand te liggen als de betaling als onderdeel van een transactie wordt gezien, maar hiervoor gelden dezelfde bezwaren als voor toestemming. Een contract aangaan is sowieso gebaseerd op wederzijdse instemming.

4.2 De onvervreemdbaarheid van rechten van betrokkenen

De onvervreemdbaarheid van het grondrecht op bescherming van persoonsgegevens werkt door in de AVG, die gebaseerd is op informationele zelfbeschikking. Dit concept is al in de jaren zestig ontwikkeld en stelt dat iedereen het recht heeft zelf te bepalen wanneer, hoe en in hoeverre zijn of haar persoonsgegevens met anderen mogen worden gedeeld.[55] Deze benadering zet persoonlijke autonomie en toestemming centraal.[56] De term duikt voor het eerst in jurisprudentie op in een zaak van het Duitse constitutionele hof in 1983.[57] Als gevolg van deze ontwikkelingen bevat de AVG meerdere rechten voor betrokkenen (datasubject-rechten) die onvervreemdbaar zijn en van invloed kunnen zijn op het verwerken van persoonsgegevens. Het gaat dan bijvoorbeeld om recht op inzage, rectificatie en verwijdering.

De AVG lijkt niet toe te staan dat deze rechten van betrokkenen aan anderen kunnen worden toegekend, gemandateerd of gedelegeerd. In het bijzonder artikel 80 AVG, een bepaling die toestaat dat betrokkenen zich laten vertegenwoordigen, voorziet niet in de mogelijkheid dat vertegenwoordigers van betrokkenen deze rechten kunnen uitoefenen namens hen. De vertegenwoordigersrol is beperkt tot juridische acties en het recht op compensatie. Hoewel het mandateren van deze rechten nergens in de AVG expliciet wordt uitgesloten, lijken ze mandateerbaar noch uitoefenbaar door anderen dan betrokkenen.[58] In het privaatrecht kunnen individuele rechten weliswaar gemandateerd of gedelegeerd worden aan anderen, maar dat lijkt niet direct toepasbaar op gegevensbescherming vanwege het grondrechtelijk karakter van deze rechten.[59] Jurisprudentie ontbreekt op dit vlak,[60] maar er zijn indicaties dat het onmogelijk is deze rechten te vervreemden, waaronder het recht om toestemming in te trekken (artikel 7 lid 3 AVG).

Vanuit het perspectief van bedrijven is dit problematisch vanwege de beperkte rechtszekerheid. Betrokkenen

behouden immers altijd hun onvervreemdbare rechten om de gegevensverwerking tegen te houden of te beperken, op elk moment en zonder verdere toelichting. In een online omgeving kan worden geredeneerd dat het intrekken van toestemming inhoudt dat de dienst vanaf dat moment niet meer kan worden gebruikt (bijvoorbeeld een gratis online krantenabonnement stopt zodra het wordt opgezegd en de 'betaling' stopt). Maar onder de AVG kunnen betrokkenen de gegevensverwerking ook beperken in plaats van stopzetten. Iemand kan bijvoorbeeld het recht op verwijdering inroepen (artikel 17 AVG) of het recht op beperken van de verwerking (artikel 18 AVG). Het inroepen van deze rechten verhindert niet dat betrokkenen de gratis online diensten niet langer kunnen gebruiken, maar het betekent wel dat betrokkenen sterk de waarde die hun persoonsgegevens hebben voor bedrijven kunnen beïnvloeden. Dit resulteert in aanzienlijke rechtsonzekerheid in transacties, aangezien het de initiële voorwaarden van een transactie wezenlijk kan veranderen in een later stadium.

Persoonsgegevens diskwalificeren als handelswaar is geen probleem, maar een data-economie bouwen op iets dat geen handelswaar is, is wel een probleem

5. Conclusie

Het grondrecht op bescherming van persoonsgegevens is gewaarborgd in artikel 8 Handvest van grondrechten van de EU. Dit recht is uniek in de wereld; vooralsnog heeft geen enkele andere jurisdictie ter wereld dit recht tot grondrecht verheven. Deze ontwikkeling hangt sterk samen met de invoering van een hoog beschermingsniveau voor persoonsgegevens dat de EU tracht te ontwikkelen met de invoering van de AVG, die breed erkend wordt als (behorend tot) de sterkste juridische bescherming van persoonsgegevens wereldwijd.

De keuze van de EU om het recht op bescherming van persoonsgegevens tot een grondrecht te verheffen is meer dan symbolisch, het heeft aanzienlijke consequenties. Het recht op bescherming van persoonsgegevens als grondrecht is onvervreemdbaar: mensen kunnen dit recht niet overdragen en er geen afstand van doen. Dat staat in de weg aan eigendom van persoonsgegevens en is lastig verenigbaar met een data-economie die is gebaseerd op handel in persoonsgegevens. Op zichzelf is dat geen probleem, want in de EU heeft juridisch gezien nooit eigendom van persoonsgegevens bestaan.[61] Grondrechten zijn geen handelswaar. Vanuit een grondrechtenperspectief is het niet logisch om de handel in persoonsgegevens of handel in rechten ten aanzien van die gegevens toe te staan.

Maar dat staat in scherp contrast met de praktijk van de huidige data-economie.[62] Veel bedrijven zijn juist gebaseerd op gratis online bedrijfsmodellen waarbij hun winsten voortkomen uit het verzamelen, analyseren en verhandelen van de persoonsgegevens die gebruikers ter beschikking stellen in ruil voor de dienstverlening. Mensen weten doorgaans dat deze onlineproducten en diensten, zoals zoekmachines en sociale media, gratis zijn omdat ze 'betalen met hun gegevens'. Met andere woorden, zowel bedrijven als gebruikers zien persoonsgegevens als handelswaar, ondanks dat persoonsgegevens binnen de EU-wetgeving geen handelswaar kunnen zijn.

Dit contrast tussen de juridische kaders en de praktijk is opmerkelijk. Het schept ook rechtsonzekerheid in transacties, bijvoorbeeld wanneer de juridisch grondslag voor het verwerken van de persoonsgegevens is gebaseerd op toestemming van betrokkene. Aangezien het recht op bescherming van persoonsgegevens onvervreemdbaar is, kunnen betrokkenen te allen tijde en naar believen hun toestemming weer intrekken, zonder verdere toelichting.

46. Zie WP29 (2014), p. 17.

47. Borgesius 2015, p. 170.

48. Zie WP29, 2014, p. 29 en p. 55.

49. Zie WP29, 2013 *Opinion 3/2013 on purpose limitation* (WP 203), p. 16: 'For these reasons, a purpose that is vague or general, such as for instance "improving users' experience", "marketing purposes", "IT-security purposes" or "future research" will – without more detail – usually not meet the criteria of being "specific".'

50. Zie WP29, 2014, p. 24.

51. WP29, 2014, p. 25.

52. I. Kamara & P. de Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach', in: Selinger, Polonetsky & Tene (eds.), *Cambridge Handbook of Consumer Privacy,* Cambridge: Cambridge University Press 2018.

53. WP29, 2014, p. 33.

54. Het verwerken van gegevens voor de intrekking is niet onrechtmatig (art. 7 lid 3 AVG), maar nieuwe verwerkingen zijn niet toegestaan. Tegelijkertijd geldt dat als er geen andere juridische grondslag is, de gegevens moeten worden verwijderd. Zie European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (Art. 70.1.b)*, 2019, p. 7).

55. A. Westin, *Privacy and Freedom*. London: Bodley Head 1967.

56. B. Custers, F. Dechesne, W. Pieters, B. Schermer & S. van der Hof, 'Consent and Privacy', in: A. Müller & P. Schaber (eds.), *Handbook of the Ethics of Consent*, London: Routledge 2018, p. 247-258.

57. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfG 65, 1.

58. S. Delacroix & N.D. Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', *International Data Privacy Law* 2019, vol. 9, iss. 4, p. 236-252.

59. O. Lynskey, *The Foundations of EU Data Protection Law,* Oxford: Oxford University Press 2015, p. 40.

60. Het EU Hof van Justitie bevestigt in C-498/16 (*Maximilian Schrems/Facebook Ireland Limited*), 25 januari 2018, §49 dat het toekennen van rechten onder EU-consumentenrecht hier niet mogelijk is (omwille van jurisdictie), maar bespreekt niet of het mandateren van consumentenrechten of rechten van betrokkenen in de AVG verboden of toegestaan is.

61. Niettemin heeft deze discussie binnen de EU lang aangehouden. Zie A. Taranowski, 'EU Drops Data Ownership', *Medium* 27 february 2020, medium.com/data-legally/eu-drops-data-ownership-807ca597fd62.

62. B.H.M. Custers & D. Bachlechner, 'Advancing the EU Data Economy; Conditions for Realizing the Full Potential of Data Reuse', *Information Polity* 2018, vol. 22, nr. 4, p. 291-309.

Het grondrecht op bescherming van persoonsgegevens in het Handvest en de rechten van betrokkenen in de AVG staan op gespannen voet met de realiteit van de alomtegenwoordige handel in persoonsgegevens

Normaal gesproken wordt bij een transactie vooraf een prijs afgesproken, maar hier betekent de onvervreemdbaarheid van de rechten van betrokkenen dat ze hun 'betaling' kunnen intrekken nadat ze de producten en diensten hebben ontvangen. Als ze hun toestemming niet volledig intrekken, maar wel rechten van betrokkenen onder de AVG inroepen, kunnen ze de gegevensverwerking aanzienlijk beperken.

De keuze van de EU-wetgever om persoonsgegevens niet als handelswaar te beschouwen staat bovendien op gespannen voet met de eigen doelstelling van de EU om een Digital Single Market te creëren.[63] Deze strategie, gestart in 2015, is bedoeld om de Europese markt met zijn vier vrijheden (vrij verkeer van goederen, kapitaal, diensten en personen) aan te vullen met een vijfde vrijheid: vrij verkeer van gegevens. Dit moet de data-economie van de EU versterken. Maar het bijbehorende juridische raamwerk lijkt verscheurd tussen twee ideeën, enerzijds het beperken van datastromen om mensen te beschermen en anderzijds het aanmoedigen van datastromen om de data-economie te bevorderen.[64] Persoonsgegevens diskwalificeren als handelswaar is geen probleem, maar een data-economie bouwen op iets dat geen handelswaar is, is wel een probleem. De EU heeft een economie gebaseerd op persoonsgegevens, maar het is de vraag of dit ondanks of dankzij de huidige wetgeving is. Een indicator is in elk geval dat de EU tot op heden geen big tech-bedrijven heeft, in tegenstelling tot de Verenigde Staten en China.[65] Dat kan zijn omdat de EU niet één land is of omdat andere bedrijven al dominante marktspelers zijn,[66] maar het kan ook aan de huidige wetgeving liggen. Een andere indicator is dat bedrijven het maar lastig vinden aan de huidige EU-wetgeving te voldoen, in het bijzonder de AVG,[67] iets dat de EU ook heeft toegegeven.[68]

Concluderend kunnen we vaststellen dat het grondrecht op bescherming van persoonsgegevens in het Handvest en de rechten van betrokkenen in de AVG op gespannen voet staan met de realiteit van de alomtegenwoordige handel in persoonsgegevens. Dit is niet enkel een positiefrechtelijk probleem, maar laat ook de ambigue doelstellingen van de EU-wetgever zien, die enerzijds mensen en hun persoonsgegevens wil beschermen, maar anderzijds een data-economie wil opbouwen op basis van handel in diezelfde gegevens. Beide zijn legitieme doelen, maar gaan niet goed samen. Het lijkt tijd voor de EU om heldere keuzes te maken. •

63. COM(2015) 192 final, A Digital Single Market Strategy for Europe, Brussels, 6 mei 2015, eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

64. Zie ook T. Zarsky, 'Incompatible: The GDPR in the Age of Big Data', *Seton Hall Law Review* 2017, vol. 47, iss. 4, article 2.

65. A. Renda, 'Europe's big tech contradiction', *Centre for European Policy Studies*, 2 april 2019, ceps.eu/europes-big-tech-contradiction/#_ftn1.

66. A.P. Jurak, 'The importance of high–Tech companies for EU economy–Overview and the EU grand strategies perspective', *Research in Social Change* 2020, vol. 12, nr. 3, p. 32-52.

67. S. Mendoza, 'GDPR Compliance-It Takes a Village' *Seattle UL Review* 2018, *42*, 1155; S. Sirur, J.R. Nurse, & H. Webb, 'Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR), in: *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* 2018, p. 88-95; M. Kutyłowski, A. Lauks-Dutka & M. Yung, 'GDPR challenges for reconciling legal rules with technical reality', in: *European Symposium on Research in Computer Security,* Cham: Springer 2020, p. 736-755.

68. J. Espinoza, 'EU admits it has been hard to implement GDPR', *Irish Times*, 23 juni 2020, irishtimes.com/business/technology/eu-admits-it-has-been-hard-to-implement-gdpr-1.4286207.