De verordening vrij verkeer van niet-persoonlijke data en blijvende onmogelijkheden van data

Een juiste prioritering van de Europese Commissie in haar DSM-strategie?

mr. O.F.A.W. van Haperen en mr. R.P. Santifort[1]

Op 13 september 2017 heeft de Europese Commissie ('EC') een verordening voorgesteld die regels voorschrijft voor vrij verkeer van 'niet-persoonlijke data'.[2] Het voorstel heeft tot doel een leemte op te vullen ten behoeve van vrij verkeer van informatie die niet tot de persoon herleidbaar is. Het voorstel vloeit voort uit de Digital Single Market ('DSM') strategie van de EC. Wij voorspellen dat deze verordening in Nederland juridisch gezien weinig impact zal hebben. Nederlandse clouddienstverleners zullen, gelet op hun koppositie in de markt, hier echter wel baat bij hebben. De verordening heeft slechts een beperkte scope, maar bevindt zich wel in een dynamische speeltuin door het uitdijende persoonsgegevensbegrip. Anderzijds blijven juridische lacunes ten aanzien van de eigendom van data bestaan. In dit artikel bespreken wij achtereenvolgens de achtergrond van het voorstel van de verordening (§ 1), haar essentie en doel (§ 2), de impact in Nederland en andere Europese landen (§ 3), de verhouding tot de AVG (§ 4) en de blijvende lacune ten aanzien van de eigendom van data (§ 5). We sluiten af met een conclusie (§ 6).

1. Achtergrond

De verordening is onderdeel van de DSM-strategie van de EC. De DSM strategie heeft tot doel Europa en haar interne markt aan te laten sluiten bij het digitale tijdperk.[3] Realisatie van de DSM strategie zou voor meer dan 400 miljard per jaar kunnen bijdragen aan de Europese economie en honderdduizenden banen creëren. Sinds mei 2015 heeft de EC hiertoe al meer dan 35 wetgevingsvoorstellen gedaan en beleidsinitiatieven gestart. Zo zagen we deze zomer nog de afschaffing van de roaming kosten in de telecombranche.[4] Eind vorig jaar passeerden al (nieuwe) verplichte auteursrechtelijke concept-regels, zoals de 'Text and Data Mining'-exceptie voor onderzoeksinstellingen, een exceptie voor digitaal onderwijs met een vergoedingsregeling en een preserveringsexceptie voor culturele erfgoedinstellingen.[5]

In de 'mid-term' review van de EC van afgelopen mei[6] noemt de EC drie belangrijke punten waarbij verdere EU-maatregelen nodig zijn: (1) het volledige potentieel van de Europese dataeconomie verwezenlijken, (2) de Europese activa beschermen door uitdagingen op het gebied van cyberveiligheid aan te pakken en (3) bevorderen dat onlineplatforms te werk gaan als verantwoordelijke actoren binnen een eerlijk internet-ecosysteem.

Het onderhavige voorstel maakt onderdeel uit van het eerste punt. De concept verordening is onder-

1. Mrs. O.F.A.W. van Haperen en R.P. Santifort zijn IT/privacy-advocaten bij Kneppelhout & Korthals advocaten te Rotterdam. Standpunten en meningen in dit artikel zijn op persoonlijke titel en vertegenwoordigen niet het standpunt van Kneppelhout & Korthals Advocaten, noch haar cliënten en/of relaties.
2. Voorstel voor een verordening van het Europees parlement en de Raad inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie COM (2017)495.
3. Zie voor meer informatie https://ec.europa.eu/digital-single-market/.
4. https://ec.europa.eu/digital-single-market/en/policies/roaming.
5. https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules.
6. https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review.

deel van een groter beleidskader genaamd de *Free Flow of Data Initiative* ('FFDI')[7] om de Europese data-economie in goede banen te leiden. Andere onderdelen van dit raamwerk zijn bijvoorbeeld de Algemene Verordening Gegevensbescherming (AVG)[8] voor persoonsgegevens, de richtlijn gegevensbescherming voor politie en strafrechtelijke autoriteiten[9] en de in 2018 in werking tredende E-privacyverordening voor het gebruik van persoonsgegevens in elektronische communicatie.[10] Daarnaast mogen we begin 2018 in dit kader een initiatief verwachten inzake toegankelijkheid en het hergebruik van publieke en door de overheid gefinancierde data, alsook een evaluatie van de databankenrichtlijn. Tot slot zal nog verder onderzoek worden gedaan naar vraagstukken rondom het stimuleren van het delen van data tussen bedrijven.

2. Essentie en doel

De verordening heeft tot doel barrières op vrij verkeer van niet-persoonlijke data binnen de EU op te heffen. Nieuwe digitale technologieën, zoals cloudcomputing, big data, AI en IoT worden ontwikkeld om efficiëntie te maximaliseren, schaalvergroting mogelijk te maken en om nieuwe diensten te verwezenlijken. Technologieën die gebruikers ongekende voordelen bieden, bijvoorbeeld op het gebied van flexibiliteit, productiviteit, snelheid van inzet en autonomie, onder meer met behulp van machine-learning. Met de verordening wil de EC ongerechtvaardigde datalocatie-eisen[11] verbieden, data-toegang voor grensoverschrijdend toezicht en handhaving faciliteren en portabiliteit[12] van niet-persoonlijke data stimuleren.

Het voorstel is van toepassing op het opslaan en verwerken van niet-persoonlijke data (gegevens die geen persoonsgegevens zijn in de zin van de AVG) binnen de EU. Het gaat bijvoorbeeld om onderhoudsdata van machines, geanonimiseerde en/of geaggregeerde statistieken en andere ongestructureerde datasets. De verordening beoogt niet in te teren op de bevoegdheid van de lidstaten, geregeld in art. 49 lid 5 AVG, om bij wet te regelen dat persoonsgegevens niet mogen worden opgeslagen of verwerkt buiten de EU.

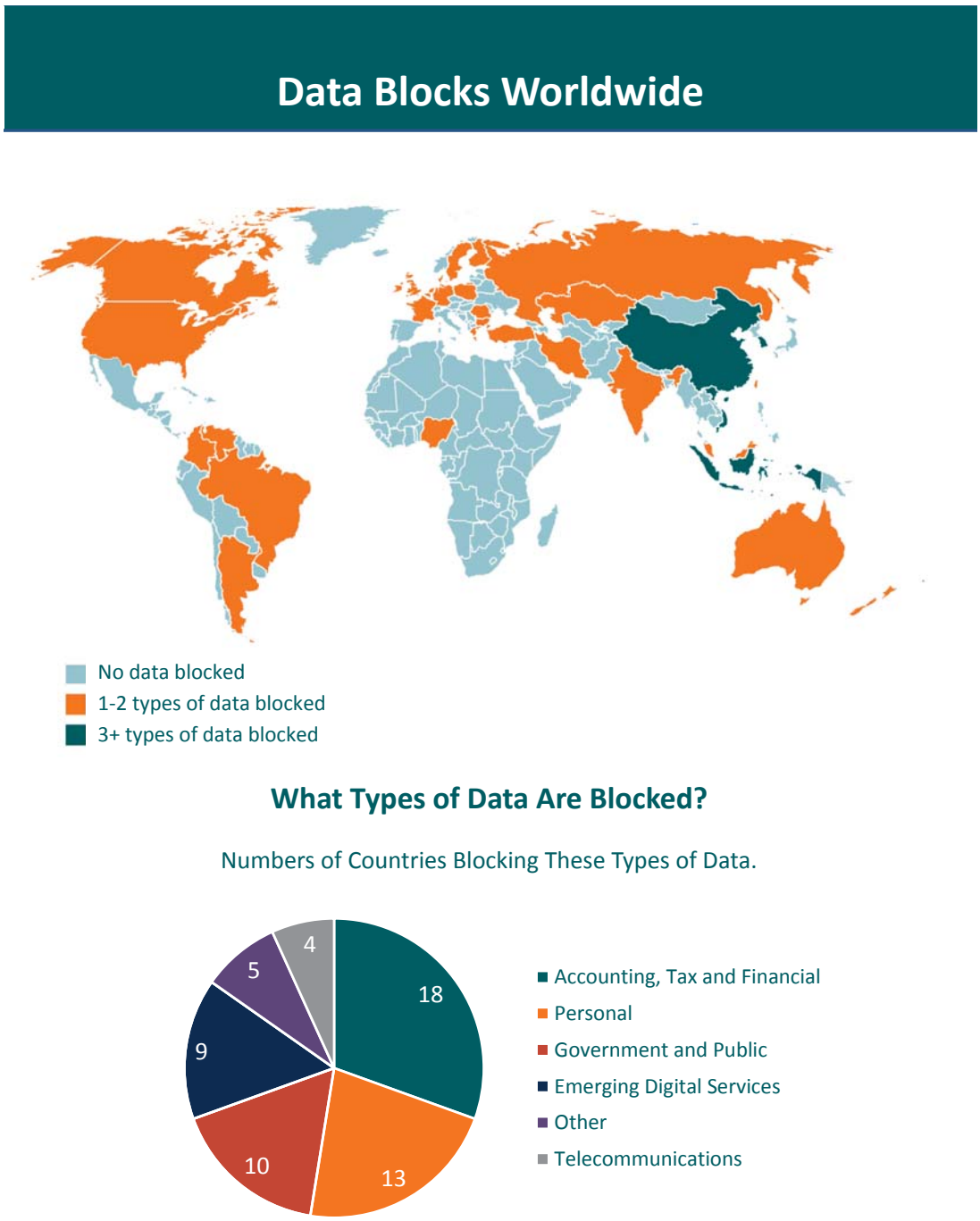
De verordening geeft aan dat binnen de reikwijdte daarvan de opslag en verwerking van data niet mag worden beperkt tot binnen de landsgrenzen van een lidstaat en dat opslag en verwerking in een andere lidstaat niet mag worden verboden, tenzij dit gerechtvaardigd wordt op basis van (belangen gelegen in de sfeer van) de openbare veiligheid.[13] Lidstaten zullen elke nieuwe datalocatie-eis die volgens hen gerechtvaardigd is om redenen van openbare veiligheid – voorafgaande aan de vaststelling daarvan – moeten melden bij de EC volgens de procedure uit de Transparantierichtlijn.[14] Alle andere datalocatie-eisen zijn in beginsel verboden.

Daarnaast gaat de verordening in op de toegang tot data voor nationale autoriteiten: een nationale autoriteit mag de toegang tot relevante data (voor handhaving en toezicht) niet worden ontzegd op basis van het feit dat de dataopslag of -verwerking plaatsvindt binnen een andere lidstaat.[15] Indien alle nationale mogelijkheden voor een bevoegde autoriteit om toegang tot de relevante data te ontvangen zijn gebruikt, beoogt de verordening een samenwerkingsnetwerk in te stellen op basis waarvan de betreffende bevoegde autoriteit assistentie kan verzoeken van de autoriteit in een andere lidstaat. Lidstaten zullen hiervoor één aanspreekpunt moeten aanwijzen. Verzoeken mogen slechts worden geweigerd indien die assistentie strijd oplevert met de openbare orde van de eigen lidstaat.

Over portabiliteit van niet-persoonlijke data geeft de verordening aan de EC de opdracht om zelfregulerende gedragscodes op Europees niveau te faciliteren en te stimuleren.[16] In deze gedragscodes worden richtsnoeren en best practices aangedragen die onder andere de transparantie over contracten moeten verhogen. Doel hiervan is om te voorkomen dat gebruikers aan contracten vast komen te zitten, waarin portabiliteit moeilijk wordt gemaakt. Daarnaast wordt een netwerk van informatiepunten opgezet om coördinatie tussen lidstaten rondom datatoegang voor autoriteiten te faciliteren.[17]

Door datalocatie-eisen in wetgeving in beginsel te verbieden moeten organisaties meer vrijheid krijgen gebruik te maken van clouddiensten van providers in andere lidstaten. De gedachte is dat door deze juridische principes onder de aandacht te brengen meer rechtszekerheid zal ontstaan rondom datastromen binnen de EU. Daarnaast zou er door het ontwikkelen van gedragscodes meer transparantie en minder informatie-asymmetrie

7. https://ec.europa.eu/digital-single-market/en/news/digital-single-market-free-flow-data-initiative.
8. Verordening (EU) 2016/679.
9. Richtlijn (EU) 2016/680.
10. Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Op 23 oktober 2017 werd door het Europees Parlement ingestemd met een mandaat waarmee onderhandelingen over de nieuwe privacyregels meteen met lidstaten gestart kunnen worden. De vraag is of men de doelstelling haalt om deze verordening tegelijk met de AVG (dus op 25 mei 2018) van toepassing te laten worden.
11. Datalocatie: geografische locatie van de opslag en verwerking van niet-persoonlijke data. De EC schat in dat de baten van het wegnemen van de huidige datalocatie-eisen tussen de € 8 miljard en € 11,7 miljard kunnen zijn.
12. Overdraagbaarheid van data tussen concurrerende dienstverleners (zoals clouddienstverleners) op verzoek van de klant.
13. Art. 4 van het voorstel.
14. 2013/50/EU
15. Art. 5 van het voorstel.
16. Art.6 van het voorstel.
17. Art.7 van het voorstel.



ontstaan in de clouddienstensector. Dit dient een *vendor lock-in*[18] te voorkomen en daardoor tot een meer concurrerende interne markt voor clouddiensten te leiden. Tegelijkertijd zou er dan flexibiliteit gecreëerd moeten worden om te grote lasten voor het bedrijfsleven te voorkomen en innovatie op peil te houden.

3. Impact van de verordening in NL/EU

Nederland heeft als digitale koploper binnen de EU een goede uitgangspositie om te kunnen profiteren van een versterkte interne markt waarin ongerechtvaardigde datalocatie-eisen verboden zijn. Met het internetknooppunt AMS-IX en de daaraan verbonden datacenter-sector beschikt Nederland over een zeer moderne infrastructuur die interessant is voor de opslag van data door buitenlandse bedrijven. Daarnaast kan het bredere Nederlandse bedrijfsleven profiteren van betere markttoegang en lagere kosten rondom dataopslag en -verwerking. Zo hoeven buitenlandse bedrijven geen onnodige extra kosten te maken om aan (ongerechtvaardigde) datalocatie-eisen te voldoen, om bijvoorbeeld toegang te houden tot een (grotere) markt. Ook zullen openbare aanbestedingen in beginsel geen

18. Vendor lock-in is het verschijnsel dat een klant zo zeer afhankelijk raakt van een leverancier dat afscheid nemen of overstappen niet langer mogelijk is zonder grote (financiële) gevolgen.

datalocatie-eisen meer mogen bevatten, omdat dit in potentie markten toch voor een gedeelte kan afschermen.

Ons kabinet heeft een aantal kanttekeningen bij de precieze uitwerking van de huidige concept verordening.[19] Zo vindt het kabinet de reikwijdte van het voorstel rondom datalocatie-eisen onduidelijk, leest zij een te beperkte formulering van de uitzonderingsgrond en is zij bang dat de verordening de contractsvrijheid raakt.

Dat de verordening de contractsvrijheid raakt is natuurlijk uit den boze en zo lezen de schrijvers dezes de onderhavige verordening ook niet. De EC daarentegen geeft in de begeleidende teksten aan dat dit niet het doel is en benoemt juist dat portabiliteit door middel van contracten dient te worden bevorderd (overwegingen 5 en 21 en artikel 6 voorstel). Daar waar wordt beoogd de interne markt te beschermen tegen ongerechtvaardigde datalocatie-eisen, ligt het wat betreft rechtvaardigheidsgronden voor datalocatie-eisen voor de hand aan te sluiten bij rechtvaardigheidsgronden die de AVG hanteert (bijvoorbeeld in art. 49 AVG). Voor het overige worden de standpunten van ons kabinet slechts beperkt onderbouwd.

Ten slotte vindt het kabinet het belangrijk dat het vraagstuk rondom datalocatie-eisen helder wordt afgebakend ten opzichte van het vraagstuk over portabiliteit. Hier liggen namelijk twee verschillende soorten problemen aan ten grondslag. Bij het vraagstuk van datalocatie-eisen gaat het om barrières voor vrij dataverkeer tussen landen die zijn opgeworpen door overheden, terwijl het bij portabiliteit gaat om contractuele of praktische beperkingen van de dienstverlener richting de klant. Wij lezen het voorstel echter zo dat met betrekking tot portabiliteit het juist de bedoeling is dat de markt zelf met gedragscodes komt en dat de EC dit proces slechts stimuleert.

Maar hoe zit het dan met die datalocatie-eisen in Nederland en de rest van Europa? Nederland stelt datalocatie-eisen in de Archiefwet, welke uitsluitend blijvende bewaring van archiefbescheiden op een *'aangewezen bewaarplaats'* mogelijk maakt.[20] Het Nederlandse kabinet vindt dergelijke datalocatie-eisen echter *'weinig marktbelemmerend'*. In Duitsland verplicht art. 113b onder 1) Duitse Telecommunicatiewet aanbieders van openbaar beschikbare telecommunicatiediensten de telecommunicatie metadata op te slaan in Duitsland en niet in een andere EU-lidstaat.[21] De EC heeft zich hier tegenover Duitsland al eerder kritisch over uitgelaten, nu dergelijke datalocatie-eisen in strijd zijn met art. 56 VWEU. Daarnaast is Frankrijk beducht met haar ministeriële regeling die lokale en regionale overheden gebiedt zogenaamde *'trésors nationaux'* in *'le cloud souverain'* (dus in Frankrijk) op te slaan. In 2012 heeft de Luxemburgse evenknie van de AFM een circulaire uitgegeven waarin staat dat financiële instellingen hun gegevens in-country moeten verwerken, tenzij de buitenlandse entiteit deel uitmaakt van hetzelfde bedrijf of als de gegevens met uitdrukkelijke toestemming worden overgedragen. Allemaal nationale preferenties dus die in beginsel indruisen tegen de verordening.

In andere Europese landen, zoals Griekenland, bevinden zich in telecommunicatiewetgeving ook nog datalocatie-eisen die verband houden met dataretentie verplichtingen. Het Europese Hof van Justitie heeft echter de algemene en ongedifferentieerde plicht voor telecombedrijven om alle verkeersgegevens en locatiegegevens van al hun abonnees en gebruikers te bewaren, in strijd met Europees recht bevonden.[22] Weer anderen zijn kritisch en tegenstander van wetgevende voorstellen als de onderhavige voor het afschaffen van geografische datalocatie-eisen, omdat niet voldoende bewezen zou zijn dat er economische schade uit voortvloeit.

4. Verhouding tot de AVG

De AVG is in beginsel van toepassing wanneer er sprake is van een geautomatiseerde verwerking van persoonsgegevens. De verordening bevat in deze zin op het eerste gezicht een duidelijke afbakening. De reikwijdte van het persoonsgegevensbegrip is echter in de praktijk niet altijd evident, omdat onder persoonsgegevens ook gegevens worden begrepen die op indirecte wijze identificatie mogelijk maken. Dat geïndividualiseerde gegevens als zodanig nog geen persoonsgegevens zijn, lijkt inmiddels wel een gegeven[23], maar gaat de strekking van dit artikel te buiten. Gezien de technische vooruitgang en de dagelijkse (door)ontwikkeling van bigdata technieken zal het 'risico' van indirecte herleidbaarheid toenemen en zullen thans niet-persoonsgegevens in de toekomst 'promoveren' tot wel-persoonsgegevens.

We signaleren in dit verband echter ook een potentieel zorgwekkende ontwikkeling dat nu al steeds meer informatie wordt gekwalificeerd als persoonsgegevens. Zie bijvoorbeeld de recente conclusie van A-G Kokott, waarin hij betoogt dat een geschreven examenwerk moet worden beschouwd als persoonsgegevens.[24] Het persoonsgegevens-

19. *Kamerstukken II* 2017/18, 22112, nr. 22405.
20. Zie art. 1 onder f Archiefwet 1995 e.v.
21. Hetgeen de 2008-versie van art. 113b Duitse Telecommunicatiewet uitdrukkelijk wel toestond.
22. HvJEU 21 december 2016, gevoegde zaken C-203/15 *Tele2 Sverige AB* tegen *Post-och telestyrelsen* en C-698/15 *Secretary of State for the Home Department* tegen *Tom Watson e.a.*
23. Rechtbank Midden-Nederland 2 augustus 2017, ECLI:NL:RBMNE:2017:4011, r.o. 4.17, met verwijzing naar HvJEU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer / Duitsland*) Zie in dit verband ook het Rapport definitieve bevindingen van de Autoriteit Persoonsgegevens over Microsoft Windows 10, zie https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_microsoft_windows_10_okt_2017.pdf.
24. Conclusie van Advocaat-Generaal J. Kokott van 20 juli

begrip wordt daarmee steeds verder opgerekt. Straks is alles een persoonsgegeven; tot aan de analyse van het weer, waarvoor associate professor Nadezhda Purtova van de Universiteit Tilburg ons waarschuwt.[25] Het gevolg is dat de AVG niet te handhaven wordt en de relevantie van de verordening voor vrij verkeer van niet-persoonsgegevens de facto afneemt. Men kan zich terecht afvragen of het de voortschrijdende ontwikkelingen in big data analyse, machine learning en artifical intelligence niet teveel in de weg staat en of we het concept van persoonsgegevens niet moeten loslaten of minstens veel sterker moeten inkaderen.

5. Blijvende lacune: eigendom van data?

Met alle initiatieven van de EC om de digitale interne markt van de EU te stimuleren, ontkomt men er niet aan om stil te staan bij lacunes in (deze) wetgeving. Data is de grondstof van het digitale tijdperk. Maar data kan in veel lidstaten, zoals Nederland, nog altijd niet juridisch worden gekwalificeerd. In de praktijk leidt dit vaak tot vreemde situaties, die moeten worden weggeschreven in contracten.

Wie is eigenaar of rechthebbende van data? Welke regels zijn daarop van toepassing? Eigendom van data kennen we niet als zodanig. Immers, de wet kent alleen eigendom van zaken: alle *'voor menselijke beheersing vatbare stoffelijke objecten'* (art. 3:2 BW). Data is onstoffelijk; het bestaat uit enen en nullen, bits en bytes. Dus is de eigendom daarvan niet mogelijk. In het verleden is wel de eigendom van virtuele objecten erkend, weliswaar in een strafrechtelijke casus.[26] Een uniek virtueel zwaard uit een spel werd weggenomen. De 'eigenaar' was deze kwijt. Voor data geldt dit over het algemeen niet. Er kan immers simpelweg een kopie van die data worden gemaakt.

De Hoge Raad vond in april 2012 met haar *Beeldbrigade*-arrest een algemeen dogmatisch antwoord nodig noch wenselijk op de vraag naar de goederenrechtelijke aard van software(data).[27] Zij deed geen uitspraak over de vraag of men bij de aanschaf van software een zaak en/of een vermogensrecht verkrijgt, laat staan of er ten aanzien van de verkregen gebruiksrechten sprake is van koop, huur of een ander type verbintenis. Slechts de toepasselijkheid van Titel 7.1 BW werd in dit arrest bevestigd.

Toen was daar het Europese Hof van Justitie, dat met haar arrest van 3 juli 2012 in de zaak *UsedSoft/Oracle* de handel in tweedehands softwarelicenties mogelijk maakte.[28] Het Hof van Justitie heeft zich er daarbij niet om de 'ravage' die zij daarmee heeft aangericht in het Nederlandse vermogensrecht bekommerd. Door een software-exemplaar beschikbaar te stellen aan een koper (door middel van een download), die op zijn beurt een eeuwigdurende licentie verkrijgt en waarvoor hij een billijke vergoeding heeft betaald, krijgt laatstgenoemde impliciet het eigendomsrecht op dat digitale software-exemplaar in zijn schoot geworpen. Het Hof van Justitie legt de uitputtingsleer zo uit dat deze zowel geldt voor levering van software op een fysieke drager als voor software die wordt gedownload. Op deze manier wordt de online- met de offlinewereld gelijkgesteld. Dit leek een stap in de goede richting, aangezien deze recht doet aan de digitalisering van onze informatiemaatschappij. Maar daarna bleef het stil...

Niet te vergeten zijn daarnaast intellectuele eigendomsrechten als het auteursrecht en het databankenrecht, welke rechten (dan weer) wel onderwerp zijn van Europese harmonisatie. Data kan immers auteursrechtelijk beschermd zijn (mits een eigen oorspronkelijk karakter en persoonlijk stempel van de maker) of er kan een databankenrecht op rusten (mits verkregen door substantiële investering). Dergelijke rechten geven de rechthebbende een exclusieve 'bevoegdheid' die data te gebruiken en daaruit (commercieel) voordeel te genieten, met uitsluiting van ieder ander. Het zijn geen rechten om (die ene unieke kopie van) die data op te eisen.

Een Europees geharmoniseerde aanspraak op data is er dus niet. Het blijft een zeer omstreden gebied, zo signaleert Tjong Tjin Tai.[29] Volgens hem wijst de praktijk wel in de richting van een eigendomsrechtelijke benadering van data, maar blijft de behoefte aan regulatie bestaan. Ook is verdere doordenking van deze benadering noodzakelijk, ten behoeve van bijvoorbeeld revindicatie, verpanding en beslag. Deze zouden deels met flexibele toepassing van het onrechtmatige-daadsrecht of andere rechtsfiguren kunnen worden aangepakt. Legio van zulke vraagstukken en onbillijke situaties zullen zich aandienen.

6. Conclusie

De onderhavige verordening moet een belangrijke bijdrage leveren aan de Europese data economie. De verordening verbiedt ongerechtvaardigde datalocatie-eisen ingesteld door lidstaten. In Nederland heeft de verordening weinig impact; in sommige andere Europese landen meer.

Het opheffen van datalocatie-eisen klinkt in beginsel dan ook positief, maar wat als die goedkopere clouddienst leverancier in Oost-Europa failliet gaat? Wat zegt het nationale recht van dat land dan

2017 (1)C-434/16, *Peter Nowak / Data Protection Commissioner.*

25. Lezenswaardig: Purtova, Nadezhda, *The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law* (September 9, 2017). Available at SSRN: https://ssrn.com/abstract=3036355.
26. HR 31 januari 2012, LJN BQ9251.
27. HR 27 april 2012, ECLI:NL:HR:2012:BV1301, *JBPR* 2012/43 m.nt. mr. drs. B.T.M. van der Wiel (*De Beeldbrigade/X*).
28. HvJEU 3 juli 2012, zaak C-128/11 (*UsedSoft/Oracle International*).
29. TjongTjin Tai, E. (2015). 'Data in het vermogensrecht'. *WPNR*, 149(7085), p. 993-998.

over de 'eigendom' of toegankelijkheid van die data in geval van faillissement? Mogelijk wat anders dan wat de Nederlandse wet (niet) zegt. En als je al grip kan krijgen op je data, in welk format? Kunnen die branchespecifieke gedragscodes voor portabiliteit hiervoor ook aan een oplossing bijdragen? Genoeg belangrijke(re) vraagstukken dus waar de EC zich in het kader van haar DSM-strategie over zou mogen (moeten) buigen.