Protecting individuals against the negative impact of big data

The potential and limitations of the privacy and data protection law approach

Oostveen, M.A.A.

Publication date
2018
Document Version
Other version
License
Other

NEDERLANDSE SAMENVATTING

HOOFDSTUK 1: INLEIDING

Dit proefschrift gaat over de bescherming van individuen tegen de negatieve impact die big data op hun privéleven kan hebben. Big data kan leiden tot positieve en veelbelovende ontwikkelingen, maar de grootschalige verzameling en verwerking van gegevens leidt ook tot veel problemen. In dit proefschrift staan de positie en de bescherming van het individu centraal wiens persoonsgegevens worden gebruikt in big data, of wie de negatieve consequenties van de toepassing van big data ondervindt.

In de Europese Unie (EU) richt de discussie rondom de negatieve kanten van big data zich voornamelijk op privacy en het gegevensbeschermingsrecht. Privacy en gegevensbescherming worden gezien als de rechten die het grootste gevaar lopen door big data, maar ook als het (juridische) antwoord op de problemen die big data veroorzaakt. Dit proefschrift onderzoekt deze privacy- en gegevensbeschermingsbenadering ter bescherming van individuen. Het draait hierbij om de vraag wat het potentieel en de beperkingen van het juridische privacy- en gegevensbeschermingskader zijn om personen te beschermen tegen de negatieve impact van big data op hun individuele rechten en vrijheden.

Hoofdstuk één introduceert het onderwerp en de onderzoeksvragen. Het bespreekt de afbakening tot de EU, de uitsluiting van het strafrechtelijk domein, en de selectie van individuele rechten en vrijheden aan de hand van het Europees Verdrag voor de Rechten van de Mens (EVRM) en het Handvest van de Grondrechten van de Europese Unie (Handvest), nader toegelicht in Hoofdstuk 2. Daarnaast bevat het een beknopte conceptuele analyse van deze individuele rechten en vrijheden en van de term big data, alsmede de methodologische verantwoording van het onderzoek.

HOOFDSTUK 2: BIG DATA

Hoofdstuk 2 bespreekt het concept big data en de daaruit voortvloeiende mogelijke negatieve consequenties voor de rechten en vrijheden van het individu. De betekenis van de term "*big data"* hangt af van de context waarin zij wordt gebezigd. In het algemeen wordt aangenomen dat de term in 2011 voor het eerst gebruikt werd, gekoppeld aan de drie op data slaande factoren *volume, velocity,* en *variety.* Deze factoren werden in 2001 genoemd als kenmerken van nieuwe manieren van gegevensmanagement en -analyse, als gevolg van technologische ontwikkelingen die deze mogelijkheden vergrootten en goedkoper maakten. Door de jaren heen is de term echter op verschillende nieuwe manieren gebruikt, variërend van als marketingterm die slechts slaat op het verwerken van veel gegevens en wordt gebezigd om aandacht te wekken en inkomsten te genereren, tot verwijzing naar een socio-

technologisch fenomeen met verregaande gevolgen voor de manier waarop wij tegen kennis en maatschappelijke ontwikkelingen aankijken.

Gezien deze verscheidenheid aan interpretaties is een verdere afbakening vereist. Immers, wanneer de inhoud van het begrip big data en de gevolgen ervan niet duidelijk zijn, is ook niet te beoordelen hoe het gereguleerd is en gereguleerd zou moeten worden. De gemene deler van de verschillende in omloop zijnde interpretaties is, dat big data in alle gevallen gezien kan worden als proces, waarin gegevens verzameld en geanalyseerd worden, om de uitkomsten van deze analyse vervolgens toe te passen. In de praktijk gaat het uiteraard om een complex iteratief proces, maar in algemene zin kunnen deze drie fasen van vergaring, analyse en toepassing in big data projecten onderscheiden worden. Deze drie fasen voorstelling maakt het mogelijk om een normatieve en juridische analyse van big data uit te voeren. In Hoofdstuk 2 worden de onderscheiden fasen uitgelegd en toegelicht aan de hand van drie praktijkvoorbeelden, te weten kredietverstrekking in de financiële dienstensector, biobanken in medisch onderzoek, en online personalisatie. Samengevat houden de fasen het volgende in. In de vergaringsfase worden gegevens verzameld. De gegevens kunnen afkomstig zijn van het individu zelf, maar zij kunnen ook gekocht worden van datahandelaren, of bijvoorbeeld gecreëerd door het combineren van verschillende datasets, waardoor nieuwe informatie wordt verkregen. Daarna vindt de analyse van de gegevens plaats. De analyse gebeurt geautomatiseerd, met behulp van gespecialiseerde software op welk gebied er continu nieuwe ontwikkelingen zijn. Uit deze analyse komt vervolgens informatie in verschillende vormen, bijvoorbeeld als kennis, model, of voorspelling. In de toepassingsfase wordt deze kennis vervolgens gebruikt om beslissingen op te baseren. Dit kunnen algemene beslissingen zijn, bijvoorbeeld over nieuw aan te leggen infrastructuur of het voorschrijven van nieuwe medicijnen(combinaties) voor bepaalde ziektes. Vaak gaat het echter ook om beslissingen die zijn toegespitst op het individu, zoals de afwijzing van persoonlijk krediet of het aanpassen van de prijs van vliegtickets op een website. Het is voor de normatieve en juridische analyse van belang om stil te staan bij het feit dat de personen wiens gegevens verzameld worden en als input dienen voor de analyse, en de personen op wie de uitkomsten worden toegepast, twee verschillende groepen zijn. Afhankelijk van het specifieke big data project kunnen ze overlappen, waarbij data uit de toepassingsfase weer tot nieuwe input leidt. Maar in beginsel zijn het vergaren en de analyse gescheiden van de toepassing; een big data model wordt ontwikkeld aan de hand van de gegevens van personen uit de eerste groep, en kan vervolgens op een onbeperkte nieuw aantal personen worden toegepast.

Op deze uiteenzetting van het fasenmodel volgt een analyse van de effecten die zich in elke fase kunnen verwezenlijken ten aanzien van de individuele rechten en vrijheden van het individu. Niettegenstaande de positieve invloed die big data kan hebben op het leven van het individu en de maatschappij in zijn geheel, wat in dit proefschrift nadrukkelijk niet wordt ontkent, ligt de focus gezien de onderzoeksvraag op de negatieve kanten van big data. De conclusie is dat elke fase op eigen wijze negatieve invloed kan hebben op individuele rechten en vrijheden, omdat er verschillende handelingen in plaatsvinden. In de vergaringsfase zijn de risico's vooral gelegen in de grootschalige verzameling en combinatie van gegevens. Dit heeft een negatief effect op de rechten op privacy en

gegevensbescherming, maar ook persoonlijke autonomie, non-discriminatie en de vrijheid van meningsuiting zijn in het geding. Immers, de wetenschap dat men wordt gemonitord en dat gegevens omtrent gedrag bijgehouden worden en opgeslagen voor de toekomst, kan van invloed zijn op het gedrag dat mensen vertonen, de keuzes die zij maken, en de informatie die zij vergaren en produceren. In de analysefase lijken de effecten beperkter, omdat de gegevens vaak zullen worden verwerkt in een vorm die niet meer tot individuele personen herleidbaar is, wat beneden in meer detail uiteengezet wordt. Hierbij moet wel worden bedacht, dat de analyse de bron is van vele negatieve effecten die zich in de toepassingsfase kunnen openbaren, zoals discriminatie. In de regel zullen noch de personen wiens gegevens de bron voor analyse zijn, noch de personen die de nadelige consequenties in de toepassingsfase ondervinden, enige invloed kunnen uitoefenen over wat er in de analysefase gebeurt. In deze zin kan men dus spreken van een negatief effect op persoonlijke autonomie: er is weinig invloed op wat er met gegevens wordt gedaan, of welke gegevens en modellen ten grondslag liggen aan een beslissing. In de toepassingsfase komt het volledige scala aan negatieve effecten voorbij, dat wil zeggen, negatieve impact op de rechten op persoonlijke autonomie, privacy en gegevensbescherming, non-discriminatie, en vrijheid van meningsuiting. Persoonlijke autonomie staat onder druk, door de manieren waarop met behulp van big data gepersonaliseerd, overtuigd, overgehaald, *genudged*, en gemanipuleerd kan worden. Hierbij moet bedacht worden dat het niet slechts om grote *high-impact* beslissingen gaat; ook kleine cumulatieve gevallen van personalisatie kunnen de keuzevrijheid, ontwikkeling, en identiteit van het individu blijvend beïnvloeden. Gezien de toenemende kennis en mogelijkheden, en de schaal waarop dit in met name de digitale omgeving gebeurt, is het van belang ook bij deze cumulatieve personalisatie stil te staan, alsmede bij de lange-effecten die het gevolg kunnen zijn voor de toekomst van het individu. Met betrekking tot privacy en gegevensbescherming en vrijheid van meningsuiting in de toepassingsfase bestaat grofweg dezelfde problematiek als in de vergaringsfase. Daarnaast kan de toepassing van big data leiden tot op zichzelf staande inbreuken op de persoonlijke levenssfeer, onafhankelijk van de verwerking van persoonsgegevens. Door personalisatie kan ook de vrije informatiegaring in het gedrang komen. Ten slotte kan de toepassing van big data leiden tot (directe of indirecte) discriminatie.

HOOFDSTUK 3: FUNDAMENTELE RECHTEN OP PRIVACY EN GEGEVENSBESCHERMING

In Hoofdstuk 3 staat de reikwijdte van de fundamentele rechten op privacy en gegevensbescherming in de EU centraal, om te bepalen wat hun normatieve inhoud is ten aanzien van big data. Het hoofdstuk onderzoekt wat de fundamentele rechten inhouden in de context van big data, en wat zij verlangen van de bescherming die het secundaire EU recht biedt. Het hoofdstuk richt zich op de op zichzelf staande waarde van deze rechten, alsmede op de beschermende functie die zij vervullen ten opzichte van de andere individuele rechten en vrijheden, wat hier de *faciliterende functie* van de rechten op privacy en gegevensbescherming wordt genoemd.

Als onderdeel van de belangrijkste fundamentele rechten instrumenten in de EU, worden art. 8 EVRM en artt. 7 en 8 Handvest vergeleken. Schendingen van het EVRM en het Handvest kunnen voor het Europees Hof voor de Rechten

van de Mens (EHRM) en het Hof van Justitie van de Europese Unie (HvJ EU) worden gebracht. Het EHRM heeft in haar lange traditie van rechtspraak op het gebied van artikel 8 EVRM veel invulling gegeven aan de inhoud van het recht op (informationele) privacy in de EU. De interpretatie van de rechten op privacy en gegevensbescherming door het HvJ EU is in sterke mate door de Straatsburgse rechtspraak beïnvloed, met name omdat het recht op privacy van het Handvest als *corresponding right* in de zin van art. 52 (3) Handvest minimumbescherming moet bieden conform art. 8 EVRM. Het Handvest voegt een apart recht op de bescherming van persoonsgegevens aan het EU fundamentele rechten niveau toe.

De interpretatie van deze fundamentele rechten in het licht van big data is om diverse redenen moeilijk. De uitspraken van beide Hoven zijn casuïstisch en sterk ingebed in de context van de voorliggende zaken, waarbij het doorgaans gaat om inbreuken (door handelen of nalaten) van Staten. Concrete zaken over big data en expliciete verwijzingen naar een faciliterende functie zijn zeldzaam. Anderzijds kan door het loslaten van de procedurele context en kijken naar de normatieve inhoud van de rechten, in combinatie met de interpretatiemethoden van de Hoven zoals de *living instrument* en *practical and effective* doctrines van het EHRM, betekenis worden gegeven aan de reikwijdte en welke beschermingsomvang van secundaire regelgeving vereist wordt.

Uit de successieve analyse van de afzonderlijke artikelen komt ten aanzien van de normatieve concepten van de rechten op privacy en gegevensbescherming in de EU een vrij coherent beeld naar voren. Het recht op privacy ziet ten aanzien van big data op de verwerking van persoonsgegevens in alle fasen, waarbij de interpretatie gekoppeld wordt aan Conventie 108 van de Raad van Europa aangaande de bescherming van persoonsgegevens, en ook metadata en locatiegegevens omvat. Of er een ongeoorloofde inmenging is, hangt echter van de ernst en omstandigheden af. Er zijn in ieder geval minimum eisen waaraan voldaan moet worden om het individu te beschermen, welke afhankelijk zijn van de inbreuk en de gevoeligheid van het type gegevens dat verwerkt wordt. Deze eisen omvatten beperkingen aan opslag en bewaartermijnen, en verplichtingen ten aanzien van het nemen van maatregelen ter bescherming van de persoonsgegevens, onder andere ter preventie van ongeautoriseerde toegang en misbruik. Los van persoonsgegevens kan het recht op privacy in het geding zijn wanneer er een inmenging is ten aanzien van woning of correspondentie, of in de sfeer van seksuele activiteiten, sociaal leven, persoonlijke relaties, of persoonlijke, morele, of fysieke identiteit. Dit zal voornamelijk spelen in de toepassingsfase. Gezien de verschillende mogelijke toepassingen van big data is het onmogelijk om hier een gedetailleerd volledig overzicht van te geven.

De reikwijdte van het normatieve concept van het recht op privacy ten aanzien van persoonsgegevens lijkt zeer ruim, maar toch is het recht op bescherming van persoonsgegevens van toegevoegde waarde. Het voegt onder andere specifieke eisen met betrekking tot de verwerking van persoonsgegevens toe. Art. 8 Handvest is preciezer geformuleerd; het bevat de gedetailleerde eisen dat de verwerking van persoonsgegevens op toestemming of een andere legitieme grond moet zijn gebaseerd, de rechten op toegang en rectificatie van persoonsgegevens, en de eis van onafhankelijk toezicht op de naleving hiervan.

De faciliterende rol van privacy en gegevensbescherming wordt erkend in de literatuur, maar er zijn geen concrete verplichtingen in de rechtspraak van beide Hoven te ontdekken. Persoonlijke autonomie wordt door het EHRM wel als onderdeel van het recht op privacy gezien, en daarmee ligt de faciliterende rol van privacy voor persoonlijke autonomie in het normatieve concept van privacy besloten. Een is een inbreuk op dit recht door het EHRM echter nooit expliciet vastgesteld, waardoor de reikwijdte ervan moeilijk vast te stellen is. Ten aanzien van vrijheid van meningsuiting legt het HvJ EU het verband en erkent daarmee de faciliterende rol, maar dit wordt niet als plicht van het recht op privacy of gegevensbescherming geformuleerd. Deze beperkte aandacht voor de faciliterende rol zou verklaard kunnen worden door de fundamentele rechten traditie in de EU: de rechten op privacy en gegevensbescherming hebben op zichzelf staande waarde, en andere rechten en vrijheden worden door de respectievelijke fundamentele rechten en vrijheden beschermd. Deze conclusies over de normatieve reikwijdte van het recht op privacy en op gegevensbescherming komen terug in de conclusie van Hoofdstuk 4, waar zij vergeleken worden met de conclusies over de bescherming door het EU gegevensbeschermingsrecht, om de te beoordelen in hoeverre het de plicht heeft individuele rechten en vrijheden te beschermen.

HOOFDSTUK 4: GEGEVENSBESCHERMINGSRECHT

Hoofdstuk 4 analyseert in hoeverre het huidige EU gegevensbeschermingsrecht in de vorm van de Algemene Verordening Gegevensbescherming (AVG) individuele rechten en vrijheden beschermt, kan beschermen, en dient te beschermen. Om deze vragen te beantwoorden, is dit hoofdstuk onderverdeeld in vier delen, die bespreken of het EU gegevensbeschermingsrecht van toepassing is op big data, hoe haar materiele normen functioneren binnen de context van big data, hoe de handhaving van de normen geregeld is, en of de normatieve concepten van de rechten op privacy en gegevensbescherming een andere implementatie van deze secundaire regelgeving vereisen.

Het eerste deel van het hoofdstuk analyseert wanneer het regelgevend kader wel en niet van toepassing is binnen het big data proces. Doorslaggevend voor deze vraag is het begrip "*persoonsgegeven*" en het daarmee samenhangende begrip *"identificeerbaarheid".* De materiële reikwijdte van het EU gegevensbeschermingsrecht is afhankelijk van of er persoonsgegevens verwerkt worden, en daarmede van de criteria die gelden voor het begrip "*persoonsgegeven*". In de context van big data is het belangrijkste criterium "*geïdentificeerd of identificeerbaar*", wat verwijst naar de herleidbaarheid van gegevens tot natuurlijke personen. Op basis hiervan kunnen vier verschillende typen persoonsgegevens worden onderscheiden: direct identificerende gegevens, indirect identificerende gegevens, gedeïdentificeerde persoonsgegevens, en niet-persoonsgegevens. De eerste twee vallen samen binnen de reikwijdte van de AVG, en worden hier aangeduid als *identificeerbare gegevens*. De twee laatste typen vallen niet onder de wet, en worden hier *niet-identificeerbare* gegevens genoemd. Op grond van deze onderverdeling zijn meerdere verwerkingsscenario's mogelijk in big data. Wanneer in een big data fase niet-identificeerbare gegevens worden verwerkt, is de wet hierop niet van toepassing, en gaat er dus geen beschermende werking uit van het EU gegevensbeschermingsrecht. Of en in welke fase identificeerbare gegevens verwerkt worden, die dus als

persoonsgegevens kwalificeren en de wet van toepassing maken, hangt af van het specifieke big data project. Er zijn projecten waarbij in alle fasen persoonsgegevens verwerkt worden, waardoor de wet dus onverminderd van toepassing is. Maar het kan ook voorkomen dat bijvoorbeeld in de vergarings- en analysefase geen gebruik maken van persoonsgegevens, maar in de toepassingsfase toch impact kunnen hebben op het individu. In de regel zal het echter zo zijn, dat persoonsgegevensverwerking vaak, maar niet noodzakelijkerwijs, voorkomt in de vergaringsfase en (beperkt) in de toepassingsfase, maar vaak niet in de analysefase. Er zijn immers sterkte prikkels voor entiteiten die aan big data doen om gegevens op een niet-identificeerbare manier te verwerken. In principe is men in big data geïnteresseerd in algemene patronen, niet in specifieke kennis over één individu. Er is doorgaans geen noodzaak om gegevens in een identificeerbare staat te houden. Deïdentificatie zorgt ervoor dat de AVG niet meer van toepassing is. Het niet van toepassing zijn van de gegevensbeschermingsregels betekent onder meer dat principes als doelbinding, dataminimalisatie en het hebben van een legitieme verwerkingsgrond niet gelden in de analysefase. De mogelijkheden met big data zijn dan groter, en de risico's ten aanzien van onder andere compliance en datalekken kleiner, wat deze sterke prikkel verklaart. De conclusie is dat het EU gegevensbeschermingsrecht in voorkomende gevallen niet van toepassing is op (delen van) het big data proces, waardoor big data zich deels aan de bescherming middels de AVG onttrekt. De eerste lacune in de bescherming van individuele rechten en vrijheden is hiermee gegeven.

Het tweede deel van Hoofdstuk 4 analyseert hoe de materiële normen van de AVG functioneren in het kader van big data, indien EU gegevensbeschermingsrecht van toepassing is. Het richt zich hierbij op de regels die van belang zijn in big data gezien de handelingen in de verschillende fasen en de potentiële negatieve effecten per fase, met tevens aandacht voor het potentieel van innovaties in het gegevensbeschermingsrecht door de AVG, zoals het recht op dataportabiliteit. De analyse van het potentieel en de beperkingen van het materiële gegevensbeschermingsrecht is onderverdeeld aan de hand van regels die de persoonsgegevensverwerking *transparant* moeten maken voor het individu, regels die het individu *controle* over de verwerking beogen te geven, en regels die specifieke *risico's* in kaart proberen te brengen of te reguleren. De plichten om individuen informatie te verstrekken over de wijze en doel van verwerking en de logica en consequenties van genomen geautomatiseerde individuele besluiten (waaronder profilering), vormen de regels waarmee transparantie wordt geschapen. Deze regels zien op de vergaringssfase, en op de toepassingsfase met name indien er sprake is van geautomatiseerde individuele besluitvorming. Van belang zijnde controlerechten zijn het vereiste van een wettelijke grondslag van gegevensverwerking en het bijbehorende toestemmingsvereiste, het recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming, het recht op gegevenswissing (recht op vergetelheid), en het recht op dataportabiliteit. Tezamen scheppen regels omtrent transparantie en controle de noodzakelijke voorwaarden voor informationele zelfbeschikking van het individu: inzicht kunnen krijgen in de gegevensverwerking en er invloed op kunnen uitoefenen. Deze informationele zelfbeschikking waarborgt persoonlijke autonomie en het recht op gegevensbescherming, kan (indirect) discriminatie kan tegengaan en beschermende effecten hebben voor het algemene recht op privacy en de vrijheid van meningsuiting. Echter, binnen de context van big data blijkt dit beschermend potentieel vaak niet tot volle wasdom

te komen. Dit komt onder andere omdat de reikwijdte van de rechten beperkt is gezien de toepassingscriteria die ervoor gelden. De regels omtrent geautomatiseerde individuele besluitvorming zijn bijvoorbeeld beperkt tot *high-impact* besluiten. Ook is het in de praktijk vaak moeilijk om aan de eisen met betrekking tot informeren en toestemming te voldoen, bijvoorbeeld omdat de toekomstige toepassingen en consequenties tijdens het vergaren van de gegevens nog niet vaststaan en voldoende duidelijk te omschrijven zijn. Maar de belangrijkste reden is dat individuele rechten en controle slecht functioneren in een omgeving van online gegevensvergaring en toepassing van big data. Gezien de complexiteit en alomtegenwoordigheid van digitale gegevensverwerking is het managen van online privacy en gegevensbescherming een vrijwel onmogelijke taak geworden voor het individu. Bovendien fungeert gegevensverwerking vaak als eis en tegenprestatie voor het leveren van een dienst, terwijl de (negatieve) gevolgen van gegevensverwerking doorgaans abstract van aard zijn, of zich pas op de lange termijn of binnen de context van cumulatieve verwerkingen openbaren. Zij lijken het individu hierdoor niet direct te raken. Dit zijn extra redenen die aangeven dat adequate bescherming van individuele rechten en vrijheden in de context van big data niet kan worden bewerkstelligd door transparantie en controle door het individu alleen.

De regels van de AVG die zich richten op het in kaart brengen of reguleren van bepaalde risico's, richten zich met name tot de verwerker van persoonsgegevens. De nadelen van voorgenoemde regels uit de sfeer van informationele zelfbeschikking kleven dus niet aan zulke regels. Belangrijk in de context van big data zijn de regels die het verwerken van bijzondere categorieën persoonsgegevens beperkt verbieden, doelbinding en dataminimalisatie, de verplichtingen omtrent het uitvoeren van *data protection impact assessments* en de regels over het implementeren van *data protection by design and default*. Het beperkte verbod op het verwerken van gevoelige gegevens vervult een belangrijke rol in de bescherming van de rechten op privacy en gegevensbescherming, maar kan daarnaast ook een middel zijn om discriminatie tegen te gaan. Het zal echter niet baten indien er sprake is van indirecte discriminatie, wat gezien de mogelijkheid van het vinden van *proxies* voor bijzondere categorieën persoonsgegevens een reëel gevaar is binnen big data. *Data protection impact assessments* en *data protection by design and default* vereisen samengevat van big data entiteiten dat zij hun verwerkingen en de daarmee gepaard gaande risico's in kaart brengen, en (technische) maatregelen nemen om zoveel mogelijk tegemoet te komen aan de persoonsgegevensbeschermingsregels, dit alles uiteraard op straffe van de boetes onder de AVG. Dat voorafgaand aan de verwerking over het risico's en het waarborgen van rechten van individuen moet worden nagedacht, heeft naar alle waarschijnlijkheid een positieve invloed op de bescherming van het individu. Er zijn echter twijfels over de praktische implementatie en handhaving van zulke regels, en daarmee over de beschermende werking die van deze bepalingen uitgaat. Hetzelfde geldt voor de regels omtrent doelbinding en dataminimalisatie. Deze regels lijken enerzijds belangrijke grenzen aan gegevensverwerking stellen, maar zijn anderzijds onverenigbaar met big data, wat onder andere tot handhavingsproblemen kan leiden. Handhavingsmogelijkheden zijn verbeterd door de komst van de AVG, onder meer door boetes die sterk verhoogd zijn ten opzichte van de Gegevensbeschermingsrichtlijn. Echter, onder meer gezien de alomtegenwoordigheid van gegevensverwerking en de blijvende frictie tussen het recht en de praktijk, blijft handhaving een probleem binnen big data.

Het laatste onderdeel van Hoofdstuk 4 omschrijft de lacunes in de door gegevensbeschermingsrecht geboden bescherming van individuele rechten en vrijheden in de context van big data. Het vergelijkt deze lacunes met de normatieve concepten van de rechten op privacy en gegevensbescherming uit Hoofdstuk 3, om conclusies te trekken over het potentieel en de beperkingen van de gegevensbeschermingsaanpak van big data problemen, en te beoordelen tot op welke hoogte gegevensbeschermingsrecht deze effecten zou *moeten* tegengaan.

De lacunes in bescherming worden onderverdeeld in drie types, afhankelijk van de oorzaken die eraan ten grondslag liggen: of het gegevensbeschermingsrecht van toepassing is, en indien dit niet het geval is, of de verwerking van gegevens (niet zijnde persoonsgegevens) de kern van het probleem vormt of niet. In het eerste type lacune is het gegevensbeschermingsrecht van toepassing, maar biedt het onvoldoende bescherming. Deze oorzaak ligt ten grondslag aan de meeste problemen in de vergaringsfase. Het kan ook spelen in de toepassingsfase, bijvoorbeeld indien personen geprofileerd worden op basis van persoonsgegevens, maar de geautomatiseerde besluitvormingsregels niet van toepassing zijn omdat de beslissingen niet *high-impact* zijn, of wanneer er menselijke interventie in het proces is. Bij deze lacune zijn er verschillende onderliggende redenen: zoals uiteengezet, functioneren controle en transparantie slecht in de context van de datagedreven samenleving in het algemeen, en in de context van kleine maar cumulatieve big data toepassingen in het bijzonder. Daarnaast maken de criteria van de AVG's bepalingen, zoals hiervoor omschreven ten aanzien van geautomatiseerde besluitvorming, dat de reikwijdte ervan beperkt is.

Het tweede type lacune bestaat wanneer gegevensbeschermingsrecht niet van toepassing is, maar de verwerking van gegevens wel de kern vormt van het probleem. Dit speelt vaak in de analysefase, waar veel gegevens gedeïdentificeerd worden voor ze analyse ondergaan, waardoor ze buiten de reikwijdte van het gegevensbeschermingsrecht vallen, terwijl de kern in deze fase de analyse van gegevens is. In zulke gevallen zijn de mogelijkheden om invloed uit te oefenen over de analyse middels gegevensbeschermingsrecht vrijwel afwezig. Er is ook geen taak voor gegevensbeschermingsrecht, omdat geen persoonsgegevens worden verwerkt. In het derde type lacune is het regelgevend kader niet van toepassing en is gegevensverwerking niet de kern van het probleem. Deze situatie doet zich voor in de toepassingsfase, waar naast geïndividualiseerde besluiten op basis van persoonsgegevens, niet-geïndividualiseerde beslissingen worden genomen. De toepassing van deze beslissingen is niet afhankelijk van persoonsgegevens, maar kan toch een (negatief) effect op het leven van individuen hebben, zoals boven omschreven.

De samenvatting van hoe gegevensbescherming functioneert in de context van big data en de indeling van lacunes in bescherming, leiden tot conclusies over de normatieve concepten van de rechten op privacy en gegevensbescherming en hoe het EU gegevensbeschermingsrecht daarmee correspondeert. In de eerste lacune (onvoldoende bescherming) blijkt gegevensbeschermingsrecht deels ingehaald door de nieuwe technologische realiteit van big data. Het lijkt echter wel te beantwoorden aan het beschermingsniveau dat de normatieve concepten van de rechten op privacy en gegevensbescherming vereisen. In feite vereist het fundamentele rechten niveau een

mate van individuele zelfbeschikking, onder meer door de rechten die het individu heeft onder art. 8 (2) Handvest, en verplichtingen aangaande te nemen maatregelen ter bescherming van persoonsgegevens. Gegevensbeschermingrecht bevat dergelijke rechten en bepalingen, ondanks de problemen met de reikwijdte en bescherming in de context van big data.

Een significant aantal van de problemen van big data, met name (een deel) van de problemen in de analyse en toepassingsfase, valt niet binnen de reikwijdte van de normatieve concepten van privacy en gegevensbescherming. Wanneer dit het geval is, dan is er geen ruimte voor een faciliterend effect van privacy en gegevensbescherming. Deze problemen staan daarmee op zichzelf. Voor lacunes van het tweede en derde type, met name wanneer de verwerking van gegevens niet de kern vormt van het probleem, is er geen duidelijk verband tussen een probleem en de rechten op privacy en gegevensbescherming. In zulke gevallen lijken de grootste problemen voort te vloeien uit de informatieasymmetrieën en machtsverschillen die worden gecreëerd door datagedreven besluitvorming, en de schadelijke effecten van bepaalde beslissingen. Dit kan zelfs het geval zijn indien de wet wel van toepassing is. Een voorbeeld is problemen in de analysefase, waar asymmetrische verhoudingen en daarmee gepaard gaande netwerkeffecten als belangrijke oorzaak kunnen worden beschouwd. Het is daarom van het grootste belang om te erkennen dat niet elk big data probleem een privacy-of gegegevensbeschermingsprobleem is. Gegevensbescherming moet niet worden beschouwd als *panacea* in de context van big data. De problemen moeten beoordeeld en aangepakt worden gebaseerd op hun individuele kenmerken. Deze constatering beïnvloedt in sterke mate welke benadering van big data de voorkeur geniet volgens dit proefschrift.

HOOFDSTUKKEN 5 EN 6: CONCLUSIES EN TOEKOMST

Big data vereist een *gecombineerde aanpak.* Privacy en gegevensbescherming spelen een belangrijke rol, maar het gaat bij big data niet om de rechten op privacy en gegevensbescherming alleen. Big data is een complex proces dat bestaat uit verschillende handelingen, hier samengevat als fasen, die elk op verschillende wijze (negatieve) consequenties kunnen hebben voor tevens verschillende individuele rechten en vrijheden. Voor een groot deel vereist een gecombineerde aanpak simpelweg dat het big data proces en de negatieve effecten ervan niet gereduceerd worden tot privacy- en gegevensbeschermingsproblemen, maar dat ze op hun eigen kenmerken beoordeeld worden. Uit een dergelijke beoordeling volgt bijvoorbeeld dat een persoon die online in een zwakke positie bevindt ten opzichte van een bedrijf dat een belangrijke dienst verleent, welke afhankelijk wordt gesteld van de verzameling van persoonsgegevens, niet alleen een betrokkene in de zin van de AVG is, maar ook een consument. En dat iemand die in het kader van een sollicitatie gediscrimineerd wordt naar aanleiding van de toepassing van big data, niet alleen een betrokkene is, maar ook een individu dat het recht heeft niet gediscrimineerd te worden en zich op nationale wetgeving kan beroepen. Dit zal vermoedelijk geen nauwgezette coördinatie vereisen, omdat het gaat om afzonderlijke rechtsgebieden waarbij handhaving niet hoeft te overlappen. Wel vereist het een open blik van onderzoekers, beleidsmakers, en handhavers, waarbij een geval of probleem niet gelijk binnen het privacy- en

gegevensbeschermingskader moet worden geplaatst zodra er persoonsgegevens in het spel zijn. Gelukkig beginnen zulke ideeën voet aan de aarde te krijgen, zowel in de literatuur als onder handhavers en beleidsmakers op nationaal en EU gebied.

Naast het uiteenzetten van de noodzaak tot een gecombineerde aanpak van big data, bespreekt Hoofdstuk 5 juridische alternatieven die er onderdeel van kunnen zijn. Deze alternatieven zijn geselecteerd op basis van de problemen die in Hoofdstuk 2 zijn geïdentificeerd en de gevonden problemen en lacunes uit Hoofdstuk 4, aan de hand van de literatuur over problemen en oplossingen in de context van (deelaspecten van) big data. Het overzicht van alternatieven poogt een gegronde aanzet tot verder onderzoek te faciliteren; gezien de reikwijdte van dit onderzoek kan geen oordeel worden geveld over de bredere maatschappelijke en juridische wenselijkheid van de afzonderlijke alternatieven.

In de eerste plaats kan gegevensbeschermingswetgeving op verschillende manieren aangepast worden om de beschermende waarde ervan te vergroten en beter aan te sluiten bij recente technologische ontwikkelingen. Het creëren van eigendomsrechten in persoonsgegevens en het uitbreiden van de reikwijdte van het gegevensbeschermingsrecht naar gegevens die niet aan de criteria voor persoonsgegevens voldoen, worden besproken. Zij worden echter niet als waardevolle oplossingen van de huidige problemen gezien. Waar wel meer aandacht naar uit zou moeten gaan, is de rol die bestaande rechtsgebieden speelt en zou kunnen spelen ter bescherming van het individu binnen big data. Consumentenrecht, mededingingsrecht, en non-discriminatiewetgeving worden alle beschouwd als gebieden die aspecten van het big data proces deels al reguleren, en deels een grotere rol zouden kunnen vervullen waardoor meer negatieve impact van big data op individuele rechten en vrijheden wordt ondervangen. Daarnaast valt uit de literatuur een aantal specifiek op big data toegespitste alternatieven te distilleren, waaronder initiatieven rondom *algorithmic transparency,* dat wil zeggen het inzicht krijgen in de werking van in big data gebruikte algoritmen*, big data ethics,* en sector-specifieke regelgeving. De laatste kan met name van belang zijn in sectoren die zich onderscheiden qua context, problemen, of regulering, zoals de financiële en medische sectoren.

Voor al deze verschillende alternatieven geldt echter dat zij op zichzelf staand geen ultieme oplossing bieden die voldoende is voor de algehele bescherming van individuele rechten en vrijheden. De algemene conclusie, uitgediept in Hoofdstuk 6, is dan ook dat de privacy- en gegevensbeschermingsaanpak op zichzelf niet volstaat, net zo min als één van de andere alternatieven. De variëteit in problemen, fasen waarin problemen zich voordoen, en individuele rechten en vrijheden waar deze problemen een invloed op hebben, maakt dat slechts een gecombineerde benadering voldoende bescherming kan bieden tegen de negatieve impact van big data op de rechten en vrijheden van het individu.