‘Ik ga akkoord’

over toestemming en privacy in het licht van Big Data

Jelle Hoekstra
mail@jellehoekstra.nl

juni 2015

Inhoudsopgave

Introductie

De wereld digitaliseert. Er is onmetelijk veel informatie beschikbaar op het wereldwijde web en de grootte van deze gegevens groeit steeds sneller. Steeds meer mensen krijgen toegang tot (betaalbare) elektronische apparaten, in bijna iedere rugtas vinden we inmiddels een smartphone en tablet of laptop. Door technologische ontwikkelingen blijft de opslagcapaciteit van deze apparaten groeien, evenals de enorme datacentra waar servers draaien die deze apparaten dag en nacht van informatie voorzien. Ook in het dagelijks leven krijgen we steeds meer te maken met de creatie van data door slimme thermostaten, mobiele applicaties, het volgen van surfgedrag, groter gebruik van sociale media enzovoorts.

In al deze omgevingen waar men data creëert, gebruikt of opslaat wordt acceptatie gebruikersovereenkomsten en privacyverklaringen geëist. In 2008 is berekend dat als je de privacyverklaring van elke website die je bezoekt zou willen lezen, je dat enkele weken per jaar kost.[1] De praktijk komt er dan ook op neer dat veel mensen deze verklaringen zonder te lezen op goed vertrouwen accepteren. Zo vertrouwen 1.44 miljard maandelijks actieve gebruikers op (de voorwaarden van) het online sociaal netwerk Facebook.[2] Een groot deel van de totale wereldbevolking heeft dus zijn gegevens met dit bedrijf gedeeld, terwijl Mark Zuckerberg, CEO en oprichter van Facebook, in 2010 zei: "*People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.*"[3] In zijn woorden kiezen mensen er bewust voor om informatie te delen en voelen ze zich daar prima bij. Veel informatie wordt echter *onbewust* gedeeld, zo houdt Facebook het surfgedrag van gebruikers scherp in de gaten en kan Google met de koppeling van accounts zijn gebruikers over verschillende platforms volgen.[4] De vergelijking van Google en Facebook met Big Brother is snel gemaakt, al is de economische realiteit stukken complexer dan het fictieve verhaal van George Orwell. De vraag die eruit voortvloeit is: wat weten deze bedrijven allemaal over je?

[1] McDonald & Cranor, *I/S* (3) 2008, afl. 4, p. 540
[2] Facebook, *Company Info*, http://newsroom.fb.com/company-info/, laatst bekeken op 24 mei 2015
[3] Johnson, *The Guardian* 11 januari 2010
[4] Roosendaal, *Digital personae and profiles in law* 2013, p. 125

Het is niet verwonderlijk dat wetgevers proberen adequaat op deze mondiale ontwikkelingen te reageren. Op dit moment wordt er op Europees niveau hard aan gewerkt om het gebruik van persoonsgegevens verder te reguleren en zo privacy van burgers te beschermen. Technologische ontwikkeling is echter moeilijk te reguleren door het effect van dubbele binding, een dilemma dat voor het eerst werd verwoord in 1980 door David Collingridge.[5] Aan de ene kant is er een informationeel probleem, we kunnen immers moeilijk voorspellen wat de impact is van technologie voordat deze is uitontwikkeld en (volledig) in gebruik is genomen. Hier staat een machtsprobleem tegenover, als een technologie zichzelf eenmaal gevestigd heeft, is het lastig om het te beheersen of veranderen. Wetgevers moeten dus rekening te houden met dit Collingridge-dilemma als ze nieuwe regels willen maken. Een manier om dit in te bewerkstelligen is het creëren van flexibele regels en algemene standaarden, waar ook onvoorziene praktijken aan kunnen worden getoetst.

Onder het huidige recht is de Europese Richtlijn 95/46/EG van toepassing, deze richtlijn is uitgewerkt in de Nederlandse Wet bescherming persoonsgegevens (Wbp). Gezien de technologische ontwikkelingen van het afgelopen decennium heeft de Europese Commissie op 25 januari 2012 een nieuw voorstel gepubliceerd, de Algemene Verordening Gegevensbescherming (AVG).[6] Dit voorstel is nog in behandeling en zal in hoofdstuk drie verder worden besproken.

Tegen deze achtergrond is het goed om te analyseren hoeveel er daadwerkelijk van de waarborging van de privacy terecht komt in de praktijk. Weinig mensen staan stil bij welke informatie we delen, toch hebben we er elke dag mee te maken. Zo uitte Lokke Moerel, hoogleraar Global ICT aan de Universiteit van Tilburg, haar zorgen over het routinematig accepteren van voorwaarden.[7] Deze praktijk vormde tevens de aanleiding van dit onderzoek, daar de auteur dit ook persoonlijk ondervond. Toestemming is immers snel gegeven, maar wat is de waarde er nog van? Dit onderzoek poogt daarom een kritische analyse van het begrip toestemming te geven, waarbij de volgende vraag centraal staat:
Is het geven van toestemming ('consent') voor het gebruik van persoonsgegevens nog een zinvolle manier om informationele privacy te waarborgen in het licht van big data?

[5] Moerel, *Big Data protection* 2014, p. 6
[6] COM(2012)0011 final
[7] Moerel, *Big Data protection* 2014, p. 26

Deze vraag zal worden beantwoord aan de hand van de volgende deelvragen, die in respectievelijk hoofdstuk één tot en met drie zullen worden behandeld:

1. Wat houdt Big Data precies in?
2. Wat is het juridische kader voor het verwerken van persoonsgegevens in de voorgestelde nieuwe Europese verordening?
3. Wat is de functie van het geven van toestemming?

In het *eerste* hoofdstuk wordt het revolutionaire ontstaan big data onder de loep genomen. Hierbij wordt een kort overzicht gegeven van de ontstaansgeschiedenis en zullen diverse aspecten van het gebruik aan bod komen. Tevens worden enkele gevolgen van het gebruik in de maatschappelijke context aangestipt. Voor beantwoording van de *tweede* deelvraag wordt in het volgende hoofdstuk het juridisch kader geschetst in de nieuwe Europese verordening. Deze uitleg zal zich toespitsen op het legitiem gebruik van persoonsgegevens in genoemde wetgeving. Tot slot zal in het *derde* hoofdstuk een filosofische beschouwing van het begrip toestemming gegeven worden. Hierbij staat de functie van het toestemmen centraal en wordt de rol van het begrip vanuit verschillende perspectieven benaderd.

1 De Big Data-revolutie

In 2000 werd een telescoop in gebruik genomen die in de eerste weken al meer informatie had verzameld dan in de hele geschiedenis van de astronomie. Een telescoop die in 2016 in bedrijf zal gaan, zal in vijf weken evenveel gegevens verzamelen als de telescoop uit 2000 in tien jaar heeft gedaan. Dit voorbeeld toont de enorme groei in rekenkracht van computers, evenals de hoeveelheid informatie die daardoor verzameld kan worden.[8] Deze technologische ontwikkelingen staan aan de basis van het fenomeen *big data* dat in dit hoofdstuk verder uitgediept zal worden.

De onderzoeksgebieden waar big data gebruikt wordt zijn enorm divers, het is dan ook lastig om er een sluitende definitie van te geven. Dit blijkt ook wel uit de ruim 40 zeer uiteenlopende definities die University Berkeley verzamelde van vooraanstaande auteurs op het gebied van big data.[9] De begrippen volume, snelheid en variëteit komen terug in de definitie van Gartner, die big data omschrijft als "*high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making*".[10] Deze omschrijving is vooral technisch van aard en legt minder de nadruk op de maatschappelijke impact van big data. In dit onderzoek staat daarom de definitie van Mayer-Schönberger en Cukier centraal: "*big data refers to things one can do at a large scale that cannot be done on a smaller one, to extract new insights or create new forms of value, in ways that changes markets, organizations, the relationship between citizens and governments, and more*".[11] Deze veranderingen zijn een gevolg van wat Mayer-Schönberger en Cukier in hun boek de Big Data-revolutie noemen. In dit hoofdstuk wordt deze revolutie beschreven die bestaat uit het doen van voorspellingen op grote schaal (paragraaf 1.1), de waarde van het leggen van verbanden (paragraaf 1.2) en de maatschappelijke gevolgen (paragraaf 1.3).

1.1 Voorspellen op basis van groot volume

[8] Mayer-Schönberger & Cukier, *Big Data* 2013, p. 7
[9] J. Dutcher, *What is Big Data?* (2014), http://datascience.berkeley.edu/what-is-big-data/ (laatst geraadpleegd 24 mei 2015)
[10] http://www.gartner.com/it-glossary/big-data/ (laatst geraadpleegd 24 mei 2015)
[11] Mayer-Schönberger & Cukier, *Big Data* 2013, p.6

Toepassing van big data draait om het doen van voorspellingen, een interessant voorbeeld hiervan is Google Flu Trends.[12] In 2009 brak er een nieuw griepvirus uit in de Verenigde Staten dat de gezondheidsautoriteiten deed vrezen dat er mogelijk een pandemie zou volgen. Om inzicht te krijgen in de ernst van de situatie en waar nodig maatregelen te nemen werd door de autoriteiten aan dokters gevraagd om hen over nieuwe ziektegevallen te informeren. Het beeld dat deze traditionele manier van tellen gaf liep echter altijd achter, omdat de cijfers slechts eenmaal per week werden doorgegeven en er vaak enkele dagen vertraging tussen ziek worden en een bezoek aan de dokter zit. Met Flu Trends slaagde Google erin om op basis van zoektermen een zeer precies en up-to-date beeld te geven waar en op welke schaal de griep zich ontwikkelde. Dit kregen ze voor elkaar door 50 miljoen zoektermen te vergelijken met de informatie van de zorgautoriteiten over vergelijkbare griepuitbraken in de periode 2003 tot en met 2008. Het systeem zocht naar de correlatie tussen frequentie van zoektermen en griepuitbraken in bepaalde gebieden. Deze resultaten werden naast de cijfers van uitbraken gelegd en leverden zo een set met geteste zoektermen op die de uitbraak van 2009 accuraat konden voorspellen. Het grote voordeel hiervan was dat deze telling continu gebeurde en er geen wachttijd tussen zat, in deze manier van data verzamelen schuilt een van de grote krachten van big data.

De term *big* data impliceert al dat grootte een element is. Dat betreft niet alleen de omvang van de *hoeveelheid* gegevens, maar ook de *schaal* waarop deze gegevens geanalyseerd kunnen worden. In traditionele databases is capaciteit en rekenkracht vaak lastig, om een grote dataset te analyseren moet een computer namelijk lang nadenken en alle onderdelen van een bestand systematisch langslopen. Dit proces kost veel tijd, geld en is foutgevoelig. Om bijvoorbeeld berekeningen of statistische analyses uit te voeren word in deze omgeving daarom vaak gebruik gemaakt van een beperkte set waarnemingen die op basis van willekeur worden verzameld. Deze aselecte steekproeven, ook wel samples genoemd, worden vervolgens omgerekend in percentages en geëxtrapoleerd om wat te kunnen zeggen over een groter geheel. Deze methode was natuurlijk niet helemaal waterdicht, maar was een goede manier om voorspellingen te doen. Om groeiende datasets overzichtelijk te houden, was het echter nodig om sterkere algoritmes te ontwikkelen. Deze sterkere algoritmes hebben ervoor gezorgd dat we in plaats van samples, weer volledige datasets kunnen gebruiken om te analyseren.

[12] Mayer-Schönberger & Cukier, *Big Data* 2013, p.1-2

Deze ontwikkeling kunnen we illustreren met een voorbeeld van volkstellingen. Dataverzamelingen gaan namelijk al lang terug, denk bijvoorbeeld aan het Kerstverhaal uit de Bijbel. Voor deze telling moesten Maria en Jozef terugkeren naar hun geboortedorp om zich te laten registreren. Dat had destijds nogal wat voeten in de aarde, maar was gezien de relatief kleine omvang van de bevolking nog mogelijk. Toen dit soort tellingen door bevolkingsgroei niet meer mogelijk was, ging men over op aselecte steekproeven om uit te rekenen hoe groot de bevolking was. Door 'nieuwe manieren van tellen' met de komst van de sterke algoritmes voor big data hebben we echter geen steekproeven meer nodig: we kunnen bij wijze van spreken nu weer *alle* bewoners tellen en daar tegelijkertijd complexe berekeningen op loslaten.

Het tellen en analyseren van 'alles' heeft als voordeel dat er meer conclusies uit getrokken kunnen worden. De keerzijde hiervan is dat bij het registreren van 'alles' er altijd onnauwkeurigheden ontstaan. Was het bij een steekproef echter nog nodig om exact te zijn, in een grote database zijn afwijkende waarden geen groot probleem. Door de enorme omvang van de dataset hebben telfouten slechts marginale invloed en kunnen door het algoritme worden genegeerd. Een voorbeeld hiervan is de ontwikkeling van automatische vertaalmachines. Vroeger werkten deze tools met woordenboeken en geprogrammeerde grammatica, er is veel geld in onderzoek gestoken om de computers regels aan te leren om goed te vertalen. Dit leverde echter lang niet altijd goede vertalingen op. Google Translate vergelijkt zinnen met alle vertalingen die op het hele wereldwijde web staan. Vanzelfsprekend zitten hier ook foute of onnauwkeurige vertalingen bij, maar door de grote schaal van de hoeveelheid beschikbare vertalingen maakt dit niet uit. Google Translate werkt lang niet altijd optimaal, maar is op dit moment een van de meest nauwkeurige vertaalmachines en het werkt beter dan oude vertaalsoftware. "Meer overtreft beter".[13]

1.2 Verbanden en verdienen

Een grote dataset zorgt ervoor dat de *correlatie* tussen fenomenen een stuk sterker wordt. Eerder werd al genoemd dat voorspellen een belangrijke toepassing van big data is, zo stelde hoofdredacteur Chris Anderson in het tijdschrift Wire: "*With enough data, the numbers speak for themselves. Petabytes allow us to say:* 'Correlation is good enough.'"[14] Een correlatie

[13] Eigen vertaling van "More trumps better". Uit: Mayer-Schönberger & Cukier, *Big Data* 2013, p.39
[14] Mayer-Schönberger & Cukier, *Big Data* 2013, p. 71

geeft echter aan *wat* er in samenhang gebeurt en niet *waarom* het gebeurt. Het is erg belangrijk om dit onderscheid goed te maken, omdat de menselijke neiging bestaat om correlaties toch in termen van causaliteit te interpreteren. Onze hersenen leggen automatisch verbanden tussen fenomenen die vaak op elkaar volgen, op deze manier scheppen we orde in onze belevingswereld. Dit betekent echter niet dat fenomenen elkaar ook *noodzakelijk* volgen, met andere woorden dat er een causaal verband is en welke richting oorzaak en gevolg op gaan.[15] De komst van big data zorgt ervoor dat het niet meer noodzakelijk is om voorafgaand aan onderzoek hypotheses op te stellen, het belang van causaliteit verdwijnt hiermee echter niet volledig. Het gebruik van big data berust immers gedeeltelijk op theorieën, bijvoorbeeld in de keuze van proxy's in de statistiek. Een proxy is een variabele die op zichzelf niet direct relevant is, maar die een onzichtbare of onmeetbare variabele kan vervangen om zo toch een indicatie te geven van een bepaald fenomeen. Een goede proxy heeft een sterke correlatie met de variabele die het moet vervangen.[16]

Om correlaties te ontdekken vertalen we steeds meer aspecten van de wereld in (digitale) gegevens, dit proces wordt dataficatie genoemd. Dit is niet hetzelfde als digitaliseren, wat slechts de conversie van analoge opslag naar digitale opslag betreft, bijvoorbeeld het scannen van een boek als afbeelding. Dataficeren gaat een stap verder en zet gegevens om in indexeerbare informatie, een gescande afbeelding wordt dan omgezet in tekst die doorzocht kan worden. Dat is de toegevoegde waarde van het Google Books project, er kan automatisch worden gezocht op overeenkomsten tussen teksten (een nuttig middel om plagiaat tegen te gaan). Dataficatie kan geld opleveren, bijvoorbeeld door de locatiegegevens van telefoons op te slaan. Ten eerste op individueel niveau, door gerichte advertenties aan te bieden op basis van waar je je bevindt. Ten tweede op geaggregeerd niveau door het aantal niet-bewegende telefoons op een snelweg te tellen en zo files in kaart te brengen.

Big data draait dus vooral om big business, data wordt de nieuwe olie van het internet en de valuta van de digitale wereld genoemd.[17] Vanuit dit oogpunt bestaan 'gratis' diensten op internet dan ook niet, omdat je betaalt met je persoonsgegevens. Het is echter lastig om data in dollars uit te drukken, zo bleek bij de beursgang van Facebook. De markt waardeerde het

[15] Meer over het concept causaliteit: Hume *Het menselijk inzicht* 2002, p. 60
[16] Proxy Statistics, In: Wikipedia, https://en.wikipedia.org/wiki/Proxy_%28statistics%29 (laatst geraadpleegd op 21 juni 2015)
[17] Meglena Kuneva, European Consumer Commissioner (2009), http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (laatst geraadpleegd op 24 mei 2015)

bedrijf destijds op 104 biljoen dollar, terwijl de waarde volgens accountantstandaarden slechts 6.3 biljoen was. Dit verschil tussen marktwaarde en boekwaarde kwam door de potentie die investeerders zagen in de beschikbare data van alle Facebookgebruikers.

Er vindt een verschuiving plaats in de houding ten opzichte van data, namelijk van primair (en eenmalig) naar secundair (en meervoudig) gebruik. Dit leidt ertoe dat zoveel mogelijk data wordt verzameld en bewaard, omdat het juist in secundair gebruik tot interessante inzichten en economisch voordeel kan leiden.[18] Van tevoren wordt niet verzonnen waar het registreren van bepaalde zaken nuttig voor is, pas na analyse komt men tot de ontdekking dat gegeven X handig is om fenomeen Y te voorspellen. Dit heeft als gevolg dat het proces van dataficering wordt versneld, omdat in elk gegeven potentiële waarde zit.

1.3 Gevolgen van de revolutie

Door deze ontwikkelingen ontstaan nieuwe bedrijven die zich specialiseren in het gebruik van big data. Verzamelaars van gegevens, dataspecialisten die ingewikkelde analyses uit kunnen voeren en bedrijven die vernieuwende manieren zoeken om big data te gebruiken. De grootste waarde zit nu nog in de laatste groep, omdat dit de pioniers zijn die de mogelijke toepassingen aan het ontdekken zijn. Als hier veel kennis over vergaard is, zal de nadruk waarschijnlijk op de beschikbaarheid van informatie en macht over gegevens komen te liggen. Een ander gevolg van big data kan zijn dat we gedwongen worden om het menselijk instinct te heroverwegen.[19] Er zijn namelijk al voorbeelden van bijvoorbeeld voetbalclubs die niet meer op basis van de ervaring van coaches werken, maar slechts beslissingen nemen die gebaseerd zijn op statistische analyse. Als deze trend zich doorzet naar andere werkvloeren zullen werknemers de vaardigheden waarover ze beschikken dus ook moeten veranderen.

Big data biedt dus een hele hoop kansen en mogelijkheden en zal de manier waarop we naar de wereld kijken drastisch veranderen. Hierbij gaat het met name om het secundair gebruik van gegevens, voor doeleinden die bij het verzamelen van de data nog niet te voorspellen zijn. Hoewel dit veelbelovend klinkt, brengt het gebruik ervan ook een grote risico's met zich mee die zeker niet uit het oog verloren moeten worden. Waardevolle gegevens kunnen in verkeerde handen immers veel schade aanrichten. Als de Stasi in het voormalige Oost Duitsland beschikking hadden gehad over de hoeveelheid gegevens die internetbedrijven nu

[18] Mayer-Schönberger & Cukier, *Big Data* 2013, p. 103
[19] Mayer-Schönberger & Cukier, *Big Data* 2013, p. 141

van ons hebben had de geschiedenis er wellicht heel anders uit gezien.[20] Machtsmisbruik is een gevaar van big data dat tevens grote gevolgen heeft voor privacy. In het volgende hoofdstuk zal daarom een juridisch kader geschetst worden met betrekking tot privacy en toestemming in het licht van big data.

[20] Mayer-Schönberger & Cukier, *Big Data* 2013, p. 150

2 Gegevensbescherming in Europese regelgeving

In dit hoofdstuk staat het juridische kader voor het verwerken van persoonsgegevens in de nieuwe Europese verordening centraal. In de eerste paragraaf zal worden ingegaan op de notie van informationele privacy en hoe dit concept zich verhoudt tot het grondrecht van privacy. Vervolgens zal worden beschreven in paragraaf 2.2 wat de achterliggende principes van de voorgestelde verordening zijn en hoe dit voorstel tot stand is gekomen. In paragraaf 2.3 van dit hoofdstuk zal een voorbeeld gegeven worden van een manier waarop gegevens worden verzameld. Tot slot zullen in de paragraaf 2.4 twee gronden worden uitgediept op basis waarvan het verwerken van persoonsgegevens volgens de nieuwe wetgeving geoorloofd is.

2.1 Informationele privacy

Iedereen weet wat er met 'privacy' wordt bedoeld, toch zijn er veel verschillende interpretaties van dit begrip. In juridische context spreekt men vaak over het recht op persoonlijke levenssfeer zoals dat ook tot uiting komt in art. 8 EVRM, het is hierbij belangrijk om privacy te onderscheiden van de bescherming van persoonsgegevens. Het algemene recht op privacy vindt met terug in de eerbiediging van de persoonlijke levenssfeer in art. 8 EVRM, terwijl de nieuwe dataprotectieverordening (AVG) is bedoeld om de *informationele privacy* te waarborgen. Deze definitie van privacy komt van Alan Westin en betreft het recht om te bepalen wie wat over jou weet.[21] In de inleiding kwam dit onderwerp reeds ter sprake, met betrekking tot de vraag wat internetbedrijven over je weten. Westins definitie laat een duidelijk element van informationele zelfbeschikking zien en gaat uit van een autonoom mensbeeld (als individu bepaal je je eigen identiteit). Informationele privacy kan ook omschreven worden als zeggenschap over wat men weet over jezelf.[22]

Naast de algemene notie van privacy in art. 8 EVRM is bescherming van persoonsgegevens ook specifiek verankerd in artikel 8 van het Handvest van de grondrechten van de EU. Dit recht wordt eveneens verwoord in artikel 16 lid 1 van het Verdrag betreffende de werking van de Europese Unie (VWEU). In lid 2 van genoemd artikel wordt de bevoegdheid om hiertoe EU-voorschriften uit te vaardigen ook expliciet vermeld.

[21] Westin, *Privacy and Freedom* 1968
[22] Engelfriet, *Tijdschrift voor Internetrecht* 2014, afl. 1, p. 15

2.2 Ratio achter bescherming persoonsgegevens

Het verwerken van persoonsgegevens is noodzakelijk voor het functioneren van de maatschappij. Om zeggenschap te waarborgen zijn er daarom regels over de verwerking van persoonsgegevens. Niet alle informatie die verzameld wordt in het kader van big data is persoonlijk, een relativering is hier dus op zijn plaats. Het onderscheid tussen persoonlijke en niet-persoonlijke informatie is soms echter lastig. Informatie over de staat van een onderdeel in je auto is bijvoorbeeld niet direct persoonlijk, de locatie waar dit onderdeel zich bevindt is dat wel (het laat immers zien waar je rijdt). Er zijn verschillende manieren om persoonlijke gegevens te beschermen, maar door de komst van big data werken een aantal van deze strategieën niet (meer) goed. Voorbeelden hiervan zijn anonymisering, opting-out en het geven van toestemming.

Anonymisering lijkt op het eerste gezicht gemakkelijk door alle gegevens te verwijderen die je identiteit zouden kunnen prijsgeven. Zo zouden we de naam en woonplaats van Willem-Alexander, woonachtig in Wassenaar kunnen verwijderen.[23] Dezelfde persoon zouden we echter ook kunnen aanduiden als "vader van drie kinderen, wonende te Wassenaar en liefhebber van voetbal, rijdt soms in een gouden koets". Door deze combinatie aan gegevens weet je (waarschijnlijk) nog steeds over wie het gaat.

Bescherming van je gegevens door ervoor te kiezen om een dienst niet te gebruiken (opting-out) wordt ook steeds lastiger. Als iedereen zijn gegevens deelt en jij bent de enige die dat niet doet is dat een dubieus signaal. Iemand die bijvoorbeeld zijn huis niet herkenbaar op Google Street View wil, kan het laten vervagen. Potentiele dieven kunnen dat echter interpreteren als een signaal dat er wat te halen valt en dan schiet je er niks mee op.

Een andere mogelijkheid om voor individuen om controle uit te oefenen op persoonlijke gegevens is de plicht voor databeheerders om te informeren en toestemming te vragen. Dit principe van *geïnformeerde toestemming* (Engelse term: 'informed consent') is de hoeksteen voor de huidige Europese regelgeving, maar is niet de enige manier waarop het mogelijk is om het verzamelen en verwerken van data te reguleren.[24] Dit heeft geleid tot enorm lange privacyvoorwaarden die nauwelijks gelezen, laat staan begrepen worden.[25] De kracht van big

[23] De Jong, *Computerrecht* 2015/40, afl. 1, p.12
[24] Mayer-Schönberger & Cukier, *Big Data* 2013, p. 153
[25] Cate, *The Failure of Fair Information Practice Principles* 2006

data is secundair gebruik waarvan het doel nog niet bekend is als de gegevens verzameld worden. Hoe kunnen bedrijven informeren over een doel dat nog niet bestaat en hoe kunnen individuen (blanco) toestemming geven voor iets wat ze niet weten? In hoofdstuk vier zal verder in worden gegaan op het nut van toestemming geven in het algemeen.

In 2012 is de eerste versie voor de Algemene Verordening Gegevensbescherming (AVG) ingediend door de Europese Commissie. De doelstelling van dit wetgevingsvoorstel is om het fundamentele recht op gegevensbescherming te waarborgen en het vrije verkeer van persoonsgegevens tussen de lidstaten te garanderen. In het voorstel wordt hetzelfde doel gehanteerd als in de op dit moment geldende Richtlijn 95/46/EG.[26] De ingrijpende technologische en sociale veranderingen in de maatschappij hebben ervoor gezorgd dat persoonsgegevens slechts fragmentarisch worden beschermd. Het nieuwe voorstel wil hier dan ook een krachtiger en coherenter juridisch kader voor geven om zo meer rechtszekerheid te bieden. Daar dit een verordening en geen richtlijn betreft, heeft het nieuwe voorstel ook meer invloed omdat het niet geïmplementeerd hoeft te worden maar direct gelding heeft.

Er zijn zo'n 4.000 amendementen ingediend bij dit conceptvoorstel, een teken dat er veel te doen is om deze wetgeving.[27] Op 12 maart 2014 is het voorstel met 350 amendementen in eerste lezing aangenomen door het Europees Parlement, de verwachting is dat het complete ontwerp van de wetgeving eind 2015 klaar zal zijn.[28] Het Europees Parlement heeft in hun voorstel onder andere artikel 20 geherstructureerd met betrekking tot *profiling* (waarover meer in paragraaf 2.3). Om deze reden is er in dit onderzoek voor gekozen om dit vernieuwde voorstel uit 2014 te analyseren in plaats van het eerste concept uit 2012. Wanneer in dit onderzoek dus naar de AVG wordt verwezen, is het aangenomen voorstel in eerste lezing van het Europees Parlement bedoeld.[29]

In artikel 4 AVG wordt de betekenis van verscheidene begrippen uiteen gezet, hieronder worden enkele daarvan toegelicht. De term "persoonsgegevens" wordt in de AVG gedefinieerd als "iedere informatie betreffende een betrokkene".[30] Blijkens het eerste lid

[26] Zo blijkt uit de toelichting van de AVG: COM(2012)0011 final, p. 1-2
[27] Kiss & Szöke, *Evolution or Revolution?* 2015, p. 328
[28] Aldus Rapporteur Jan Philipp Albrecht in een statement op zijn website (laatst geraadpleegd 21 juni 2015): http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf
[29] AVG: P7_TA-PROV(2014)0212 Europees Parlement Wetgevingsresolutie (aangenomen op 12 maart 2014), geraadpleegd via: http://www.europarl.europa.eu/
[30] Art. 4 lid 2 AVG

wordt onder betrokkene een geïdentificeerde natuurlijke persoon verstaan, of iemand die als zodanig kan worden gekwalificeerd. Met de omschrijving "iedere informatie" heeft de wetgever een brede interpretatie van het begrip persoonsgegevens beoogd, zo valt te concluderen uit een publicatie van de Groep Gegevensbescherming Artikel 29 (ook wel Artikel 29 Werkgroep genoemd).[31] Dit is een werkgroep die is opgericht onder de Richtlijn 95/46/EC en bestaat uit afgevaardigden van de verschillende nationale autoriteiten op het gebied van gegevensbescherming. Een ander begrip is de *data controller*, oftewel de "voor de verwerking verantwoordelijke" partij (persoon of organisatie).[32] De verantwoordelijke bepaalt het doel van de verwerking van de gegevens en wie gebruik maakt van de gegevens. Onder het gebruik van de gegevens valt ook de verkoop van data of daaruit voortvloeiende profielen.

2.3 Profiling

Een veelgebruikte procedure om een grote hoeveelheid gegevens te categoriseren is de techniek van *automated profiling.* Dit gebeurt in diverse omgevingen, zoals justitieel onderzoek, marketing, zorginstellingen en nog veel meer. *Profiling* vindt onder andere plaats door het online volgen van surfgedrag. Dat gebeurt met behulp van cookies (bestanden die informatie over gebruik van je webbrowser registreren) of gebruikersaccounts (bijvoorbeeld bij diensten als Facebook en Google). Het maken van een profiel (indeling in een 'groep') is een manier om grote hoeveelheden gegevens met betrekking tot een gebruiker ordelijk te verzamelen. Een profiel laat veel zien over de persoonlijkheid van de persoon die erachter zit en vormt zo een digitale afspiegeling van een individu dat sterk raakt aan de identiteit van een persoon. Dit is een gewilde bron van informatie voor adverteerders, maar op andere plekken kan gerelateerde informatie ook gebruikt worden om bepaalde groepen wel of niet van producten te voorzien. Op basis van een profiel kan bijvoorbeeld besloten worden wat de premie is die je voor een bepaalde verzekering betaalt. Een set met kenmerken (een profiel dus) kan worden gebruikt om beslissingen te nemen ten aanzien van personen, waar soms zelfs geen menselijke tussenkomst meer voor nodig is.[33]

Op voorstel van het Europees Parlement is een definitie van dit soort technieken in de AVG gekomen. In art. 4 lid 3a wordt *profiling* omschreven als "*any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or*

[31] WP 136, 4/2007, Opinie van Art. 29 Werkgroep (over het begrip persoonsgegeven), geraadpleegd via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf
[32] Art. 4 lid 5 AVG
[33] Hildebrandt & Gutwirth 2008, p. 18

to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior". In deze definitie komt ook de brede toepassing van profiling in de maatschappij tot uiting. Volgens het EP is een goede definitie van profiling noodzakelijk om geïnformeerde toestemming voor onderwerping aan dit soort praktijken mogelijk te maken.[34] De plicht tot informatieverstrekking aan betrokkenen staat beschreven in art. 14 AVG. In lid 1 sub ga van dit artikel wordt de *data controller* ook verplicht gesteld om de betrokkene over het bestaan van profiling te informeren, evenals over de gevolgen en achterliggende mechanismes ervan. Informatieverstrekking dient op een heldere wijze te gebeuren, dit komt tot uiting in art. 15, waar het recht van toegang van de betrokkene is neergelegd. Interessant in dezen is de toevoeging van het EP dat deze informatie in "*clear and plain language*" moet worden gegeven.[35] Deze toevoeging is waarschijnlijk bedoeld om uitgebreide juridische uitleg te voorkomen. Zoals reeds is betoogd worden veel van dit soort ingewikkelde documenten immers nauwelijks gelezen, laat staan begrepen.

In art. 20 wordt een algemeen verbod op profiling (volgens art. 4 AVG) geïntroduceerd, dit is het geval met alle manieren om data te verzamelen, verwerken of gebruiken. Profiling is alleen toegestaan op grond van een wettelijke basis (art. 20 lid 2). Naast toestemming kan dat gebeuren als dat nodig is voor de uitvoering van een contract of als het uitdrukkelijk geëist wordt op grond van EU-wetgeving of nationale wetgeving (art. 20 lid 2 sub b en c). De praktijk is echter dat veel profielen worden aangemaakt zonder dat betrokkenen daarvan weten.[36]

2.4 Rechtmatig gebruik van persoonsgegevens

In paragraaf 2.2 is reeds genoemd dat toestemming één van de wettelijke grondslagen is uit de AVG om legaal gegevens te kunnen verzamelen.[37] Andere mogelijke grondslagen zijn een overeenkomst, wettelijke verplichting of als het gaat om het beschermen vitale belangen (bijvoorbeeld in medische dossiers) of taken van algemeen belang en openbaar gezag. In paragraaf 2.4.1 wordt eerst het concept van geïnformeerde toestemming verder uitgewerkt en vervolgens in paragraaf 2.4.2 het principe van accountability toegelicht.

[34] AVG, amendement nr. 87
[35] AVG, amendement nr. 136
[36] AVG, amendement nr. 158
[37] Art. 6 lid 1 sub a AVG

2.4.1 Geïnformeerde toestemming

Reeds is genoemd dat toestemming van de betrokkene een centrale rol speelt in databeschermingswetgeving.[38] Een definitie ervan wordt gegeven art. 4 lid 8 AVG, "*elke vrije, specifieke, op informatie berustende en uitdrukkelijke wilsuiting waarmee de betrokkene, door middel van hetzij een verklaring hetzij een ondubbelzinnige actieve handeling aanvaardt dat hem betreffende persoonsgegevens worden verwerkt voor één of meerdere doeleinden*". Het onderstreepte is een toevoeging door het Europees Parlement. Dit vereiste van doeleinde is een belangrijke voorwaarde die ook terugkomt in art. 7 van de AVG, dit doeleinde moet bovendien specifiek zijn. Blanco toestemming zonder het precieze doel van de verwerking te specificeren is niet acceptabel, zo blijkt uit een opinie van de Artikel 29 Werkgroep over toestemming ('consent').[39] In deze opinie worden verschillende elementen toestemming volgens de huidige richtlijn geanalyseerd, deze definitie luidt als volgt: "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".*[40] Deze definitie heeft veel raakvlakken met de definitie uit de voorgestelde AVG en is daarom nog steeds relevant, hieronder zullen enkele elementen worden toegelicht.

Met de woorden "*... any ... indication of his wishes ... signifying ...*"[41] is een brede interpretatie van de indicatie van de toestemming beoogd, het woord "geschreven" is vanwege flexibiliteit dan ook vermeden. De termen "*indication"* en "*signifying*" wijzen echter wel in de richting dat een actie nodig is. Het valt daarom te betwisten of het ontbreken van enig gedrag (passieve actie) altijd een indicatie is, maar dit is mogelijk in een zekere context. "*... freely given ...*" (oftewel "*vrije wilsuiting"* in de AVG) laat zien dat er sprake moet zijn van een ongedwongen beslissing.[42] In het geval van intimidatie, bedrog, ongelijkheid of een andere omstandigheid waardoor de keuzevrijheid van het individu wordt beperkt is er geen sprake van vrije toestemming.
Eerder werd al genoemd dat toestemming *"... specific...*" ("*specifiek*" in de AVG) moet zijn en daarmee dus ook begrijpelijk.[43] Het kan niet van toepassing zijn op een set van activiteiten met een open einde, waardoor de context waarin toestemming kan worden gebruikt beperkt is. Dit vereiste is dus sterk verbonden met het feit dat de betrokkene goed geïnformeerd moet

[38] WP187, 15/2011 Opinie van Art. 29 Werkgroep ('on the definition of consent'), p. 3
[39] WP187, 15/2011 Opinie van Art. 29 Werkgroep ('on the definition of consent'), p.17
[40] Art. 2(h) Richtlijn 95/46/EC
[41] WP187, 15/2011 Opinie van Art. 29 Werkgroep ('on the definition of consent'), p. 11
[42] WP187, 15/2011 Opinie van Art. 29 Werkgroep ('on the definition of consent'), p. 12
[43] WP187, 15/2011 Opinie van Art. 29 Werkgroep ('on the definition of consent'), p. 17

worden. De toestemming moet dus betrekking hebben op verwerking die redelijk en noodzakelijk is met betrekking tot het geformuleerde doel.
"... informed ..." (oftewel "*op informatie berustende"*) is het laatste element van de definitie van toestemming.[44] Hoewel op het verstrekken van informatie niet altijd toestemming volgt (er kan ook een andere wettelijke grond voor verwerking gebruikt worden), impliceert het geven van toestemming wel het beschikken over de benodigde informatie. Het is immers nodig dat de betrokkene weet wat de gevolgen ervan zijn. Hierbij is de kwaliteit van informatie van belang, een gemiddelde gebruiker moet het kunnen begrijpen, en de toegankelijkheid ervan. Het is niet voldoende dat informatie 'ergens' beschikbaar is, zo werd ook benadrukt door het Hof van Justitie in 2004 in een zaak waar in een werknemerscontract werd verwezen naar bepaalde condities die elders te vinden waren.[45]

2.4.2 Verantwoordelijkheid

Er is ook een bepaling die het mogelijk maakt voor *data controllers* om op basis van een gerechtvaardigd belang gebruik te maken van persoonsgegevens.[46] Dit kan alleen als deze belangen fundamentele rechten van de betrokkene niet schaden, voorts moeten *data controllers* dan ook openbaar aannemelijk maken waarom dit een legitiem belang is. Dit laatste element is door het Europees Parlement toegevoegd, het doel van deze aanpassing is om meer duidelijkheid te bieden over het gebruik van gegevens op basis van een legitiem belang. Het betreft hier dus een belangenafweging die goed moet worden beargumenteerd om hier een geslaagd beroep op te doen. Hier is nog geen jurisprudentie over omdat de verordening nog niet is aangenomen, de praktijk zal dus uit moeten wijzen hoe dit tot uiting zal komen. In deze bepaling wordt bescherming dus gerealiseerd door de *data controller* verantwoordelijk te maken voor het gebruik van persoonsgegevens en zo een bepaalde ethiek te ontwikkelen. Dit principe wordt ook wel aangeduid met de Engelse term 'accountability' en vormt een belangrijk onderdeel van de vernieuwde kijk op databeschermingswetgeving. Mayer-Schönberger en Cukier zien dit als de toekomst van de wetgeving: "*We envision a very different privacy framework for the big-data age, one focused less on individual consent at the time of collection and more on holding data users accountable for what they do.*"[47]
Alvorens conclusies te trekken uit deze toekomstvisie zal in het volgende hoofdstuk eerst de functie van toestemming nader beschouwd worden.

---

[44] WP187, 15/2011 Opinie van Art. 29 Werkgroep ('on the definition of consent'), p. 19
[45] HvJ EU 5 oktober 2004, gevoegde zaken C-397/01 tot en met C-403/01
[46] Art. 6 lid 1a AVG
[47] Mayer-Schönberger & Cukier, *Big Data* 2013, p. 173

3 De functie van toestemming

Ergens in toestemmen betekent dat je je goedkeuring ergens aan verleent of iets inwilligt. In dit hoofdstuk staat het begrip 'toestemming' in brede zin centraal en zal onderzocht worden wat achterliggende waarden zijn (paragraaf 3.1), hoe toestemming tot uiting komt in de praktijk (paragraaf 3.2) en of wat eventuele alternatieven zijn (paragraaf 3.3).

3.1 Toestemming als uiting van zelfbeschikking

Roosendaal gaat uit van de *menselijke waardigheid* als een overkoepelende waarde die de basis is voor fundamentele rechten.[48] In zijn optiek moet de mens gerespecteerd worden en daarom vrij zijn van kwellingen als slavernij en marteling, dit soort onmenselijke gedragingen tast namelijk zijn *autonomie* aan. Autonomie geeft ons de mogelijkheid en verantwoordelijkheid om beslissingen te nemen en vormt tevens een voorwaarde voor het hanteren van moraal en waarden. De manier waarop we met zaken omgaan, bepaalt hoe we worden gezien door anderen en geeft zo uiting aan onze *identiteit*. We kiezen er zelf voor welke delen van deze identiteit we laten zien, afhankelijk van de situatie waarin we ons begeven. Het recht, maar tevens het vermogen om dit te doen is een uiting van *informationele zelfbeschikking*. Dit geeft ons zeggenschap over het leven en is een inherente waarde van ons mens zijn, we hebben de keuze en controle om informatie wel of niet te delen. De controle om zelf keuzes te kunnen maken is daarmee zowel een voorwaarde als een gevolg van toestemming: het geeft de betrokkene invloed op het beheer van zijn gegevens.

Het verschijnsel dat informatie in een bepaalde omgeving blijft en niet zomaar elders heen getransporteerd wordt is *contextuele integriteit.* Als informatie wel wordt getransporteerd, dient dit te gebeuren in overeenstemming met de regels die relateren aan de originele context waarin de informatie gepubliceerd is. We beoordelen onze privacy anders in verschillende situaties, zo geeft filosofe Helen Nissbaum als voorbeeld dat we het prima vinden als een douanebeambte op het vliegveld de inhoud van onze toilettas bekijkt, terwijl we een wildvreemde die dat bij de bakker wil waarschijnlijk een klap verkopen.[49]

[48] Roosendaal, *Digital personae and profiles in law* 2013, p. 68-69
[49] Martijn, *De Correspondent* 5 november 2014

Een voorwaarde voor het realiseren van zelfbeschikking is het beschikken over informatie, daarvoor is transparantie nodig van de *data controller* naar de *betrokkene*. Transparantie is op zichzelf geen grond voor het verwerken van gegevens, maar een essentieel vereiste om ervoor te zorgen dat toestemming valide is. Dit houdt in dat alle relevante informatie dient te worden verstrekt die nodig is om een serieuze afweging te kunnen maken.[50]

Als ik toestemming geef om bepaalde persoonsgegevens te gebruiken, betekent dat niet dat ik hiermee inlever op mijn privacy. Het recht van privacy houdt namelijk (onder andere) in dat ik controle heb over wat er met mijn gegevens gebeurt, zelf kunnen bepalen wie wat over je weet is dus een uitoefening van dat recht. Problematisch hierbij is echter dat we slecht zicht hebben op welke (persoonlijke) gegevens worden verwerkt en door wie.[51] Zelfs als we dat wel zouden weten, blijft het lastig om te overzien wat daar de gevolgen van zullen zijn.

3.2 Toestemming in de praktijk

Roosendaals beschrijving van het autonome individu gaat uit van de mens als een rationeel denkend wezen, oftewel een persoon die zijn opties naast elkaar legt en een weloverwogen beslissing maakt die in zijn eigen belang is. Sociaal onderzoek wijst echter uit dat we ons lang niet altijd als zo'n *homo economicus* (een berekenende mens) gedragen.[52] In plaats daarvan reageren we vaak op basis van oerdriften en impulsen, waarbij we fouten maken en beslissingen nemen die helemaal niet voordelig voor ons uitpakken. In deze gevallen is onze zelfbeschikking eigenlijk dus nauwelijks aanwezig. Een groeiende zorg rondom gegevensbescherming is dat individuen vaak geen idee hebben waar ze in toestemmen en dat als er om toestemming gevraagd wordt er vaak geen echt alternatief voor acceptatie is. Dit leidt tot de praktijk waarin het accepteren van voorwaarden een routinematige klus wordt en daarmee dus eigenlijk haar betekenis verliest.[53] Het daadwerkelijke effect van privacywetging in de praktijk wordt dan ook in twijfel getrokken door Zuiderveen Borgesius, die verbonden is aan het Instituut voor Informatierecht van de Universiteit van Amsterdam.[54]

Het accepteren van voorwaarden en gebruik van internetdiensten is een alledaagse praktijk. Elke dag bezoeken we websites, bekijken we updates op Facebook en zoeken we wat op via

[50] WP187, 15/2011 Opinie van Art. 29 Werkgroep ('on the definition of consent'), p. 9
[51] Hildebrandt & Gutwirth 2008, p.308
[52] Moerel, *Big Data protection* 2014, p. 24
[53] Moerel, *Big Data protection* 2014, p. 26
[54] Zuiderveen Borgesius, *Nederlands Juristenblad* 2015

Google. Op al deze terreinen worden veel persoonsgegevens verwerkt, vaak met toestemming van de betrokkene. Gebruikers weten echter nauwelijks dat hun gegevens verzameld worden, waar deze voor worden gebruikt en wat de gevolgen daarvan kunnen zijn.[55]

Er is dus een grote informatieasymmetrie tussen *betrokkene* en degene die de informatie verzamelt. Door de manier waarop partijen hun informatie verpakken wordt deze kloof in de praktijk niet verkleind. Verder blijkt uit gedragsstudies dat we sterk worden beïnvloed in de manier waarop we ons gedragen door de *biases* die we hebben. Zuiderveen Borgesius haalt deze onderzoeken aan in zijn artikel over big data en schrijft over de *default bias* en de *present bias*.[56] De eerste bias beschrijft de neiging om geen actieve keuze te maken, maar de standaardinstellingen te accepteren of toestemming te geven door geen bezwaar te maken. Dit laatste gebruikt Google bijvoorbeeld met haar zoekmachine, door zoektermen in te voeren accepteer je automatisch hun gebruiksvoorwaarden.[57] De *present bias* laat zien dat mensen er vaak voor kiezen om *nu* van voordeel te genieten in plaats van in de toekomst. Denk hierbij aan voorbeelden als dat het moeilijk is om geld te sparen of gezond te blijven eten. Dit heeft ook betrekking op privacy, als mensen voorwaarden moeten accepteren om een website te bezoeken of een bepaalde dienst of applicatie te kunnen gebruiken zullen zij sneller geneigd zijn om toekomstige nadelen met betrekking tot privacy te negeren.

In de enge zin van het woord hebben gebruikers wel degelijk de keuze om bepaalde voorwaarden wel of niet te accepteren. Door de sterke en invloedrijke positie van bedrijven als Facebook en Google is er echter vaak sprake van een ‘locked-in-choice’. Als 1.44 miljard mensen op de wereld van dezelfde sociale netwerkdienst gebruik maken en dit medium de belangrijkste manier is om met elkaar in contact te blijven, is het nauwelijks een alternatief om voor een ander netwerk te kiezen. De keuze is dan wel gebruiken of niet gebruiken, de sociale druk zorgt dan dus ook voor een inperking van de privacy zonder dat daar een duidelijke wilsuiting aan ten grondslag ligt. In hoeverre is dan nog sprake van vrijwillig gegeven toestemming?

[55] Acquisti & Grossklags, *What Can Behavioral Economics Teach Us About Privacy?* 2007
[56] Zuiderveen Borgesius, *Nederlands Juristenblad* 2015
[57] Roosendaal, *Digital personae and profiles in law* 2013, p. 142

3.3 Alternatieven voor toestemming

De roep in de wetenschappelijke literatuur om het principe van 'accountability' in te voeren, en zo data controllers verantwoordelijk te maken voor ethisch gebruik, is een goed alternatief om de hierboven beschreven discrepantie tussen doel en het effect van de maatregelen op te heffen (zie ook paragraaf 2.4.2). Hiermee kan daadwerkelijk controle over gegevens gerealiseerd worden. Daarnaast is het beginsel van 'Privacy by Design' ook opgenomen in art. 23 van de AVG, wat inhoudt dat ontwikkelaars eraan gehouden zijn om applicaties zo te ontwerpen dat er rekening gehouden wordt met de privacy van de gebruikers. In het verlengde daarvan pleiten anderen voor een stelsel van morele normen en waarden voor organisaties die persoonsgegevens verwerken, vandaar dat wordt opgeroepen tot een maatschappelijk debat.[58] De focus van de Artikel 29 Werkgroep en de Europese Commissie met betrekking tot toestemming is slechts gericht op definitie van het begrip en geharmoniseerde interpretatie daarvan.[59] De vraag hoe toestemming ('consent') tegenwoordig in de praktijk wordt gebruikt en of het nog wel het doel dient waartoe het ooit was ontworpen komt hier echter niet ter sprake. Dat is een gemiste kans, omdat deze analyse zou kunnen zorgen voor wetgeving die beter aansluit bij de huidige praktijken in de samenleving.

De oorspronkelijke rol van toestemming was strikt gerelateerd aan individuele autonomie en zelfbeschikking.[60] De beschreven praktijk van routinematig accepteren van voorwaarden omschrijft naar mijn idee echter een compleet andere realiteit. Toestemming heeft niet meer de functie van controle die het oorspronkelijk als doel had. In onze digitale samenleving vormen online platforms en applicaties namelijk zulke belangrijke communicatiemiddelen dat het welhaast onmogelijk is om alle grote ICT-spelers te omzeilen als je in contact wilt blijven met anderen. Om te zorgen dat het recht meegaat met de veranderingen in de maatschappij, is het dus belangrijk om rekening te houden met de invloed van de grote ICT-spelers. De huidige herziening van het EU-dataprotectieraamwerk biedt dus de kans om niet alleen naar de definitie van toestemming te kijken, maar ook naar de primaire functie ervan in specifieke context.[61] Om in de huidige tijd effectief persoonsgegevens te beschermen is meer focus nodig op de daadwerkelijke effecten van privacywetgeving.

[58] Zuiderveen Borgesius, *Nederlands Juristenblad* 2015, p. 882
[59] Kosta, *Unravelling Consent in European Data Protection Legislation* 2011, p. 29
[60] Roosendaal, *Digital personae and profiles in law* 2013, p. 183
[61] Roosendaal, *Digital personae and profiles in law* 2013, p. 316

Conclusie

Anno 2015 lijkt het credo van Francis Bacon ‘kennis is macht’ nog steeds op te gaan, al dient dit dan eerder geïnterpreteerd te worden als ‘gegevens is geld’. Met de toepassing van big data is veel te verdienen, vooral door het meervoudig gebruik van gegevens. Hoe meer gegevens er beschikbaar zijn, des te meer men kan analyseren. Door dataficering en de groei van voor handen zijnde gegevens wordt dit dus steeds interessanter.

De vraag die in dit onderzoek centraal stond was of in het kader van deze ontwikkelingen het geven van toestemming nog een zinvolle manier is om de informationele privacy te waarborgen. Data heeft een enorm prominente rol in bedrijven en andere organisaties verworven, zonder dat degenen op wie de gegevens betrekking hebben dat door hebben gehad of konden voorzien. Het gebruik van gegevens nu, is veel groter dan men voor de komst van big data ooit had kunnen vermoeden. Ondertussen zijn gebruikers gewend geraakt aan alle ‘gratis’ diensten die het internet en de rest van de ICT-industrie rijk is, de betaling hiervoor vindt echter plaats met persoonsgegevens. Met big data als valuta van het internet, zijn persoonsgegevens een lustobject geworden, met een honger die niet zomaar is gestild.

Het gevaar van de groeiende vraag naar data zit hem in de zorgeloosheid en desinteresse waarmee gebruikers deze gegevens verstrekken. Geïnformeerde toestemming vormt de traditionele manier om hier bewustwording te scheppen en zo de controle en autonomie van het individu te versterken. De praktijk leert ons echter dat mensen hier op een volstrekt andere manier mee omgaan dan vroeger, hetgeen naar mijn idee te wijten is aan de grote afhankelijkheid van diensten en de gewenning van het achteloos accepteren. Hoewel privacy een gevoelig onderwerp is en wel degelijk leeft onder de bevolking, weten veel mensen niet precies wat de status ervan is. Mensen zijn er makkelijker in geworden om bepaalde informatie te delen, maar zich er tegelijkertijd ook heel bewust van met wie ze dat doen.[62] Ondertussen heerst er naar mijn gevoel ook een soort van gelatenheid, iedereen doet het immers en alleen kan je er niks aan veranderen. Al je digitale communicatiemiddelen afzweren betekent jezelf in een sociaal isolement plaatsen. Daarnaast zou dat ook het kind met het badwater weggooien zijn, de technologieën maken immers ook een hele hoop goeds

[62] Zo blijkt uit onderzoek dat veel jongeren hun ouders (ook al hebben zij een account) niet als vriend op Facebook hebben. Zie: Moerel, *Big Data protection* 2014, p.43

mogelijk. Voorts zijn veel van de diensten die gegevens over je verzamelen ook leuk, nuttig en praktisch (wederom Google en Facebook).

Vasthouden aan het geven toestemming als principaal middel om privacy te waarborgen is in mijn optiek dus zinloos. In zekere zin is het geven van toestemming al verworden tot een betekenisloze actie (namelijk het routinematig aanklikken van 'ok'). De betekenis en zin van het geven van toestemming zal nog meer slinken door de komst van big data. De grootste kracht en waarde van big data ligt immers in secundair gebruik dat vooraf niet gedefinieerd kan worden. Een formulering met een open einde karakter maakt dat het beschermen van privacy met behulp van toestemming al helemaal een lege huls wordt, blanco toestemming biedt namelijk alsnog totaal geen bescherming van de informationele privacy.

In dat kader is het een goede ontwikkeling dat er gekeken wordt naar andere manieren om privacy *effectief* te beschermen. Toestemming als concept is hierin achterhaald door de praktijk en biedt dus eigenlijk niet genoeg bescherming meer. We hebben een ander model nodig, de roep om ethiek in de ICT en het verantwoordelijk maken van de gebruikers van big data voor ethisch gebruik van persoonsgegevens is daarom een goed alternatief. De voorgestelde veranderingen met de principes van 'Privacy by Design' en 'accountability' zijn daarom een stap in de goede richting. Op deze manier blijft privacy in de veranderende tijd toch beschermd. Van een systeem van informationele zelfbeschikking gaan we dan steeds meer naar een systeem van automatische bescherming.[63] Op deze manier is bescherming van de privacy van individuen gegarandeerd, zelfs als mensen hun persoonsgegevens in routinematige achteloosheid prijsgeven. De *data controllers* worden zo verantwoordelijk gemaakt voor het respecteren van de gegevens van betrokkenen, wat een eerlijke verdeling is: de *data controllers* verdienen er immers geld aan.

Het verdient nader onderzoek om te kijken in hoeverre het gebruik van toestemming helemaal kan worden afgeschaft. De verhouding tussen accountability en toestemming zou kunnen worden onderzocht, om te zien welk concept het meest duurzaam de bescherming van privacy effectief kan waarborgen. Er zijn al signalen dat grote internetondernemingen deze ontwikkelingen in het recht aan zien komen. Zo heeft Facebook middelen ingebouwd om te bepalen welke berichten je met wie deelt en heeft Google recentelijk een nieuw portaal

[63] Kiss & Szöke, *Evolution or Revolution?* 2015, p. 325

gelanceerd waar gebruikers centraal de privacyinstellingen van alle diensten kunnen wijzigen.[64] In heldere taal wordt hier uitgelegd wat voor gegevens het bedrijf verzamelt, hoe versleuteling werkt en waar instellingen veranderd kunnen worden. Het is wellicht een kleine stap, maar naar mijn idee is het een positief teken dat er verantwoordelijkheid genomen wordt, al is de omvang ervan gering. Nu is het taak voor ons allen om aan te geven of we dit genoeg vinden…

[64] R. Finge, 'Google opent check-up voor privacy en beveiliging', *NOS* 1 juni 2015. Geraadpleegd via: http://nos.nl/artikel/2038841-google-opent-check-up-voor-privacy-en-beveiliging.html

Literatuurlijst

Acquisti & Grossklags, *What Can Behavioral Economics Teach Us About Privacy?* 2007

A. Acquisti & J. Grossklags, 'What Can Behavioral Economics Teach Us About Privacy?' in: A. Acquisti e.a. (red.), Digital Privacy: Theory, Technologies and Practices, Londen: Taylor and Francis Group 2007.

Cate, *The Failure of Fair Information Practice Principles* 2006

Fred H. Cate, "The failure of Fair Information Practice Principles," in Jane K. Winn, ed., *Consumer Protection in the Age of the "Information Economy"* Ashgate 2006, p. 341 e.v.

Engelfriet, *Tijdschrift voor Internetrecht* 2014

A. Engelfriet, 'Big data: Hype of trend?', *Tijdschrift voor Internetrecht* 2014, afl. 1, p. 15-17

Hildebrandt & Gutwirth 2008

Hildebrandt, M., & Gutwirth, S. (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Heidelberg: Springer 2008.

Hume, *Het menselijk inzicht* 2002

D. Hume, *Het menselijk inzicht,* Amsterdam: Uitgeverij Boom 2002 (eerste uitgave 1748).

Johnson, *The Guardian* 11 januari 2010

B. Johnson, 'Privacy no longer a social norm, says Facebook founder', *The Guardian* 11 januari 2010.

De Jong, *Computerrecht* 2015/40, afl. 1

A. de Jong, 'Fundamentele rechten in een veranderende wereld', *Computerrecht* 2015/40, afl. 1.

Kiss & Szöke, *Evolution or Revolution?* 2015

A. Kiss & G.L. Szöke, 'Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation', in: S. Gutwirth, R. Leenes, P. de Hert (red.), *Reforming European Data Protection Law*, Dordrecht: Springer 2015, p. 311-332.

Kosta, *Unravelling Consent in European Data Protection Legislation* 2011

E. Kosta, *Unravelling Consent in European Data Protection Legislation; a prospective study on consent in electronic communications,* Leuven, K.U. Leuven 2011.

Martijn, *De Correspondent* 5 november 2014

M. Martijn, 'Deze bevlogen professor helpt je doorgronden wat privacy is', *De Correspondent* 5 november 2014.

Mayer-Schönberger & Cukier, *Big Data* 2013

V. Mayer-Schönberger & K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton: Mifflin Harcourt 2013.

McDonald & Cranor, *I/S* (3) 2008

A.M. McDonald & L.F. Cranor, 'The Cost of Reading Privacy Policies', *I/S: A Journal of Law and Policy for the Information Society* (3) 2008, afl. 4, p. 540.

Moerel, *Big Data protection* 2014

L. Moerel, *Big Data protection. How to make the draft EU Regulation on Data Protection future proof* (oratie Tilburg), Tilburg: Tilburg University 2014.

Roosendaal, *Digital personae and profiles in law* 2013

A.P. Roosendaal, *Digital personae and profiles in law: Protecting individuals' rights in online contexts,* Oisterwijk: Wolf Legal Publishers 2013.

Westin, *Privacy and Freedom* 1968

A. Westin, *Privacy and Freedom*, New York: Atheneum 1968.

Zuiderveen Borgesius, *Nederlands Juristenblad* 2015

F.J. Zuiderveen Borgesius, 'Privacybescherming online kan beter', *Nederlands Juristenblad* 2015, afl. 14, p. 878-883.