Algemeen arsaequi.nl/maandblad AA20190546

De soeverein is niet thuis

Self-Sovereign Identity (SSI) en Attribute Based Credentials (ABC)

Mireille Hildebrandt*

In deze bijdrage wordt onderzocht hoe de idee van *self-sovereign identity* (SSI) zich verhoudt tot kernbegrippen uit de juridische gegevensbescherming. Daarnaast wordt SSI vergeleken met de inzet van *attribute based credentials* (ABC).

1 Inleiding

Self-Sovereign Identity (SSI) bestaat niet. De term verwijst naar een verzameling voorstellen om controle uit te kunnen oefenen over de eigen persoonsgegevens, en wordt vaak geassocieerd met pogingen om die controle afhankelijk te maken van blockchain-technologie (*distributed ledger technologies*, DLT), hoewel opslag in datakluizen er ook wel onder wordt gebracht.[1] Kort gezegd gaat het om een systeem dat persoonsgegevens opslaat op een blockchain, zodat degene wiens gegevens het betreft daarover naar eigen willekeur zou kunnen beschikken. Vandaar ook de term 'soeverein'. Een heldere definitie of omschrijving ontbreekt en op dit moment zijn er geen systemen die daadwerkelijk leveren wat de voorvechters van SSI beloven. Dat hangt samen met het feit dat SSI afhankelijk is van de bereidheid van heel veel partijen om hun verwerking van persoonsgegevens (inclusief het verzamelen daarvan) zo in te richten dat gegevens altijd via een daartoe ontworpen blockchain worden verzameld.[2] Juristen houden van vastomlijnde begrippen, omdat juridische begrippen rechtsgevolg kunnen hebben en het dus nogal uitmaakt of een begrip zus of juist zo wordt gedefinieerd. Het schermen met een term als SSI zal juristen daarom gemakkelijk irriteren, want er is eenvoudigweg geen overeenstemming over de betekenis en er zijn ook geen operationele voorbeelden voorhanden (ook al wordt er van alles beweerd en bepleit).

Het schermen met een term als SSI zal juristen gemakkelijk irriteren, want er is eenvoudigweg geen overeenstemming over de betekenis en er zijn ook geen operationele voorbeelden voorhanden

SSI is een van de vele pogingen om het zogenaamde 'identiteitsprobleem' op 'het internet' op te lossen, waarmee wordt gedoeld op het feit dat het in online omgevingen enerzijds vaak lastig is om zeker te zijn met wie men van doen heeft, met wie men persoonsgegevens deelt, en wat daar vervolgens mee gebeurt, terwijl het anderzijds vaak lastig is te achterhalen of verstrekte, geobserveerde en afgeleide persoonsgegevens juist zijn. Daarbij mag duidelijk zijn dat de belangen van zogenaamde eindgebruikers verschillen van die van dienstverleners, adverteerders,

* Prof.mr. M. Hildebrandt is hoogleraar Interfacing Law and Technology, aan de Faculteit Rechten en Criminologie van de Vrije Universiteit Brussel, en hoogleraar Smart Environments, Data Protection and the Rule of Law aan de Faculteit Natuurwetenschappen, Wiskunde en Informatica van de Radboud Universiteit.
Met dank aan Jaap-Henk Hoepman voor een scherpe blik op de technische aspecten; eventueel resterende fouten en onjuistheden zijn uitsluitend aan mijzelf te wijten.

1 Zie bijvoorbeeld R. Joosten, 'Self-Sovereign identities: it is going to happen! May 2018', *TNO* (blog), *https://blockchain.tno.nl/blog/self-sovereign-identities-it-is-going-to-happen/*. Joosten schaart ABC ook onder SSI, hieronder zal duidelijk worden waarom ik daarmee niet akkoord ben. Zie ook Blockchain Bundesverband, 'Self Sovereign Identity defined', 15 november 2018, *https://bundesblock.de/new-position-paper-self-sovereign-identity-defined/*; M. Graglia, Chr. Mellon & T. Robustelli, *The nail finds a hammer. Self-Sovereign Identity, design principles, and property rights in the developing world* (rapport van New America), 17 oktober 2018, *www.newamerica.org/future-property-rights/reports/nail-finds-hammer/*. Bij mijn weten gaat het bij de voorvechters

Foto: Manon Heinsman | © Ars Aequi

advertentie-netwerken, deelnemers aan de gig-economie, en tech-platformen. Sommige partijen hebben er belang bij dat zoveel mogelijk gegevens beschikbaar komen en bovendien juist zijn, eindgebruikers hebben daar vanwege privacyinbreuken en mogelijke discriminatie meestal geen belang bij. Daarnaast speelt beveiliging een hoofdrol, want 'identiteiten' kunnen worden 'gestolen' en identiteitsfraude leidt tot allerlei vormen van leed en schade. Het zogenaamde 'identiteitsprobleem' speelt op het *world wide web*, bij online dienstverlening door zowel overheden als commerciële partijen, bij mobiele applicaties en zal naar verwachting in nog ernstiger mate gaan spelen als het 'internet van de dingen' (IoT van *internet of things*) verder doorbreekt (denk aan de slimme koelkast die melk bestelt als het pak leeg is, maar ook aan 'connected cars' en 'remote healthcare').

Attribute based credentials (ABC) is een systeem dat het mogelijk maakt om alleen die gegevens te delen die noodzakelijk zijn voor de te verlenen dienst

Dit artikel beoogt een aantal van de onderliggende ideeën van SSI te verhelderen en richt zich vervolgens op een alternatieve manier om de problematiek van het delen van persoonsgegevens te bemiddelen, namelijk via *attribute based credentials* (ABC). ABC is een systeem dat het mogelijk maakt om alleen die gegevens te delen die noodzakelijk zijn voor de te verlenen dienst. Iemand die sterke drank wil kopen deelt dan alleen het gegeven dat zij ouder is dan 18, in plaats van een identiteitsbewijs waar ook allerlei andere gegevens op staan (zoals de precieze leeftijd). Het artikel beperkt zich grotendeels tot gegevens die betrokkenen zelf verstrekken, omdat noch SSI noch ABC zich richten op het grootschalig 'mijnen' van gedragsgegevens (online surfdata, rijgedragdata, locatiedata, biometrische gedragsdata van 'wearables'). Omdat privacyinbreuken, discriminatie en ondermijning van menselijke autonomie vaak in verband worden gebracht met het afleiden van kennis uit gedragsdata zal ik toch regelmatig terugkomen op gedragsdata, nu het juist daar ontbreekt aan controle voor eindgebruikers van ICT-systemen. Om SSI en ABC op waarde te schatten moet helder zijn welke problemen vooralsnog niet worden opgelost.

Hieronder ga ik eerst in op de kwestie waarvoor SSI een oplossing zoekt, te weten controle over persoonsgegevens voor betrokkenen (par. 2). Die controle wordt vaak onder de noemer gebracht van eigendom, alsof het mogelijk zou zijn om een exclusief recht op persoonsgegevens te vestigen, vergelijkbaar met bijvoorbeeld het auteursrecht op een beschermd werk. SSI kiest voor een andere metafoor, namelijk die van de soevereiniteit, waarbij de gedachte is dat men 'de baas' zou zijn over de eigen persoonsgegevens, zoals een soeverein 'de baas' is over haar onderdanen.[3] Ik zal kort aangeven waarom beide metaforen weinig productief zijn en een fundamenteel onjuist beeld geven van de verhouding tussen een persoon en haar gegevens. Dat brengt mij tot een relationele opvatting van persoonsgegevens, die beter recht doet aan de eigen aard van die gegevens en aan de relaties tussen betrokken partijen (par. 3). Na dit grondwerk bespreek ik SSI en ABC in meer detail (par. 4), gevolgd door een bespreking van (1) welke problemen wel en (2) welke niet worden opgelost, en (3) welke worden gecreëerd. Mijn stelling is dat deze drie vragen bij de introductie van iedere technologische innovatie moeten worden gesteld, waarbij niet alleen mag worden vergeleken met de status quo, maar ook moet worden gekeken naar alternatieve innovaties. Door uit te gaan van de problemen die wel of niet worden opgelost of gecreëerd kunnen de meer abstracte vragen naar voor- en nadelen en die naar kosten en baten beter worden beantwoord. Ik sluit af met een korte bespreking van de relatie tussen soevereiniteit, controle en consent, waarbij ik drie niveaus onderscheid ten aanzien van de rol die consent speelt in de Algemene Verordening Gegevensverwerking (par. 5).

2 Controle over persoonsgegevens: soevereiniteit of eigendom?

Een soeverein heerst over haar onderdanen. De Nederlandse rechtsfilosoof Glastra van Loon heeft in dit blad wel eens opgemerkt dat 'bevelen van een souverein […] alleen goed [kunnen] worden uitgevoerd door onderdanen die zelf een onbetwist bevel voeren over hun ledematen'.[4] Onderdanen, subjecten, die soeverein heersen over zichzelf. Dat schept het probleem van de *homunculus*, de 'ik' die heerst over het 'zelf', alsof er in ons een 'mannetje' woont dat ons aanstuurt, als waren we tegelijk heerser en beheerst. In het verlengde van deze problematische visie op hoe mensen in elkaar zitten (de soeverein is namelijk niet

van SSI vrijwel altijd om blockchain-oplossingen en spreken de voorvechters van decentrale datakluizen zelf niet van *self-sovereign identity* (uitzonderingen daargelaten). Zo ontwikkelde Sir Tim Berners Lee (de uitvinder van het *world wide web*) een vergelijkbaar systeem van datakluizen, maar claimt hij daarmee geen *self-sovereign identity* te leveren, zie *https://solid.inrupt.com/how-it-works*.

2 Om te slagen is een SSI-applicatie afhankelijk van de gelaagde opbouw van internet, *world wide web*, en de daarop gebouwde applicaties, zie bijvoorbeeld O. Terbu, 'The Self-Sovereign Identity Stack', *Decentralized Identity Foundation* (blog), 27 januari 2019, *https://medium.com/decentralized-identity/the-self-sovereign-identity-stack-8a2cc95f2d45*.

3 In deze bijdrage wordt consistent met een vrouwelijk verwijswoord terugverwezen naar termen die zowel naar mannelijke als vrouwelijke personen kunnen verwijzen, zoals bijvoorbeeld persoon, gebruiker, soeverein. Dit om de leesbaarheid te bevorderen (geen hij/zij of zijn/haar) en om niet te vervallen in 'hij' of 'zijn', het gebruikelijke *pars pro toto*. Zie bijvoorbeeld *http://taaladvies.net/taal/advies/tekst/110/verwijzingsproblemen_met_voornaamwoorden_van_de_derde_persoon_enkelvoud_algemeen/* of *www.learnersdictionary.com/qa/the-he-or-she-dilemma* (in Nederland valt dit waarschijnlijk onder radicaal feminisme).

4 J.F. Glastra van Loon, 'Norm en handeling. Hoe regelen wij ons handelen', *Ars Aequi* (34) 1985, afl. 12, p. 697 (AA19850697).

5 P. Ricoeur, *Freud and philosophy: an essay on interpretation*, New Haven: Yale University Press 1977, waarin hij met Marx, Nietzsche en Freud de idee aan de kaak stelt dat 'wij' baas zouden zijn binnen ons 'zelf'.

6 De term data verwijst naar een of meer digitale gegevens. Zoals gebruikelijk in de informatica wordt 'data' hier altijd in het enkelvoud gebruikt

thuis),[5] wordt een deel van het privacy-debat beheerst door een wat naïef controleperspectief, waarbij eenieder wordt geacht in beginsel de baas te zijn over informatie met betrekking tot zichzelf. Zo'n controleperspectief laat zich op twee manieren inkleuren: door de metafoor van de soeverein, die naar willekeur gezag kan uitoefenen over persoonlijke informatie en de metafoor van de eigendom, die de eigenaar toestaat naar willekeur te handelen met persoonlijke informatie.

De metafoor van de eigenaar suggereert een privaatrechtelijke eigendomsrelatie (met de meest omvattende beschikkingsrechten), inclusief het recht om anderen die beschikking naar eigen inzicht te ontzeggen. Als data echter onder een vorm van eigendom valt,[6] moeten we kunnen uitsluiten dat het tegelijkertijd in bezit van meerdere personen is (het moet rivaliserend zijn), en zekerstellen dat alleen de eigenaar beschikkingsbevoegd is ten aanzien van gebruik en vervreemding (het moet om een exclusief recht gaan).[7] Persoonsgegevens, dat wil zeggen data die betrekking heeft op een geïdentificeerd of identificeerbaar natuurlijk persoon, zijn echter inherent niet-rivaliserend; het feit dat iemand toegang heeft tot mijn naam, adres of tot mijn biometrische gedragsgegevens betekent niet dat anderen er daarom geen toegang meer toe hebben. Net als in geval van intellectuele-eigendomsrechten zouden we theoretisch wellicht een exclusief recht kunnen toekennen door anderen te verbieden onze persoonsgegevens te verwerken, tenzij op basis van een licentie, maar dan zou het samenleven nodeloos ingewikkeld zo niet onmogelijk worden. We zouden allemaal eindeloze registers bij moeten houden van wie op grond van welke licentie welke van onze persoonsgegevens verwerkt. En we zouden een markt moeten organiseren waarop de licenties een prijs krijgen, waarbij we in beginsel kunnen achterhalen welke derden al dan niet zonder recht onze data verwerken. Probleem van de economische waarde van bijvoorbeeld onze gedragsdata (van toetsenbordgedrag tot energieverbruiksgedrag),[8] is dat die waarde eigenlijk pas wordt gecreëerd wanneer op basis van machinaal leren nieuwe informatie wordt afgeleid uit een aggregaat van gegevens (het gaat om schaalvoordelen); individuele datapunten zijn niet veel waard en hun waarde fluctueert en hangt sterk samen met de beschikbaarheid van andere datapunten.[9] Het voorbeeld van de intellectuele rechten gaat enerzijds niet op omdat het hierbij altijd gaat om een expressie, uitvinding of ontwerp dat de handtekening van de auteur, uitvinder of ontwerper draagt; het gaat steeds om een creatie. Dat perkt de verzameling te beschermen objecten enigszins in (tot onder meer werken, uitvindingen, ontwerpen), terwijl de verzameling persoonsgegevens schier oneindig is. Anderzijds biedt de handhavingsproblematiek van de intellectuele rechten weinig aanknopingspunten tot optimisme inzake de idee van eigendomsrechten op persoonsgegevens.

De metafoor van de soeverein, die vooropstaat bij de idee van SSI, is niet bijzonder productief. Deze metafoor suggereert namelijk een publiekrechtelijke relatie ten aanzien van persoonsgegevens die gebaseerd is op soevereine willekeur

Behalve praktische argumenten zijn er twee fundamentele bezwaren. Ten eerste gaat het hier om gegevens die betrekking hebben op het zelf, die dat zelf tot op zekere hoogte 'maken'. Net zoals het feit dat ik mijn lichaam 'heb' alleen opgaat zolang ik ook mijn lichaam 'ben', zou het handelen in persoonsgegevens die bijzondere verhouding tussen zelf en persoonsgegeven miskennen. Ten tweede miskent de eigendomsopvatting van persoonsgegeven dat de bescherming van individuele autonomie niet alleen een privaat belang is, maar ook een publiek goed, waarmee dus niet naar willekeur gehandeld kan worden.

De metafoor van de soeverein, die vooropstaat bij de idee van *self-sovereign identity* (SSI), is mede daarom niet bijzonder productief. Deze metafoor suggereert namelijk een publiekrechtelijke relatie ten aanzien van persoonsgegevens die gebaseerd is op soevereine willekeur (een uitgewerkt idee dat de soeverein zich zou moeten richten op de *res publica* maakt tot nu toe geen deel uit van het gedachtegoed van SSI). De suggestie dat wij als soevereine vorst regeren over onze persoonsgegevens veronderstelt, net als bij de eigendom, dat we anderen de verwerking van die gegevens naar eigen willekeur kunnen ontzeggen. Die veronderstelling gaat niet op. Veel van onze persoonsgegevens staan niet onder ons gezag. Een naam is ons gegeven door anderen (de staat en de ouders), niet om mee in een hoekje te zitten, maar om ons vindbaar en aanspreekbaar te maken. Energieverbruiksgegevens, die door een

en niet als meervoud van het Latijnse *datum*. Net als 'informatie' wordt het gezien als een zelfstandig naamwoord dat geen meervoudsvorm heeft (een zogenaamde *mass noun*). Zie bijvoorbeeld 'Data', Oxford Dictionaries | English, laatste bezoek 21 februari 2019, *https://en.oxforddictionaries.com/definition/data*.

7 Zie bijvoorbeeld de relevante rechtspraak inzake de vraag wanneer 'iets' een 'goed' is in de zin van art. 310 Sr: HR 23 mei 1921, *NJ* 1921/564 (*Elektriciteitsarrest*), en verdere updates: HR 11 mei 1982, *NJ* 1982/583 (toewijzing in geval van giraal geld); HR 13 juni 1995, ECLI:NL:HR:1995:ZD0064 (afwijzing bij afpersing of chantage ten einde iemand te dwingen een pincode te verklappen); HR 3 december 1996, ECLI:NL:HR:1996:ZD0584 (afwijzing inzake diefstal van data, waarna de wetgever computervredebreuk strafbaar stelde); HR 19 april 2005, ECLI:NL:HR:2005:AS9237 (toewijzing inzake geldopname met gesloten smartcard en pincode); HR 26 maart 2013, ECLI:NL:HR:2013:BY9718 (afwijzing inzake diefstal van bandbreedte); HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251 (toewijzing inzake diefstal van sms-berichten en belminuten). De HR toetst hier eigenlijk steeds aan de vraag of sprake is van een identificeerbaar niet-rivaliserend goed waarop een exclusief recht kan worden uitgeoefend.

8 Zie over het onderscheid tussen verstrekte data, gedragsdata en afgeleide data *infra* par. 4.3.

9 Hierover bijvoorbeeld G. Barber, 'Here's how much money I made when I sold my own data', *Wired* 17 december 2018, *www.wired.com/story/i-sold-my-data-for-crypto/*.

slimme meter worden opgemeten, vastgelegd en doorgegeven, hebben een duidelijk doel dat niet door ons maar door de netwerkbeheerder en de energieleverancier wordt bepaald (om de levering veilig te stellen en de rekening te sturen). Wij kunnen niet eisen dat we elektriciteit af kunnen nemen zonder identificeerbare verbruiksgegevens te delen. Kortom, persoonsgegevens zijn relationele gegevens die betrekkingen mogelijk maken tussen degene die het betreft en anderen, bijvoorbeeld om belasting te kunnen heffen, een bestelling af te leveren, of een verzekeringspremie te kunnen vaststellen. Daarmee is gelijk ook duidelijk dat noch de betrokkene, noch degene die verwerkt naar willekeur – als een soeverein – over de verwerking kan beslissen.

Herhaaldelijk gaan stemmen op om de relatie tussen persoon en persoonsgegevens als een eigendomsrelatie te kwalificeren, vaak als goedbedoelde poging om meer bescherming te bieden. Dat zou meer problemen scheppen dan oplossen

In de context van het gegevensbeschermingsrecht gaan (met name in de VS) herhaaldelijk stemmen op om de relatie tussen persoon en persoonsgegevens als een eigendomsrelatie te kwalificeren, vaak als goedbedoelde poging om meer bescherming te bieden.[10] Zoals hierboven aangegeven zou dat meer problemen scheppen dan oplossen. Interessant is te vermelden dat de metafoor van de soeverein in geval van SSI oorspronkelijk uit de hoek komt van de zogenaamde crypto-anarchisten, die zich tegen de staat keren en het privaatrecht als een soort natuurrecht zien, waar individuen allemaal soeverein zijn en zich niets laten opleggen door anderen, laat staan door een staat. Dat leidt ertoe dat de metafoor van de soeverein in allerlei opzichten samenvalt met die van de eigendom.[11] De crypto-anarchistische achtergrond zien we terug in het wantrouwen van SSI-voorvechters jegens centrale instituties en een idealistisch geloof in zogenaamd gedecentraliseerde oplossingen, zoals bijvoorbeeld de *public non-permissioned* blockchain (of DLT).[12] Je zou kunnen zeggen dat het wantrouwen jegens de-staat-als-soeverein is omgeslagen in een verheerlijking van het-individu-als-soeverein.

3 Een relationele opvatting van persoonsgegevens

Om van de metafoor van de soevereiniteit af te komen is het zaak te erkennen dat ten aanzien van een en hetzelfde gegeven meerdere rechten kunnen worden uitgeoefend (gegevensbeschermingsrechten en verwerkingsrechten), door verschillende rechtssubjecten (de betrokkene, de gemeente, de buurman, een leverancier), terwijl bij de verwerking ook verschillende plichten spelen voor onderscheiden verantwoordelijken en verwerkers (inzake transparantie, verwijdering, beveiliging, en vertrouwelijkheid). Daarmee komen we aan bij het complexe samenspel van rechten en plichten dat vorm heeft gekregen in de Algemene Verordening Gegevensverwerking (AVG),[13] waarin de relationele aard van persoonsgegevens vooropstaat. Dat laatste betekent dat de concrete rechten en plichten ten aanzien van een persoonsgegeven altijd spelen binnen een specifieke rechtsverhouding tussen een identificeerbare betrokkene (degene wiens data het betreft, art. 4(1)) en een identificeerbare verantwoordelijke, waarbij die verantwoordelijke altijd een specifiek, expliciet en legitiem doel moet hebben met de verwerking (art. 4(7) en 5(1)(b)) en bovendien alleen mag verwerken wanneer daarvoor een juridische basis is aangewezen (art. 6). De betrokkene kan zich niet zonder meer tegen iedere verwerking verzetten, en kan zelfs verplicht zijn om de verwerking mogelijk te maken. De verantwoordelijke is intussen per definitie aansprakelijk voor de rechtmatigheid van die verwerking. Die aansprakelijkheid ziet onder de AVG niet alleen op het voldoen aan de juridische verplichtingen die de AVG oplegt en het respecteren van de rechten van de betrokkene. Op meerdere punten blijkt de verantwoordelijke aansprakelijk wanneer zij onvoldoende onderzoek heeft gedaan naar mogelijke inbreuken op fundamentele rechten en vrijheden van de betrokkene (art. 35), dan wel onvoldoende maatregelen heeft getroffen om zulke inbreuken te voorkomen (art. 25). Er wordt dus niet alleen zorgvuldigheid in de omgang met persoonsgegevens gevraagd, maar ook voorzorg en proactief optreden wanneer daar aanleiding voor is.

In deze bijdrage zal ik concluderen dat SSI zich verlaat op problematische ideologische uitgangspunten en dat de bescherming die SSI zou kunnen bieden sterk afhangt van het ontwerp en de inrichting. Daarnaast zal ik, als aangegeven, onderzoeken hoe SSI zich verhoudt tot ABC, een systeem dat goed is afgestemd op de AVG en een evenwichtiger

10 L. Lessig, 'Privacy as property', *Social Research* (69) 2002, afl. 1, p. 247-269; voor een genuanceerd overzicht van de problematiek vanuit een meer Europees perspectief N. Purtova, *Property rights in personal data*, Alphen aan den Rijn: Kluwer Law International 2012 en M. Hildebrandt, 'Recht en markt: met falen en opstaan', in L. Mommers et al. (red.), *Het binnenste buiten. Liber Amicorum Aernout H.J. Schmidt*, Leiden: Meijers Instituut 2010, p. 275-289.

11 Zie de analyse van M. Verstraete, 'The Stakes of Smart Contracts', (SSRN Scholarly Paper), Rochester, NY: Social Science Research Network, 14 mei 2018, *https://papers.ssrn.com/abstract=3178393*.

12 Een public blockchain is een blockchain waar iedereen aan kan deelnemen en die door iedereen – mits cryptografisch onderlegd – kan worden gelezen. Een non-permissioned blockchain betekent dat alle deelnemers – mits cryptografisch onderlegd – ook kunnen schrijven op de blockchain. Bij private blockchains is het lezen voorbehouden aan bepaalde deelnemers, bij permissioned blockchains is het schrijven voorbehouden aan bepaalde deelnemers. Zie bijvoorbeeld J.H. Hoepman, 'Het gebruik van blockchain technologie in het verkiezingsproces', PI.lab, 18 april 2018, *https://pilab.nl/onewebmedia/het-gebruik-van-blockchaintechnologie-in-het-verkiezingsproces(3).pdf*, hoofdstuk 3 'Over blockchain technologie. Zie ook *infra* voetnoot 37.

13 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 95/46/EG (algemene verordening gegevensbescherming). In dit artikel verwijzen alle artikelen naar de AVG, tenzij anders vermeld.

verhouding schept tussen verantwoordelijke, verwerker en betrokkene. In het algemeen zijn systemen die betrokkenen meer controle hopen te geven over hun persoonsgegevens interessant voor zover ze bijdragen aan praktische en effectieve bescherming daarvan, zonder noodzakelijke verwerking in de weg te staan. Die dubbele instrumentaliteit is geënt op het relationele karakter van persoonsgegevens en bevestigt de constitutieve en limitatieve functie van het gegevensbeschermingsrecht,[14] en daarmee de eis dat het samenspel van rechten en plichten tegelijk instrumenteel is en rechtsbescherming biedt.[15] De term 'noodzakelijk' is hier op zijn plaats want alle juridische gronden eisen dat de verwerking noodzakelijk is voor de betreffende grond (art. 6): voor het doel van een verwerking op basis van consent (art. 6.1(a) jo. art. 5(b)), voor een contract (art. 6.1(b)), uit hoofde van een wettelijke verplichting (art. 6.1(c)), om de vitale belangen van betrokkene of anderen te beschermen (art. 6.1(d)), om de uitoefening van een publieke taak te waarborgen (art. 6.1(e)), dan wel om het legitieme belang van de verwerker te behartigen (mits de rechten en vrijheden van de betrokkene dat belang niet overstijgen, cf. art. 6(f)).

Die noodzakelijke verwerking moet bovendien aan nog een aantal voorwaarden voldoen, zoals genoemd in artikel 5: de verwerking moet ten aanzien van betrokkene rechtmatig, behoorlijk en transparant zijn, correct zijn en niet langer duren dan noodzakelijk voor het betreffende doel, en beveiligd worden tegen onrechtmatige verwerking. Dat betreft de beginselen van rechtmatigheid, behoorlijkheid, transparantie, dataminimalisering, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, naast de hierboven al genoemde doelbinding.

Het is belangrijk te onderkennen dat zogenaamd soeverein beheer van persoonsgegevens niet alleen een onjuist beeld geeft van de rechten en plichten die met de verwerking van persoonsgegevens zijn verbonden, maar bovendien niet garandeert dat de fundamentele rechten en vrijheden van 'de soeverein' worden beschermd. Wie naar eigen willekeur data verstrekt, heeft niet per se zicht op de verwerking daarvan en kan ook niet per se voorkomen dat die verwerking leidt tot ongewenste *targeting*. Data wordt vaak 'gemijnd' om daar 'nieuwe' – niet per se persoonsgebonden – informatie uit af te leiden, waarmee anderen kunnen worden 'getarget'. Dat speelt met name bij gedragsdata, die overigens nauwelijks een rol speelt in de huidige voorstellen rond SSI.[16] Zo kan uit online gedragsdata worden afgeleid welke voorkeuren gebruikers hebben bij de aanschaf van boeken of meubels, en op basis van Facebook-likes kan onder meer politieke voorkeur, seksuele geaardheid en etnische achtergrond worden afgeleid. Persoonlijke voorkeuren of risico's worden in zo'n geval afgeleid uit geaggregeerde data, op basis van statistische verbanden tussen bepaalde gedrags- of andere kenmerken en andere kenmerken of gedrag. Een voorbeeld van zo'n verband zou kunnen zijn dat mensen die 's nachts na twee uur bestellingen doen een hogere risicoscore hebben ten aanzien van het niet voldoen van schulden. Dat kan ertoe leiden dat zo iemand niet achteraf mag betalen, omdat zij wordt 'getarget' als een hoog betalingsrisico. Dit valt onder de noemer van profilering of *micro-targeting* en het is precies deze praktijk die onze informatie-omgeving teistert, voor zover het tot onzichtbare manipulatie en discriminatie leidt en tot een ongewenste fragmentatie en polarisatie van de publieke ruimte. Dat laatste komt bijvoorbeeld doordat algoritmes die advertentie-inkomsten optimaliseren klaarblijkelijk leiden tot zogenaamde 'extreme content', omdat het vasthouden van de aandacht op korte termijn beter lukt met steeds sensationelere inhoud.[17]

Het is daarom cruciaal om te onderzoeken onder welke voorwaarden SSI dan wel ABC (1) recht doet aan het relationele karakter van persoonsgegevens en (2) schending van fundamentele rechten en vrijheden als gevolg van onrechtmatige verwerking (waaronder *targeting*) zoveel mogelijk voorkomt.

SSI zou het beheer van persoonsgegevens mogelijk moeten maken voor 'gebruikers', door die gegevens op te slaan op een blockchain en degene wiens gegevens het betreft de sleutel te geven waarmee anderen toegang kunnen verkrijgen tot de data

4 Wat is SSI en wat is ABC?

4.1 SSI

SSI zou het beheer van persoonsgegevens mogelijk moeten maken voor 'gebruikers', door die gegevens op te slaan op een blockchain en degene wiens gegevens het betreft

14 Vergelijk de constitutieve en limitatieve functie van het strafvorderlijk legaliteitsbeginsel, C.P.M. Cleiren, *De openheid van de wet, de geslotenheid van het recht*, Arnhem: Gouda Quint 1992, *https://openaccess.leidenuniv.nl/handle/1887/3085*, p. 15.

15 R. Foqué & A.C. 't Hart, *Instrumentaliteit en rechtsbescherming*, Arnhem/Antwerpen: Gouda Quint/Kluwer Rechtswetenschappen 1990.

16 Dat is wel het geval bij sommige voorstellen om datakluizen te integreren in de ICT-infrastructuur van internet, www en IoT, zie bijvoorbeeld S. Spiekermann & A. Novotny, 'A vision for global privacy bridges: technical and legal measures for international data markets', *Computer Law & Security Review* (31) 2015, afl. 2, p. 181-200, *https://doi.org/10.1016/j.clsr.2015.01.009*, maar het lijkt erop dat ten aanzien van gedragsdata ook Spiekermann zich eerder richt op wat zij noemt 'safe harbor for big data', vergelijkbaar met Pentlands oplossing, waarbij gedragsdata geaggregeerd wordt beveiligd en beschikbaar gesteld voor bigdata-analyse. Zie A. Pentland, *Social physics: how good ideas spread – the lessons from a new science*, New York: Penguin 2014.

17 M. Bridge, 'YouTube program drives viewers to extreme content', *The Times* 9 februari 2018. Over de vraag of gedragsgestuurd adverteren (het verdienmodel van veel 'gratis' diensten) eigenlijk wel werkt zoals vaak wordt verondersteld, zie J. Frederik & M. Martijn, 'Dit is de nieuwe internetbubbel: online advertenties', *De Correspondent* 19 januari 2019.

de sleutel te geven waarmee anderen toegang kunnen verkrijgen tot de data. Christofer Allen, de 'uitvinder' van SSI (althans van de tenaamstelling), ontwikkelde tien beginselen van SSI:[18] (1) het moet gaan om gebruikers (dingen of personen) die onafhankelijk van hun digitale identiteit bestaan, (2) het gaat om gebruikers die controle hebben over hun identiteiten, (3) gebruikers moeten toegang hebben tot hun eigen data, (4) de systemen en algoritmes die identiteiten beheren moeten transparant zijn, (5) de identiteiten moeten enige duurzaamheid hebben in de tijd, (6) informatie en dienstverlening inzake identiteiten moeten 'draagbaar' in de zin van 'transporteerbaar' zijn, (7) identiteiten moeten in zoveel mogelijk systemen kunnen worden gebruikt, (8) gebruikers moeten te allen tijde kunnen beslissen over het al of niet delen van identiteiten, (9) het delen van gegevens moet worden geminimaliseerd, en (10) de rechten van gebruikers moeten worden beschermd.

Allen meent dat het uitgangspunt van de 'I' in SSI (*self-sovereign identity*) gezocht moet worden in de Cartesiaanse *cogito*: 'ik denk dus ik ben'.[19] Vanuit een relationeel mensbegrip is het verstandig om te erkennen dat aan de *cogito* een *cogitas* vooraf gaat: 'jij denkt dus ik besta'. Of, nog liever, dat de *cogito* en de *cogitas* tegelijk ontspringen op het moment dat de ene mens de andere aanspreekt.[20] De relationele aard van persoonsgegevens hangt daarmee samen; wie zich niet laat aanspreken kan geen identiteit ontwikkelen.

De I van SSI gaat niet over identiteit, maar over data die identificatie mogelijk maakt, dat wil zeggen data die het mogelijk maakt een persoon als uniek te onderscheiden van andere personen. Of data identificatie mogelijk maakt, verschilt per context

Daarnaast is het zaak afstand te nemen van de verwarring tussen *identity* (identiteit) en *identifier* (identificator of identificatiecode). De I van SSI gaat niet over identiteit, maar over data die identificatie mogelijk maakt, dat wil zeggen data die het mogelijk maakt een persoon (of zelfs een ding) als uniek te onderscheiden van andere personen (of dingen).[21] Of data identificatie mogelijk maakt, verschilt per context. Binnen een groep van driehonderd blanke mannen, en één zwarte vrouw is het gegeven 'is zwart' identificerend, omdat het voldoende is om de zwarte vrouw van alle anderen te onderscheiden. Hetzelfde geldt voor het gegeven 'is vrouw'. Maar binnen een groep van zevenduizend blanke vrouwen en zevenduizend zwarte vrouwen zijn de gegevens 'is zwart' en 'is vrouw' geen identificatoren. Het zijn wel gegevens die iets over personen kunnen zeggen. Zo'n gegeven wordt ook wel een attribuut genoemd. Voorbeelden van attributen zijn leeftijd, geslacht, het hebben van een bepaald diploma, woonplaats, werkgever, of locatie. In beginsel zouden gedragsgegevens ook als attributen kunnen worden opgeslagen, denk aan online surfgedrag, mobiliteitsgedrag, rijgedrag, eetgedrag, en zo meer. Of een bepaald attribuut of een set van attributen identificatie mogelijk maakt, hangt dus af van de omstandigheden (denk aan het hierboven gegeven voorbeeld van de zwarte vrouw).

Het gaat bij de I van SSI dus niet over *wie* een persoon is (identiteit in eigenlijke zin), maar eerder over *wat* een persoon is (digitale representatie van identiteit, door middel van de set van attributen waarmee een persoon binnen een bepaalde context kan worden beschreven),[22] en over een of meer attributen die in een bepaalde context identificatie mogelijk maken.

We kunnen nu wat puntjes op de i zetten. Een identificator kan een nummer zijn of een set attributen.[23] Een identificator is per definitie een persoonsgegeven. Een attribuut of een set attributen is alleen een persoonsgegeven wanneer daarmee redelijkerwijs identificatie mogelijk is (gezien de definities van 'persoonsgegeven' in art. 4(1) jo. overweging 26 AVG). Of identificatie aan de hand van een attribuut redelijkerwijs mogelijk is hangt af van (1) hoe uniek het gegeven is voor een bepaalde persoon in de betreffende context, en (2) welke gegevens aan elkaar kunnen worden gekoppeld als behorende bij eenzelfde persoon (dit wordt *linkability* genoemd). In de hierboven gegeven voorbeelden is het gegeven 'is vrouw' een identificator binnen de groep van driehonderd blanke mannen en één vrouw. In het andere voorbeeld (zevenduizend mannen en zevenduizend vrouwen) is het gegeven 'is vrouw' op zichzelf genomen niet identificerend, maar kan desondanks tot identificatie leiden als andere gegevens bekend zijn. Stel dat van iemand in die groep bekend is dat zij vrouw is, ouder dan achttien, rechten heeft gestudeerd, waar zij woont en op welke krant zij is geabonneerd. Dan is de kans veel groter dat zij identificeerbaar is. Dat betekent dat hoe

18 Zie de website van C. Allen: 'The path to self-sovereign identity', 25 april 2016, *www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html*.

19 Allen 2016.

20 E. Bayamlioglu et al. (red.), *BEING PROFILED:COGITAS ERGO SUM. 10 Years of profiling the European citizen*, Amsterdam: Amsterdam University Press 2018; W. Schreurs et al., 'Cogitas ergo sum: the role of data protection law and non-discrimination law in group profiling in the private sphere', en M. Hildebrandt, 'Profiling and the identity of the European citizen', beide in M. Hildebrandt & S. Gutwirth (red.) *Profiling the European citizen: cross-disciplinary perspectives*, Dordrecht: Springer 2008, p. 141-270 en 303-343.

21 De International Telecommunication Union (ITU) definieert 'identiteit' als: 'Information about an entity that is sufficient to identify that entity in a particular context', vgl. *Telecommunication Standardization Sector – NGN Identity Management Framework*, p. 3 nr. 3.3.9, zie *www.itu.int/rec/T-REC-Y.2720-200901-I*.

22 G. Alpár, J.H. Hoepman & J. Siljee, 'The identity crisis. Security, privacy and usability issues in identity management', *Journal of Information System Security* (9) 2013, afl. 1, p. 23-53. De auteurs bespreken het concept 'digitale identiteit' op p. 24 en 27-28. Over het onderscheid tussen 'wie' ('ik', eerste persoon enkelvoud) en 'wat' ('mij', derde persoon enkelvoud), en de dynamische relatie tussen beide zie Ricoeur 1990.

23 Ook een 'ding', zoals een smartcard, kan een identificator zijn, maar dat is dan het geval vanwege hetgeen de card bevat (een of meer nummers en/of attributen).

meer attributen van eenzelfde persoon bekend zijn, hoe eenvoudiger het wordt die persoon te identificeren.

De set van attributen die wordt vereist om toegang te krijgen tot een bepaalde dienst, is dus niet per se een identificator. Wie sterke drank wil kopen heeft aan één attribuut genoeg ('is ouder dan 18 jaar), wie een auto wil huren zal mogelijk meerdere attributen moeten delen ('heeft een geldig rijbewijs', 'nationaliteit'). Voordelen van ABC zijn dat, voor zover de attributen op een betrouwbare manier zijn geverifieerd, de dienstverlener redelijk zeker kan zijn dat ze kloppen, terwijl de betrokkene in beginsel kan beslissen alleen noodzakelijke attributen te delen. Een bijkomend voordeel *kan* zijn dat wanneer dezelfde persoon opnieuw toegang vraagt, de dienstverlener opnieuw kan zien dat de attributen kloppen maar niet dat het dezelfde persoon is. Laat staan dat derde partijen (advertentienetwerken) dat kunnen achterhalen. Dat heeft nogal wat voordelen, omdat het afleiden van individuele gedragspatronen de hierboven al genoemde *micro targeting* mogelijk maakt (denk aan gedragsprofielen bij online *advertising*, maar ook aan risico-scores bij kredietverlening en verzekeringspremies). Als creditcard-data, woonplaats of andere identificatoren moeten worden gedeeld kan de dienstverlener de betrokkene in beginsel wel *targeten* omdat verschillende identificaties dan aan elkaar kunnen worden gelinkt.

Een set attributen kan dus een identificator zijn, maar dat hoeft niet. Het attribuut 'is ouder dan 18' is een attribuut, maar hoogstwaarschijnlijk geen identificator omdat het enkele gegeven dat iemand ouder is dan 18 niet voldoende is om iemand te identificeren. Maar, wanneer zo'n attribuut redelijkerwijs kan worden gekoppeld aan andere gegevens die tot identificatie kunnen leiden, is zo'n attribuut of set van attributen desondanks een persoonsgegeven. In dat geval spreekt de AVG van een pseudoniem gegeven. Pseudonimisering wordt namelijk in artikel 4(5) gedefinieerd als:

> 'het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld'.[24]

Attributen die geen identificatie toestaan zijn anonieme gegevens, waarop de AVG niet van toepassing is. Pseudonieme gegevens zijn per definitie persoonsgegevens, maar zolang ze op een systematische wijze gescheiden blijven van relevante aanvullende gegevens gelden zij als een manier om aan de eisen van de AVG te voldoen, precies omdat zij de kans op identificatie aanzienlijk verkleinen. Zo zijn versleutelde gegevens in beginsel niet anoniem, zolang anderen dan de betrokkene de gegevens redelijkerwijs kunnen ontsleutelen. Het zijn evident wel pseudonieme gegevens in de zin van de AVG. De vraag of een versleuteld gegeven anoniem of pseudoniem is hangt dus af van het sleutelbeheer.

De beginselen van Allen zijn ontroerend in termen van goede bedoelingen maar geven weinig inzicht in wat SSI nu eigenlijk is

De beginselen van Allen zijn ontroerend in termen van goede bedoelingen maar geven weinig inzicht in wat SSI nu eigenlijk is. SSI lijkt zich te beperken tot de uitwisseling van identificatoren (beginselen 2 en 4 t/m 8), maar Allen spreekt toch ook van 'eigen data' (3), het delen van gegevens (9) en het beschermen van de rechten van 'gebruikers' (10). Het doel van SSI lijkt bovendien gericht op het beheren en beschikbaar stellen van identificatoren, want uiteindelijk moet SSI een oplossing bieden voor online identificatie.[25] Zoals de naam aangeeft is de gedachte dat de betrokkene heerst over de 'eigen' gegevens, zoals een soeverein heerst over de eigen onderdanen. Feitelijk gaat het echter om controle over de cryptografische sleutels waarmee persoonsgegevens kunnen worden gedeeld.[26] Nu de meeste mensen geen verstand hebben van cryptografische sleutels is het maar de vraag of de inzet van systemen die daar gebruik van maken daadwerkelijk controle biedt aan de gebruiker. Op basis van de technologie garandeert SSI eigenlijk niet meer dan twee zaken: de integriteit van de data die wordt verstrekt en het 'soeverein' beheer over die data door degene die de private sleutels beheert. Integriteit is hier een begrip uit de informatica dat ziet op het feit dat data niet ongemerkt of zonder toestemming kan worden veranderd;[27] 'integriteit' zegt niets over de juistheid van de data. Integendeel, wanneer eenmaal een onjuist gegeven wordt ingevoerd, blijft precies dat onjuiste gegeven ongewijzigd aanwezig in bijvoorbeeld de blockchain. Het feit dat het beheer (het gezag of de macht) over de data

24 Over het onderscheid tussen anonimisering en pseudonimisering zie de European Data Protection Board (EDPB, voorheen Art. 29 Werkgroep, het onafhankelijke adviesorgaan, ingesteld in art. 68 AVG, bestaande uit de hoofden van de nationale toezichthouders, met als taak het verzekeren van de consistente toepassing van de AVG), *Advies 5/2014 over anonimiseringstechnieken,* 10 april 2014, WP217; zie ook HvJ EU, 10 oktober 2016, C-582/14 (*Breyer tegen Duitsland*), waar het hof – onder voorgaande richtlijn – besluit dat een dynamisch IP-adres in casu gezien moet worden als een pseudoniem persoonsgegeven.

25 Identiteitsmanagement kan worden geregeld vanuit het gecentraliseerde perspectief van een organisatie, die identificatoren toekent aan medewerkers, leveranciers, klanten of andere gebruikers. Dit leidt ertoe dat gebruikers een veelheid aan identificatoren moeten beheren (voor iedere organisatie of website waarmee ze te maken hebben), en weinig of geen controle hebben over welke identificatoren wanneer met wie worden gedeeld. Ook federatieve oplossingen (waarbij meerdere organisaties gezamenlijk dezelfde 'identificatoren' gebruiken, zoals bijvoorbeeld een e-mailadres, of Facebook-login) bieden weinig controle en nog minder transparantie. SSI hoopt die controle radicaal om te draaien en bij de gebruiker te leggen.

26 Bijvoorbeeld: 'With a SSI solution, control is given to the identity subject in the form of control over the associated cryptographic keys', Blockchain Bundesverband 2018 *supra* noot 1, p. 42.

27 K.M.M. de Leeuw & J. Bergstra (red.), *The history of information security: a comprehensive handbook*, Oxford: Elsevier Science 2007.

bij de sleutelbeheerder ligt, betekent intussen niet dat deze daarom naar eigen inzicht gegevens kan delen. Weigering kan immers leiden tot het weigeren van dienstverlening (bij commerciële dienstverlening) of het opleggen van een boete (als het verstrekken van gegevens een wettelijke plicht is, zoals bij de belastingaangifte). Zolang sociale netwerken een verdienmodel hanteren dat is gebaseerd op het monetariseren van persoonsgegevens kunnen zij toegang weigeren aan personen die hun gegevens afschermen,[28] daar doet SSI niet aan af.

ABC richt zich, anders dan SSI, niet alleen naar de wensen van de betrokkene. Naast de beperking van dataverwerking tot hetgeen noodzakelijk is gezien het verwerkingsdoel, richt ABC zich ook op de betrouwbaarheid van de verstrekte attributen

4.2 ABC

SSI wekt de indruk dat een individu te allen tijde naar eigen willekeur moet kunnen besluiten om al dan niet identificatoren te delen. Nog interessanter zou zijn om een systeem zo in te richten dat van begin af aan niet meer data wordt gedeeld dan noodzakelijk is voor het doel waarvoor de data zal worden gebruikt. Dat betekent onder meer dat in veel gevallen zelfs in het geheel geen identificator hoeft te worden gedeeld. Dus, wie het zwembad bezoekt, deelt het gegeven 'heeft een abonnement' en verder niets. Daarmee kan niet worden gecheckt om wie het gaat en ook niet hoe vaak of wanneer een bepaald persoon komt zwemmen. Hoewel Allens negende beginsel verwijst naar dataminimalisering, wordt dat niet systematisch uitgewerkt.[29] Bij ABC is dit echter de hoofddoelstelling, naast het bewerkstelligen van de betrouwbaarheid van de data.

ABC is een vorm van attributen-beheer, waarbij attributen (*claims*) na verificatie worden opgeslagen in de beveiligde omgeving van de betrokkene.[30] De verificatie vindt plaats door degene die de attributen uitgeeft, die ze in de vorm van een *credential* (een versleutelde container) opslaat en voorziet van een digitale handtekening. Wanneer bijvoorbeeld een wettelijke plicht bestaat om data te delen, of wanneer de toegang tot een dienst afhankelijk is van de verstrekking van bepaalde attributen, kan de verstrekking dankzij de ABC-applicatie worden beperkt tot de noodzakelijke data.[31] Als die data geen persoonsgegevens bevat, is het profileren (en *targeten*) van de betrokkene op basis van opeenvolgend verstrekte attributen niet mogelijk. De exploitant van het zwembad kan dus wel tellen hoeveel mensen hoe laat komen zwemmen, maar weet niet wie dat zijn (en kan ook geen analyse maken van individueel bezoekersgedrag). Je zou kunnen zeggen dat ABC het beheer van persoonsgegevens in dat geval toestaat terwijl 'de soeverein' (de betrokkene) niet thuis is, of in ieder geval onzichtbaar blijft voor de verantwoordelijke verwerker.

ABC richt zich bovendien, anders dan SSI, niet alleen naar de wensen van de betrokkene. Naast de beperking van dataverwerking tot hetgeen noodzakelijk is gezien het verwerkingsdoel, richt ABC zich ook op de betrouwbaarheid van de verstrekte attributen. Omdat SSI op radicale wijze kiest voor een gedecentraliseerd systeem, is het in beginsel afhankelijk van peer-to-peer-verificatie (oftewel reputatiebeheer). ABC kiest ervoor om de attributen decentraal op te slaan in de vorm van een *credential*, maar de uitgifte en verificatie vindt in beginsel plaats door centrale instituties zoals de gemeente (adres, geboortedatum, burgerlijke stand), de staat (nationaliteit) of een bank (accountinformatie).[32] Daarbij kunnen attributen horen als 'woont in deze wijk', 'is geboren na 2000', 'is ouder dan 18 jaar', 'is gehuwd', 'heeft niet de Nederlandse nationaliteit', 'heeft voldoende saldo', in plaats van volledige adresinformatie, precieze geboortedatum, of de gegevens over met wie men is getrouwd. Zolang aanvullende informatie niet noodzakelijk is voor het doel van de verstrekking, kan de gebruiker van ABC-applicatie besluiten die niet te delen. Het feit dat attributen zijn uitgegeven en geverifieerd door een instantie die zulke gegevens gezaghebbend vast kan stellen, is een voordeel voor degene die op basis daarvan toegang verleent tot een bepaalde dienst. Daarmee is dan niet alleen *unlinkability* gerealiseerd tussen verschillende transacties door dezelfde betrokkene. Er wordt in beginsel ook geen persoonsgegeven gedeeld, tenzij het attribuut redelijkerwijs kan worden gelinkt aan de betrokkene, want dan gaat het om een pseudoniem gegeven. In het eerste geval is de AVG niet van toepassing, in het tweede geval lijkt dit type pseudonimisering het eenvoudiger te maken om *compliance* met de AVG af te dwingen, met name ten aanzien van dataminimalisering en doelbinding.

28 Hoewel additionele verwerking waarschijnlijk onrechtmatig is onder de AVG, zie art. 7.4 jo. overweging 43. 'Big Tech' zal eigener beweging het huidige verdienmodel niet aanpassen, daarvoor zal een uitspraak van het HvJ EU nodig zijn. De Nederlandse Autoriteit Persoonsgegevens bepaalde intussen al wel dat consent voor additionele verwerking niet geldig is wanneer de toestemming wordt afgedwongen door de toegang tot een website of applicatie te weigeren, zie Normuitleg Cookiewalls Autoriteit Persoonsgegevens, maart 2019, *www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_cookiewalls.pdf*.

29 Ook al menen sommigen dat SSI bij uitstek naleving van de AVG mogelijk maakt, zie E.M. Renieris, 'Is Self-Sovereign Identity the ultimate GDPR compliance tool?' (3 delen), *Medium* (blog) 25 mei 2018. Zij lijkt echter te denken dat de AVG vooral gaat over consent, wat niet het geval is. Zie *infra* paragraaf 5 voor een bespreking van de rol van consent in de AVG.

30 Dat kan lokaal zijn, op de eigen randapparatuur, of in de 'cloud'. Beiden hebben voor- en nadelen. Een andere term voor attribuut is een *claim*, zie bijvoorbeeld Alpár, Hoepman & Siljee 2013, p. 24, of X. Zhu & Y. Badr, 'Identity management systems for the Internet of Things: a survey towards blockchain solutions', *Sensors* (18) 2018, afl. 12, 4215, p. 9/18, *https://doi.org/10.3390/s18124215*.

31 M. Koning et al., 'The ABC of ABC: an analysis of attribute-based credentials in the light of data protection, privacy and identity', in: J. Balcells, (red.), *Internet, Law & Politics: A decade of transformations. Proceedings of the 10th International Conference on Internet, Law & Politics*, Barcelona : Huygens Editorial 2014, p. 359. Op p. 360-361 en 363-364 wordt onder andere de rol van de 'scheme authority' besproken die het protocol bepaalt waarin wordt vastgesteld welke attributen voldoende zijn voor het

verkrijgen van specifieke toegang of dienstverlening. Zie bijvoorbeeld *https://privacybydesign.foundation/uitgifte/*.

32 Zie de bespreking van een aantal SSI- en ABC-systemen die het ophalen van attributen bij de overheid mogelijk maakt, en een zekere mate van eigen beheer door de burger veilig stellen, B. Jacobs, 'Praktijklessen Voor Datakluizen', *IBestuur* (blog) 22 februari 2019, mede naar aanleiding van de Initiatiefnota van de leden Middendorp en Verhoeven: Online identiteit en regie op persoonsgegevens, *Handelingen II* 2017/18, 34993, 2. Voor een overzicht van de instanties die geverifieerde attributen uitgeven zie *https://privacybydesign.foundation/uitgifte/*. Daaronder vallen ook sociale netwerken, zie daarover noot 36.

33 Zie K. Rannenberg, J. Camenisch & A. Sabouri (red.), *Attribute-Based Credentials for trust: identity in the information society*, New York: Springer 2014; A. Sabouri, I. Krontiris & K. Rannenberg, 'Attribute-based credentials for trust (ABC4Trust)', in S. Fischer-Hübner, S. Katsikas & G. Quirchmayr (red.), *Trust, privacy and security in digital business* (Lecture Notes in Computer Science), Berlijn: Springer 2012, p. 218-219.

34 Zie IRMA: *https://privacybydesign.foundation*.

35 Rieks Joosten 2018.

36 Bij IRMA kunnen bijvoorbeeld ook attributen van sociale netwerken worden opgeslagen, maar het betreffende netwerk kan niet zien hoe die gegevens worden verstrekt (aan wie, wanneer, hoe vaak).

37 World Economic Forum, 'Personal data: the emergence of a new asset class', rethinking personal data, 2011, *www.weforum.org/reports/personal-data-emergence-new-asset-class*. Zie ook EDPB (voorheen Art. 29 Werkgroep), WP251rev01 6 februari 2018, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, p. 9.

Het ontwerp van ABC bestaat al geruime tijd,[33] en de eerste applicatie is inmiddels in gebruik.[34] Hoewel sommigen wellicht menen dat ABC een vorm is van SSI,[35] lijkt SSI door te slaan naar oncontroleerbare willekeur aan de kant van de betrokkene. Die willekeur is echter een illusie (omdat gebruikers vaak verplicht of gedwongen worden hun data te delen) en zal bovendien niet werken als een dienstverlener zeker moet zijn van de identificatie van de betrokkene (die bijvoorbeeld een bijstandsuitkering of studiebeurs aanvraagt, of belastingaangifte doet). ABC lijkt veel meer in lijn met de relationele opvatting van persoonsgegevens en zou daarmee een evenwichtiger alternatief kunnen bieden voor de huidige problemen van digitale identificatie.

Een probleem dat noch SSI- noch ABC-systemen kunnen oplossen is de handel in gedragsgegevens. En laat dat nu juist één van de cruciale pijnpunten zijn van de huidige, gemankeerde informatieomgeving

4.3 Welke problemen lossen SSI en ABC wel en niet op, en welke problemen creëren ze?

ABC-systemen kunnen in ieder geval een aantal problemen oplossen. Ten aanzien van personen gaat het dan in beginsel om oplossingen die zijn gebaseerd op de opslag van geverifieerde attributen in een beveiligde, persoonlijke datakluis: (1) ABC zorgt dat attributen worden verstrekt zonder dat de partij die de attributen uitgaf en verifieerde bij kan houden wanneer en met wie ze worden gedeeld (dat is bij 'traditionele' identity-management-systemen meestal wel zo),[36] (2) ABC kan zekerheid bieden dat de juiste personen op grond van de juiste informatie toegang verkrijgen tot ruimtes, diensten, producten, kennis en informatie, omdat ABC de mogelijkheid biedt om institutionele verificatie te garanderen door relevante centrale partijen (gemeente, bank, staat, verzekeraar), (3) ABC beperkt de te delen informatie tot hetgeen noodzakelijk is voor het doel van de verstrekking, doordat met attributen wordt gewerkt in plaats van volledige identiteiten, (4) ABC biedt bescherming tegen profilering doordat herhaalde verstrekkingen van gegevens door eenzelfde persoon niet aan elkaar kunnen worden gelinkt, zelfs niet als het gaat om dezelfde dienstverlener, laat staan dat een persoon 'gevolgd' kan worden op basis van interacties met verschillende dienstverleners.

SSI-systemen die niet werken met institutioneel geverifieerde *attributen* (1 en 2), die gebruikers niet toestaan zich te beperken tot noodzakelijke attributen (3) en geen *unlinkability* verzekeren (4) kunnen genoemde garanties echter niet bieden. Omdat SSI gekoppeld is aan de blockchain en uitgaat van een systematisch wantrouwen ten aanzien van gevestigde instituties zal de uitgifte van *credentials* niet via bestaande instituties verlopen (1 en 2 vervallen daarmee). In hoeverre SSI toestaat om zich te beperken tot noodzakelijke attributen en *unlinkability* is onduidelijk; de nadruk op soeverein beheer doet vermoeden dat het vooral gaat om het peer-to-peer-aspect (wantrouwen jegens centrale instituties) en veel minder om dataminimalisering.

Een aantal problemen kunnen SSI- en ABC-systemen niet oplossen. Ten eerste zal de vraag of de attributen juist zijn, afhangen van de vraag of de sleutelbeheerder (nog steeds) degene is waarnaar de attributen verwijzen. Als het sleutelbeheer in handen is van degene die een smartcard bij zich draagt of degene die toegang heeft tot de smartphone en de daarop geïnstalleerde SSI- of ABC-applicatie, dan kunnen we ons allerlei scenario's voorstellen van identiteitsfraude.

Het tweede probleem dat noch SSI- noch ABC-systemen kunnen oplossen is de handel in gedragsgegevens. En laat dat nu juist één van de cruciale pijnpunten zijn van de huidige, gemankeerde informatieomgeving. Het World Economic Forum heeft ooit een onderscheid voorgesteld tussen drie soorten data:[37] vrijwillig verstrekte, geobserveerde en afgeleide data. De eerste soort betreft verstrekte data, het type gegevens waar SSI en ABC het patent op hebben: allerlei attributen die we bewust en opzettelijk met dienstverleners delen om toegang te krijgen tot relevante diensten (in brede zin), bijvoorbeeld leeftijd, dienstverband, haarkleur, een cijferlijst, geboortedatum, een genetisch profiel of het brutoloon. Bewust en opzettelijk verlenen veronderstelt overigens geen 'consent' in de zin van art. 6(1)(a), want vaak zijn betrokkenen wettelijk verplicht om dergelijke gegevens te verstrekken, of zijn ze noodzakelijk voor de betreffende dienstverlening (zie de afsluitende paragraaf over de rol van consent).

De tweede soort betreft gedragsdata die door online platforms die we bezoeken (of IoT-omgevingen) wordt uitgelezen en opgemeten dankzij allerhande software (of sensortechno-

logie), waarbij het gaat om 'klik- en typegedrag', surfgedrag, de tijd die we spenderen op bepaalde pagina's binnen een site, de browser die we gebruiken, de zoektermen die we intypen, ons like-gedrag, de frequentie waarmee we tweeten of posten, het woordgebruik dat we hanteren, of ons energieverbruiksgedrag, rijgedrag, of zelfs eet- en slaapgedrag. Veel van die gedragsdata ziet op onbewuste processen, die ons in staat stellen om intuïtief, snel en effectief te handelen zonder steeds te pauzeren om daarover bewust te beslissen. Dit type geobserveerde data (gedragsdata) bestaat niet uit attributen die we zelfstandig 'uploaden' in de SSI- of ABC-applicatie, met een serie instructies over hoe ze wel en niet mogen worden gebruikt. Integendeel, deze data wordt door anderen 'gevangen' op basis van spyware zoals cookies, *browser fingerprints*, camera's en zo meer. Het is niet ondenkbaar dat zulke gedragsdata via webbrowsers en sensortechnologie rechtstreeks in een digitale datakluis wordt opgeslagen en alleen na bijvoorbeeld microbetalingen aan dienstverleners wordt verstrekt.[38] Dat leidt tot interessante verschuivingen in de beschikbaarheid van de betreffende data, want wie genoeg geld heeft kan die verstrekking standaard uitzetten, waardoor mogelijk alleen de data van minderbedeelde 'gebruikers' beschikbaar is. Bovendien kan iemand de gegevensstroom in beginsel naar eigen willekeur (als een soeverein) aan- en uitzetten, naargelang zij wel of niet traceerbaar willen zijn in een bepaalde omgeving. Dat zou tot problemen kunnen leiden bij de betrouwbaarheid van de kennis en informatie die uit het aggregaat van gedragsdata wordt afgeleid.[39] Vanuit het perspectief van de mensenrechten kan dat overigens als een voordeel worden gezien, omdat die onbetrouwbaarheid de inzet van profilering zou kunnen terugdringen.

Gedragsdata bestaat niet uit attributen die we zelfstandig 'uploaden' in de SSI- of ABC-applicatie. Integendeel, deze data wordt door anderen 'gevangen' op basis van spyware

De derde soort van data betreft het resultaat van geautomatiseerde analysemethoden (machinaal leren). Dat resultaat wordt afgeleid uit grote aggregaten van vrijwillig verstrekte en geobserveerde data. Die afgeleide data is op dit moment meestal in handen van de partij die de analyse maakt of laat maken. In eerste instantie zal het bij dat resultaat niet per se gaan om persoonsgegevens, maar om min of meer abstracte patronen, waarop de AVG niet van toepassing is. De soevereiniteit over die data ligt sowieso niet binnen het bereik van de betrokkene wiens data is gebruikt, al was het maar omdat die data pas beschikbaar komt na verwerking van heel veel data van heel veel personen. Zodra die afgeleide data (patronen) echter wordt toegepast op een identificeerbaar persoon (bijvoorbeeld door een advertentie te plaatsen op een webpagina die zij bezoekt), is de AVG weer van toepassing en zal met name het verbod van geautomatiseerde beslissingen een rol gaan spelen (art. 22).[40] Afgeleide data kan niet als attribuut in een SSI-applicatie worden geüpload. Enerzijds omdat deze data niet in handen is van de betrokkene maar van derden en anderzijds omdat het vaak gaat om bijzonder dynamische data die voortdurend wordt aangepast op basis van fluctuerende gedragsdata.

Ten aanzien van de tweede en derde soort data zien we inmiddels een roep om die beschikbaar te maken als 'open data' en/of als 'common good'.[41] Dat zou betekenen dat er een morele of zelfs juridische verplichting op betrokkenen en/of dienstverleners rust om deze data op een gesecuritiseerde wijze beschikbaar te stellen, zodat daar met behulp van kunstmatige intelligentie nieuwe kennis uit kan worden afgeleid. Dat wil zeggen dat de data wordt opgeslagen op een wijze die de integriteit van de data waarborgt (zonder securitisering is de data onbetrouwbaar en daarmee eigenlijk waardeloos). Mogelijk kunnen SSI- of ABC-toepassingen hieraan bijdragen voor zover de IoT-infrastructuur en de infrastructuur van het *world wide web* zodanig worden heringericht dat gedragsdata uitsluitend via 'eigen' digitale datakluizen wordt verzameld en vervolgens hetzij vrijwillig hetzij verplicht wordt toegevoegd aan gesecuritiseerde datastapels (die in beginsel ook weer gedistribueerd kunnen worden opgeslagen en decentraal kunnen worden beheerd). Indien vrijwillig, speelt hier weer het probleem dat zulke datastapels alsdan incompleet zullen zijn; indien verplicht, zijn we dichtbij David Brins *The Transparent Society*,[42] waar niet iedereen dolenthousiast van zal worden. Voorlopig is het nog niet zover, ik laat dit punt met het oog op de beperkte ruimte rusten.

De problemen die SSI- en ABC-systemen creëren hangen af van hoe deze zijn ontworpen, ingebed in en afgestemd op beschikbare infrastructuur. Voor zover een SSI op een

38 J. Lanier, *Who owns the future?*, New York: Simon & Schuster 2014.

39 Hoewel het sowieso een illusie is te menen dat gedragsdata compleet zou kunnen zijn; zie bijvoorbeeld de discussie rond de vraag of 'deep learning' een vorm van alchemie is of betrouwbare wetenschap: D. Sculley et al., 'Winner's curse? On pace, progress, and empirical rigor', 12 februari 2018, *https://openreview.net/forum?id=rJWF0Fywf* en M. Hildebrandt, 'Preregistration of machine learning research design. Against P-Hacking', in: Bayamlioglu et al. 2018. Om nog maar te zwijgen van de bias die inherent is aan bigdata-analyse, zie bijvoorbeeld de daaraan gewijde conferenties van de ACM *https://fatconference.org/2019/acceptedpapers.html*.

40 Zie hieronder in par. 5.

41 M. Mazzucato, 'Let's make private data into a public good', *MIT Technology Review* 27 juni 2018, *www.technologyreview.com/s/611489/lets-make-private-data-into-a-public-good/*. Zie ook het onderzoeksproject van Tamar Sharon over 'Digital good – the digital disruption of health research and the common good', *www.ru.nl/ptrs/research/research-projects/digital-good/*.

42 David Brin, *The transparent society. Will technology force us to choose between privacy and freedom?*, Massachusetts: Perseus Books 1998.

blockchain wordt gebouwd, heeft deze alle nadelen die kleven aan blockchain-toepassingen, bijvoorbeeld: de onverantwoorde hoeveelheid energie die het vraagt, de afhankelijkheid van *miners* of *validators* die zogenaamd gedistribueerd zijn maar meestal in China zitten, en de kwetsbaarheid voor aanvallen en bugs. Blockchain-toepassingen worden vaak aan de man gebracht met een beroep op *trustless computing*, maar vragen in feite om vertrouwen in bestaande instituties te vervangen door vertrouwen in technologie die de meeste mensen niet begrijpen en dus in de protocollen die de technologie doen werken. Daarmee wordt eigenlijk vertrouwen gevraagd in een technocratische elite (de ontwikkelaars van de *core* code, die het systeem samen met de *miners* ook moeten onderhouden). Daar komt bij dat de blockchain allerlei problemen oproept met aansprakelijkheid. Zo is het lastig te achterhalen wie men kan aanspreken, en vaak is de wederpartij niet identificeerbaar. Een ander *unique selling point* is de zogenaamde 'immutability', maar dat blijkt gemakkelijk een nadeel te worden als inputdata die van buiten de blockchain komt niet juist is;[43] SSI werkt namelijk niet noodzakelijkerwijs met betrouwbare attributen, waardoor de betrouwbaarheid feitelijk in de lucht komt te hangen.

ABC lijkt minder problemen te scheppen, maar de inzet van ABC-toepassingen hangt net als bij SSI af van de beschikbaarheid van een infrastructuur die ABC mogelijk maakt

ABC lijkt minder problemen te scheppen, maar de inzet van ABC-toepassingen hangt net als bij SSI af van de beschikbaarheid van een infrastructuur die ABC mogelijk maakt. Een mogelijk probleem is dat ook wanneer niet-identificerende attributen worden gebruikt, het nog steeds mogelijk is om – weliswaar niet gepersonaliseerd – te profileren op datapunten. Hoewel de risico's daarvan worden ingeperkt doordat verschillende attributen van dezelfde persoon niet aan elkaar kunnen worden gelinkt, maakt het feit dat data door een gemeente of bank is geverifieerd de afgeleide kennis betrouwbaarder. Dat heeft gevolgen voor het eventuele *targeten* met die afgeleide kennis.[44] Nader onderzoek is hier gewenst, waarbij de mogelijkheid om zich te verzetten tegen geautomatiseerde *targeting* cruciaal is (art. 22).[45] Daarbij speelt ook dat ABC het feitelijk mogelijk maakt bepaalde vormen van *targeting* onmogelijk te maken, voor zover het verstrekken van relevante attributen kan worden geweigerd. Daardoor kan echter niet alleen de toegang maar ook de functionaliteit van een IoT-omgeving in gevaar komen, omdat de aanvoer van gedragsgegevens stagneert of incompleet is.[46]

5 Slotbemerkingen: soevereiniteit, controle en consent

Tot slot nog enige overwegingen over de rol van consent. In de Engelse versie van de AVG wordt gesproken van *consent*, dat een iets andere connotatie heeft dan toestemming. Nu consent ook een Nederlands woord is, spreek ik hier liever van 'consent', ook al gebruikt de Nederlandse versie van de AVG 'toestemming'. Toestemming is een vertaling van *permission*; in de AVG gaat om het bredere begrip 'consent'.

De soevereiniteitsgedachte die in de idee van SSI tot uitdrukking komt – en die volgens bovenstaande een onjuiste indruk wekt van wat SSI de facto vermag – hangt sterk samen met het zogenaamde controleperspectief op gegevensbescherming. Anders dan sommigen beweren,[47] vormt dat perspectief niet de eenduidige hoofdlijn van de AVG. Het is weliswaar de bedoeling van de Europese wetgever om betrokkenen meer controle te geven over hun persoonsgegevens, maar niet als een soeverein die de lakens uitdeelt. Dat kan worden afgeleid uit het feit dat consent weliswaar als enige juridische basis expliciet wordt genoemd in het fundamentele recht op gegevensbescherming (art. 8.2 Handvest van de fundamentele rechten van de EU), maar dat ook in die context al duidelijk wordt aangegeven dat andere gronden evenzeer tot legitimatie van noodzakelijke verwerking kunnen leiden. In de AVG zijn om die reden vijf andere gronden voorzien (zie hierboven in par. 2), variërend van een contractuele rechtsverhouding en het gerechtvaardigd belang van de verantwoordelijke tot wettelijke plichten en publieke taakuitoefening.

De verwarring rond consent hangt mogelijk samen met het feit dat voor gebruikers, dienstverleners en informatici het verrichten van een feitelijke handeling, zoals het klikken op een button, gelijk staat aan het geven van consent. Juridisch gezien ligt dat echter niet voor de hand. Voor een jurist is consent een rechtshandeling, dat wil zeggen een handeling

43 Blockchain-oplossingen combineren cryptografische technologie met peer-to-peer-netwerken (P2P-netwerken), zie ook *supra* voetnoot 12. Zie bijvoorbeeld A. Walch, 'The path of the blockchain lexicon (and the law)', *Review of Banking & Financial Law* (36) 2017, p. 713; A. Walch, 'Deconstructing "decentralization": exploring the core claim of crypto systems' (SSRN Scholarly paper), Rochester, NY: Social Science Research Network, 30 januari 2019, *https://papers.ssrn.com/abstract=3326244*. Zeer helder: Hoepman 2018, *supra* noot 12.

44 Zie ook Koning et al. 2014, p. 369-370.

45 Zie *infra* par. 5.

46 Zie voor mogelijke implicaties ook Koning et al. 2014, p. 361-365.

47 B. Prainsack, 'Logged out: ownership, exclusion and public value in the digital data and information commons', *Big Data & Society* (6) 2019, afl. 1, 2053951719829773, *https://doi.org/10.1177/2053951719829773*, p. 2.

met beoogd rechtsgevolg (art. 3:33 BW). Die rechtshandeling kan eventueel uit zo'n feitelijke handeling worden afgeleid, maar valt er nooit mee samen. Consent als rechtshandeling speelt in het kader van de AVG in ieder geval op drie niveaus.

De verwarring rond consent hangt mogelijk samen met het feit dat voor gebruikers, dienstverleners en informatici het verrichten van een feitelijke handeling, zoals het klikken op een button, gelijk staat aan het geven van consent. Juridisch gezien ligt dat echter niet voor de hand

Ten eerste als rechtshandeling waarmee een juridische basis wordt veiliggesteld voor het verwerken van persoonsgegevens (art. 6(a)). Het moet gaan om een 'vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt' (art. 4(11)). In dat geval is het rechtsgevolg dat de verwerking van de betreffende persoonsgegevens in beginsel rechtmatig is. Dat gaat echter alleen op als de consent is gericht op verwerking die noodzakelijk is voor een specifiek, expliciet en legitiem doel (art. 6(a) jo. 5.1(b)). Daarnaast stelt artikel 7 nog een aantal harde eisen aan consent als verwerkingsgrond. Zo moet, indien de consent deel uitmaakt van een geschreven verklaring waarin ook andere zaken worden geregeld, het verzoek om consent 'in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig [worden] gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden' (op straffe van nietigheid) (art. 7.2). Wanneer SSI of ABC het mogelijk maakt om zich te identificeren in het kader van een schriftelijke overeenkomst zal specifiek aandacht aan dit punt moeten worden besteed. Denk aan een medische behandelovereenkomst waarin consent is opgenomen om de uitslag van testen en andere behandeldata ook voor medisch onderzoek te mogen verwerken (dat lijkt in strijd met art. 7.2). Daarnaast heeft betrokkene het recht haar consent te allen tijde in te trekken en moet die intrekking even gemakkelijk te doen zijn als de verlening (art. 7.3). Dat betekent dat uit een simpele druk op de knop van de SSI-applicatie onder bepaalde voorwaarden consent mag worden afgelezen, maar dat die met een even simpele druk op eenzelfde knop weer ongedaan kan worden gemaakt. Interessant is ook dat wanneer consent wordt gegeven omdat de dienstverlener de dienst anders weigert, die consent in beginsel niet geldig is als de data niet noodzakelijk is voor het verlenen van de dienst (art. 7.4 jo. overweging 43).

Het tweede niveau waarop consent speelt in de AVG betreft de verwerking van bijzondere persoonsgegevens (inzake etnische achtergrond, gezondheid e.d.), die in beginsel verboden is (art. 9.1). Toestemming is een van de uitzonderingen op grond waarvan desondanks mag worden verwerkt (art. 9.2(a)). Deze uitzondering valt niet samen met de verwerkingsgrond van artikel 6(a).[48] Zo kan er bijvoorbeeld worden verwerkt op basis van een overeenkomst of het legitieme belang van de verantwoordelijke, waarbij bovendien een van de uitzonderingsgronden van artikel 9.2 van toepassing moet zijn, wil de verwerking rechtmatig zijn. Hier gaat het om 'uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden' (art. 9.2(a)). Uitdrukkelijk is het tegenovergestelde van impliciet; het zal van de omstandigheden van het geval afhangen of het verlenen van consent via een SSI- of ABC-applicatie gelijk staat met uitdrukkelijk verleende toestemming. Ook dan blijft het de vraag of de toestemming vrijwillig is verleend dan wel onder druk is gegeven.

Het derde niveau waar consent speelt in de AVG betreft de inzet van geautomatiseerde beslissingen, hetwelk behoudens drie uitzonderingen in beginsel verboden is (art. 22.1). Een geautomatiseerde beslissing is aan de orde als er geen sprake is van menselijke tussenkomst, dus bijvoorbeeld wanneer een IoT-omgeving allerlei beslissingen neemt die volautomatisch worden uitgevoerd. Bovendien gaat het alleen om beslissingen die rechtsgevolg hebben ten aanzien van betrokkene, dan wel haar anderszins in aanzienlijke mate treft. Het scheppen van een betalingsverplichting is evident een kwestie van rechtsgevolg, en het feit dat iemand in een hoge risicocategorie wordt ingeschaald die tot een hogere verzekeringspremie leidt, zal al snel gelden als een beslissing die hen in aanzienlijke mate treft. Toestemming is een van de drie uitzonderingsgronden op het verbod van geautomatiseerde beslissingen en net als bij

48 EDPB, 23 januari 2019, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), punt 15, p. 5, *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf*. Over de EDPB zie *supra* noot 24.

bijzondere persoonsgegevens gaat het hier om uitdrukkelijke toestemming. De European Data Protection Board (EDPB) merkt op dat menselijke tussenkomst alleen meetelt als de betreffende persoon de beslissing begrijpt en bevoegd is een andere beslissing te nemen.[49] Stel dat geautomatiseerde systemen beslissingen voorbereiden die vervolgens worden genomen door medewerkers die (a) niet weten waarom het systeem een bepaalde beslissing voordraagt en (b) feitelijk geacht worden de aangedragen beslissing te volgen. In dat geval geldt zo'n beslissing als een geautomatiseerde beslissing in de zin van artikel 22, die behoudens de uitzonderingen verboden is.

Bij ABC-systemen lijkt een evenwichtige afweging te zijn ingebouwd die de relationele aard van persoonsgegevens bevestigt en naïef soevereiniteitsdenken voorkomt

Wanneer via een SSI- of ABC-applicatie attributen worden aangeleverd op basis waarvan een geautomatiseerde beslissing wordt genomen, kan niet automatisch worden aangenomen dat sprake is van rechtsgeldige toestemming. Dat zal juridisch afhangen van de concrete omstandigheden van het geval en met name van de vraag of de gebruiker redelijkerwijs kon voorzien wat de gevolgen van de toestemming zouden zijn, dan wel geacht moet worden het risico te dragen dat zij met het verstrekken van de data nam. Bij ABC-systemen kan dat gezien het ontwerp en de geboden bescherming sneller worden aangenomen dan bij SSI-systemen, waar veel zal afhangen van het concrete ontwerp en de default instellingen.

De conclusie is in ieder geval dat de AVG geen soevereine betrokkene veronderstelt en zware voorwaarden stelt aan consent, waardoor dit vaak geen betrouwbare verwerkingsgrond zal zijn. Ook kan niet zonder meer worden aangenomen dat het verstrekken van attributen noodzakelijkerwijs geldt als toestemming bij de verwerking van bijzondere gegevens dan wel geautomatiseerde beslissingen in de zin van artikel 22. Dit is geen reden om SSI of ABC af te wijzen als bijdrage aan praktische en effectieve gegevensbescherming. Het is wel een reden om dit soort systemen steeds te bezien in het licht van andere factoren, die mede bepalen of degene die er gebruik van maakt voldoende kon voorzien wat de gevolgen zouden zijn van het delen van attributen. Zoals aangegeven is het om andere redenen verstandig om SSI-oplossingen en -toepassingen te gebruiken die niet afhankelijk zijn van een blockchain. ABC-systemen dragen in ieder geval bij aan een versterking van de individuele autonomie van betrokkenen, terwijl zij tegelijkertijd een grote mate van zekerheid bieden aan overheden en commerciële dienstverleners dat gedeelde persoonsgegevens juist zijn. ABC draagt zonder meer bij aan naleving van de AVG, bij SSI is daar weinig over te zeggen omdat het verwijst naar een veelheid van ontwerpen met wisselende implicaties. Doordat het ontwerp van ABC-systemen de nadruk legt op dataminimalisering en doelbinding (alleen die gegevens worden gedeeld die noodzakelijk zijn voor de te verlenen toegang of dienstverlening), en zoveel mogelijk voorkomt dat gegevens worden gelinkt op een manier die manipulatie mogelijk maakt, lijkt bij ABC-systemen een evenwichtige afweging te zijn ingebouwd die de relationele aard van persoonsgegevens bevestigt en naïef soevereiniteitsdenken voorkomt.

49 EDPB (voorheen Art. 29 Werkgroep), WP251rev01 6 februari 2018, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, 24. Zie ook – in het kader van de vraag of zogenaamde 'smart contracts' onder art. 22 AVG vallen: M. Finck, 'Smart contracts as a form of solely automated processing under the GDPR' (SSRN Scholarly paper), Rochester, NY: Social Science Research Network, 8 januari 2019, *https://papers.ssrn.com/abstract=3311370*.