EUROPESE
COMMISSIE

Brussel, 10.1.2017
COM(2017) 9 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

"BOUWEN AAN EEN EUROPESE DATA-ECONOMIE"

{SWD(2017) 2 final}

"BOUWEN AAN EEN EUROPESE DATA-ECONOMIE"

1. INLEIDING

Gegevens zijn uitgegroeid tot een essentiële motor van economische groei, werkgelegenheid en maatschappelijke vooruitgang. Gegevensanalyse vergemakkelijkt de optimalisering van processen en besluiten, innovatie en de voorspelling van toekomstige gebeurtenissen. Deze wereldwijde tendens heeft een enorm potentieel op diverse gebieden, variërend van gezondheid, milieu, voedselveiligheid, klimaat en hulpbronefficiëntie tot energie, intelligente vervoerssystemen en slimme steden.

De "data-economie"[1] wordt gekenmerkt door een ecosysteem van verschillende soorten marktspelers — zoals fabrikanten, onderzoekers en leveranciers van infrastructuur — die er samen voor zorgen dat gegevens toegankelijk en bruikbaar zijn. De marktspelers kunnen waarde putten uit deze gegevens door een breed gamma aan applicaties te creëren die een groot potentieel hebben om het dagelijkse leven te verbeteren (bv. verkeersbeheer, optimalisering van oogsten of gezondheidszorg op afstand).

In een studie uit 2014 werd de waarde van de Europese data-economie geraamd op 257 miljard euro, wat overeenkomt met 1,85 % van het bbp van de EU[2]. In 2015 was deze markt gegroeid tot 272 miljard euro, 1,87 % van het bbp van de EU (een groei van 5,6 % op één jaar tijd). In die studie wordt ook voorspeld dat de waarde zal stijgen tot 643 miljard euro in 2020, ofwel 3,17 % van het totale bbp van de EU, op voorwaarde dat tijdig de nodig beleidsmatige en juridische randvoorwaarden worden gecreëerd.

Krachtens de algemene verordening gegevensbescherming[3] zal vanaf mei 2018 in de hele Unie één reeks van regels van toepassing zijn, in tegenstelling tot de huidige 28 nationale wetgevingen. Het nieuwe één-loketmechanisme[4] zal ervoor zorgen dat één gegevensbeschermingsautoriteit verantwoordelijk is voor het toezicht op grensoverschrijdende gegevensverwerking door een bedrijf in de EU. De coherente interpretatie van de nieuwe regels wordt gegarandeerd. Met name in grensoverschrijdende gevallen waarbij diverse nationale

---

1 De data-economie meet het algemene effect van de data-markt - d.w.z. de markt waar digitale gegevens worden verhandeld in de vorm van producten of diensten die zijn afgeleid van ruwe gegevens - op de economie als geheel. Dit omvat de productie, vergaring, opslag, verwerking, verspreiding, analyse, ontwikkeling, levering en exploitatie van gegevens die tot stand zijn gekomen door digitale technologieën (European Data Market Study, SMART 2013/0063, IDC, 2016).

2 European Data Market Study, SMART 2013/0063, IDC, 2016.

3 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/56/EG (algemene verordening gegevensbescherming), PB L 119 van 4.5.2016, blz. 1.

4 Artikel 56 van de algemene verordening gegevensbescherming.

gegevensbeschermingsautoriteiten zijn betrokken, wordt één besluit genomen om te garanderen dat gemeenschappelijke oplossingen worden gevonden voor gemeenschappelijke problemen. De algemene verordening gegevensbescherming zorgt voorts ook voor een gelijk speelveld tussen bedrijven uit de EU en bedrijven van buiten de EU; bedrijven van buiten de EU zullen dezelfde regels moeten toepassen als Europese bedrijven wanneer zij goederen en diensten aanbieden of het gedrag van personen in de EU monitoren. Een toename van het consumentenvertrouwen zal ten goede komen van commerciële marktdeelnemers uit de EU en daarbuiten.

De e-privacyrichtlijn heeft betrekking op de vertrouwelijkheid van elektronische communicatiediensten in de EU. De herziene e-privacyrichtlijn, die samen met deze mededeling wordt voorgesteld in de vorm van een verordening[5], streeft naar een hoge mate van bescherming, in volledige samenhang met de verordening gegevensbescherming. Krachtige regels inzake gegevensbescherming creëren het vertrouwen dat nodig is voor de ontwikkeling van de digitale economie in de gehele interne markt.

Zoals voorzitter Juncker op 14 september 2016 heeft benadrukt in zijn rede over de toestand van de Europese Unie: *"Europeaan zijn betekent dat u recht heeft op de bescherming van uw persoonsgegevens door middel van krachtige Europese wetten. Want Europeanen houden er niet van als al hun bewegingen door overvliegende drones worden geregistreerd, of als ondernemingen elke muisklik opslaan. Daarom hebben het Parlement, de Raad en de Commissie in mei dit jaar overeenstemming bereikt over een gemeenschappelijke Europese verordening inzake gegevensbescherming. Het betreft een strenge Europese wet die van toepassing is op ondernemingen ongeacht waar zij gevestigd zijn en telkens wanneer zij uw gegevens verwerken. Want privacy doet ertoe in Europa. Het is een kwestie van menselijke waardigheid*."

In haar mededeling uit 2012 "Privacywaarborging in het online tijdperk – Een Europees gegevensbeschermingskader voor de 21e eeuw"[6] en haar mededeling uit 2014 "Naar een bloeiende data-economie"[7] heeft de Commissie erkend dat moderne, coherente regels in de hele EU noodzakelijk zijn om gegevens vrij te laten stromen van de ene lidstaat naar de andere, dat de Europese digitale economie traag was in het omarmen van de datarevolutie in vergelijking met de VS, en dat het haar ook aan vergelijkbare industriële capaciteiten ontbeerde. Zij kwam tot de slotsom dat het ontbreken van een rechtskader dat is aangepast aan de handel in gegevens in de EU er mogelijk toe bijdroeg dat de toegang tot grote gegevensreeksen ontoereikend is, dat nieuwe marktdeelnemers moeilijk toegang krijgen tot de markt en dat innovatie in de kiem wordt gesmoord.

Ongerechtvaardigde **beperkingen op het vrije verkeer van gegevens** zullen waarschijnlijk een rem zetten op de ontwikkeling van de data-economie in de EU. Deze beperkingen vloeien voort uit eisen van overheden aangaande de locatie waar gegevens mogen worden opgeslagen of verwerkt. De kwestie van het vrije verkeer van gegevens heeft betrekking op alle types gegevens: ondernemingen en spelers in de data-economie werken met industriële en door machines voortgebrachte gegevens, al dan niet

5 COM(2017) 10.

6 COM(2012) 9.

7 COM(2014) 442.

persoonsgegevens, en met gegevens die ontstaan door menselijke activiteiten. In de strategie voor de digitale eengemaakte markt heeft de Commissie aangekondigd dat zij een initiatief zal voorstellen om beperkingen op het vrije verkeer van gegevens om andere redenen dan de bescherming van persoonsgegevens in de EU aan te pakken, en om ongefundeerde beperkingen op de locatie waar gegevens mogen worden opgeslagen of verwerkt op te heffen. Tot dergelijke beperkingen behoren rechtshandelingen die door de lidstaten zijn vastgesteld en administratieve voorschriften en praktijken die hetzelfde effect hebben. Naarmate de data-economie groeit, neemt ook het aantal beperkingen toe, waardoor onzekerheid ontstaat over de plaats waar gegevens mogen worden opgeslagen of verwerkt. Dit kan gevolgen hebben voor alle sectoren van de economie, en voor zowel particuliere als openbare organisaties, die moeilijkheden kunnen ondervinden om toegang te krijgen tot innovatievere en/of goedkopere datadiensten. Ongerechtvaardigde beperkingen inzake gegevenslokalisatie zijn in strijd met de in het Verdrag vastgelegde vrijheid van dienstverlening en vrijheid van vestiging, en met de relevante secundaire wetgeving. Zij kunnen leiden tot versnippering van de markt, waardoor de kwaliteit van de dienstverlening voor de gebruikers en het concurrentievermogen van de dienstverleners, met name kleinere entiteiten, afneemt.

Ongerechtvaardigde beperkingen inzake gegevenslokalisatie komt ook aan bod in de besprekingen tussen de EU en haar handelspartners, gezien het toenemende belang van gegevens en gegevensdiensten in de wereldeconomie en de mogelijke houding van derde landen ten aanzien van deze kwestie. In het kader van vrijhandelsovereenkomsten kan niet worden onderhandeld over de EU-voorschriften inzake gegevensbescherming. Zoals uiteengezet in de mededeling over de uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld[8] moet het overleg over gegevensbescherming los staan van handelsbesprekingen met derde landen. Zoals aangegeven in de mededeling "Handel voor iedereen"[9] zal de Commissie vervolgens trachten gebruik te maken van EU-vrijhandelsovereenkomsten om regels op te stellen voor e-handel en grensoverschrijdende gegevensstromen en om nieuwe vormen van digitaal protectionisme te bestrijden, volledig in overeenstemming met en onverminderd de Europese regelgeving inzake gegevensbescherming.

Naarmate de datagestuurde transformatie verder doordringt in de economie en de samenleving worden steeds grotere hoeveelheden gegevens voortgebracht door machines of processen, op basis van ontluikende technologieën zoals het internet van de dingen (Internet of Things, IoT), fabrieken van de toekomst en autonome geconnecteerde systemen. Connectiviteit zelf verandert de manier waarop gegevens kunnen worden geraadpleegd: gegevens die vroeger meestal toegankelijk waren via fysieke verbindingen worden nu steeds meer op afstand geraadpleegd. De enorme verscheidenheid van gegevensbronnen en -types, en de ruime mogelijkheden om op tal van domeinen, waaronder ook de ontwikkeling van openbaar beleid, inzichten te verwerven op basis van gegevens, worden nu pas duidelijk. Om deze kansen te kunnen benutten, moeten zowel publieke als private spelers op de gegevensmarkt toegang hebben tot grote en diverse gegevensreeksen. De vragen met betrekking tot de toegankelijkheid en overbrenging van de gegevens die worden voortgebracht door deze machines of processen zijn dan ook

[8] COM(2017) 7.

[9] COM(2015) 497.

cruciaal voor het ontstaan van een data-economie en moeten zorgvuldig worden geanalyseerd.

Dit doet ook andere vragen rijzen, onder meer over de toepassing van de aansprakelijkheidsregels voor schade ten gevolge van een defect in een geconnecteerd toestel of een robot, en over de meeneembaarheid en interoperabiliteit van gegevens. Nieuwe technologieën zoals het internet van de dingen of robotica geven aanleiding tot complexe en gesofisticeerde onderlinge interdependenties, zowel binnen producten (op basis van hardware en software) als tussen gekoppelde systemen. Er kunnen ook nieuwe problemen ontstaan omdat het onverwachte en onbedoelde gedrag van autonome machines schade kan toebrengen aan personen en voorwerpen. Deze verschijnselen kunnen leiden tot rechtsonzekerheid met betrekking tot de toepassing van het bestaande kader inzake aansprakelijkheid en veiligheid.

Zoals aangekondigd in de strategie voor de digitale eengemaakte markt, streeft de Commissie naar een duidelijk en aangepast beleids- en rechtskader voor de data-economie; om dit te bereiken zal zij de resterende belemmeringen voor het vrije verkeer van gegevens uit de weg ruimen en de juridische onzekerheid die ontstaan is door nieuwe technologieën aanpakken. Voorts heeft deze mededeling tot doel de beschikbaarheid en het gebruik van gegevens te doen toenemen, nieuwe op gegevens gebaseerde bedrijfsmodellen aan te moedigen, de voorwaarden voor toegang tot gegevens te verbeteren en gegevensanalyse te ontwikkelen in de EU. De Commissie stelt dan ook duidelijk afgebakende discussiepunten voor, teneinde te "bouwen aan een Europese data-economie".

In deze mededeling wordt daarom nader ingegaan op de volgende punten: vrije gegevensstroom; toegankelijkheid en overbrenging van gegevens die door machines zijn voortgebracht; aansprakelijkheid en veiligheid in de context van opkomende technologieën; en meeneembaarheid van niet-persoonsgebonden gegevens, interoperabiliteit en normen. Deze mededeling bevat ook suggesties voor experimenten met gemeenschappelijke regelgevende oplossingen in reële omstandigheden.

De Commissie start een brede dialoog met de belanghebbenden over de vraagstukken die in deze mededeling worden onderzocht. De eerste stap van deze dialoog is een openbare raadpleging, die parallel met het pakket inzake de data-economie wordt opgestart[10].

2. VRIJ VERKEER VAN GEGEVENS

Voor een goed werkende en dynamische data-economie moeten gegevens vrij en beveiligd kunnen stromen in de interne markt. In een snel veranderende technologische context is veilig en betrouwbaar verkeer van gegevens cruciaal voor de bescherming van de vier fundamentele vrijheden van de interne markt van de EU die in de Verdragen zijn neergelegd (vrij verkeer van goederen, werknemers, diensten en kapitaal). Datadiensten groeien sterk in de EU en de rest van de wereld. Een doeltreffende interne markt zonder barrières zou in deze sector grote mogelijkheden creëren voor extra groei en banen.

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

Deze groei en innovatie in de data-economie en de tenuitvoerlegging van grensoverschrijdende openbare diensten kunnen in het gedrang worden gebracht door belemmeringen voor het vrije verkeer van gegevens in de EU, zoals ongerechtvaardigde eisen van openbare instanties inzake gegevenslokalisatie. Maatregelen met betrekking tot gegevenslokalisatie komen neer op de herinvoering van digitale "grenscontroles"[11]. Ze variëren van toezichthoudende instanties die financiële dienstverleners verplichten hun gegevens lokaal op te slaan tot de toepassing van regels inzake het beroepsgeheim, die erop neerkomen dat gegevens lokaal moeten worden opgeslagen of verwerkt, en ingrijpende regelgeving waarbij het vereist is dat gearchiveerde door de overheidssector voortgebrachte gegevens lokaal worden opgeslagen, ongeacht hun gevoeligheid.

Bezorgdheid over privacy is terecht, maar mag niet door overheidsinstanties worden gebruikt als reden om het vrije verkeer van gegevens op een ongerechtvaardigde manier te beperken. Zoals hierboven is uiteengezet, voorziet de algemene verordening gegevensbescherming in één reeks regels met een hoog niveau van bescherming van persoonsgegevens in de hele EU. Ze versterkt het vertrouwen van de consument in onlinediensten, en zorgt voor een eenvormige toepassing van de regels in alle lidstaten via sterkere nationale gegevensbeschermingsautoriteiten. De verordening bevordert het noodzakelijke vertrouwen in gegevensverwerking en vormt de grondslag voor het vrije verkeer van persoonsgegevens in de EU. De verordening verbiedt beperkingen op het vrije verkeer van persoonsgegevens in de Unie indien deze gebaseerd zijn op redenen die verband houden met de bescherming van persoonsgegevens[12]. Beperkingen om andere redenen dan de bescherming van persoonsgegevens, om redenen die te maken hebben met belasting- of boekhoudwetgeving, vallen niet onder de verordening. Niet-persoonsgebonden gegevens, d.w.z. gegevens die geen verband houden met een geïdentificeerde of identificeerbare natuurlijke persoon[13], blijven buiten het toepassingsgebied van de algemene verordening gegevensbescherming en kunnen bijvoorbeeld betrekking hebben op niet-persoonsgeboden gegevens die zijn voortgebracht door machines.

Beperkingen met betrekking tot de locatie van gegevens kunnen voortvloeien uit wettelijke bepalingen of bestuurlijke richtsnoeren of praktijken die vereisen dat de opslag of verwerking van gegevens[14] in een elektronisch formaat[15] plaatsvindt binnen een bepaald geografisch gebied of een bepaalde jurisdictie. Soms leggen de lidstaten beperkingen op omdat zij ervan overtuigd zijn dat toezichthoudende autoriteiten lokaal opgeslagen gegevens gemakkelijker kunnen controleren. Men gaat er ook van uit dat

---

11 OESO, "Emerging Policy Issues: Localisation Barriers to Trade", 2015 en lopende werkzaamheden.

12 Artikel 1, lid 3. Een dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk wordt gemaakt voor het publiek, vormt ten aanzien van die aanbieder bijvoorbeeld een persoonsgegeven in de zin van voormelde bepaling wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust. Zie het arrest in zaak C-582/14, Breyer, ECLI:EU:C:2016:779, punt 49.

13 Zoals gedefinieerd in artikel 4, lid 1, van de algemene verordening gegevensbescherming.

14 Zowel particuliere als openbare gegevens.

15 Met inbegrip van kopieën van gegevensreeksen.

lokalisatie garanties biedt op het gebied van privacy, controle, rechtshandhaving en beveiliging van gegevens. In de praktijk dragen deze maatregelen echter zelden bij tot de verwezenlijking van de beoogde doelstellingen.

Behalve de plaats waar de gegevens fysiek zijn opgeslagen, is informatiebeveiliging ook afhankelijk van een reeks andere factoren, zoals de handhaving van de vertrouwelijkheid en integriteit wanneer de gegevens buiten de opslagplaats beschikbaar zijn. Veilige opslag en verwerking van gegevens is dus niet zozeer afhankelijk van beperkingen met betrekking tot de plaats waar de gegevens worden opgeslagen en verwerkt, maar eerder van state-of-the-art ict-beheer op een veel grotere schaal dan individuele systemen. Om gegevens te beveiligen tegen lokale natuurrampen of cyberaanvallen kunnen installaties voor gegevensopslag in verschillende lidstaten dienst doen als back-up voor elkaar en gebruik maken van de technische en organisatorische maatregelen waarin de richtlijn betreffende de beveiliging van netwerk- en informatiesystemen[16] (de NIB-richtlijn) voorziet. Bovendien kan de beschikbaarheid van gegevens voor regelgevende of toezichthoudende taken, die geenszins in vraag wordt gesteld, beter worden gegarandeerd door de samenwerking tussen nationale autoriteiten of tussen deze autoriteiten en de particuliere sector te versterken, dan door beperkingen met betrekking tot gegevenslokalisatie. Op domeinen die worden gekenmerkt door nauwe samenwerking tussen toezichthoudende autoriteiten, zoals financiële diensten, zouden eisen inzake gegevenslokalisatie contraproductief kunnen zijn[17].

In bepaalde omstandigheden of met betrekking tot bepaalde gegevens kunnen eisen inzake gegevenslokalisatie echter gerechtvaardigd en evenredig zijn, met name vóór effectieve regelingen voor grensoverschrijdende samenwerking zijn vastgesteld, teneinde te garanderen dat bepaalde gegevens over kritieke energie-infrastructuur veilig worden behandeld, dat elektronisch bewijsmateriaal (bijv. lokale kopieën van gegevensreeksen) beschikbaar zijn voor rechtshandhavingsinstanties, of dat gegevens in bepaalde openbare registers lokaal worden opgeslagen.

Helaas bestaat er zowel in Europa als wereldwijd een tendens naar gegevenslokalisatie, een aanpak die vaak gebaseerd is op de misvatting dat lokale diensten automatisch veiliger zijn dan grensoverschrijdende diensten. Bovendien wordt de markt voor datadiensten sterk beïnvloed door een gebrek aan duidelijke regels en een sterke overtuiging van de noodzaak om gegevens lokaal op te slaan. Dit kan de toegang van bedrijven en organisaties uit de publieke sector tot goedkopere en innovatievere datadiensten beperken, of ondernemingen die over de grenzen heen actief zijn, dwingen om te veel gegevensopslag- en verwerkingscapaciteit te voorzien. Hierdoor kunnen datagestuurde bedrijven, met name start-ups en het mkb, worden verhinderd om hun activiteiten uit te breiden, nieuwe markten te betreden (bijv. omdat zij moeten investeren

[16] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, PB L 194 van 19.7.2016, blz. 1.

[17] Een aantal EU-bepalingen inzake financiële diensten en het Europese systeem voor financieel toezicht vereisen dat toezichthouders toegang hebben tot gegevens van financiële instellingen en transacties op het volledige grondgebied van de EU. De verplichting om gegevens op te slaan op het grondgebied van een bepaalde lidstaat of voorwaarden voor de toegang van toezichthouders tot administratieve procedures kunnen tot gevolg hebben dat toezichthoudende instanties slechts beperkt toegang hebben tot gegevens die zij nodig hebben voor de uitvoering van hun mandaat.

in datacentra in 28 lidstaten) of gegevens- en analysecapaciteit te centraliseren voor de ontwikkeling van nieuwe producten en diensten.

Momenteel wordt aan 84 % van de vraag naar "ict-gerelateerde" diensten (consulting, hosting, ontwikkeling) voldaan vanuit de EU zelf. Indien het gemakkelijker zou worden om deze diensten grensoverschrijdend aan te bieden in de EU, door het opheffen van beperkingen inzake gegevenslokalisatie, zou het bbp tot 8 miljard euro per jaar toenemen dankzij de kostenbesparingen en efficiëntiewinsten[18].

Eisen inzake gegevenslokalisatie vormen ook een belemmering voor een ruimer gebruik van opslag en rekenkracht in de cloud. Dit zou ook bredere maatschappelijke gevolgen kunnen hebben. Een efficiënter gebruik van it-middelen zou er inderdaad kunnen toe bijdragen dat het energieverbruik en de koolstofemissies netto met 30 % of meer afnemen. Een klein bedrijf dat overstapt naar de cloud kan zijn energieverbruik en koolstofemissies met meer dan 90 % terugdringen door zijn bedrijfsapplicaties in de cloud te laten draaien in plaats van op eigen infrastructuur. Wereldwijd wordt verwacht dat de markt voor energie-efficiënte datacentra tegen eind 2020 zal groeien tot bijna 90 miljard euro. Een versnipperde markt voor gegevensdiensten zou verhinderen dat deze energie-efficiëntere diensten volledig tot ontwikkeling komen in de EU en zou ook de investeringsbereidheid in het gedrang brengen.

Om de bovenvermelde problemen en beperkingen aan te pakken en het potentieel van de Europese data-economie volledig te benutten, moeten alle maatregelen van de lidstaten die gevolgen hebben voor de opslag of verwerking van gegevens gebaseerd zijn op het "**beginsel van vrij verkeer van gegevens in de EU**", als gevolg van de verplichtingen van de lidstaten in het kader van de Verdragsbepalingen inzake vrij verkeer van diensten en vrijheid van vestiging en relevante secundaire wetgeving. Nieuwe beperkingen met betrekking tot de plaats waar gegevens mogen worden opgeslagen en verwerkt, moeten zorgvuldig worden gerechtvaardigd op grond van het Verdrag en de toepasselijke secundaire wetgeving teneinde te kunnen nagaan of zij noodzakelijk en evenredig zijn om een dwingende doelstelling van algemeen belang, zoals openbare veiligheid, te verwezenlijken[19].

Het beginsel van vrij verkeer van persoonsgegevens[20], dat is vastgelegd in primaire en secundaire wetgeving, moet ook van toepassing zijn in de gevallen waarin de algemene verordening gegevensbescherming de lidstaten toestaat om specifieke kwesties zelf te regelen. De lidstaten moeten worden aangemoedigd om geen gebruik te maken van de

---

18 "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", ECIPE, 2016, berekening gebaseerd op toegenomen concurrentiedruk in een "industriële" digitale eengemaakte markt met volledige prijstransparantie.

19 Rekening houdend met het feit dat uitzonderingen op het Verdrag restrictief moeten worden uitgelegd. Deze secundaire wetgeving omvat de algemene verordening gegevensbescherming, Richtlijn 2000/31/EG (de richtlijn e-handel), Richtlijn 2006/123/EG (de dienstenrichtlijn) en, wat de ontwerpen voor technische voorschriften en ontwerpregels betreffende de diensten van de informatiemaatschappij betreft, Richtlijn 2015/1535 (de transparantierichtlijn).

20 Het vrij verkeer van persoonsgegevens is vervat in artikel 16 van het Verdrag betreffende de werking van de Europese Unie, en de voorschriften inzake het vrij verkeer van persoonsgegevens zijn vastgelegd in de huidige en toekomstige EU-wetgeving inzake gegevensbescherming. In artikel 1, lid 3, van de algemene verordening gegevensbescherming is als volgt bepaald: "Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens."

open clausules in de algemene verordening gegevensbescherming om het vrije verkeer van gegevens verder te beperken.

In zijn conclusies van 15 december 2016 heeft de Europese Raad opgeroepen tot het opheffen van de resterende belemmeringen in de interne markt, met inbegrip van belemmeringen voor het vrij verkeer van gegevens[21].

Met het oog op de toepassing van het beginsel van vrij verkeer van gegevens zal de Commissie de volgende twee maatregelen nemen:

- Na de bekendmaking van deze mededeling zal de Commissie gestructureerd overleg plegen met de lidstaten en andere belanghebbenden over de rechtvaardiging voor en de evenredigheid van maatregelen inzake gegevenslokalisering, waarbij de tot dusver door de Commissie geconstateerde beperkingen als uitgangspunt worden genomen.

- Naar aanleiding van de resultaten van dit overleg en de verdere bewijzen die zijn verzameld over de omvang en de aard van de beperkingen inzake gegevenslokalisering en de gevolgen daarvan, met name voor het mkb en startende ondernemingen, onder meer via de bijgaande openbare raadpleging, zal de Commissie indien nodig inbreukprocedures inleiden tegen ongerechtvaardigde of onevenredige eisen inzake de plaats waar gegevens mogen worden opgeslagen of verwerkt en zal zij, indien nodig, verdere maatregelen nemen met betrekking tot het vrije verkeer van gegevens. In deze context worden alle eventuele vervolgmaatregelen ondernomen in overeenstemming met de beginselen van betere regelgeving.

3. TOEGANKELIJKHEID EN OVERBRENGING VAN GEGEVENS

Steeds meer gegevens worden voortgebracht door machines of processen op basis van nieuwe technologieën, zoals het internet van de dingen. Deze gegevens worden steeds vaker gebruikt als essentieel onderdeel van nieuwe, innovatieve diensten, teneinde producten of productieprocessen te verbeteren en de besluitvorming te ondersteunen.

De diversiteit van de gegevens die worden voortgebracht door deze machines of processen biedt zeer veel mogelijkheden voor spelers in de datamarkt om te innoveren en inzichten te verwerven op basis van deze gegevens. De gegevens die worden geregistreerd door sensoren in moderne boerderijen kunnen bijvoorbeeld worden gebruikt om een applicatie te ontwikkelen om de oogst te optimaliseren, of de gegevens die worden voortgebracht door sensoren in verkeerslichten kunnen worden gebruikt om een applicatie voor verkeersbeheer of route-optimalisering te ontwikkelen.

Om zoveel mogelijk waarde uit dit type gegevens te halen, moeten marktdeelnemers toegang hebben tot grote en diverse gegevensreeksen. Dit wordt echter bemoeilijkt wanneer de voortbrengers van de gegevens deze voor zichzelf houden; dit heeft tot gevolg dat de gegevens op geïsoleerde wijze worden geanalyseerd. De vragen met betrekking tot de toegankelijkheid en overbrenging van ruwe gegevens (gegevens die niet

[21] http://www.consilium.europa.eu/nl/press/press-releases/2016/12/15-euco-conclusions-final/

zijn verwerkt of gewijzigd sinds ze zijn opgeslagen) die worden voortgebracht door deze machines of processen zijn dan ook cruciaal voor het ontstaan van een data-economie en moeten zorgvuldig worden beoordeeld.

Het probleem van de toegankelijkheid van gegevens die door machines zijn voorgebracht staat op de agenda in verscheidene sectoren, zoals vervoer, energiemarkten, slimme woningen en de gezondheids- en zorgsector.

Alvorens in te gaan op de huidige situatie op het gebied van de toegankelijkheid van gegevens in de EU, is het belangrijk te verduidelijken om welke soorten gegevens het gaat.

3.1. Soorten gegevens

In het algemeen wordt een onderscheid gemaakt tussen persoonsgegevens en niet-persoonsgebonden gegevens. Zo kunnen gegevens die zijn verkregen door temperatuursensoren in huizen persoonsgegevens zijn als ze in verband kunnen worden gebracht met een levende persoon, terwijl gegevens over bodemvochtigheid niet-persoonsgebonden zijn. Persoonsgegevens kunnen worden omgezet in niet-persoonsgebonden gegevens door ze anoniem te maken. Wanneer gegevens als persoonsgegevens kunnen worden beschouwd[22], is het kader voor gegevensbescherming, met name de algemene verordening gegevensbescherming, van toepassing.

Door machines voortgebrachte gegevens komen tot stand zonder rechtstreekse tussenkomst van een mens, via computerprocessen, applicaties of diensten, of via sensoren die informatie verwerken die ontvangen is van reële of virtuele apparatuur, software of machines.

Door machines voortgebrachte gegevens kunnen persoonsgegevens of niet-persoonsgebonden gegevens zijn. Wanneer door machines voortgebrachte gegevens het mogelijk maken een natuurlijke persoon te identificeren, kunnen ze worden beschouwd als persoonsgegevens. Dit heeft tot gevolg dat alle regels inzake persoonsgegevens van toepassing zijn zolang de gegevens niet volledig anoniem zijn gemaakt (bijv. locatiegegevens van mobiele toepassingen).

De link tussen het vrije verkeer van gegevens en de nieuwe vraagstukken omtrent toegankelijkheid en overbrenging van gegevens wordt gevormd door het feit dat bedrijven en spelers in de data-economie omgaan met zowel persoonsgegevens als niet-persoonsgebonden gegevens, en dat gegevensstromen en gegevensreeksen dus regelmatig uit beide soorten gegevens zullen bestaan. Elke beleidsmaatregel moet rekening houden met deze economische realiteit en met het rechtskader voor de bescherming van persoonsgegevens, met inachtneming van de grondrechten van het individu.

[22] Zoals gedefinieerd in artikel 4, lid 1, van de algemene verordening gegevensbescherming.

3.2. Beperkte toegankelijkheid van gegevens

Om dit ontluikende probleem te kunnen beoordelen, moet eerst worden geanalyseerd hoe bedrijven en andere marktspelers toegang kunnen krijgen tot de grote en diverse gegevensreeksen die nodig zijn in de data-economie.

Uit het beschikbare bewijsmateriaal[23] blijkt dat ondernemingen die over grote hoeveelheden gegevens beschikken doorgaans gebruik maken van interne analysecapaciteit. In de meeste gevallen worden gegevens voortgebracht en geanalyseerd door dezelfde onderneming, en zelfs wanneer de analyse van de gegevens wordt uitbesteed, is het mogelijk dat de gegevens niet opnieuw worden gebruikt. In sommige gevallen houden fabrikanten, ondernemingen die diensten aanbieden of andere marktdeelnemers de door hun machines of via hun producten en diensten voortgebrachte gegevens voor zichzelf, waardoor zij het mogelijke hergebruik van de gegevens op downstreammarkten beperken. Veel ondernemingen trekken geen profijt van of voorzien niet in de mogelijkheid van gebruikersvriendelijke interfaces voor applicatieprogrammering (API's)[24] (waarin wordt aangegeven hoe verschillende applicaties met elkaar interageren), die dienst kunnen doen als veilige toegangspoorten voor nieuw en innovatief gebruik van gegevens van deze ondernemingen.

Kortom, de uitwisseling van gegevens blijft momenteel beperkt. Er ontstaan langzaam datamarkten, maar ze worden nog maar weinig gebruikt. Het is mogelijk dat bedrijven niet over de juiste instrumenten en vaardigheden beschikken om de economische waarde van hun gegevens te kwantificeren, of vrezen dat hun concurrentievoordeel in het gedrang komt of helemaal verdwijnt wanneer gegevens beschikbaar worden voor concurrenten.

3.3. Ruwe door machines voortgebrachte gegevens: juridische situatie op het niveau van de EU en op nationaal niveau

Ruwe door machines voortgebrachte gegevens worden niet beschermd door bestaande intellectuele-eigendomsrechten omdat ze niet als het resultaat van een intellectuele inspanning worden beschouwd en/of niet geacht worden een graad van originaliteit te bezitten. Het recht sui generis van de richtlijn databanken (96/9/EG) — dat makers van databanken het recht verleent om te verhinderen dat de inhoud van een databank of een substantieel deel ervan zonder hun toestemming opgevraagd en/of hergebruikt wordt — biedt alleen bescherming op voorwaarde dat de totstandbrenging van de databank gepaard gaat met een substantiële investering in de verkrijging, controle of presentatie van de inhoud ervan. De onlangs goedgekeurde richtlijn inzake de bescherming van bedrijfsgeheimen (2016/943/EU), die uiterlijk in juni 2018 in nationaal recht moet worden omgezet, biedt bescherming tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken van bedrijfsgeheimen. Gegevens worden alleen als "bedrijfsgeheim" beschouwd wanneer maatregelen zijn genomen om de informatie, die het "intellectuele kapitaal" van het bedrijf vertegenwoordigt, geheim te houden.

---

23 IDC, European Data Market Study, First Interim Report, 2016; Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, First interim report, 2016; conferentie op hoog niveau van het DG CONNECT, 17 oktober 2016.

24 Bijvoorbeeld https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

Onder het recht van verschillende lidstaten kunnen alleen rechtsvorderingen worden toegepast op gegevens wanneer die gegevens voldoen aan specifieke voorwaarden om te kunnen worden beschouwd als, bijvoorbeeld, een intellectuele-eigendomsrecht, een databankrecht of een bedrijfsgeheim. Op het niveau van de EU voldoen ruwe door machines voortgebrachte gegevens meestal echter niet aan de relevante voorwaarden.

Daarom bestaan er op nationaal of EU-niveau momenteel geen uitgebreide beleidskaders voor ruwe door machines voortgebrachte gegevens die geen persoonsgegevens zijn, of voor de voorwaarden voor de economische exploitatie en verhandelbaarheid van die gegevens. Deze kwestie wordt meestal in contracten geregeld. Het gebruik van bestaande instrumenten van het algemene verbintenissenrecht en het mededingingsrecht in de Unie kan een afdoende antwoord bieden. Voorts kunnen vrijwillige of overkoepelende regelingen worden overwogen in bepaalde sectoren. Wanneer de verschillende marktdeelnemers een ongelijke onderhandelingspositie hebben, is het echter mogelijk dat marktgebaseerde oplossingen alleen niet volstaan om eerlijke en innovatievriendelijke resultaten te garanderen, om de toegang voor nieuwe marktdeelnemers te vergemakkelijken en om lock-insituaties te voorkomen.

3.4. Situatie in de praktijk

In sommige gevallen kunnen fabrikanten of dienstverleners de facto "eigenaar" worden van de gegevens die door hun machines of processen worden voortgebracht, zelfs als die machines eigendom zijn van de gebruiker. De facto controle over deze gegevens kan een bron zijn van differentiatie en een concurrentievoordeel opleveren voor de producenten. Dit kan echter problematisch zijn, omdat de gebruiker vaak door de fabrikant wordt verhinderd om de gegevens door een andere partij te laten gebruiken.

Al naargelang de specifieke kenmerken van de markten kunnen de verschillende marktspelers die de gegevens controleren dus profiteren van lacunes in het regelgevingskader of van de hierboven beschreven juridische onzekerheid door oneerlijke standaard-contractvoorwaarden op te leggen aan de gebruikers of via technische middelen, zoals formats waar eigendomsrechten op rusten of encryptie. Sommige lidstaten hebben het toepassingsgebied van de bepalingen inzake consumentenbescherming van de richtlijn betreffende oneerlijke bedingen ook uitgebreid tot B2B-transacties, maar niet allemaal. Dit kan bijvoorbeeld tot gevolg hebben dat gebruikers en bedrijven vastzitten aan exclusieve regelingen voor de exploitatie van gegevens. Het is mogelijk dat in bepaalde contracten sprake is van vrijwillige uitwisseling van gegevens, maar de onderhandelingen over dergelijke contracten kunnen leiden tot aanzienlijke transactiekosten voor de zwakkere partijen wanneer er sprake is van ongelijke onderhandelingsposities of wegens de aanzienlijke kosten voor het inhuren van juridische deskundigheid.

3.5. Een toekomstig EU-kader voor toegang tot gegevens

Sommige lidstaten onderzoeken momenteel of het mogelijk is de toegang tot door machines voortgebrachte gegevens te garanderen; het is mogelijk dat deze lidstaten beslissen deze kwestie zelf te regelen. Het risico bestaat dat een ongecoördineerde aanpak tot versnippering leidt en schadelijk is voor de ontwikkeling van de data-economie in de EU en de werking van grensoverschrijdende datadiensten en -technologieën in de interne markt.

De Commissie is dan ook voornemens overleg op te starten met de lidstaten en andere belanghebbenden om na te gaan of het mogelijk is in de toekomst een EU-kader betreffende de toegankelijkheid van gegevens op te zetten. De Commissie is van mening dat dit overleg betrekking moet hebben op de meest doeltreffende manieren om de volgende doelstellingen te verwezenlijken:

- **De toegang tot anonieme door machines voortgebrachte gegevens verbeteren**: Door het delen, hergebruiken en samenvoegen van door machines voortgebrachte gegevens, worden deze gegevens een bron van waardecreatie, innovatie en diversiteit van bedrijfsmodellen[25].

- **De uitwisseling van dergelijke gegevens vergemakkelijken en stimuleren**: Een toekomstige oplossing moet de effectieve toegang tot gegevens bevorderen, rekening houdend met, bijvoorbeeld, eventuele verschillen in onderhandelingspositie tussen marktspelers.

- **Investeringen en activa beschermen**: Een toekomstige oplossing moet ook rekening houden met de rechtmatige belangen van marktspelers die investeren in productontwikkeling, zorgen voor een eerlijk rendement op hun investeringen en aldus bijdragen tot innovatie. Tegelijkertijd moet de toekomstige oplossing zorgen voor een eerlijke verdeling van de baten tussen houders van gegevens[26], verwerkers en aanbieders van applicaties binnen waardeketens.

- **Voorkomen dat vertrouwelijke gegevens worden bekendgemaakt**: Een toekomstige oplossing moet het risico op bekendmaking van vertrouwelijke gegevens, met name aan bestaande of potentiële concurrenten, beperken. In dit verband moet de oplossing het ook mogelijk maken dat een correcte classificatie wordt uitgevoerd, voorafgaand aan de beoordeling of bepaalde gegevens mogen worden gedeeld.

- **Lock-in-effecten tot een minimum beperken**: De ongelijke onderhandelingspositie van bedrijven en particulieren moet in aanmerking worden genomen. Lock-in-situaties, in het bijzonder voor het mkb en starters, moeten worden vermeden.

De Commissie is voornemens om in de gesprekken met belanghebbenden de volgende opties te bespreken om het probleem van de toegankelijkheid van door machines voortgebrachte gegevens op te lossen; deze opties verschillen wat betreft hun niveau van interventie:

- **Richtsnoeren over de wijze waarop bedrijven kunnen worden gestimuleerd om gegevens te delen**: Om de gevolgen van uiteenlopende nationale regelgevingen te beperken en meer rechtszekerheid te bieden aan ondernemingen, kan de Commissie richtsnoeren opstellen over de wijze waarop de zeggenschapsrechten over niet-persoonsgebonden gegevens in contracten moeten worden aangepakt. Deze richtsnoeren zullen gebaseerd zijn op bestaande wetgeving, met name de eisen inzake transparantie en eerlijkheid die zijn

[25] Als het om persoonsgegevens gaat, is de algemene verordening gegevensbescherming van toepassing.

[26] De entiteit die de door machines voortgebrachte gegevens in de praktijk beheert en bewaart.

vastgesteld in de marketing- en consumentenwetgeving van de EU, de richtlijn inzake bedrijfsgeheimen en de wetgeving inzake auteursrechten, met name de richtlijn databanken. De Commissie is voornemens om de richtlijn databanken in 2017 te evalueren.

- **De ontwikkeling stimuleren van technische oplossingen voor betrouwbare identificatie en uitwisseling van gegevens**: Traceerbaarheid en duidelijke identificatie van gegevensbronnen zijn een eerste vereiste voor echte controle van gegevens op de markt. De vaststelling van betrouwbare en zo mogelijk gestandaardiseerde protocollen voor continue identificatie van gegevensbronnen kan nodig zijn om vertrouwen in het systeem tot stand te brengen. Application Programming Interfaces (API's) kunnen eveneens bijdragen tot het creëren van een ecosysteem van applicatie- en algoritmeontwikkelaars die geïnteresseerd zijn in de gegevens die bedrijven in hun bezit hebben. API's kunnen ondernemingen en openbare instanties helpen om verschillende soorten hergebruik van de gegevens waarover zij beschikken te identificeren en er profijt van te trekken. Op basis hiervan kan een breder gebruik van open, gestandaardiseerde en goed gedocumenteerde API's worden overwogen, via technische richtsnoeren, met inbegrip van de vaststelling en verspreiding van beste praktijken voor bedrijven en openbare organen. Hierbij kan het gaan om gegevens die ter beschikking worden gesteld in machineleesbare formaten en de levering van bijbehorende metagegevens.

- **Standaard-contractvoorschriften**: Standaardvoorschriften kunnen een beschrijving bevatten van een evenwichtige benchmarkoplossing voor contracten met betrekking tot gegevens, met inachtneming van de lopende geschiktheidscontrole van de algemene werking van de richtlijn inzake oneerlijke bedingen in overeenkomsten. Zij kunnen worden gekoppeld aan de invoering van een oneerlijkheidstoets in B2B-contractrelaties[27] die zou leiden tot het ongeldig verklaren van contractbepalingen die buitensporig afwijken van de standaardvoorschriften. Zij kunnen ook worden aangevuld met een reeks aanbevolen standaardcontractbepalingen die zijn ontworpen door de belanghebbenden. Deze aanpak kan de juridische belemmeringen voor kleine bedrijven doen afnemen en het onevenwicht in de onderhandelingsposities verkleinen, met behoud van een grote mate van contractuele vrijheid.

- **Toegang om redenen van openbaar belang en voor wetenschappelijke doeleinden**: Openbare instanties kunnen toegang krijgen tot gegevens als dit in het "algemeen belang" is en de werking van de overheidsdiensten aanzienlijk zou verbeteren; voorbeelden hiervan zijn de toegang tot bedrijfsgegevens door statistische bureaus of de optimalisering van verkeersbeheersystemen op basis van real-timegegevens van particuliere voertuigen. Toegang tot bedrijfsgegevens door statistische instanties zal meestal tot gevolg hebben dat de marktdeelnemers zelf minder statistische gegevens moeten rapporteren. De toegang tot gegevens uit verschillende bronnen en de mogelijkheid om die gegevens te combineren is ook van cruciaal belang voor wetenschappelijk onderzoek op gebieden zoals medische, sociale en ecologische wetenschappen.

[27] De benchmark voor oneerlijkheid in B2B-contracten moet natuurlijk verschillen van die in B2C-contracten, aangezien de contractuele vrijheid in B2B-relaties groter is.

- **Rechten van de voortbrenger van de gegevens**: Een recht om niet-persoonsgebonden gegevens te gebruiken of toestemming te geven voor het gebruik ervan kan worden toegekend aan de "voortbrenger van de gegevens", d.w.z. de eigenaar of langetermijngebruiker (huurder) van het toestel. Deze aanpak heeft tot doel de juridische situatie te verduidelijken en de voortbrenger van de gegevens meer keuze te bieden door gebruikers de mogelijkheid te geven hun gegevens te gebruiken en zo bij te dragen tot het ontsluiten van door machines voortgebrachte gegevens. De uitzonderingen moeten echter duidelijk worden omschreven, met name wat betreft het verlenen van niet-exclusieve toegang tot de gegevens door de fabrikant of door overheidsinstanties, bijvoorbeeld voor verkeersbeheer of om milieuredenen. Indien het om persoonsgegevens gaat, behoudt de betrokkene het recht om zijn toestemming voor het gebruik van de gegevens weer in te trekken. Alvorens de andere partij toestemming mag geven voor verder gebruik van persoonsgegevens, moeten deze zodanig anoniem worden gemaakt dat de persoon niet of niet meer identificeerbaar is. De algemene verordening gegevensbescherming blijft van toepassing op alle persoonsgegevens (al dan niet voortgebracht door machines) tot die gegevens anoniem zijn gemaakt.

- **Toegang tegen betaling**: Op basis van een aantal kernbeginselen, zoals eerlijke, redelijke en niet-discriminerende voorwaarden, kan een kader worden ontwikkeld waarbij houders van gegevens, zoals fabrikanten, dienstverleners of andere partijen, tegen betaling toegang kunnen verlenen tot de gegevens waarover zij beschikken, nadat deze gegevens anoniem zijn gemaakt. Daarbij moet rekening worden gehouden met relevante legitieme belangen en met de noodzaak om bedrijfsgeheimen te beschermen. Voorts kan worden overwogen om verschillende toegangsregelingen te hanteren voor verschillende sectoren en/of bedrijfsmodellen, teneinde rekening te houden met de specifieke kenmerken van elke sector. In sommige gevallen kan (volledige of gedeeltelijke) open toegang tot gegevens bijvoorbeeld de voorkeur genieten, zowel voor het bedrijfsleven als voor de samenleving.

De Commissie zal de belanghebbenden raadplegen over de hierboven uiteengezette kwesties, teneinde meer informatie te verzamelen over de werking van de datamarkten per sector en mogelijke oplossingen te bestuderen. In deze context is een brede discussie op macroniveau van essentieel belang voor het bespreken van mogelijke oplossingen en het voorkomen van onbedoelde neveneffecten die innovatie zouden afremmen of concurrentie zouden belemmeren. Bovendien zullen sectorspecifieke besprekingen worden gevoerd met relevante belanghebbenden in de waardeketen van gegevens.

4. AANSPRAKELIJKHEID

Een ander opkomend probleem betreft de toepassing van de huidige aansprakelijkheidsregels in de data-economie op producten en diensten die gebaseerd zijn op nieuwe technologieën zoals het internet van de dingen (IoT), fabrieken van de toekomst en autonome geconnecteerde systemen. Het internet van de dingen is een snel groeiend netwerk van dagelijkse voorwerpen zoals horloges, voertuigen en thermostaten die zijn verbonden met het internet. Autonome geconnecteerde systemen, zoals zelfrijdende voertuigen, werken onafhankelijk van de mens en kunnen hun omgeving begrijpen en interpreteren. Deze opkomende technologieën maken gebruik van sensoren

om de vele soorten gegevens te verkrijgen die vaak nodig zijn voor de werking van het product of de dienst.

Naar verwachting zullen al deze innovaties bijdragen tot meer veiligheid en levenskwaliteit, maar de mogelijkheid van ontwerpfouten, storingen of manipulatie blijft onvermijdelijk bestaan voor elk toestel. Het kan gaan om verzending van onjuiste gegevens door een sensor, bijvoorbeeld als gevolg van softwarestoringen, verbindingsproblemen of slechte werking van het apparaat. Door de aard van deze systemen kan het moeilijk zijn om de precieze bron te achterhalen van een probleem dat tot schade leidt, wat de vraag doet rijzen hoe deze systemen veilig kunnen worden gemaakt voor de gebruikers, zodat schade zoveel mogelijk wordt voorkomen, en wie aansprakelijk is voor schade indien deze zich voordoet.

De vraag hoe zekerheid kan worden geboden aan zowel de gebruikers als de fabrikanten van dergelijke toestellen met betrekking tot hun mogelijke aansprakelijkheid is dus van cruciaal belang voor de ontwikkeling van een data-economie.

4.1. Aansprakelijkheidsregels van de EU

In het burgerlijk recht wordt over het algemeen een onderscheid gemaakt tussen twee soorten van wettelijke aansprakelijkheid: contractuele, waarbij de aansprakelijkheid voor de schade voortvloeit uit de contractuele betrekkingen tussen de partijen; en niet-contractuele[28], waarbij de aansprakelijkheid buiten het contract wordt geregeld. Een belangrijke vorm van niet-contractuele aansprakelijkheid is de aansprakelijkheid voor producten met gebreken. Op EU-niveau is in de richtlijn inzake de aansprakelijkheid voor producten met gebreken (85/374/EEG) (“richtlijn productaansprakelijkheid”) het beginsel van strikte aansprakelijkheid vastgesteld, d.w.z. aansprakelijkheid buiten schuld: wanneer een consument schade lijdt ten gevolge van een product met gebreken, kunnen de fabrikanten aansprakelijk worden gesteld, zelfs wanneer er geen sprake is van nalatigheid of fout. Om de volgende redenen kan het echter moeilijk of onduidelijk zijn hoe de bepalingen van deze richtlijn[29] moeten worden toegepast op IoT en autonome geconnecteerde systemen (bijv. robotica): de kenmerken van deze systemen, bijvoorbeeld een complexe waardeketen van producten of diensten, waarbij leveranciers, fabrikanten en andere derde partijen onderling van elkaar afhankelijk zijn; onzekerheid over de juridische aard van IoT-toestellen, d.w.z. of het gaat om producten, diensten of producten die samen met een dienst worden verkocht; en het autonome karakter van deze technologieën.

De Commissie heeft de aanzet gegeven tot een brede evaluatie van de richtlijn productaansprakelijkheid, teneinde de algemene werking ervan te evalueren en na te gaan of de regels, die ontwikkeld zijn voor een totaal verschillende omgeving, ook kunnen worden toegepast op ontluikende technologieën als IoT en autonome geconnecteerde systemen.

---

[28] De EU-aansprakelijkheidsregels hebben alleen betrekking op niet-contractuele aansprakelijkheid.

[29] Ook in andere wetgeving inzake de veiligheid van producten wordt verwezen naar de strikte aansprakelijkheid van producenten in het geval van producten met gebreken, zoals de richtlijn inzake radioapparatuur (2014/53/EU), de verordeningen inzake medische hulpmiddelen, de machinerichtlijn (2006/42/EG) en de richtlijn algemene productveiligheid (2001/95/EG).

4.2. Mogelijke verdere stappen

De Commissie streeft ernaar de rechtszekerheid met betrekking tot aansprakelijkheid in de context van ontluikende technologieën te vergroten en aldus gunstige omstandigheden voor innovatie te creëren. Behalve de status quo[30] kunnen ook diverse andere benaderingen worden overwogen, zoals:

- **Een benadering waarbij de veroorzaker aansprakelijk is voor het risico of een benadering waarbij de risico's worden beheerd**: In het kader van deze benaderingen kan aansprakelijkheid worden toegewezen aan de marktspelers die een groot risico veroorzaken voor anderen of aan de marktspelers die het best geplaatst zijn om dit risico tot een minimum te beperken of te voorkomen.

- **Vrijwillige of verplichte verzekeringsregelingen**: Dergelijke regelingen kunnen worden gekoppeld aan de bovenvermelde benaderingen van aansprakelijkheid. Op die manier kunnen partijen die schade hebben geleden, worden gecompenseerd (bijv. consumenten). In het kader van deze benadering moet worden voorzien in rechtsbescherming voor investeringen van bedrijven, en moeten slachtoffers erop kunnen vertrouwen dat zij een eerlijke compensatie krijgen of passend verzekerd zijn in geval van schade.

Bij elke aanpak moet rekening worden gehouden met de acties van de personen die de technologie gebruiken, en moet meer bepaald worden vastgesteld wat de rol van is van de gebruikers van die technologie.

De Commissie zal de belanghebbenden vragen of de huidige EU-aansprakelijkheidsregels passend zijn in de context van IoT en autonome geconnecteerde systemen, en welke benaderingen mogelijk zijn om de huidige problemen met de toewijzing van aansprakelijkheid op te lossen. Parallel wordt ook een openbare raadpleging over de algemene evaluatie van de toepassing van de richtlijn productaansprakelijkheid gehouden. De Commissie zal de resultaten beoordelen en nagaan welke stappen in de toekomst kunnen worden gezet.

5. MEENEEMBAARHEID, INTEROPERABILITEIT EN NORMEN

Andere nieuwe aandachtspunten in de data-economie zijn de meeneembaarheid van niet-persoonsgebonden gegevens, de interoperabiliteit van diensten om gegevensuitwisseling mogelijk te maken, en passende technische normen voor de tenuitvoerlegging van zinvolle meeneembaarheid.

5.1. Meeneembaarheid van niet-persoonsgebonden gegevens

Meeneembaarheid van gegevens betekent dat consumenten en bedrijven gemakkelijk hun gegevens van het ene systeem naar het andere kunnen overbrengen. Dit gaat meestal gepaard met lage overstapkosten, waardoor de drempels voor overstappen laag zijn in de

[30] De Commissie kan richtsnoeren uitvaardigen betreffende de toepassing van de EU regels inzake aansprakelijkheid op IoT en robotica.

data-economie. De algemene verordening gegevensbescherming verleent personen het recht om de aan de dienstverlener verstrekte persoonsgegevens te ontvangen in een gestructureerd machineleesbaar formaat, alsook het recht om die gegevens over te brengen naar een andere dienstverlener[31].

Wat niet-persoonsgebonden gegevens betreft, bestaan er momenteel geen verplichtingen om zelfs maar een minimumniveau van meeneembaarheid van gegevens te waarborgen, zelfs voor op grote schaal gebruikte onlinediensten zoals aanbieders van cloud hosting. Dit is deels te wijten aan het feit dat de voorschriften voor de toepassing van meeneembaarheid van gegevens technisch veeleisend en duur kunnen zijn omdat het mogelijk is dat verschillende aanbieders van dezelfde diensten de gegevens op verschillende wijze opslaan.

Meeneembaarheid van niet-persoonsgebonden gegevens is alleen maar zinvol wanneer rekening wordt gehouden met ruimere overwegingen inzake de governance van gegevens, zoals transparantie voor gebruikers, beheer van de toegang tot gegevens en interoperabiliteit om verschillende platforms te koppelen op een manier die stimulerend is voor innovatie.

5.2. Interoperabiliteit

Overwegingen op het gebied van de meeneembaarheid van gegevens houden vaak nauw verband met vraagstukken over gegevensinteroperabiliteit, waardoor meervoudige digitale diensten naadloos gegevens kunnen uitwisselen; dit wordt nog vergemakkelijkt door passende technische specificaties. In de richtlijn inzake overheidsinformatie en de bijbehorende richtsnoeren (met inbegrip van het Europees interoperabiliteitskader) wordt benadrukt dat rijke, gestandaardiseerde metadata volgens gevestigde vocabularia belangrijk zijn om zoekopdrachten en interoperabiliteit te vergemakkelijken. De richtlijn inzake infrastructuur voor ruimtelijke informatie in de Gemeenschap (INSPIRE) en de interoperabiliteitsregels en richtsnoeren voor ruimtelijke gegevensdiensten en gegevens, met inbegrip van sensorobservatiegegevens, zijn momenteel van toepassing op ruimtelijke gegevens van de overheidssector[32].

In het geval van online-platforms vergemakkelijkt de interoperabiliteit van gegevens niet alleen de overstap tussen, maar ook het gelijktijdige gebruik van verschillende platforms (“multi-homing”), alsook wijdverbreide platformoverschrijdende gegevensuitwisseling, die het potentieel heeft om innovatie in de digitale economie te verbeteren.

5.3. Normen

Om meeneembaarheid zinvol ten uitvoer te leggen op een technologisch neutrale wijze, moet effectief beleid inzake meeneembaarheid worden ondersteund door passende technische normen. De Commissie heeft zich ertoe verbonden[33] steun te verlenen aan

[31] Artikel 20.

[32] Door machines voortgebrachte gegevens zijn “ruimtelijke gegevens” omdat sensoren, samen met de metingen, meestal ook hun rechtstreekse of onrechtstreekse positie (locatie) verzenden.

[33] COM(2016) 176 final: ICT-normalisatieprioriteiten voor de digitale eengemaakte markt

passende normen ter verbetering van de interoperabiliteit, meeneembaarheid en beveiliging van clouddiensten, door de werkzaamheden van "open source"-gemeenschappen beter te integreren in het proces voor het vaststellen van normen op Europees niveau. Voorbeelden van een dergelijke benadering zijn de TOSCA-specificatie voor cloudtoepassingen, die tot doel heeft de meeneembaarheid en het operationeel beheer van cloudtoepassingen en -diensten te verbeteren[34], en de technische specificaties en richtsnoeren van de INSPIRE-uitvoeringsverordeningen[35].

5.4. Mogelijke verdere stappen

Mogelijke verdere stappen om bovengenoemde kwesties aan te pakken:

- **Aanbevolen contractbepalingen opstellen om de overstap naar een nieuwe dienstverlener te vereenvoudigen**: Aangezien de meeneembaarheid van gegevens en de overstap naar andere aanbieders van datadiensten onlosmakelijk met elkaar zijn verbonden, kan worden onderzocht of standaard-contractbepalingen kunnen worden ontwikkeld die de dienstverlener verplichten om de klant toe te staan zijn gegevens mee te nemen.

- **De rechten inzake meeneembaarheid van gegevens verder ontwikkelen**: Voortbouwend op het recht op meeneembaarheid van gegevens waarin de algemene verordening gegevensbescherming voorziet en op de voorgestelde regels inzake contracten voor de levering van digitale inhoud, kunnen verdere rechten op meeneembaarheid van niet-persoonsgebonden gegevens worden geïntroduceerd, met name in een B2B-context, rekening houdende met het resultaat van de lopende geschiktheidscontrole van essentiële delen van de marketing- en consumentenwetgeving van de EU[36].

- **Sectorspecifieke experimenten met betrekking tot normen**: Om te komen tot een robuuste benadering van regels inzake meeneembaarheid die zijn vastgelegd in normen, kan het startschot worden gegeven voor sectorspecifieke experimentele benaderingen. Gewoonlijk zijn daar diverse belanghebbenden bij betrokken, waaronder standaardiseringsinstanties, het bedrijfsleven, de technische wereld en overheden.

De Commissie zal de belanghebbenden raadplegen over deze kwesties, en zal op basis daarvan nagaan of verdere actie nodig is, mogelijk in de vorm van de bovengenoemde maatregelen, individueel of in combinatie met elkaar.

6. EXPERIMENTEN EN TESTS

Experimenten spelen een belangrijke rol in het onderzoek van ontluikende aandachtspunten in de data-economie. De mogelijkheid om Horizon 2020-middelen te

[34] https://www.oasis-open.org/committees/tosca

[35] INSPIRE-wetgeving: http://inspire.ec.europa.eu/inspire-legislation/26

[36] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

gebruiken voor de ondersteuning van deze proeven en experimenten zal worden onderzocht.

Alvorens conclusies te trekken over de geschiktheid van mogelijke oplossingen voor de problemen inzake toegankelijkheid van gegevens en aansprakelijkheid, moeten specifieke tests van deze oplossingen in een reële omgeving worden georganiseerd, in samenwerking met de belanghebbenden. Er is behoefte aan een Europese oplossing, die gebaseerd is op samenwerking tussen de lidstaten en op experimenten.

Op samenwerking gebaseerde, geconnecteerde en geautomatiseerde mobiliteit[37] kan worden overwogen voor een dergelijke test, gezien de grensoverschrijdende dimensie van deze sector.

In diverse lidstaten lopen al projecten om op samenwerking gebaseerde systemen en hogere niveaus van automatisering te ontwikkelen[38]. Het gaat om projecten waarbij voertuigen in verbinding staan met elkaar en met de infrastructuur langs de weg, zoals verkeerslichten en -borden. De Commissie is ook voornemens om, in samenwerking met een groep van belanghebbende lidstaten, een rechtskader voor tests en experimenten vast te stellen op basis van geharmoniseerde regels inzake toegankelijkheid van gegevens en aansprakelijkheid. Om de toegang tot een voldoende groot volume aan gegevens te waarborgen, moeten de tests gebaseerd zijn op 5G en naadloos samenwerken met technologieën die reeds worden toegepast, op basis van het beginsel van complementariteit[39].

Een ander interessant experiment vindt plaats in de sector geografisch-ruimtelijke informatie, met de opkomst van een nieuw gegevens-ecosysteem dat is opgebouwd rond Copernicus, het EU-programma voor aardobservatie en de derde grootste gegevensprovider ter wereld. De Commissie ontwikkelt innoverende oplossingen om de ontwikkeling van applicaties op basis van Copernicus en andere ruimtelijke gegevens aan te moedigen, en houdt zich met name bezig met de kwesties van toegang tot gegevens, interoperabiliteit en voorspelbaarheid.

7. CONCLUSIE

Om te kunnen bouwen aan de data-economie heeft de EU behoefte aan een beleidskader dat het mogelijk maakt gegevens in de gehele waardeketen te gebruiken voor wetenschappelijke, maatschappelijke en industriële doeleinden. Daarom start Commissie een brede dialoog met de belanghebbenden over de vraagstukken die in deze mededeling worden onderzocht. De eerste stap van deze dialoog is een openbare raadpleging. De kwesties van toegankelijkheid van gegevens en aansprakelijkheid zullen ook worden getest in een reële situatie op het gebied van coöperatieve, geconnecteerde en geautomatiseerde mobiliteit.

[37] Zie COM(2016) 766 van 30.11.2016.

[38] Zie COM(2016) 766: Een Europese strategie voor coöperatieve intelligente vervoerssystemen.

[39] Zie COM(2016) 588: 5G voor Europa: een actieplan.

Wat het vrije verkeer van gegevens betreft, blijft de Commissie de hierboven uiteengezette aanpak volgen om het beginsel van vrij verkeer van gegevens volledig toe te passen in de EU, indien nodig en passend via prioritaire handhavingsmaatregelen. De Commissie zal ook toezicht blijven uitoefenen en bewijzen blijven verzamelen en zal, indien nodig, overwegen om verdere initiatieven te nemen met betrekking tot het vrije verkeer van gegevens.

Op basis van de resultaten van het overleg met de belanghebbenden zal de Commissie ook besluiten of verdere actie nodig is met betrekking tot deze ontluikende aandachtspunten en zal zij dienovereenkomstig oplossingen voorstellen. Experimenten in reële omstandigheden kunnen een belangrijke rol spelen in deze context.