KU LEUVEN

FACULTEIT RECHTSGELEERDHEID

Academiejaar 2018 - 2019

To blockchain or not to blockchain?

De opportuniteit van blockchaintechnologie voor controle over persoonsgegevens uit de Algemene Verordening Gegevensbescherming

Promotor: PROF. A. VEDDER

Begeleidster: MEVR. E. VAN NERUM

Masterscriptie ingediend door

Dylan Verhulst

bij het eindexamen voor de graad

MASTER IN DE RECHTEN

KU LEUVEN

FACULTEIT RECHTSGELEERDHEID

Academiejaar 2018 - 2019

To blockchain or not to blockchain?

De opportuniteit van blockchaintechnologie voor controle over persoonsgegevens uit de Algemene Verordening Gegevensbescherming

Promotor: PROF. A. VEDDER

Begeleidster: MEVR. E. VAN NERUM

Masterscriptie ingediend door

Dylan Verhulst

bij het eindexamen voor de graad

MASTER IN DE RECHTEN

SAMENVATTING

Het schandaal over Facebook en Cambridge Analytica kwam in maart 2018 aan het licht. Dat brengt een heikel punt in het Europese gegevensbeschermingssysteem naar boven: de controle door de betrokkene over diens persoonsgegevens. Rechtsoverweging 7 stelt die controle als doelstelling van de Algemene Verordening Gegevensbescherming. Dit onderzoek poogt een oplossing te bieden voor dat probleem. Het kijkt daarvoor in de richting van blockchaintechnologie. Het onderzoek zal de opportuniteiten van de technologie voor de rechten van de betrokkene uit de Algemene Verordening Gegevensbescherming afwegen tegenover de conformiteitsproblemen van de technologie met de Verordening. Ook zal het SOVRIN project het voorwerp van analyse uitmaken, om zo te voorzien in een praktisch voorbeeld waartegen de theorie kan afgetoetst worden.

Het onderzoek geeft eerst een juridisch en technisch kader van de relevante wetsbepalingen en de technologie die van belang is voor dit onderzoek, met name blockchain. Het toont ook aan dat de uitoefening van de rechten, toegekend door de Algemene Verordening Gegevensbescherming, essentieel zijn om de beoogde controle te bewerkstelligen. Vervolgens worden de belangrijkste opportuniteiten, die blockchaintechnologie biedt voor die rechten, opgesomd. Nadien volgt een analyse van twee fundamentele moeilijkheden van de technologie voor conformiteit met de Algemene Verordening Gegevensbescherming: het recht op gegevensverwerking en de positie van de verwerkingsverantwoordelijke. Het onderzoek oppert dat die moeilijkheden niet onoverkomelijk zijn. Voornamelijk technische middelen lijken de oplossing te zijn: *off-chain* opslag van persoonsgegevens en een *permissioned* karakter van de gebruikte blockchain. Ook het SOVRIN project implementeert gelijkaardige middelen. Het onderzoek besluit in een positieve evaluatie van de opportuniteit van blockchaintechnologie voor de controle door de betrokkene over diens persoonsgegevens, in het licht van de Algemene Verordening Gegevensbescherming. Het maakt echter een caveat, namelijk dat de technologie nog zeer jong is en de toekomst meer duidelijkheid zal moeten bieden inzake eventuele moeilijkheden. Ten slotte geeft het onderzoek een aantal *best practices* voor blockchainontwikkelaars voor de naleving van de bepalingen uit de Algemene Verordening Gegevensbescherming.

DANKWOORD

Ik wens een heleboel mensen te bedanken, zonder wie ik dit werk nooit zou hebben kunnen volbrengen. Op momenten dat ik het niet meer zag zitten, gaven zij mij de kracht om te blijven doorzetten. Via deze weg wil ik iedereen bedanken, die me geholpen en bijgestaan hebben, en meer in het bijzonder:

Ten eerste wil ik graag mijn promotor prof. Vedder en begeleidster mevr. Van Nerum bedanken voor de professionele begeleiding en vakkennis die ze me aanboden bij het schrijven van dit onderzoek. Dankzij hun uitstekende adviezen kon ik dit werk voltooien.

Vervolgens wil ik graag mijn ouders, familie en vrienden bedanken, die me steeds bijstonden en me de mogelijkheid gaven om het beste van mezelf te geven. Bovenal wens ik Evi, mijn vriendin, te bedanken omdat zij steeds mijn klankbord was en deze opdracht samen met mij heeft doorstaan.

Ten slotte wens ik ook U, beste lezer, te bedanken voor de tijd en moeite om dit onderzoek te lezen. Ik hoop dat U enige inzichten kan puren uit dit werk.

Graag wil ik dit dankwoord afsluiten met de woorden van Stephen Hawking: However difficult life may seem, there is always something you can do, and succeed at it. What matters is that you don’t give up.”

Dylan Verhulst

Inhoudsopgave

INLEIDING

1. **UITEENZETTING VAN HET ONDERWERP -** Dit onderzoek zal handelen over de relatie tussen blockchaintechnologie en het Europese gegevensbeschermingssysteem. Meer bepaald peilt het naar de opportuniteit van het gebruik van blockchaintechnologie voor de controle door de betrokkene, in het licht van de Algemene Verordening Gegevensbescherming (hierna: AVG)[1]. De keuze voor het onderwerp vloeit voort uit de berichten over de vermeende privacyschendingen van Facebook en Cambridge Analytica, die midden maart 2018 de pers haalden.[2] De gegevens van 86 miljoen facebookgebruikers zouden onrechtmatig verzameld zijn.[3] Dat gegeven maakt meteen de noodzaak duidelijk van een sterk gegevensbeschermingssysteem en het belang van de controle door de betrokkene over diens eigen persoonsgegevens. De AVG zal het uitgangspunt vormen van dit onderzoek in de studie van het Europese gegevensbeschermingssysteem.

2. **PROBLEEMSTELLING –** De AVG is de nieuwe gegevensbeschermingsverordening van de Europese Unie die sinds haar inwerkingtreding op 25 mei 2018 het vorige regime uit Richtlijn 95/46/EG (hierna: Richtlijn Gegevensbescherming)[4] vervangt.[5] De bedoeling van de AVG is betere bescherming van persoonsgegevens te verwezenlijken en de regelgeving te vereenvoudigen met het oog op de digitale eengemaakte markt.[6] Eén van de doelstellingen van de AVG is dat natuurlijke personen de controle hebben over hun persoonsgegevens.[7] Een gevolg van die doelstelling is een uitgebreidere formulering van de rechten van de betrokkene ten

---

[1] 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), *Pb. L.* 27 april 2016, afl. 119, 1 (hierna: AVG).

[2] P. HUYGHEBAERT, "Groot Facebooklek: bedrijf van bannon maakte gegevens van 50 miljoen mensen buit", Brussel, 17 maart 2018, laatst geraadpleegd op 24 maart 2018, *https://www.vrt.be/vrtnws/nl/2018/03/17/facebook--schorst--bedrijf-cambridge-analytica-dat-voor-trump-ca/*; T. B. LEE, "Facebook's cambridge analytica scandal, explained", Californië, 20 maart 2018, laatst geraadpleegd op 22 maart 2018, *https://arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained/*; R. MEYER, "My facebook was breached by cambridge analytica. Was yours?", Washington D.C., 10 april 2018, laatst geraadpleegd op 30 april 2018, *https://www.theatlantic.com/technology/archive/2018/04/facebook-cambridge-analytica-victims/557648/.*

[3] *Ibid.*

[4] Richtlijn 95/46/EG van het europees parlement en de raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb. L.* 23 november 1995, afl. 281, p. 31.

[5] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law,* Luxemburg, Publications Office of the European Union, 2018, 30.

[6] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law,* Luxemburg, Publications Office of the European Union, 2018, 30; A. VAN DE MEULEBROUCKE, "De algemene verordening gegevensbescherming", *RW* 2015, 1562.

[7] Rechtsoverweging (7) AVG.

opzichte van de Richtlijn Gegevensbescherming. Er is echter nog onzekerheid over de effectieve afdwinging van die rechten, wat een utopie kan lijken in een tijd waarin *big data analytics* en het *Internet of Things* hun opmars maken.[8] De afdwinging van de rechten heeft controle over persoonsgegevens tot gevolg. Ook is het nog te bekijken of blockchaintechnologie in overeenstemming is met de bepalingen uit de AVG. Meer bepaald het recht op gegevenswissing en de aanwijzing van een verwerkingsverantwoordelijke kunnen problematisch zijn. ALBRECHT, rapporteur bij het Europees Parlement tijdens de wetgevingsprocedure voor de AVG[9], heeft een eerder pessimistische visie op de conformiteit van blockchaintechnologie met de AVG.[10] Deze masterscriptie zal een meer genuanceerd antwoord formuleren op de vraag of blockchain in overeenstemming kan zijn met de AVG.

3. **RELEVANTIE VAN HET ONDERZOEK -** De relevantie van het onderzoek ligt in de ontwikkelingen van digitalisering. Door de opkomst van fenomenen zoals Facebook, LinkedIn en Instagram ontstaan nieuwe mogelijkheden voor burgers. Zij kunnen immers een digitaal imago creëren en makkelijker met andere mensen contact leggen. Ondanks de nieuwe mogelijkheden komt digitalisering ook mogelijk met negatieve aspecten. De virtuele aard van de ontwikkeling bedreigt met name de controle over persoonsgegevens. Het is niet vanzelfsprekend voor een normale internetgebruiker om te weten wat er met zijn gegevens gebeurt. Dat staat in contrast met de bedoeling van de AVG om de controle over zijn persoonsgegevens bij de betrokkene te leggen.

4. **ONDERZOEKSVRAAG –** Het onderzoek is opgedeeld in vier subvragen:

    1) Wat zijn de centrale concepten voor dit onderzoek en wat is de context ervan binnen de Europese rechtsorde?
    2) Wat zijn de potentiële opportuniteiten en moeilijkheden van blockchaintechnologie voor de controle over persoonsgegevens door de betrokkene?
    3) Case study: vormt de SOVRIN blockchain een oplossing voor de probleemstelling van deze masterscriptie en zo ja, is de blockchain conform de AVG?

---

[8] O. LYNSKEY, *The foundations of EU data protection law*, New York, Oxford University Press, 2015, 1.

[9] EUR-LEX, "Document 32016R0679", Brussel, s.d., laatst geraadpleegd op 6 februari 2019, *https://eur-lex.europa.eu/legal-content/NL/HIS/?uri=celex:32016R0679*.

[10] D. MEYER, "Blockchain technology is on a collision course with EU privacy law, Porthsmouth, 27 februari 2018, laatst geraadpleegd op 11 november 2018, *https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/*; C. MILLARD, "Blockchain and law: incompatible codes?*"*, *Computer Law & Security Review* 2018, (843) 844.

4) Hoe verhouden de voor- en nadelen van blockchaintechnologie en controle over persoonsgegevens zich tot elkaar?

Die subvragen moeten leiden tot het beantwoorden van de centrale onderzoeksvraag, die als volgt luidt: “Is het gebruik van blockchaintechnologie opportuun voor controle door de betrokkene over zijn persoonsgegevens, in het licht van de Algemene Verordening Gegevensbescherming?”.

5. **ONDERZOEKSMETHODE -** Het beantwoorden van de onderzoeksvraag zal gestoeld zijn op drie pijlers: ten eerste zal het onderzoek een overwegend juridische visie van het probleem behandelen, maar waar nodig zullen ook technische elementen behandeld worden om een volledig beeld te geven van het blockchainfenomeen. Ten tweede zal, naast de overwegend theoretische benadering van het probleem, het vierde deel van het onderzoek ook een praktisch voorbeeld analyseren om theoretische bevindingen af te toetsen aan de realiteit. De derde pijler is het specifieke voorwerp van de verschillende subvragen: het onderzoek bestaat achtereenvolgens uit een descriptief, een evaluatief en een kort normatief deel dat een opsomming vormt van de observaties doorheen het onderzoek. Dat moet leiden tot een brede theoretische analyse van het onderzoeksprobleem.

   Het onderzoek blijft beperkt tot gegevensbeschermingswetgeving van de Europese Unie. Meer bepaald zal het de AVG onder de loep nemen. Blockchain is ook een globaal gegeven, dus is het eerder opportuun de context van de Europese Unie te bespreken en niet de louter Belgische context. De bespreking van die context is fundamenteel, aangezien het onderzoek blockchaintechnologie daartegen aftoetst. Als tweede afbakening zal het onderzoek zich beperken tot het specifieke onderwerp van controle over persoonsgegevens. Gelet op de beperkte omvang van het onderzoek is het noodzakelijk om het denkkader van het onderzoek nauw te houden. Als derde en laatste afbakening is het belangrijk om (het geheel van) persoonsgegevens te onderscheiden van digitale identiteit. Dit onderzoek zal handelen over de controle door de betrokkene over zijn persoonsgegevens, niet over diefstal van digitale identiteit. Daarom zal dit onderzoek de term “geheel van persoonsgegevens” gebruiken om verwarring te vermijden, tenzij in het Hoofdstuk over SOVRIN waarin het wel degelijk gaat om digitale identiteiten.

   Twee methoden van bronnenanalyse komen hier aan te pas: de sneeuwbalmethode en selectieve analyse. De sneeuwbalmethode laat toe om de belangrijkste bronnen te vinden. Selectieve analyse van de bronnen maakt het mogelijk om veel bronnen op korte tijd te bekijken.

HOOFDSTUK I. BEGRIPSBESCHRIJVING EN JURIDISCH KADER

AFDELING I. BEGRIPSBESCHRIJVING

6. **DOELSTELLING VAN DE AFDELING -** Blockchain, verwerking van persoonsgegevens en controle over persoonsgegevens door de betrokkene in de AVG zijn, zoals gesteld in de Inleiding, de centrale concepten in deze masterproef. Daarom zal deze Afdeling zich wijden aan het verduidelijken van de belangrijkste begrippen.

7. **DEFINITIE VAN BLOCKCHAIN –** De bedoeling van blockchaintechnologie is decentralisatie van gegevens. Dat gebeurt door een netwerk van *nodes* (afzonderlijke deelnemers van het computernetwerk) dat handelt in de plaats van een centrale tussenpersoon, wat voor de decentralisatie moet zorgen. Er zijn twee soorten *nodes*: *validating nodes* mogen gegevens aan de blockchain toevoegen volgens de vooraf vastgelegde regels, het zgn. *consensus mechanism*. *Participating nodes* slaan kopieën van de blockchaingegevens op en zijn de entiteiten waarmee particulieren in verband staan om toegang te krijgen tot de blockchaingegevens. Daarnaast kan de particulier, via de *participating nodes* die de gegevens ter goedkeuring aan de *validating nodes* voorleggen, gegevens aan de blockchain toe te voegen. Elke *block* van de blockchain bevat een reeks transacties, alsook een verwijzing (*hash*) naar alle voorgaande *blocks*. Doordat elke nieuwe *block* verwijst naar de voorgaande, ontstaat een keten of *chain*. Daar komt de benaming 'blockchain' vandaan. De verwijzing naar voorgaande *blocks* moet de integriteit van blockchain garanderen wanneer een nieuwe *block* (en dus nieuwe transacties) aan blockchain worden toegevoegd. De *nodes* moet immers consensus bereiken over de validiteit van de nieuwe *block* in de *chain*. De vergelijking kan gemaakt worden met een grootboek (*ledger*). In een grootboek staan alle transacties opgelijst die sinds het begin van het grootboek zijn gesteld, net zoals bij blockchain. Daar heet het begin van het grootboek de *genesis block*. Iedereen kan nagaan of toegevoegde transacties niet raken aan de integriteit van het grootboek. Bijzonder aan blockchaintechnologie is dat de gegevens van transacties geëncrypteerd zijn. Dat heeft tot gevolg

dat het niet onmiddellijk zichtbaar is welke gegevens in een bepaalde transactie vervat liggen. De encryptie[11] in het blockchainsysteem leidt dus tot pseudonimisatie van persoonsgegevens.[12]

In een *permissionless* blockchain kan iedere internetgebruiker als *validating node* handelen en participeren aan de infrastructuur van die blockchain, zonder dat daarvoor toestemming moet gegeven worden. Dat staat in tegenstelling tot *permissioned* blockchains, waar enkel een aantal, vooraf door het protocol van regels van de blockchain, geselecteerde *validating nodes* kunnen participeren aan de infrastructuur van de blockchain. Enkel die *nodes* zullen dan transacties goedkeuren en nieuwe *blocks* aan die blockchain toevoegen. Een vergelijkbaar onderscheid zien we ook terug bij *public* en *private* blockchains. *Public* blockchains zijn toegankelijk (*i.e.* leesbaar en bruikbaar) voor iedereen, waar *private* blockchains enkel toegankelijk zijn voor een bepaalde groep *participating nodes*.[13]

DEFINITIE VAN VERWERKING VAN PERSOONSGEGEVENS - Het begrip verwerking van persoonsgegevens valt uiteen in twee componenten: persoonsgegevens en de verwerking daarvan. Art. 4, 1) AVG definieert persoonsgegevens als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon («betrokkene»)". Verder geeft het artikel een opsomming van wat als 'identificeerbaar' kan worden beschouwd. Identificeerbaarheid van de betrokkene is de bepalende factor om informatie als persoonsgegeven te bestempelen.[14] De persoonsgegevens van de betrokkene vormen het voorwerp van deze masterscriptie. Ze bevinden zich normaal gezien

[11] Encryptie is een methode om via een wiskundig algoritme en een digitale sleutel gegevens te versleutelen, DUTCH LAW ENCYCLOPEDIC DICTIONARY, "Encryptie", X, 2018, laatst geraadpleegd op 9 april 2019, *https://www.juridischwoordenboek.nl/zoek/encryptie*.

[12] Randnummer gebaseerd op: D. DRESCHER, *Blockchain basics: a non-technical introduction in 25 Steps*, Frankfurt am Main, Apress, 2017, 4-7; EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, Brussel, EU Blockchain Observatory and Forum, 2018, 14-15; M. FINCK, "Blockchains: regulating the unknown", *German Law Journal* 2018, (665) 666-667 L. D. IBÁÑEZ, K. O'HARA, en E. SIMPERL, *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*; M. NOFER, P. GOMBER, O. HINZ en D. SCHIERECK, "Blockchain", *Business & Information Systems Engineering* 2017, (183) 183-184; D. ZETZSCHE, R. BUCKLEY en D. ARNER, "The distributed liability of distributed ledgers: legal risks of blockchain", *University of Illinois Law Review* 2018, (1361) 1371-1372; E. W. VERHELST, "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, 17; X. XU, I. WEBER en M. STAPLES, *Architecture for blockchain applications*, Cham, Springer, 2019, 5-6.

[13] *Ibid.*

[14] O. SUSTRONCK, *Praktijkboek internetrecht*, Mechelen, Wolters Kluwer, 2017, 141.

op een blockchain als een *hash*.[15] Wanneer een *hash* persoonsgegevens bevat of ernaar verwijst, valt het onder de ruime definitie van 'persoonsgegeven' uit art. 4, 1) AVG.[16]

De definitie van verwerking vinden we terug in art. 4, (2) AVG: "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of van een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens". Als we naar de definitie van verwerking van persoonsgegevens kijken, is het duidelijk dat dit een hele ruime toepassing vindt. Een blockchain zal persoonsgegevens als *hash* opslaan, en dus doen aan de verwerking van persoonsgegevens. Daarmee voldoet het aan het materiële toepassingsgebied uit art. 2 AVG.

8. **DEFINITIE VAN CONTROLE OVER PERSOONSGEGEVENS -** Eén van de doelstellingen van de AVG is dat natuurlijke personen de controle hebben over hun persoonsgegevens.[17] VAN DALE ONLINE definieert controle hebben als: "in bedwang hebben, beheersen"[18]. Het draait om het beheersen van de betrokkene over diens eigen persoonsgegevens. Een gevolg van de doelstelling is een uitgebreidere formulering van de rechten van de betrokkene ten opzichte van de Richtlijn

---

[15] J. BACON, J. D. MICHELS, C. MILLARD en J. SINGH, *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 6; G. JENSEN, "Reconciling GDPR rights to erasure and rectification of personal data to blockchain", Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018, *https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain*; D. IBÁÑEZ, K. O'HARA, en E. SIMPERL, *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*; V.I. LAAN en A. RUTJES, "Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?", *Computerrecht* 2017, (253) 256; W. MAXWELL en J. SALMON, *A guide to blockchain*, Brussel, Hogan Lovells LLP, 2017, 9; C. WIRTH en M. KOLAIN, *Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data,* Amsterdam, European Society for Socially Embedded Technologies, 2018, 5.

[16] J. BACON e.a. , *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 41; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 26; G. JENSEN, "Reconciling GDPR rights to erasure and rectification of personal data to blockchain", Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018, *https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain*; D. IBÁÑEZ, K. O'HARA, en E. SIMPERL, *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*; W. MAXWELL en J. SALMON, *A guide to blockchain*, Brussel, Hogan Lovells LLP, 2017, 7; Y. POULLET en H. JACQUEMIN, "Blockchain: une révolution pour le droit?" *JT* 2018, (801) 808-809; WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Opinion 05/2014 on anonymisation techniques,* 10 april 2014, 0829/14/EN WP 216, 20.

[17] Rechtsoverweging (7) AVG; C. WIRTH en M. KOLAIN, *Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data,* Amsterdam, European Society for Socially Embedded Technologies, 2018, 5.

[18] VAN DALE UITGEVERS, "Controle", Utrecht, 2018, laatst geraadpleegd op 1 november 2018, *https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/controle#.W9sXI5NKhPY*.

Gegevensbescherming.[19] Artikelen 12 tot 22 AVG omvatten die rechten. De uitoefening ervan vormt dus een inherent deel van de controlemogelijkheden van de betrokkene. Daarom zullen de rechten van de betrokkene een belangrijk houvast vormen voor dit onderzoek, en zal blockchaintechnologie daaraan afgetoetst worden. Naast de versterking van die rechten halen de Belgische en Nederlandse gegevensbeschermingsautoriteiten aan dat organisaties die persoonsgegevens verwerken een informatieplicht hebben, wat de controle door de betrokkene over diens persoonsgegevens moet vergroten.[20]

9. **INTERACTIE TUSSEN DE BELANGRIJKSTE BEGRIPPEN -** Persoonsgegevens en het verwerken ervan ligt aan de grondslag van controle over persoonsgegevens. Ondernemingen verwerken die persoonsgegevens en dat dreigt de controle door de betrokkene in het gedrang te brengen. Afdeling I van het volgende Hoofdstuk toont het gevaar aan van de grote macht van internetgiganten zoals Facebook en Google voor die controle.

AFDELING II. JURIDISCH KADER BINNEN DE EUROPESE UNIE

10. **RECHT OP GEGEVENSBESCHERMING ALS GRONDRECHT -** Het recht op gegevensbescherming ligt vervat in het Handvest van de grondrechten van de Europese Unie (hierna: Handvest)[21], alsook (zij het impliciet) in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM)[22]. Artikel 8.2 Handvest zegt expliciet dat eenieder het recht heeft om toegang te verkrijgen tot de gegevens die over hem of haar worden verzameld. Dat recht heeft dus de status van grondrecht binnen de Europese Unie.[23] Ook Verdrag nr. 108 van de Raad van Europa (hierna: Verdrag nr. 108)[24] waarborgt dat recht. In de zaken Gaskin t. Verenigd Koninkrijk[25], Odièvre t.

---

[19] GEGEVENSBESCHERMINGSAUTORITEIT, "Behoud de controle over jouw gegevens!", Brussel, 2018, laatst geraadpleegd op 21 november 2018, *https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-burger*; C.C.M. KROEKS-DE RAAIJ, R.J.J. WESTERDIJK en G.J. ZWENNE, "De algemene verordening gegevensbescherming", *Tijdschrift voor Internetrecht* 2016, 56.

[20] AUTORITEIT PERSOONSGEGEVENS, "Controle over je data", Den Haag, 2018, laatst geraadpleegd op 1 november 2018, *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/controle-over-je-data*; GEGEVENSBESCHERMINGSAUTORITEIT, "Behoud de controle over jouw gegevens!", Brussel, 2018, laatst geraadpleegd op 21 november 2018, *https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-burger*.

[21] Art. 8 Handvest van de grondrechten van de europese unie, *Pb. L.* 26 oktober 2012, afl. 326, 391.

[22] Art. 8 EVRM.

[23] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law,* Luxemburg, Publications Office of the European Union, 2018, 28.

[24] Art. 8 Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981, *BS* 30 december 1993, 29.024.

[25] EHRM 7 juli 1989, nr. 10454/83, ECLI:CE:ECHR:1989:0707JUD001045483, Gaskin/Verenigd Koninkrijk.

Frankrijk[26], K.H. e.a. t. Slovakije[27] en Godelli t. Italië[28] stelt het Europees Hof voor de Rechten van de Mens (hierna: EHRM) dat het recht op toegang haar oorsprong vindt in het recht op eerbiediging voor het privéleven.[29]

11. **DE ROL VAN DE AVG -** Ook primair Europees Unierecht (hierna: EU-recht) legt het recht op bescherming van persoonsgegevens vast. Art. 16 (1) Verdrag betreffende de werking van de Europese Unie (hierna: VWEU) beschermt dat recht, en vormt de juridische grondslag voor de AVG.[30] De AVG is heel belangrijk voor dit onderzoek, aangezien daarin de doelstelling van controle over persoonsgegevens vervat ligt in Rechtsoverweging 7.

Volgens ALBRECHT, rapporteur voor het Europees Parlement bij de aanneming van de AVG[31], zal de AVG niet alleen Europese gegevensbeschermingswetgeving zal veranderen, "maar niets minder dan de wereld zoals we hem kennen".[32] Die stelling toont het belang aan van de invoering van de nieuwe Verordening. Het vervangt de Richtlijn Gegevensbescherming die als grondslag Verdrag nr. 108 heeft.[33] De Richtlijn Gegevensbescherming vormt de Europese basis voor de Belgische Wet Verwerking Persoonsgegevens (hierna: WVP)[34].[35] Daarnaast is op 30 juli 2018 de Belgische kaderwet van 30 juli 2018 (hierna: Kaderwet)[36] uitgevaardigd, die een aantal zaken

---

[26] EHRM 13 februari 2003, nr. 42326/98, ECLI:CE:ECHR:2003:0213JUD004232698, Odièvre/Frankrijk.
[27] EHRM 28 april 2009, nr. 32881/04, ECLI:CE:ECHR:2009:0428JUD003288104, K.H. e.a./Slovakije.
[28] EHRM 25 september 2012, nr. 3783/09, ECLI:CE:ECHR:2012:0925JUD003378309, Godelli/Italië.
[29] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 217.
[30] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 29; A. SAVIN, *EU internet law*, Cheltenham, Edward Elgar Publishing, 2017, 283.
[31] EUR-LEX, "Document 32016R0679", Brussel, s.d., laatst geraadpleegd op 6 februari 2019, *https://eur-lex.europa.eu/legal-content/NL/HIS/?uri=celex:32016R0679*.
[32] J. P. ALBRECHT, "How the GDPR will change the world", *European data protection law review* 2016, 287.
[33] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, "Duiding bij de privacywet", Brussel, 2018, laatst geraadpleegd op 27 maart 2018, *https://www.privacycommission.be/nl/duiding-bij-de-privacywet*; A. SAVIN, *EU internet law*, Cheltenham, Edward Elgar Publishing, 2017, 282.
[34] Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993 (hierna: WVP).
[35] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, "Duiding bij de privacywet", Brussel, 2018, laatst geraadpleegd op 27 maart 2018, *https://www.privacycommission.be/nl/duiding-bij-de-privacywet*.
[36] Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018, 68616 (hierna: Kaderwet).

regelt bij de tenuitvoerlegging van de bepalingen uit de AVG.[37] De WVP is opgeheven door de Kaderwet.[38]

De WVP bood aan de Belgische burgers al een aantal rechten op de controle over hun persoonsgegevens. De AVG gaat daarin nog verder en accentueert transparantie en controle.[39] Het gaat ook verder dan de loutere toegang tot en verbetering van persoonsgegevens door de betrokkene. Naast verscherping van de controle over persoonsgegevens brengt het een aantal vernieuwingen met zich mee. Voorbeelden daarvan zijn het recht op overdraagbaarheid van gegevens[40] en gegevensbescherming door ontwerp en door standaardinstellingen[41].[42] De AVG is van toepassing binnen de Europese Unie sinds 25 mei 2018[43], en heeft tot doel de bescherming van persoonsgegevens te verbeteren en tevens de regelgeving, in het licht van de digitale eengemaakte markt, te vereenvoudigen.[44] De waarschijnlijke impact van de AVG ligt in het handhavingsmechanisme dat grote sancties voorziet, waardoor de toepassing van de regels strikter moet zijn dan bij de Richtlijn Gegevensbescherming.[45]

12. **WETGEVINGSINITIATIEVEN ROND BLOCKCHAINTECHNOLOGIE -** Op dit moment ligt de focus van de Europese Unie in blockchainmaterie bij de regulering van cryptovaluta. Blockchain is de daaraan onderliggende technologie. Toch zijn er ook initiatieven over andere materies dan cryptovaluta op Europees vlak. De Europese Commissie heeft, met het oog op een eengemaakt beleid over blockchaintechnologie, het *EU Blockchain Observatory and Forum* in het leven

---

[37] GEGEVENSBESCHERMINGSAUTORITEIT, "Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Kaderwet)", Brussel, 2018, laatst geraadpleegd op 1 november 2018, *https://www.gegevensbeschermingsautoriteit.be/wet-betreffende-de-bescherming-van-natuurlijke-personen-met-betrekking-tot-de-verwerking-van#overlay-context=wet-van-3-december-2017-tot-oprichting-van-de-gegevensbeschermingsautoriteit.*

[38] Art. 280 Kaderwet.

[39] AUTORITEIT PERSOONSGEGEVENS, "Behoud de controle over jouw gegevens!", Brussel, 2018, laatst geraadpleegd op 21 november 2018, *https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-burger*; A. VAN MEULEBROUCKE, "De algemene verordening gegevensbescherming", *RW* 2015, 1562.

[40] Art. 20 AVG.

[41] Art. 25 AVG.

[42] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 30; A. SAVIN, *EU internet Law*, Cheltenham, Edward Elgar Publishing, 2017, 283; O. SUSTRONCK, *Praktijkboek internetrecht*, Mechelen, Wolters Kluwer, 2017, 141.

[43] Art. 99, 2. AVG.

[44] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 30; A. VAN DE MEULEBROUCKE, "De algemene verordening gegevensbescherming", *RW* 2015, 1562.

[45] O. SUSTRONCK, *Praktijkboek internetrecht*, Mechelen, Wolters Kluwer, 2017, 140.

geroepen.[46] Later in dit onderzoek zal die entiteit verder aan bod komen. De *Ethics Advisory Group* van de *European Data Protection Supervisor* (hierna: EDPS) geeft in haar jaarrapport van 25 januari 2018[47] haar mening over blockchain. Dat jaarrapport dient als louter advies[48]. Het rapport stelt dat blockchain vertrouwensproblemen bij gegevensbescherming kan verminderen, maar dat de technologie zelf ook andere problemen doet ontstaan.[49] In haar jaarrapporten van 2016 en 2017 heeft de EDPS ook gesproken over blockchain, zij het zeer summier. In het jaarrapport van 2016 haalt het voornamelijk aan dat blockchain de onderliggende technologie van de cryptovaluta *Bitcoin* is.[50] Ook geeft de EDPS aan dat er nog veel onduidelijkheid bestaat over de verenigbaarheid van blockchaintechnologie met de Europese gegevensbeschermingsregels.[51] Het wil onderzoek doen naar een privacy-vriendelijke blockchain, gebaseerd op het principe van gegevensbescherming door ontwerp.[52] Dat principe vinden we terug in artikel 25 AVG. In het jaarrapport van 2017 zegt de EDPS dat het onderzoek doet naar het potentieel van blockchain en hoopt daarover te kunnen rapporteren in 2018.[53] Ten slotte wijst de Europese Commissie erop dat een duidelijk en stabiel regelgevend kader moet worden uitgewerkt voor blockchaintechnologie.[54] Het zou moeten gaan om nieuwe regelgeving die de technische aspecten van blockchain in rekening neemt.[55] Verder informeert de Commissie over de mogelijke toekomstige rol van de technologie in veel verschillende soorten domeinen.[56]

AFDELING III. TUSSENBESLUIT

13. In het eerste deel van dit Hoofdstuk zijn de begrippen blockchain, verwerking van persoonsgegevens en controle over persoonsgegevens verduidelijkt.

---

[46] EUROPESE COMMISSIE, "Blockchain technologies", Brussel, 2018, laatst geraadpleegd op 11 maart 2019, *https://ec.europa.eu/digital-single-market/en/blockchain-technologies*.
[47] EDPS ETHICS ADVISORY GROUP, *Report 2018*, Brussel, Edit Directorate, 2018, 1.
[48] *Ibid.*, 5.
[49] *Ibid.*, 21.
[50] EUROPEAN DATA PROTECTION SUPERVISOR, *Annual report 2016*, Luxemburg, Publications Office of the European Union, 2017, 43.
[51] *Ibid*.
[52] *Ibid*.
[53] *Ibid.*, 11.
[54] BUSINESS INNOVATION OBSERVATORY, *Trend report - optimal recycling, big data from space, and blockchain applications: disruption and policy response*, Brussel, Europese Commissie, 2016, 15.
[55] *Ibid.*.
[56] *Ibid.*, 15-16.

Het is duidelijk dat die begrippen ook interageren en die interactie vormt precies de basis van dit onderzoek. In het tweede deel is aangetoond dat het recht op gegevensbescherming als grondrecht is beschermd in Europa en de Europese Unie. Daarna is de rol van de AVG en de historiek van controle over persoonsgegevens uiteengezet. Ten slotte is stilgestaan bij wetgevingsinitiatieven over blockchaintechnologie. Daarmee is voldaan aan de bedoeling om een beschrijving te geven van de belangrijkste begrippen en het juridisch kader voor deze scriptie.

HOOFDSTUK II. OPPORTUNITEITEN EN MOEILIJKHEDEN VAN BLOCKCHAINTECHNOLOGIE VOOR CONTROLE OVER PERSOONSGEGEVENS DOOR DE BETROKKENE

14. **OPZET VAN DIT HOOFDSTUK –** Dit hoofdstuk handelt over de opportuniteiten en moeilijkheden van blockchaintechnologie voor de controle over persoonsgegevens door de betrokkene. Ten eerste komt de reden van zo'n blockchainoplossing in de huidige stand van zaken aan bod. Vervolgens komt een onderzoek naar de technische mogelijkheid van een blockchainoplossing, die de controle door de betrokkene kan faciliteren en de potentiële opportuniteiten voor de rechten van de betrokkene moet reflecteren. Ten slotte zijn een aantal potentiële moeilijkheden denkbaar die zo'n oplossing heeft in relatie tot de bepalingen uit de AVG. Dat zijn de doorgifte van persoonsgegevens naar derde-landen, het recht op gegevenswissing, de aanwijzing van de verwerkingsverantwoordelijke en daaraan gekoppeld de verscheidene verplichtingen van de verantwoordelijke ten aanzien van de betrokkene, de verwerking van bijzondere categorieën van persoonsgegevens en de verplichte verwerkingsovereenkomst tussen de verwerkingsverantwoordelijke en de verwerker. Dit onderzoek zal zich beperken tot de bespreking van twee belangrijke problemen, die het *EU Blockchain Observatory and Forum* ook heeft geïdentificeerd: het recht op gegevenswissing en de aanwijzing van de verantwoordelijke voor de verwerking.[57] Het onderzoek zal proberen aan te tonen dat, hoewel daarover veel negativiteit bestaat, blockchaintechnologie via technische of juridische middelen toch kan voldoen aan de regels van de AVG.

[57] EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, Brussel, EU Blockchain Observatory and Forum, 2018, 5.

AFDELING I. DE "RAISON D'ÊTRE" VAN EEN BLOCKCHAINOPLOSSING

15. **GEBREK AAN CONTROLE VAN DE BETROKKENE** – Een probleem bij conventionele gegevensbeschermingsmechanismen is het gebrek aan controle. Het vloeit voort uit het feit dat een centrale entiteit de persoonsgegevens in bezit heeft en er dan ook technisch over kan beschikken.[58] LYNSKEY benoemt de macht van die centrale entiteiten met de term 'Platform Power'.[59] Grote platformen zoals Facebook, Google en Amazon hebben een grote invloed op de manier waarop wij online handelen, zoektermen opzoeken, online aankopen doen… waardoor zij heel veel gegevens van ons verkrijgen die ze verzamelen en verwerken.[60] Met die gegevens kunnen zij hun machtspositie verder uitbouwen, waardoor zij meer en meer controle krijgen over de persoonsgegevens van de gebruikers van die platformen.[61]

De machtspositie van centrale entiteiten ligt niet in lijn met de doelstelling van de AVG om de controle door de betrokkene zelf te bewerkstelligen, aangezien zij net de controle over de persoonsgegevens overnemen zoals hierboven uiteengezet. Volgend randnummer zal aantonen hoe blockchaintechnologie aan het hier beschreven probleem kan remediëren en eventueel andere verbeteringen kan aanbrengen aan de conventionele beschermingsmechanismen.

---

[58] BLOCKCHAINHUB, "Identity as a bottleneck for blockchain, Berlijn, 17 oktober 2017, laatst geraadpleegd op 2 november 2018, *https://blockchainhub.net/blog/blog/decentralized-identity-blockchain/*; M. A. CALLAHAN, "How blockchain can be used to secure sensitive data storage", State City, 7 november 2017, laatst geraadpleegd op 30 oktober 2018, *http://www.dataversity.net/blockchain-can-used-secure-sensitive-data-storage/*; ; D. DE JONGHE en V. I. LAAN, "Blockchain in de realiteit", *Computerrecht* 2017, (251) 254; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 20; D. SCHRIER, W. WU en A. PENTLAND, *Blockchain & infrastructure (identity, data security*), Massachusetts, Massachusetts Institute of Technology, 2016, 10; D. ZETZSCHE, R. BUCKLEY en D. ARNER, "The distributed liability of distributed ledgers: legal risks of blockchain", *University of Illinois Law Review* 2018, (1361) 1370; G. ZYSKIND, O. NATHAN en A. PENTLAND, "Decentralising privacy: using blockchain to protect personal data", *Security and Privacy Workshops* 2015, 180.

[59] O. LYNSKEY, *Regulating 'platform power'*, Londen, LSE Legal Studies Working Paper, 2017, 3.

[60] P. DE FILIPPI, *The interplay between decentralisation and privacy: the case of blockchain technologies,* Parijs, Université Paris II, 2016, 3; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 20; D. SCHRIER, W. WU en A. PENTLAND, *Blockchain & infrastructure (identity, data security*), Massachusetts, Massachusetts Institute of Technology, 2016, 10; E. W. VERHELST, "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, (17) 19; G. ZYSKIND, O. NATHAN en A. PENTLAND, "Decentralising privacy: using blockchain to protect personal data", *Security and Privacy Workshops* 2015, 180.

[61] P. DE FILIPPI, *The interplay between decentralisation and privacy: the case of blockchain technologies,* Parijs, Université Paris II, 2016, 3; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 20.

16. **DE ROL VAN BLOCKCHAINTECHNOLOGIE VOOR CONTROLE -** Decentralisatie is een van de eigenschappen van blockchain. Als één computer of *node* uit het netwerk wegvalt, zouden de andere *nodes* ervoor moeten zorgen dat de blockchain verder functioneert.[62] Hoe groter het netwerk van *nodes*, hoe meer gedecentraliseerd de specifieke blockchain is. Dat in tegenstelling tot een gecentraliseerd systeem, waarbij het systeem faalt als de centrale speler wegvalt. De decentralisatie van de blockchainstructuur heeft tot gevolg dat de *nodes* ook de gegevens gedecentraliseerd verzamelen, opslaan en verwerken.[63]

Een tweede eigenschap van blockchain is vertrouwen door consensus. Een netwerk van *nodes* moet via onderlinge consensus beslissen over de toevoeging van een nieuwe *block*.[64] Die eigenschap en de daarmee gepaard gaande keuze voor de betrokkene om gegevens toe te vertrouwen aan de (verschillende *nodes* in de) blockchain of niet, draagt bij aan de controle door betrokkenen over hun persoonsgegevens.[65] De keuze vloeit voort uit het feit dat het geen centrale entiteit is die autonoom kan bepalen om de gegevens te verwerken, maar de *nodes* die enkel transacties in een *block* toevoegen als de betrokkene zijn persoonsgegevens daaraan toevertrouwt. Het is dus de betrokkene die bepaalt wat er gebeurt met zijn persoonsgegevens. Op die manier zou de nieuwe technologie de doelstelling van de AVG van controle uit Rechtsoverweging (7) kunnen helpen verwezenlijken.[66]

---

[62] J. BACON e.a., *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 12-13; G. ZYSKIND, O. NATHAN en A. PENTLAND, "Decentralising privacy: using blockchain to protect personal data", *Security and Privacy Workshops* 2015, 180.

[63] P. DE FILIPPI, *The interplay between decentralisation and privacy: the case of blockchain technologies*, Parijs, Université Paris II, 2016, 4-5; D. DE JONGHE en V. I. LAAN, "Blockchain in de realiteit", *Computerrecht* 2017, 251; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 20.

[64] J. BACON e.a., *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 12; M. BERBERICH en M. STEINER, "Blockchain technology and the GDPR – how to reconcile privacy and distributed Ledgers", *European Union Data Protection Law Review* 2016, 422; D. DRESCHER, *Blockchain basics: a non-technical introduction in 25 Steps*, Frankfurt am Main, Apress, 2017, 4-7; P. HRISTOV en W. DIMITROV, "The blockchain as a backbone of GDPR compliant frameworks", *Quality-access to success* 2019, (305) 307; M. NOFER, P. GOMBER, O. HINZ en D. SCHIERECK, "Blockchain", *Business & Information Systems Engineering* 2017, (183) 183-184; E. W. VERHELST, "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, (17) 18; D. ZETZSCHE, R. BUCKLEY en D. ARNER, "The distributed liability of distributed ledgers: legal risks of blockchain", *University of Illinois Law Review* 2018, (1361) 1371.

[65] D. DE JONGHE en V. I. LAAN, "Blockchain in de realiteit", *Computerrecht* 2017, (251) 252; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 20.

[66] *Ibid.*

Een derde belangrijke eigenschap van de technologie is de onveranderbaarheid van gegevens op de blockchain. Het is de bedoeling om de verandering van de gegevens in de *blocks* duidelijk zichtbaar te maken via de *hash.* Door de duidelijke zichtbaarheid kunnen de *nodes* beslissen om onrechtmatige veranderingen af te wijzen en zo misbruik te voorkomen, wat ook dient om het vertrouwen in de technologie te verzekeren. De gegevens op de blockchain zijn leesbaar voor iedereen (bij *public* blockchains) of voor de bestemmelingen (bij *private* blockchains), maar eens een nieuwe *block* door de *nodes* aan de blockchain is toegevoegd liggen de gegevens die in de *block* vervat liggen vast en zijn ze in principe niet wijzigbaar of verwijderbaar. De combinatie van decentralisatie en de ketens van de blockchain die aan elkaar verbonden zijn door middel van *hashes* zouden dus voor de onveranderbaarheid van gegevens moeten zorgen.[67]

Die eigenschappen verdienen echter ook enige vorm van nuance. Drie problemen duiken mogelijk op: het blockchainsysteem is niet zo gedecentraliseerd als het vooropstelt, de eigenschap van vertrouwen door consensus speelt niet en gegevens kunnen veranderd worden. Drie problemen duiken met name op in een bepaald type blockchain, de *proof of work* blockchains. Deze blockchainvorm vereist rekenkracht om transacties uit te voeren, en de aanbieders van die rekenkracht heten *miners*.[68] Doordat *miners* transacties uitvoeren, controleren zij het systeem.[69] Die controlemogelijkheid kan de eigenschap van decentralisatie aantasten wanneer een te klein aantal *miners* de controle krijgt over het netwerk.[70] Onderlinge afspraken tussen de *miners* kan de eigenschap van vertrouwen door consensus aantasten en ook de onveranderbaarheid van gegevens kan aangetast worden wanneer *miners* over voldoende rekenkracht beschikken om voorgaande

---

[67] Alinea gebaseerd op: H. CHANG, *Blockchain: disrupting data protection?*, Hong Kong, University of Hong Kong Faculty of Law Research, 2017, 2; V. DALMACIO POSADAS, "The internet of things: the GDPR and the blockchain may be incompatible", *Journal of Internet Law* 2017-18, afl. 11 (21) 25; D. DRESCHER, *Blockchain basics: a non-technical introduction in 25 Steps*, Frankfurt am Main, Apress, 2017, 135-143; M. FINCK, "Blockchains: regulating the unknown", *German Law Journal* 2018, (665) 666; C. MILLARD, "Blockchain and law: incompatible codes?*", Computer Law & Security Review* 2018, (843) 844; E. PISCINI, D. DALTON en L. KEHOE, *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 7; X. XU, I. WEBER en M. STAPLES, *Architecture for blockchain applications*, Cham, Springer, 2019, 97-98.

[68] E. WITJES, "Wat is het verschil tussen 'proof of work' en 'proof of stake'", X, 7 juli 2017, laatst geraadpleegd op 9 april 2019, *https://cryptomaan.nl/blogs/news/wat-is-het-verschil-tussen-proof-of-work-en-proof-of-stake*.

[69] *Ibid*.

[70] D. DRESCHER, *Blockchain basics: a non-technical introduction in 25 Steps*, Frankfurt am Main, Apress, 2017, 255 p.; LEARNCRYPTOGRAPHY.COM, "51% attack", X., 2019, laatst geraadpleegd op 7 februari 2019, *https://learncryptography.com/cryptocurrency/51-attack*; E. PISCINI, D. DALTON en L. KEHOE, *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 7; D. ZETZSCHE, R. BUCKLEY en D. ARNER, "The distributed liability of distributed ledgers: legal risks of blockchain", *University of Illinois Law Review* 2018, (1361) 1378.

transacties te wijzigen.[71] Het zal afhankelijk zijn van de keuzes van een specifieke blockchainoplossing om uit te maken in hoeverre die voldoet aan de hier beschreven eigenschappen.

AFDELING II. TECHNISCHE ANALYSE VAN EEN BLOCKCHAINMODEL

17. **AFWIJKING VAN DE GANGBARE TECHNISCHE TOEPASSING -** De doelstelling van het gebruik van blockchaintechnologie in deze context is het faciliteren van controle over persoonsgegevens. Dat wijkt af van de vandaag meest gangbare toepassing van blockchain, namelijk virtuele munten of *cryptocurrencies*. Bij het opzoeken naar toepassingen van blockchain komen *cryptocurrencies*, en meer specifiek de meest bekende *cryptocurrency* Bitcoin, zeer sterk naar voren. Waar virtuele munten een louter financieel oogmerk hebben, is voor de doelstelling van controle over persoonsgegevens meer nodig.[72] De gegevens moeten kunnen "opgeslagen, opgevraagd en gedeeld worden"[73]. De technische toepassing van blockchain voor controle over persoonsgegevens zou die bijkomende mogelijkheden dus moeten verwerken.

18. **TECHNISCHE BESCHRIJVING VAN EEN RELEVANTE BLOCKCHAIN -** In hun paper[74] getiteld 'Decentralising Privacy: Using Blockchain to Protect Personal Data' beschrijven ZYSKIND, NATHAN en PENTLAND een blockchainoplossing die rekening houdt met de vereisten van opslag, opvraging en deelbaarheid. Gelet op de beperkte omvang zal deze masterscriptie enkel een korte beschrijving van de belangrijkste kenmerken van hun blockchainoplossing geven. Ze laten zich leiden door drie belangrijke principes in hun paper: eigendom van de gegevens behoort toe aan de betrokkene, volledige transparantie over welke gegevens verwerkt worden en wie toegang heeft tot die gegevens en ten slotte de noodzaak van een mechanisme dat de toestemming om toegang te krijgen tot persoonsgegevens regelt en in de tijd kan beperken.

ZYSKIND, NATHAN en PENTLAND vertrekken van een simpele driepartijenrelatie tussen de gebruikers van een smartphone applicatie, de aanbieders van zo'n applicatie en de *nodes* in het netwerk van de blockchain. De blockchain kan twee types transacties verwerken, namelijk

---

[71] *Ibid.*
[72] G. ZYSKIND, O. NATHAN en A. PENTLAND, "Decentralising privacy: using blockchain to protect personal data", *Security and Privacy Workshops* 2015, 180.
[73] *Ibid.*
[74] Randnummer gebaseerd op: G. ZYSKIND, O. NATHAN en A. PENTLAND, "Decentralising privacy: using blockchain to protect personal data", *Security and Privacy Workshops* 2015, 180-184.

transacties die de toegang tot de gegevens moeten regelen (Taccess) en transacties die opslag en het terugtrekken van de gegevens uit de blockchain moeten regelen (Tdata). Een applicatie voor smartphones kan die functionaliteiten dan integreren. De auteurs geven een voorbeeld van hoe het kan werken: "een gebruiker installeert een applicatie dat een platform gebruikt om privacy te beschermen. Wanneer de gebruiker zich de eerste keer aanmeldt, maakt die een nieuwe gedeelde (gebruiker, dienst) identiteit die, samen met de daartoe verbonden toestemmingen, aan de blockchain wordt toegevoegd in een Tacces transactie. Gegevens die op de smartphone verzameld zijn (zoals locatiegegevens) worden geëncrypteerd door middel van een gedeelde encryptiesleutel en naar de blockchain gestuurd in een Tdata transactie, die vervolgens de gegevens naar een *off-chain*[75] sleutelwaarde-opslag stuurt, waarbij enkel een aanwijzing (SHA-256 *hash* van de gegevens) van die gegevens aan de *public ledger* wordt toegevoegd. Zowel de dienst als de gebruiker kunnen nu de gegevens opzoeken door middel van een Tdata transactie met de sleutel die daarmee verbonden is. De blockchain verifieert dan de digitale handtekening van ofwel de gebruiker ofwel de dienst. Bij de dienst wordt ook de vereiste toestemming om toegang te krijgen geverifieerd. De gebruiker kan ten slotte de toestemming, die het de dienst gaf, op elk moment veranderen door middel van een Taccess transactie in een andere soort toestemming, waaronder het terugtrekken van de toestemming om toegang te krijgen tot vooraf opgeslagen gegevens."

Het voorstel gaat uit van een voldoende gerandomiseerde verdeling van de gegevens over de *nodes* om het systeem te verzekeren tegen ongewenste aanpassingen en zelfs cyberaanvallen. Daarnaast vereisen de auteurs ook van de gebruikers van het systeem dat ze hun encryptiesleutel (*private key*) goed bewaren. Indien bovenstaande voorwaarden voldaan zijn, is het systeem volgens de auteurs beschermd tegen ongewenste toegang tot de persoonsgegevens die opgeslagen liggen in de blockchain.

19. De auteurs gaan uit van een blockchainmodel waarbij de persoonsgegevens enkel *off-chain* opgeslagen zijn en enkel de *hash* die naar de persoonsgegevens verwijst op de publiek toegankelijke blockchain zichtbaar is. Het is dus hoogst noodzakelijk dat de ontwikkelaars van de blockchain passende encryptiemechanismen implementeren die het voor niet-gemachtigden onmogelijk maken om via de *hash* de persoonsgegevens te achterhalen. Daarnaast bepaalt de

[75] Buiten de blockchain bewaren van gegevens of transacties die buiten de blockchain om gebeuren, J. FRANKENFIELD, "Off-chain transactions (cryptocurrency)", New York City, 10 april 2018, laatst geraadpleegd op 9 april 2019, *https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp*.

gebruiker welke persoonsgegevens zichtbaar zijn voor de dienst en kan hij de toegangsmachtiging terugtrekken, wat wijst op controle door de betrokkene. De mogelijkheid om de toegangsmachtiging terug te trekken ligt ook in lijn met de vereiste uit het derde lid van art. 7 AVG dat stelt dat de betrokkene het recht heeft om de toestemming te allen tijde in te trekken. Dat komt ook terug in Rechtsoverweging (42) AVG, dat stelt dat toestemming niet vrij kan zijn zonder de mogelijkheid om de toestemming in te trekken of te weigeren zonder nadelige gevolgen. Het model faciliteert die vereiste. Aangezien de *nodes* de digitale handtekening van de dienst verifiëren, is het niet mogelijk om de persoonsgegevens van de betrokkene door te geven aan derde-partijen (zonder diens toestemming). Dat elimineert het probleem van verkoop van persoonsgegevens aan derden.

Het model kent ook een aantal problemen. Ten eerste lijkt het erop dat de betrokkene bij elke dienst een nieuwe identiteit moet aanmaken, een bepaalde toegang moet verschaffen aan de dienst en ook die toegang moet beheren. Het aanmaken van verschillende identiteiten en het beheren van de toegangsmachtigingen zou tijdrovend zijn. Daarnaast lijkt het quasi-onmogelijk voor de betrokkene om, in het geval hij van meerdere diensten gebruik wenst te maken, alle verschillende toegangsmachtiging diligent te beheren. Een gecentraliseerde identiteitsapplicatie is daarom aangewezen, waarop verschillende diensten kunnen inloggen en om toegangsmachtiging vragen. Dat zou diligente controle door de betrokkene mogelijk moeten maken. Daarnaast houdt het model geen rekening met het recht op gegevenswissing en de vraag naar de verwerkingsverantwoordelijke. Die problemen worden in Hoofdstuk III behandeld. De auteurs laten ook open of het om een *permissioned*, dan wel *permissionless* blockchain zou gaan. Mijns inziens lijken beide opties mogelijk, maar dat heeft dan mogelijk wel een impact op de aanwijzing van de verwerkingsverantwoordelijke. Samengevat is het model van ZYSKIND, NATHAN en PENTLAND een goed vertrekpunt voor een blockchainoplossing die de controle door de betrokkene faciliteert, maar zijn zeker nog wijzigingen nodig om het model werkbaar en conform de AVG te maken. Het lijkt dus technisch mogelijk om een blockchainmodel te creëren dat controle door de betrokkene faciliteert.

AFDELING III. POTENTIËLE MOGELIJKHEDEN VAN BLOCKCHAIN VOOR DE RECHTEN VAN DE BETROKKENE

20. **RECHT OP INFORMATIE EN TRANSPARANTIE -** Artt. 12 tot 14 AVG bepalen dat de betrokkene op een transparante manier informatie moet krijgen over de persoonsgegevens die de

verwerkingsverantwoordelijke over die betrokkene verzamelt. Er zijn versterkte waarborgen ingebouwd wanneer de verwerkingsverantwoordelijke de persoonsgegevens niet rechtstreeks van de betrokkene heeft ontvangen.[76] De bedoeling van het recht op informatie is het faciliteren van de andere rechten van de betrokkene.[77] De AVG omschrijft het transparantiebeginsel: "Overeenkomstig het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn, en moet duidelijke en eenvoudige taal worden gebruikt. Dat beginsel betreft met name het informeren van de betrokkenen over de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking, alsook verdere informatie om te zorgen voor behoorlijke en transparante verwerking met betrekking tot de natuurlijke personen in kwestie en hun recht om bevestiging en mededeling te krijgen van hun persoonsgegevens die worden verwerkt."[78] Transparantie is ook terug te vinden als beginsel inzake verwerking van persoonsgegevens in art. 5, 1., a) AVG. In de Richtsnoeren[79] over transparantie zegt Werkgroep Gegevensbescherming Art. 29 (hierna: WP29) dat transparantie een overkoepelende verplichting in de AVG is, die de drie componenten uit Rechtsoverweging (39) AVG omvat.[80] Het is een beginsel dat een belangrijke positie heeft in het recht van de Europese Unie, zoals opgenomen in artikelen 1 en 11, lid 2 VEU, art. 15 VWEU en art. 8 Handvest met betrekking tot de toegangscomponent van het beginsel.[81] Het is nauw verbonden met de nieuwe verantwoordingsplicht van de verwerkingsverantwoordelijke in de AVG. De toegangscomponent zal verder in deze Afdeling besproken worden.[82] In online-situaties gebeurt de kennisgeving van de informatie vaak via de Privacy Policy.[83]

21. Transparantie is één van de kenmerken van blockchaintechnologie, aangezien alle transacties aan de *ledger* opgelijst staan en dus iedereen op elk moment de (gegevens-) transacties kan zien. Het lijkt dus zeker dat blockchain voordelen kan bieden voor het recht op informatie uit artikel 12 AVG. Artikel 12 geeft ook aan dat de informatie kan meegedeeld worden met elektronische of

---

[76] Art. 14 AVG.
[77] Art. 12, 1. AVG.
[78] Rechtsoverweging (39) AVG.
[79] WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Richtsnoeren inzake transparantie overeenkomstig verordening 2016/679*, 29 november 2017, 17/NL WP 260, 47 p.
[80] *Ibid.*, 4.
[81] *Ibid.*, 5.
[82] *Ibid.*
[83] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 213; O. SUSTRONCK, *Praktijkboek internetrecht*, Mechelen, Wolters Kluwer, 2017, 121; E. W. VERHELST, "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, (17) 19.

andere passende middelen, wat het gebruik van blockchain niet uitsluit. De vraag is echter of daarmee wel echt aan de waarborgen van transparantie voldaan is. De informatie is immers enkel als een *hash* verwerkt in een blockchain, waardoor het toch betrekkelijk moeilijker kan worden voor de betrokkene om afdoende informatie te verkrijgen. Dat probleem is echter makkelijk opgelost: in het blockchainmodel uit vorige Afdeling bepaalt de betrokkene zelf wie de toestemming krijgt om de persoonsgegevens te verwerken en voor welke doeleinden. Aangezien de betrokkene zelf zijn geheel van persoonsgegevens samenstelt, weet hij welke persoonsgegevens verwerkt worden, waardoor er volledige transparantie ontstaat. De aanwijzing van de verwerkingsverantwoordelijke zal in het volgende Hoofdstuk besproken worden. Die aanwijzing is nodig om transparant te kunnen zijn over de identiteit van de verwerkingsverantwoordelijke, wat art. 12 AVG waarborgt.

22. **RECHT OP INZAGE -** De toegangscomponent van het transparantiebeginsel, ook wel het recht op inzage, vinden we terug in art. 15 AVG. Samengevat heeft de betrokkene het recht om te weten te komen of zijn persoonsgegevens verwerkt worden en indien dat het geval is, kan hij verzoeken om verdere informatie van de betrokkene. Die verdere informatie omvat de doeleinden van de verwerking, de categorieën van persoonsgegevens, wie de persoonsgegevens ontvangt, de bewaringstermijn of ten minste hoe die termijn berekend wordt en informatie over de andere rechten van de betrokkene.[84] Daarnaast heeft de betrokkene ook het recht te weten of de doorgifte van zijn gegevens naar derde-landen plaatsvindt en hoe de bescherming van zijn gegevens is gewaarborgd.[85]

Hoewel het op het eerste gezicht moeilijk lijkt om het recht op inzage af te dwingen in een blockchaincontext, zijn er toch voordelen te vinden. Het is moeilijk om de verwerkingsverantwoordelijke te identificeren in een systeem waarbij heel veel *nodes* de transacties moeten verifiëren, zoals we in het deel over de aanwijzing van de verwerkingsverantwoordelijke zullen zien. Dat heeft tot gevolg dat de betrokkene geen aanspreekpunt heeft om zekerheid te krijgen of zijn persoonsgegevens al dan niet verwerkt worden.

[84] Art. 15, 1. AVG.
[85] Art. 15, 2. AVG.

Afgezien daarvan, is het toch mogelijk dat blockchaintechnologie het recht op inzage faciliteert. Aangezien de betrokkene, zoals in de volgende Afdeling zal blijken, zelf zou moeten kunnen bepalen welke gegevens hij toevertrouwt aan een blockchain en wie dan toegang heeft tot die gegevens, is aan het recht op inzage *de facto* voldaan. De betrokkene weet dan voor welke gegevens verwerking toegestaan is door welke verwerkingsverantwoordelijke en voor welke doeleinden, aangezien enkel hij de macht heeft om toestemming te geven voor de verwerking voor afgelijnde doeleinden, voor een bepaalde periode en onder welke voorwaarden. De betrokkene heeft steeds de mogelijkheid om de toestemming weer in te trekken in het blockchainmodel uit vorige Afdeling. Daarnaast heeft de betrokkene een eigen decryptiesleutel (*private key)* die het mogelijk maakt om de *hash* te decrypteren en zo op elk moment te weten welke persoonsgegevens onder gehashte vorm op de blockchain aanwezig zijn. Als het onmogelijk is om gegevens door te geven zonder de machtiging van de betrokkene en wanneer de betrokkene zelf bepaalt wie die machtiging krijgt, weet hij wie toegang heeft tot de gegevens want dat bepaalt hij zelf. Dat is de bedoeling van de (verbeterde) versie van het blockchainmodel uit vorige Afdeling. Het is dan technisch onmogelijk voor derde partijen om, zonder decryptiesleutel die de betrokkene via de machtiging aan de gemachtigde verleent, toegang te hebben tot de persoonsgegevens en ze zonder toestemming van de betrokkene te gebruiken. Blockchaintechnologie die die infrastructuur en functionaliteiten heeft, faciliteert het recht op inzage uit art. 15 AVG.

23. **RECHT OP RECTIFICATIE -** Art. 16 AVG omvat het recht op rectificatie: "De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht aanvulling van onvolledige gegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken." Art. 19 AVG voegt daaraan een kennisgevingsplicht toe voor de verwerkingsverantwoordelijke wanneer die persoonsgegevens van de betrokkene heeft gerectificeerd, tenzij dat onmogelijk is of onevenredig veel inspanning vergt.

24. Ook hier kan blockchaintechnologie voordelen opleveren. Als we het blockchainmodel van vorige Afdeling bekijken, dan zien we dat het de betrokkene zelf is die de identiteit in de applicatie maakt. De betrokkene bepaalt dus zelf welke van zijn persoonsgegevens aan de blockchain worden toegevoegd. Dat verkleint al op enorme wijze de kans op onjuiste gegevens en dus de nood tot rectificatie. Indien de gegevens toch onjuist zouden zijn, kan het eventueel mogelijk zijn om nieuwe gegevens aan de *block* met juiste gegevens aan de *ledger* toe te voegen en zo de

onjuiste gegevens te verbeteren.[86] FINCK haalt aan dat die oplossing makkelijk toepasbaar is in een blockchain waarbij enkel gegevens aan de blockchain toegevoegd worden zonder ze te kunnen wijzigen, zoals in het model.[87] Dat komt ook terug in art. 16 AVG zelf, dat spreekt over een aanvullende verklaring. Nog een optie is eerst het verwijderen van de gegevens van de blockchain, en achteraf de correcte gegevens toe te voegen.[88] Dat kan echter problematisch zijn voor blockchains, aangezien het verwijderen van gegevens niet vanzelfsprekend is. Verdere bespreking daarover volgt in Hoofdstuk III. Ter opsomming lijkt het dat we kunnen stellen dat blockchaintechnologie inderdaad het recht uit art. 16 AVG faciliteert. Dat omwille van de verhoogde autonomie van de betrokkene, dankzij het zelf opstellen van de identiteit, en de verschillende opties die blockchaintechnologie bieden om te voldoen aan het recht op rectificatie.

AFDELING IV. HET RECHT OP GEGEVENSWISSING

25. **JURIDISCHE BASIS -** Art. 17 AVG bevat het recht op gegevenswissing, ook bekend als het recht op vergetelheid. Het bepaalt dat de betrokkene wissing van zijn persoonsgegevens kan vragen aan de verwerkingsverantwoordelijke, die daaraan verplicht moet voldoen in 6 gevallen:[89]

1) Wanneer de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor ze verwerkt worden;

2) Wanneer de betrokkene zijn toestemming tot de verwerking terugtrekt en er geen andere rechtsgrond voor de verwerking is;

3) Wanneer de betrokkene zijn recht op bezwaar uitoefent en er geen dwingende gerechtvaardigde gronden zijn;

4) Wanneer de persoonsgegevens onrechtmatig worden verwerkt;

---

[86] M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 29; J. SIMAL, *Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR*, onuitg. masterproef Rechten KU Leuven, 35.

[87] M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 29.

[88] M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 29; G. JENSEN, "Reconciling GDPR rights to erasure and rectification of personal data to blockchain", Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018, *https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain*.

[89] Art. 17, 1. AVG.

5) Ter voldoening aan een wettelijke plicht die op de verwerkingsverantwoordelijke rust;

6) Wanneer de persoonsgegevens verzameld zijn in verband met een aanbod van diensten van de informatiemaatschappij aan kinderen zoals bedoeld in art. 8, lid 1 AVG.

De problematiek van de aanwijzing van de verwerkingsverantwoordelijke komt later in dit Hoofdstuk terug. Nu is het belangrijk na te gaan in welke gevallen de betrokkene het recht op gegevenswissing kan uitoefenen.

Het recht op gegevenswissing is belangrijk met het oog op het beginsel van minimale gegevensverwerking uit art. 5, 1., c) AVG.[90] Een rechtszaak waarin het recht op gegevenswissing sterk naar voor kwam is de Google Spain-zaak[91], waarna Werkgroep 29 een lijst met Richtsnoeren[92] uitbracht over de implementatie van dat arrest in het Europese gegevensbeschermingssysteem.[93] De Werkgroep geeft in de Richtlijnen aan dat men een balansoefening moet maken tussen de rechten van de betrokkene en de rechtmatige belangen van de onderneming, wat betekent dat het recht op gegevenswissing niet absoluut is, en het afhankelijk is van geval per geval welk recht prevaleert.[94]

26. **VERENIGING VAN BLOCKCHAIN EN RECHT OP GEGEVENSWISSING -** Het conflict tussen blockchaintechnologie en het recht op gegevenswissing vinden we terug in de architectuur van de technologie: in principe blijven gegevens altijd op de blockchain staan, doordat *hashes* verwijzen naar vorige *blocks* die die gegevens bevatten.[95] Dat staat haaks op het recht op gegevenswissing

---

[90] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 221.

[91] HvJ 13 mei 2014, nr. C-131/12, ECLI:EU:C:2014:317, Google Spain.

[92] WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Guidelines on the implementation of the court of justice of the european union judgement on "Google Spain and INC v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, 26 november 2014, 14/EN WP 225, 20 p.

[93] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 225-226.

[94] R. HERIAN, "Regulating disruption: blockchain, GDPR, and questions of data sovereignty" *Journal of Internet Law* 2018-19, afl. 2, (7) 13; WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Guidelines on the implementation of the court of justice of the european union judgement on "Google Spain and INC v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, 26 november 2014, 14/EN WP 225, 5-6.

[95] J. BACON e.a., *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 6-7; M. BERBERICH en M. STEINER, "Blockchain technology and the GDPR – how to reconcile privacy and distributed ledgers", *European Union Data Protection Law Review* 2016, 422; G. JENSEN, "reconciling GDPR rights to erasure and rectification of personal data to blockchain", Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018,

uit art. 17 AVG, dat zoals gezegd uitgaat van het principe van minimale gegevensverwerking. Eén van de eigenschappen van blockchaintechnologie is immers de principiële onveranderbaarheid en de daaruit voortvloeiende onwisbaarheid van gegevens, zoals eerder in Hoofdstuk II aangehaald. Het probleem is echter niet onoverkomelijk. Encryptie kan de sleutel zijn tot de vereniging van het recht op gegevenswissing en blockchaintechnologie. Door de persoonsgegevens te encrypteren, kunnen enkel de personen met een decryptiesleutel ze ontcijferen. Wanneer de betrokkene zijn recht op gegevenswissing wilt uitoefenen, zou het kunnen volstaan om de decryptiesleutel te vernietigen, waardoor niemand de gegevens meer kan lezen en de facto de gegevens gewist zijn.[96] Uit de Richtsnoeren van Werkgroep 29 over de implementatie van de Google Spain-zaak blijkt dat het recht op gegevenswissing niet absoluut is.[97] Hoewel de persoonsgegevens zelf niet van de blockchain gewist zijn, zouden ze door het vernietigen van de decryptiesleutel niet meer leesbaar zijn.[98] Dat heeft tot gevolg dat de gegevens de betrokkene niet meer zouden kunnen identificeren, waardoor de gegevensbeschermingsregels uit de AVG niet van toepassing zijn.[99] Het lijkt dan ook logisch dat deze vorm van encryptie en bescherming van persoonsgegevens op de blockchain de balanstoets met het recht op gegevenswissing doorstaat. De vraag blijft echter of in de toekomst, door ontwikkeling van

---

https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain; V.I. LAAN en A. RUTJES, "Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?", *Computerrecht* 2017, (253) 253-254; S. MARIËN, "Blockchain en GDPR op ramkoers?", *datanews* 2018, (32) 34; W. MAXWELL en J. SALMON, *A guide to blockchain*, Brussel, Hogan Lovells LLP, 2017, 15.

[96] ARCHER SOFT, "The right to be forgotten (GDPR) vs blockchain technology, New York, 7 juni 2018, laatst geraadpleegd op 26 november 2018, *http://www.archer-soft.com/en/blog/right-be-forgotten-gdpr-vs-blockchain-technology*; H. CHANG, *Blockchain: disrupting data protection?*, Hong Kong, University of Hong Kong Faculty of Law Research, 2017, 2; J. BACON e.a., *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 48; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 30; P. HRISTOV en W. DIMITROV, "The blockchain as a backbone of GDPR compliant frameworks", *Quality-access to success* 2019, (305) 309; G. JENSEN, "Reconciling GDPR rights to erasure and rectification of personal data to blockchain", Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018, *https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain*; E. PISCINI, D. DALTON en L. KEHOE, *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 7.

[97] WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Guidelines on the implementation of the court of justice of the european union judgement on "Google Spain and INC v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, 26 november 2014, 14/EN WP 225, 20 p.

[98] ARCHER SOFT, "The right to be forgotten (GDPR) vs blockchain technology, New York, 7 juni 2018, laatst geraadpleegd op 26 november 2018, *http://www.archer-soft.com/en/blog/right-be-forgotten-gdpr-vs-blockchain-technology*; G. JENSEN, "Reconciling GDPR rights to erasure and rectification of personal data to blockchain", Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018, *https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain*; D. IBÁÑEZ, K. O'HARA, en E. SIMPERL, *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*.

[99] Rechtsoverweging (26) AVG; WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Opinion 05/2014 on anonymisation techniques*, 10 april 2014, 0829/14/EN WP 216, 5.

nieuwe decryptiemogelijkheden zoals *quantum decryption*[100], vernietiging van de decryptiesleutel zal volstaan om persoonsgegevens werkelijk anoniem te maken. Gevoelige gegevens en persoonlijke gegevens die lange tijd (in geëncrypteerde vorm) op de blockchain blijven staan, zijn een mogelijke goudmijn voor cyberdieven die beschikken over *quantum decryption.*[101] Toch lijkt het mogelijk om, via aangepaste methodes en blijvende evolutie, encryptie te garanderen. Zo bestaan er vandaag al oplossingen voor het probleem van *quantum decryption*, zoals het versleutelen van gegevens op verschillende niveaus (*double encryption*) en veranderen van versleutelingswijze (*crypto-agility).*[102]

Een tweede optie is het *off-chain* bewaren van persoonsgegevens en enkel maar een verwijzing naar de persoonsgegevens, in de vorm van een *hash*, aan de publieke blockchain toe te voegen.[103] Dat zou de verwijdering van de persoonsgegevens, die *off-chain* bewaard zijn, mogelijk maken, waarbij de *hash* louter verwijst naar verwijderde gegevens.[104] Het voorgestelde model uit Hoofdstuk II voorziet in de *off-chain* bewaring van persoonsgegevens. Daar zou simpelweg de verwijdering van de persoonsgegevens uit de applicatie tot gevolg hebben dat de *hash* op de publieke blockchain enkel verwijst naar verwijderde persoonsgegevens.

27. **TECHNISCHE IMPLEMENTATIE -** Op technisch vlak lijkt de beste encryptiewijze een driezijdige manier van encrypteren. Zowel de betrokkene, de verwerkingsverantwoordelijke als de bedrijven die gebruik wensen te maken van de persoonsgegevens van de betrokkene krijgen via de applicatie die beschreven is in Hoofdstuk II, Afdeling II een decryptiesleutel. Wanneer alle drie decryptiesleutels nodig zijn om de persoonsgegevens leesbaar te maken, kan de betrokkene zijn decryptiesleutel vernietigen en zijn de gegevens niet leesbaar meer.[105] Aan het recht op

---

[100] Het decrypteren van versleutelde gegevens dankzij quantum computers, die een grote rekenkracht hebben, C. BURCHETT, "How to fight the coming quantum decryption threat", San Diego, 12 juli 2018, laatst geraadpleegd op 9 april 2019, *https://www.enterprisetech.com/2018/07/12/how-to-fight-the-coming-quantum-data-decryption-threat/*.

[101] *Ibid.*

[102] *Ibid.*

[103] C. LIMA, "How decentralised blockchain internet will comply with GDPR data privacy*"*, X, juni 2018, laatst geraadpleegd op 21 maart 2019, *https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf*; V.I. LAAN en A. RUTJES, "Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?", *Computerrecht* 2017, (253) 258; E. PISCINI, D. DALTON en L. KEHOE, *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 7; E. W. VERHELST, "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, (17) 22.

[104] *Ibid.*

[105] G. JENSEN, "Reconciling GDPR rights to erasure and rectification of personal data to blockchain", Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018, *https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain*.

gegevenswissing zou daarmee dan voldaan zijn, en de betrokkene krijgt daardoor meteen controle over zijn persoonsgegevens. Het systeem van toestemming zoals beschreven in Afdeling II van Hoofdstuk II zou die encryptiewijze kunnen implementeren, waarbij de toestemming de decryptie inhoudt. De bedrijven die gebruik willen maken van de gegevens kunnen die gegevens dan lezen, zolang de betrokkene de toestemming en de daarmee gepaard gaande decryptie in stand houdt. Zoals vermeld, moeten ontwikkelaars van blockchainapplicaties in de toekomst wel rekening houden met decryptiemechanismen zoals *quantum decryption* en daartegen passende initiatieven nemen, om te zorgen dat de vernietiging van de decryptiesleutel ook werkelijk het de anonimisering van persoonsgegevens inhoudt. Echter, m.i. kan *off-chain* opslag van persoonsgegevens tot betere resultaten leiden in het kader van het recht op gegevenswissing. De *hash* verwijst dan naar persoonsgegevens in bv. een applicatie zoals bedoeld in Hoofdstuk II. De verwijdering van de gegevens uit de applicatie zou er dan toe leiden dat de *hash* louter verwijst naar verwijderde gegevens en het recht op gegevenswissing op die manier nageleefd wordt.

AFDELING V. POSITIE VAN VERWERKINGSVERANTWOORDELIJKE

28. **JURIDISCHE KWALIFICATIE VAN VERWERKINGSVERANTWOORDELIJKE** – De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking vaststelt.[106] Het aanwijzen van een verwerkingsverantwoordelijke is problematisch bij blockchaintechnologie: er is (meestal) geen centrale entiteit die het doel en de middelen van de verwerking vaststelt zoals bedoeld in art. 4, 7) AVG. Volgens Werkgroep 29 bestaan er drie criteria om de verwerkingsverantwoordelijke aan te stellen: een personeel criterium ("een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan"), een eventueel pluralistisch criterium ("alleen of samen met anderen") en een materieel criterium ("het doel van en de middelen voor de verwerking vaststelt").[107] Die begrippen zijn autonoom en moeten functioneel geïnterpreteerd worden, d.w.z. dat de feitelijke omstandigheden prevaleren over formele omstandigheden zoals contractuele bepalingen.[108] Wie het doel en de essentiële elementen van de middelen (bewaartermijn, welke gegevens verwerkt worden, wie toegang heeft) bepaalt, is de

[106] Art. 4, 7) AVG.
[107] WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Opinion 01/2010 on the concepts of "controller" and "processor"*, 6 februari 2010, 00264/10/EN WP 169, 1.
[108] *Ibid*., 32.

verwerkingsverantwoordelijke.[109] De verwerker, d.i. de entiteit die voor de verwerkingsverantwoordelijke de persoonsgegevens verwerkt[110], mag van de verwerkingsverantwoordelijke het mandaat krijgen om de technische en organisatorische elementen van de middelen van de verwerking te bepalen.[111]

29. ***IN CONCRETO*** **-** Het probleem bij blockchaintechnologie is dat de aanwijzing van de verwerkingsverantwoordelijke niet vanzelfsprekend is. Het onderscheid tussen *private permissioned* en *public permissionless* blockchains is hier van belang. Bij *private permissioned* blockchains is er een centrale entiteit die de toestemming geeft om toe te treden tot de blockchain, die dan ook het doel en de middelen bepaalt en dus zelf de verwerkingsverantwoordelijke is.[112] Bij *public permissionless* blockchains kan echter iedereen toetreden tot de blockchain en besturen de *nodes*, die vaak onbekend zijn, het geheel.[113] Die *nodes* zijn gedecentraliseerde entiteiten en zien vaak enkel de *hashes* of de geëncrypteerde versies van de persoonsgegevens, waardoor het voor de betrokkene moeilijk is om de *nodes* aan te spreken en zijn rechten uit te oefenen.[114]

---

[109] *Ibid.*

[110] Art. 4, 8) AVG.

[111] WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Opinion 01/2010 on the concepts of "controller" and "processor"*, 6 februari 2010, 00264/10/EN WP 169, 33.

[112] EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, Brussel, EU Blockchain Observatory and Forum, 2018, 17; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 26; L. MOEREL, "Blockchain & data protection … and why they are not on a collision course, *European Review of Private Law* 2019, (825) 830; E. W. VERHELST, "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, (17) 20; C. WIRTH en M. KOLAIN, *Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data*, Amsterdam, European Society for Socially Embedded Technologies, 2018, 5.

[113] M. BERBERICH en M. STEINER, "Blockchain technology and the GDPR – how to reconcile privacy and distributed ledgers", *European Union Data Protection Law Review* 2016, (422) 424; J. CZARNECKI, "Blockchain and personal data protection regulations explained", New York, 26 april 2017, laatst geraadpleegd op 22 november 2018, *https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained*; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 26; P. JO PESCH en C. SILLABER, "Distributed ledger, joint control? – blockchain and the GDPR's transparency requirements" *Computer Law Review International* 2017, (166) 170; L. VANDERDONCKT, *Decentralising the GDPR: an analysis of distributed ledger technology against ratio legis of the GDPR*, onuitg. masterproef rechten KU Leuven, 2018, 28-29.

[114] J. BACON e.a., *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 45; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 26; L. MOEREL, "Blockchain & data protection … and why they are not on a collision course, *European Review of Private Law* 2019, (825) 831; L. VANDERDONCKT, *Decentralising the GDPR: an analysis of distributed ledger technology against ratio legis of the GDPR*, onuitg. masterproef rechten KU Leuven, 2018, 29;

C. WIRTH en M. KOLAIN, *Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data*, Amsterdam, European Society for Socially Embedded Technologies, 2018, 5-6.

Een optie voor de kwalificatie van de verwerkingsverantwoordelijke is de betrokkene zelf aanduiden als verwerkingsverantwoordelijke en de *nodes* kunnen de niet-essentiële elementen van de middelen van de verwerking bepalen in dat scenario.[115] FINCK en BACON e.a. zien dat als een logische uitkomst, gezien het feit dat door de *private keys* of decryptiesleutels de betrokkene meer controle krijgt over zijn persoonsgegevens en het de betrokkene is die gegevens toevoegt aan de blockchain. [116] Het *EU Blockchain Observatory and Forum* en de Franse gegevensbeschermingsautoriteit (*Commission Nationale de l'Informatique et des Libertés*, hierna: CNIL) sluiten zich daar niet bij aan. Zij gaan uit van een commercieel of professioneel criterium: netwerkgebruikers die uit commerciële of professionele overwegingen persoonsgegevens aan de blockchain toevoegen, zullen naar alle waarschijnlijkheid als verwerkingsverantwoordelijke aan te merken zijn.[117] Voorbeelden hiervan zijn notarissen en banken die in dienst van hun cliënten, persoonsgegevens aan een blockchain toevoegen.[118] Natuurlijke personen die niet voor commerciële of professionele doeleinden persoonsgegevens aan een blockchain toevoegen, vallen volgens het CNIL en *EU Blockchain Observatory and Forum* onder de uitzondering van het toepassingsgebied wegens zuiver persoonlijke of huishoudelijke activiteit uit art. 2, 2., c) AVG en kunnen zodanig niet de verwerkingsverantwoordelijke zijn.[119]

Een tweede optie is het geheel van *nodes* als gezamenlijke verwerkingsverantwoordelijken (art. 26 AVG) aan te duiden in *public permissionless* blockchains. Dat ligt echter moeilijk gelet op het feit dat die *nodes* gedecentraliseerde entiteiten zijn en dus moeilijk zowel het doel als de middelen

---

[115] M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 27; S. MARIËN, "Blockchain en GDPR op ramkoers?", *datanews* 2018, (32) 35.

[116] J. BACON e.a., *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 45;M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 27; J. SIMAL, *Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR*, onuitg. masterproef Rechten KU Leuven, 24.

[117] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain*, Parijs, Commission Nationale de l'Informatique et des Libertés, 2018, 2; EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, Brussel, EU Blockchain Observatory and Forum, 2018, 18.

[118] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain*, Parijs, Commission Nationale de l'Informatique et des Libertés, 2018, 2.

[119] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain*, Parijs, Commission Nationale de l'Informatique et des Libertés, 2018, 3; EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, Brussel, EU Blockchain Observatory and Forum, 2018, 18.

van de verwerking kunnen bepalen.[120] Die gemeenschappelijke bepaling is echter noodzakelijk voor art. 26, 1. AVG. Zelfs indien dat zou lukken, blijft het moeilijk voor de betrokkene om zijn rechten uit te oefenen, aangezien het moeilijk is om iedere afzonderlijke *node* aan te spreken.[121]

Ook de optie dat iedere afzonderlijke *node* verwerkingsverantwoordelijke zou zijn, brengt veel moeilijkheden voor de betrokkene met zich meeom zijn rechten uit te oefenen en te bepalen wie hij moet aanspreken.

IBÁÑEZ, O'HARA en SIMPERL[122] stellen twee scenario's voor in de bepaling van de verwerkingsverantwoordelijke bij *public permissionless* blockchains. Ten eerste het scenario waarbij de gebruiker rechtstreeks in contact komt met een *public permissionless* blockchain: daarin zal de gebruiker zelf de verwerkingsverantwoordelijke zijn bij gebrek aan een andere mogelijke verwerkingsverantwoordelijke. Zij stellen voor dat, in dat geval, de ontwikkelaars de blockchain zo creëren dat conformiteit met de gegevensbeschermingsregels verzekerd is via technische maatregelen. Dat lijkt op een toepassing van het beginsel van gegevensbescherming door ontwerp uit art. 25, 1. AVG. De auteurs wijzen twee belangrijke punten aan: ten eerste moeten de ontwikkelaars het onmogelijk maken dat gebruikers bepaalde soorten persoonsgegevens aan de blockchain toevoegen (bv. gevoelige gegevens uit art. 9 AVG). Ten

---

[120] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain,* Parijs, Commission Nationale de l'Informatique et des Libertés, 2018, 3; M. FINCK, "Blockchains and Data Protection in the European Union", *European Data Protection Law Review* 2017, (17) 26-27; D. IBÁÑEZ, K. O'HARA, en E. SIMPERL, *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*; P. JO PESCH en C. SILLABER, "Distributed ledger, joint control? – blockchain and the GDPR's transparency requirements" *Computer Law Review International* 2017, (166) 170; J. SIMAL, *Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR*, onuitg. masterproef Rechten KU Leuven, 24; L. VANDERDONCKT, *Decentralising the GDPR: an analysis of distributed ledger technology against ratio legis of the GDPR*, onuitg. masterproef rechten KU Leuven, 2018, 29; E. W. VERHELST, "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, (17) 20.

[121] M. BERBERICH en M. STEINER, "Blockchain technology and the GDPR – how to reconcile privacy and distributed ledgers", *European Union Data Protection Law Review* 2016, (422) 424; M. FINCK, "Blockchains and data protection in the european union", *European Data Protection Law Review* 2017, (17) 26-27; D. IBÁÑEZ, K. O'HARA, en E. SIMPERL, *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*; J. SIMAL, *Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR*, onuitg. masterproef Rechten KU Leuven, 24; L. VANDERDONCKT, *Decentralising the GDPR: an analysis of distributed ledger technology against ratio legis of the GDPR*, onuitg. masterproef rechten KU Leuven, 2018, 28-29.

[122] L. D. IBÁÑEZ, K. O'HARA, en E. SIMPERL, *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*.

tweede moet de blockchain om een rechtmatige verwerkingsgrond (art. 6 AVG) vragen, vooraleer de gebruiker zijn gegevens aan de blockchain kan toevoegen. Om betere garanties te bieden voor gegevensbescherming van betrokkenen, kan de blockchain bepaalde maatregelen nemen zoals *zero-knowledge proof* mechanismen. Het eerste scenario lijkt voor de doelstelling uit Rechtsoverweging (7) AVG een aantrekkelijke optie. In het model uit Hoofstuk II kan de betrokkene het doel van de verwerking bepalen door gebruik te maken van het al dan niet toekennen van zijn toestemming (en daarmee gepaard gaande decryptie). Daarnaast bepaalt de betrokkene welke gegevens hij toevoegt aan het geheel van persoonsgegevens op de applicatie. Via zijn toestemming en daarmee gepaard gaande decryptie bepaalt hij wie toegang heeft tot zijn gegevens en hoe lang de persoonsgegevens op de blockchain bewaard blijven. Door die controle over het doel en de essentiële elementen van de middelen van de verwerking kunnen we stellen dat de betrokkene zelf de rol van verwerkingsverantwoordelijke kan dragen. Dat zou dan wel tot gevolg hebben dat ook de verplichtingen van de verwerkingsverantwoordelijke op de betrokkene zelf komen te liggen. De betrokkene zal dan ook zelf moeten nagaan in hoeverre een bepaalde blockchain voldoet aan de bepalingen van AVG, wat het moeilijker maakt voor de betrokkene om beschermd te zijn. Ook zou het een hele ommekeer betekenen in de ideologie van de AVG, die uitgaat van een duidelijke aflijning van een betrokkene en een verwerkingsverantwoordelijke die een aantal verplichtingen heeft ten aanzien van de betrokkene. De vraag is in hoeverre gegevensbeschermingsautoriteiten zo'n oplossing aanvaarden.

Het tweede scenario van IBÁÑEZ, O'HARA en SIMPERL gaat uit van een applicatie waarmee de gebruikers in contact komen en waarin de persoonsgegevens *off-chain* opgeslagen liggen, en waarbij een blockchain de rol inneemt van communicatiemiddel tussen de betrokkenen en de entiteiten die gebruik willen maken van de persoonsgegevens. In dat scenario zijn de eigenaars van de applicatie de verwerkingsverantwoordelijke. Zij bepalen immers het doel en de essentiële bestanddelen van de middelen van de verwerking. Het tweede scenario lijkt sterk op het model uit Hoofdstuk II en geeft een duidelijke aanwijzing van de verwerkingsverantwoordelijke.

30. Samengevat is de aanwijzing van de verwerkingsverantwoordelijke afhankelijk van de gebruikte blockchain. In *private permissioned* blockchains is het mogelijk een centrale entiteit aan te duiden die het doel en de middelen van de verwerking bepaalt en dus verwerkingsverantwoordelijke is. Bij *public permissionless* blockchains is het moeilijker om de verwerkingsverantwoordelijke aan te duiden. Ook hier ontstaat een onderscheid: indien de blockchaingebruiker commerciële of professionele doeleinden nastreeft, zal die gebruiker als verwerkingsverantwoordelijke aan te

merken zijn. Wanneer de gebruiker geen commerciële of professionele doeleinden nastreeft, is de bepaling van de verwerkingsverantwoordelijke afhankelijk van de directe of indirecte band die de gebruiker heeft met de blockchain. Bij een direct contact tussen de gebruiker en de blockchain zal de gebruiker de verwerkingsverantwoordelijke zijn, wanneer de gebruiker een applicatie gebruikt en enkel een indirecte band heeft met de blockchain zal de eigenaar van de applicatie de verwerkingsverantwoordelijke zijn.

AFDELING VI. TUSSENBESLUIT

31. In dit hoofdstuk is een analyse gemaakt van de opportuniteiten en moeilijkheden van blockchaintechnologie voor de doelstelling van controle over persoonsgegevens uit de AVG. In het eerste deel van dit Hoofdstuk zagen we dat in traditionele gegevensbeschermingssystemen het fenomeen van "Platform Power" een probleem is voor de controle over persoonsgegevens. De blockchaineigenschappen van decentralisatie en vertrouwen door consensus kunnen aan dat probleem remediëren. Om die redenen zouden we de technologie als gegevensbeschermingsinstrument kunnen inzetten. In het tweede deel werd een technische analyse gemaakt van een blockchainmodel dat de controle van de betrokkene moet versterken. Het werd duidelijk dat het technisch gezien mogelijk is om een blockchain te creëren die de controle bij de betrokkene legt, mits de betrokkene de nodige maatregelen neemt. Vervolgens is besproken voor welke rechten blockchaintechnologie mogelijkheden biedt. Dat is duidelijk voor het recht op informatie, het recht op inzage en het recht op rectificatie. In de laatste twee Afdelingen werden twee problemen besproken in het kader van de conformiteit van blockchaintechnologie met de AVG: het recht op gegevenswissing en de positie van de verwerkingsverantwoordelijke. Hoewel in beginsel technisch moeilijk, komt dit onderzoek tot de conclusie dat de betrokkene zijn recht op gegevenswissing kan uitoefenen door technische maatregelen. In het onderzoek komen volgende opties naar voren: *de facto* anonimiseren van gegevens door decryptiesleutels te vernietigen of het verwijderen van persoonsgegevens die *off-chain* opgeslagen zijn, waardoor de *hash* louter naar verwijderde gegevens verwijst. Afhankelijk van de infrastructuur van de specifieke blockchain zullen de ontwikkelaars van de blockchain een keuze moeten maken tussen die twee opties. Eenzelfde onderscheid reikt zich aan bij de aanwijzing van de verwerkingsverantwoordelijke. In *private permissioned* blockchains is het mogelijk een centrale entiteit aan te duiden die het doel en de middelen van de verwerking bepaalt en dus verwerkingsverantwoordelijke is. Bij *public permissionless* blockchains ontstaat een

verder onderscheid, afhankelijk van de al dan niet commerciële of professionele doeleinden van de gebruiker en de band tussen de gebruiker en de blockchain.

HOOFDSTUK III. CASE STUDY: SOVRIN PROJECT

32. **OPZET VAN DIT HOOFDSTUK –** Dit Hoofdstuk zal de theoretische bevindingen uit vorige hoofdstukken aftoetsen aan een praktisch voorbeeld, met name het SOVRIN project. Ten eerste volgt een beschrijving van het project en haar functionaliteiten, vervolgens komt een opsomming van de eventuele voordelen van het project voor de rechten van de betrokkene en diens controle over zijn persoonsgegevens en ten slotte volgt een analyse van het project in het licht van de problemen besproken in Hoofdstuk III.

AFDELING I. BESPREKING VAN HET SOVRIN PROJECT

33. **DOEL VAN HET SOVRIN PROJECT –** Het SOVRIN project stelt zichzelf voor in haar *Whitepaper*[123] (document uitgegeven door blockchainprojecten, dat het project omschrijft) als een blockchainprotocol dat het probleem van gebrek aan betrouwbare digitale identiteiten op het internet wilt oplossen. Dat probleem bestaat volgens het project al sinds het ontstaan van het internet, en volgt uit het feit dat het gaat om een virtuele wereld zonder betrouwbare autoriteit die de claims van internetgebruikers kan legitimeren. Er bestaat geen equivalent op het internet van fysieke identiteitskaarten, rijbewijzen of geboortecertificaten. Dat gebrek aan verifieerbare identiteitsgegevens op het internet heeft ook een impact op gegevensbescherming en de controle door de betrokkene over diens gegevens: gegevensontvangers vragen vaak te veel informatie om de identiteit van de betrokkene te verifiëren en beschikken op die manier over gegevens van de betrokkene waarover ze in de fysieke wereld niet zouden beschikken.

Het project wilt aan bovenstaand probleem remediëren door blockchaintechnologie in te zetten om de claims van internetgebruikers te verifiëren en op die manier vertrouwen te creëren op het internet. Het *consensus mechanism* van de door SOVRIN gebruikte blockchain moet ervoor zorgen dat de gegevens van internetgebruikers op gedecentraliseerde manier verwerkt worden, in

[123] Randnummer gebaseerd op: SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 42 p.

tegenstelling tot voorgaande gang van zaken waarbij centrale partijen moeten zorgen voor vertrouwen en de gegevens verwerken. Die gedecentraliseerde manier van gegevensverwerking zorgt er volgens SOVRIN voor dat de betrokkenen zelf de controle hebben over hun persoonsgegevens. Daarnaast moet het gebruik van blockchaintechnologie er ook voor zorgen dat de gegevens onveranderbaar zijn.

34. **FUNCTIONALITEITEN VAN HET PROJECT –** SOVRIN maakt gebruik van een *public permissioned* blockchain, de HYPERLEDGER INDY blockchain.[124] Het gebruik van een *public permissioned* blockchain betekent dat elke internetgebruiker kan toetreden tot de blockchain.[125] Maar, om als *node* te kunnen fungeren, moet de internetgebruiker voldoen aan een reeks voorwaarden die beschreven staan in het *Sovrin governance framework V2 Master Document*, zoals gegevensbescherming door ontwerp en door standaardinstellingen en de beginselen inzake verwerking van persoonsgegevens uit art. 5 AVG.[126] De *Whitepaper* geeft ook expliciet aan dat het project aan de voorwaarden van de AVG moet voldoen.[127]

Het project vertrekt vanuit een gedecentraliseerde digitale identiteit (*decentralised identifier*, hierna: DID).[128] Dat gebeurt via het opslaan van de geëncrypteerde *public key* van de betrokkene op de blockchain.[129] SOVRIN gebruikt een systeem van gepseudonimiseerde identificatoren, de zgn. *cryptonyms*, die geëncrypteerd zijn.[130] Aangezien het om een gedecentraliseerd adres gaat dat niet uitgaat van een centrale entiteit, heeft de betrokkene zelf controle over die digitale identiteit en kan deze er onafhankelijk over beschikken. Daarnaast kunnen DID's ervoor zorgen dat iedereen die daartoe een belang heeft, een claim van de betrokkene kan verifiëren dankzij de gedecentraliseerde tussenkomst van de *nodes*.[131] SOVRIN opteert voor een systeem van één DID per relatie tussen een betrokkene en een gegevensontvanger die claims van de betrokkene wenst

---

[124] *Ibid.*, 15.
[125] EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, Brussel, EU Blockchain Observatory and Forum, 2018, 14-15.
[126] SOVRIN FOUNDATION, "Sovrin governance framework V2 master document", Provo, 31 oktober 2018, laatst geraadpleegd op 15 maart 2019, *https://docs.google.com/document/d/1WqUOqdTBc3JACIlRviJoWJRcJHTNTNzk9_As9v-jwrY/edit*.
[127] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 20.
[128] SOVRIN FOUNDATION, *Sovrin: what goes on the ledger*, Provo, Sovrin Foundation, 2018, 2.
[129] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 10.
[130] P. WINDLEY, "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml*.
[131] SOVRIN FOUNDATION, *Sovrin: what goes on the ledger*, Provo, Sovrin Foundation, 2018, 2.

te verifiëren.[132] Het claimsysteem van SOVRIN wordt hierna verder besproken. Door de reikwijdte van een DID te beperken tot een specifieke betrokkene-gegevensontvanger-relatie, heeft het voor hackers weinig nut een specifieke DID te stelen en is de impact van diefstal beperkt.[133] Dat bevordert de veiligheid van een digitale identiteit. Een nadeel hiervan is het probleem van het opvolgen van verschillende DID's en de tijds- en moeitekosten die daaraan verbonden zijn voor de betrokkene. Dat werd ook aangehaald in Hoofdstuk II, bij de aangepaste versie van het blockchainmodel.

In de technische *Whitepaper*[134] van SOVRIN staat verder beschreven welke rol de betrokkene inneemt in het project. Ten eerste is de belangrijkste taak van de betrokkene om hun *private key*, die digitale identiteit kunnen decrypteren, veilig te bewaren. Speciaal aan de *private keys* in het SOVRIN systeem is dat ze onafhankelijk zijn van een bepaald computerbesturingssysteem en zelfs onafhankelijk van het SOVRIN project zelf. Een heel belangrijke factor in het Sovrin project is het claimsysteem, dat de controle door de betrokkene moet bewerkstelligen. Sovrin definieert een claim als "a statement that one identity owner, such as a person or organization, makes about itself or another identity owner"[135]. De claims kunnen uitgaan van de betrokkene, die bijvoorbeeld zijn of haar naam wil bekendmaken aan de gegevensontvanger, of van een overheid die bijvoorbeeld een geldig rijbewijs van de betrokkene kan bevestigen. SOVRIN maakt een onderscheid tussen twee soorten claims. Enerzijds zijn er de publieke claims die op de *ledger* komen en waarvan SOVRIN stelt dat ze geen persoonsgegevens mogen bevatten zoals publiek beschikbare informatie van een overheidsidentiteit, en anderzijds zijn er private claims waar persoonsgegevens aan te pas komen maar die niet zichtbaar zijn op de *ledger*. Het project gaat dus uit van *off-chain* opslag van persoonsgegevens. Belangrijk hierbij is dat de betrokkene toestemming moet geven wanneer de gegevensontvanger bepaalde persoonsgegevens-gerelateerde informatie wenst, waardoor de betrokkene op die manier controle heeft. Die toestemming voor de verwerking van persoonsgegevens door de gegevensontvanger is specifiek

[132] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised Trust,* Provo, Sovrin Foundation, 2018, 21.
[133] *Ibid.*
[134] SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 25 p.
[135] *Ibid.*, 20.

gelinkt aan een bepaald doel, en komt op *ledger* onder gehashte vorm. De *hash* zelf bevat geen verdere informatie over de toestemming of de persoonsgegevens waarop ze betrekking heeft.[136]

AFDELING II. OPPORTUNITEITEN VAN SOVRIN VOOR DE RECHTEN VAN DE BETROKKENE

35. **NALEVING VAN DE AVG –** In verschillende documenten verwijst SOVRIN naar haar bedoeling om de bepalingen van de AVG na te leven in haar project.[137] Het vertrekt van de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen uit art. 25 AVG, zowel voor de *nodes* die het redelijk mogelijke moeten doen om die beginselen na te leven als in de algemene *Whitepaper* waarin het stelt dat die beginselen een mogelijkheid zijn om een netwerk-effect te creëren bij de gebruikers van het systeem.[138]

36. **HET RECHT OP INFORMATIE EN TRANSPARANTIE –** Een eerste voordeel van het SOVRIN project voor de rechten van de betrokkene ligt in het recht op informatie en transparantie uit artt. 12-14 AVG. Zoals aangegeven in de algemene bespreking van die rechten uit Hoofdstuk II, zou blockchaintechnologie het mogelijk moeten maken dat de betrokkene zelf bepaalt welke persoonsgegevens van hem of haar verwerkt worden en voor welke doelstellingen doordat de betrokkene zelf zijn geheel van persoonsgegevens samenstelt en zelf de toestemming geeft voor gegevensverwerking voor bepaalde doelstellingen. Daar gaat het project ook vanuit: de betrokkene maakt zelf zijn of haar geheel van persoonsgegevens.[139] Daarnaast bepaalt de betrokkene zelf wie de persoonsgegevens mag verwerken en voor welke doelstellingen, door

---

[136] Alinea gebaseerd op: SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 20-21; P. WINDLEY, "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml*.

[137] SOVRIN FO1UNDATION, "Sovrin governance framework V2 master document", Provo, 31 oktober 2018, laatst geraadpleegd op 15 maart 2019, *https://docs.google.com/document/d/1WqUOqdTBc3JACIlRviJoWJRcJHTNTNzk9_As9v-jwrY/edit*; SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust,* Provo, Sovrin Foundation, 2018, 20; SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 21.

[138] SOVRIN FOUNDATION, "Sovrin governance framework V2 master document", Provo, 31 oktober 2018, laatst geraadpleegd op 15 maart 2019, *https://docs.google.com/document/d/1WqUOqdTBc3JACIlRviJoWJRcJHTNTNzk9_As9v-jwrY/edit*; SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust,* Provo, Sovrin Foundation, 2018, 20.

[139] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust,* Provo, Sovrin Foundation, 2018, 10; P. WINDLEY, "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml*.

middel van toestemming die onder gehashte vorm op de *ledger* van de blockchain staat.[140] Dat moet tegelijkertijd ook leiden tot transparantie wanneer de betrokkene zijn *private key* gebruikt om de gehashte toestemming te decrypteren.

37. **RECHT OP INZAGE –** Het faciliteren van het recht op inzage van de betrokkene uit art. 15 AVG vormt het tweede voordeel van het SOVRIN project. Vooreerst heeft de betrokkene, via haar toestemming, de mogelijkheid om te bepalen wie zijn of haar persoonsgegevens mag verwerken en voor welke doelstellingen, maar de betrokkene kan ook haar toestemming intrekken en de specifieke DID verwijderen zodat geen relatie meer bestaat tussen de betrokkene en een specifieke gegevensontvanger.[141] Op die manier bepaalt de betrokkene zelf wie machtiging heeft om zijn persoonsgegevens te verwerken en weet dus wie er bijgevolg inzage heeft. Specifiek voor SOVRIN is de *permissioned* aard van de blockchain zoals in vorige Afdeling besproken.[142] Aangezien SOVRIN de centrale entiteit is die de *nodes* aanduidt, zal het de essentiële elementen van de middelen van de gegevensverwerking bepalen en op die manier verwerkingsverantwoordelijke zijn, waardoor de betrokkene een aanspreekpunt heeft om zijn recht van inzage uit art. 15 AVG uit te oefenen.

38. **RECHT OP RECTIFICATIE –** Het derde voordeel dat het project biedt is terug te vinden in het faciliteren van het recht op rectificatie uit art. 16 AVG. Ondanks de onveranderbare aard van gegevens die op de *ledger* van de blockchain staan, kan de betrokkene zelf ten eerste zelf zijn geheel van persoonsgegevens bepalen waardoor de kans op onjuiste gegevens verkleint. Bovendien gaat het bij SOVRIN om *off-chain* opslag van persoonsgegevens, met enkel een *hash* die de toestemming van de verwerking van die persoonsgegevens vertegenwoordigt op de *ledger*

---

[140] SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 21; P. WINDLEY, "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml.*

[141] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 21; P. WINDLEY, "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml*.

[142] SOVRIN FOUNDATION, "Sovrin governance framework V2 master document", Provo, 31 oktober 2018, laatst geraadpleegd op 15 maart 2019, *https://docs.google.com/document/d/1WqUOqdTBc3JACIlRviJoWJRcJHTNTNzk9_As9v-jwrY/edit*; SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 16; SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 21; P. WINDLEY, "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml*.

van de blockchain.[143] Zoals in de eerste Afdeling van Hoofdstuk III aan bod komt, zou de verbetering van persoonsgegevens of het verwijderen van onjuiste gegevens in de *private ledger* van de betrokkene tot gevolg hebben dat de *hash* verwijst naar onbestaande gegevens, zodat op die manier het recht op rectificatie vereenvoudigd wordt voor de betrokkene omdat hij zelf controle heeft over de digitale identiteit in de *private ledger*.[144]

39. **RECHT OP OVERDRAAGBAARHEID VAN GEGEVENS –** Een bijzondere mogelijkheid biedt zich aan in het SOVRIN project, die niet aan bod kwam bij de algemene bespreking van de voordelen van blockchaintechnologie voor de rechten van de betrokkene: facilitering van het recht op overdraagbaarheid van gegevens uit art. 22 AVG. Het doel van het project is het creëren van een digitale identiteit voor de betrokkene die hij of zij zelf controleert, zonder afhankelijk te zijn van een bepaald blockchainplatform of centrale entiteit.[145] Dankzij de onafhankelijkheid van de HYPERLEDGER INDY blockchain en het feit dat DID's gekoppeld zijn aan een persoon en niet aan een centrale entiteit,[146] kan gesteld worden dat het project het recht op overdraagbaarheid van gegevens faciliteert.

AFDELING III. HET RECHT OP GEGEVENSWISSING EN DE POSITIE VAN DE VERWERKINGSVERANTWOORDELIJKE VERSUS HET SOVRIN PROJECT

40. **RECHT OP GEGEVENSWISSING –** Het eerste conformiteitsprobleem van blockchaintechnologie met de bepalingen uit de AVG is het recht op gegevenswissing uit art. 22 AVG. In Hoofdstuk III komen verschillende oplossingen voor dat probleem aan bod, waaronder het *off-chain* opslaan van persoonsgegevens. In dat geval leidt het verwijderen van persoonsgegevens uit bv. een applicatie die die persoonsgegevens verzamelt ertoe dat de *hash* die naar die persoonsgegevens verwijst louter verwijst naar verwijderde gegevens.[147] Dat zorgt er op die manier voor dat aan het recht op gegevenswissing van de betrokkene uit art. 22 AVG voldaan is, analoog aan de redenering m.b.t. het recht op rectificatie uit de vorige Afdeling. SOVRIN voorziet in die

---

[143] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised Trust*, Provo, Sovrin Foundation, 2018, 22.

[144] C. LIMA, "How decentralised blockchain internet will comply with GDPR data privacy*"*, X, juni 2018, laatst geraadpleegd op 21 maart 2019, *https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf*; E. PISCINI, D. DALTON en L. KEHOE, *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 7.

[145] E. PISCINI, D. DALTON en L. KEHOE, *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 13-16.

[146] *Ibid.*, 10.

[147] C. LIMA, "How decentralised blockchain internet will comply with GDPR data privacy*"*, X, juni 2018, laatst geraadpleegd op 21 maart 2019, *https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf*; E. PISCINI, D. DALTON en L. KEHOE, *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 7.

functionaliteit: de persoonsgegevens staan *off-chain* opgeslagen in de *private ledger* van de betrokkene, die zijn of haar digitale identiteit vertegenwoordigt.[148] Enkel een *hash* die de toestemming van de betrokkene vertegenwoordigt en de geëncrypteerde *public key* staan op de *public ledger*.[149] Wanneer de betrokkene dan gegevens uit zijn *private ledger* verwijdert, zal de *hash* louter naar verwijderde persoonsgegevens verwijzen,waarbij de geëncrypteerde *public key* geen waarde heeft zonder gebruik door de betrokkene. Op die manier voldoet het SOVRIN project aan het recht op gegevenswissing.

41. **POSITIE VAN DE VERWERKINGSVERANTWOORDELIJKE** – De positie van de verwerkingsverantwoordelijke is het tweede geanalyseerde probleem in Hoofdstuk III. SOVRIN biedt ook voor dat probleem een oplossing: het project biedt een *permissioned* blockchain[150] aan, waardoor SOVRIN zelf, als centrale entiteit die de essentiële elementen van de middelen bepaalt, de positie van verwerkingsverantwoordelijke kan innemen. De betrokkene zal zelf het doel van de verwerking bepalen door middel van zijn toestemming. Die duidelijke rolverdeling biedt de mogelijkheid voor de betrokkene om zijn rechten op een diligente manier af te dwingen.

AFDELING IV. TUSSENBESLUIT

42. In dit Hoofdstuk is een *case-study* gemaakt van het SOVRIN project, om de observeringen uit vorige Hoofdstukken aan de realiteit te toetsen. Eerst volgde een beschrijving van het doel van het project en haar functionaliteiten. Belangrijk was daar het doel om de betrokkene controle te geven over een verifieerbare digitale identiteit en de *permissioned* aard van de door SOVRIN gebruikte blockchain. Vervolgens kwamen de voordelen van het project voor de rechten van de betrokkene aan bod. De voordelen voor de rechten van de betrokkene uit Hoofdstuk II spelen ook in het project, maar daarnaast biedt SOVRIN ook een mogelijkheid voor de facilitering van het

---

[148] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised Trust,* Provo, Sovrin Foundation, 2018, 22; SOVRIN FOUNDATION, *Sovrin: what goes on the ledger,* Provo, Sovrin Foundation, 2018, 10-11.

[149] SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 22; SOVRIN FOUNDATION, *Sovrin: what goes on the ledger*, Provo, Sovrin Foundation, 2018, 10-11; SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 21.

[150] SOVRIN FOUNDATION, "Sovrin governance framework V2 master document", Provo, 31 oktober 2018, laatst geraadpleegd op 15 maart 2019, *https://docs.google.com/document/d/1WqUOqdTBc3JACIlRviJoWJRcJHTNTNzk9_As9v-jwrY/edit*; SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 16; SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 21; P. WINDLEY, "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml*.

recht op overdraagbaarheid van gegevens uit art. 20 AVG. Ten slotte werd kort gekeken naar de verhouding tussen de geanalyseerde problemen uit het derde Hoofdstuk en de manier waarop SOVRIN daarmee omgaat. Twee krachtlijnen zijn daar op te merken: naleving van het recht op gegevenswissing dankzij *off-chain* opslag van persoonsgegevens, en SOVRIN als verwerkingsverantwoordelijke door de *permissioned* aard van de gebruikte blockchain. In volgend Hoofdstuk volgt een evaluatie van de observaties uit vorige Hoofdstukken en een normatieve kijk op de probleemstelling van dit onderzoek.

HOOFDSTUK IV. EVALUATIEVE EN NORMATIEVE BENADERING VAN BLOCKCHAINTECHNOLOGIE VOOR DE CONTROLE DOOR DE BETROKKENE

43. Dit onderzoek zal afsluiten met een evaluatie van de observaties uit vorige Hoofdstukken, waarna op een normatieve manier de probleemstelling vergeleken wordt met die analyse. De bedoeling is uiteindelijk een finaal antwoord te kunnen geven op de centrale onderzoeksvraag.

44. **EVALUATIEFACTOREN –** Hoofdstuk II van dit onderzoek brengt drie voordelen aan het licht met betrekking tot de relatie tussen blockchaintechnologie en de rechten van de betrokkene, die de controle door de betrokkene over diens persoonsgegevens moet faciliteren zoals gezien in Hoofdstuk I. De technologie helpt ten eerste bij de rechten op informatie en transparantie uit artt. 12 en 14 AVG. Ten tweede faciliteert de technologie het recht op inzage uit art. 15 AVG. Ten slotte vergemakkelijkt het ook het recht op rectificatie uit art. 16 *io.* 19 AVG, doordat de toevoeging van correcte gegevens de foute gegevens op de *public ledger* kunnen verbeteren. In Hoofdstuk II kwamen ook twee conformiteitsproblemen van blockchaintechnologie met de AVG aan bod: het recht op gegevenswissing uit art. 22 AVG en de positie van de verwerkingsverantwoordelijke. Het onderzoek duidt toch op mogelijke oplossingen voor die problematiek, dankzij technische of juridisch-creatieve middelen. Het SOVRIN project toont diezelfde insteek. Het biedt het naast de algemene voordelen uiteengezet in het tweede Hoofdstuk, ook de mogelijkheid om het recht op overdraagbaarheid van persoonsgegevens uit art. 22 AVG uit te oefenen.

45. **EVALUATIE –** Een afweging van de voor- en nadelen van blockchaintechnologie voor de rechten van de betrokkene en de daarmee gepaard gaande controle over diens persoonsgegevens, lijkt eerder positief. De technologie biedt mogelijkheden voor de controle, zowel op theoretisch vlak

als in de realiteit zoals werd aangetoond met de *case-study* van het SOVRIN project. De conformiteitsproblemen van de technologie met de bepalingen van de AVG kennen mogelijke oplossingen, waardoor dat als negatieve factor enige nuance verdient.

Er zijn echter ook caveats: ten eerste is dit onderzoek te beperkt om een volledig beeld te geven van alle mogelijke problemen die denkbaar zijn bij de conformiteit van blockchaintechnologie met de AVG of andere wetgevende bepalingen die van toepassing kunnen zijn op het probleem. Het tweede caveat, dat voor de praktijk veel belangrijker is, is de vraag naar het gebruik van blockchaintechnologie. 2017 was het jaar van de grote hype rond blockchaintechnologie, maar in 2018 kwamen de problemen en het gebrek aan gebruik ervan meer en meer op de voorgrond.[151] Toch moeten we hierin genuanceerd zijn: hoewel blockchaintechnologie problemen kent, waaronder die vastgesteld in dit onderzoek, mogen ze innovatie niet hinderen. Ook het gebrek aan gebruik van blockchaintechnologie mag niet overdreven worden. Vandaag zijn talloze voorbeelden van blockchaingebruik in verschillende sectoren van de economie, zoals Ripple en R3 die blockchain gebruiken in de financiële wereld en IBM in de supply chain naast SOVRIN die het gebruikt voor digitale identiteiten.[152] Hopelijk kan 2019 het jaar blijken van het geïnformeerde debat over de technologie.

Die caveats in rekening genomen, is de evaluatie van de technologie in de facilitering van de doelstelling uit Rechtsoverweging (7) AVG positief op basis van de observaties van dit onderzoek. De analyse uit dit onderzoek duidt op een positief antwoord op de centrale onderzoeksvraag, namelijk is het gebruik van blockchaintechnologie opportuun voor controle door de betrokkene over zijn persoonsgegevens, in het licht van de Algemene Verordening Gegevensbescherming. Ook het EU BLOCKCHAIN OBSERVATORY AND FORUM

---

[151] G. ZYSKIND, "2018: when privacy and decentralization collided", New York, 8 januari 2019, laatst geraadpleegd op 17 maart 2019, *https://www.coindesk.com/2018-when-privacy-and-decentralization-collided*.

[152] V. DALMACIO POSADAS, "The internet of things: the GDPR and the blockchain may be incompatible", *Journal of Internet Law* 2017-18, afl. 11 (21) 23; D. DE JONGHE en V. I. LAAN, "Blockchain in de realiteit", *Computerrecht* 2017, (251) 253-254; EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain innovation in europe*, Brussel, EU Blockchain Observatory and Forum, 2018, 10-11; B. MARR, "30+ real examples of blockchain technology in practice", Jersey City, 14 mei 2018, laatst geraadpleegd op 17 maart 2019, *https://www.forbes.com/sites/gradsoflife/2019/03/04/to-end-the-ever-growing-skills-gap-employers-must-change-their-outdated-hiring-practices/#44329de62d16*; J. OLLY, "Is it possible to comply with GDPR using blockchain?" *International Financial Law Review* 2 mei 2018, 1; H. TREIBLMAIER en R. BECK, *Business transformation through blockchain*, II, Cham, Springer, 2019, xxviii + 362.

identificeert blockchaintechnologie als mogelijkheid om die doelstelling van de AVG te verwezenlijken.[153]

46. **NORMATIEF –** Hier volgt een korte opsomming van *best practices* voor blockchainontwikkelaars in het licht van de AVG en de controle door de betrokkene. Het eerste belangrijke aandachtspunt is de gebruiksvriendelijkheid van het systeem voor de betrokkene. Tijdrovende en veeleisende systemen bemoeilijken diligente controle door de betrokkene. Een gecentraliseerde identiteitsapplicatie is daarom aangewezen, waarop verschillende diensten kunnen inloggen en om toegangsmachtiging vragen. Het tweede belangrijke aandachtspunt is *off-chain* opslag van persoonsgegevens en met daaraan gekoppeld loutere verwijzing naar de persoonsgegevens door een *hash* op de blockchain. Het verwijderen van de *off-chain* opgeslagen gegevens leidt er dan toe dat de publiek zichtbare *hash* louter verwijst naar verwijderde gegevens, wat het recht op gegevenswissing uit art. 17 AVG in een blockchaincontext mogelijk maakt. Ten derde is het aangewezen om een *permissioned* blockchain te gebruiken wanneer het de bedoeling is om persoonsgegevens te verwerken. Dat resulteert in een duidelijke rolverdeling waarbij de centrale entiteit verwerkingsverantwoordelijke is en als aanspreekpunt voor de betrokkene kan dienen voor de uitoefening van diens rechten. Ten slotte is een vierde aandachtspunt de facilitering van het recht op overdraagbaarheid van gegevens uit art. 22 AVG. Het blockchainproject zou moeten voorzien in de mogelijkheid voor de betrokkene om zijn (geheel van) persoonsgegevens, zonder enige moeilijkheden, over te dragen naar een ander platform.

[153] EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain innovation in europe*, Brussel, EU Blockchain Observatory and Forum, 2018, 17.

BESLUIT

47. Dit onderzoek gaat over de vraag of het gebruik van blockchaintechnologie opportuun is voor de controle door de betrokkene over diens persoonsgegevens, in het licht van de Algemene Verordening Gegevensbescherming. Het eerste Hoofdstuk geeft een beschrijving van de belangrijkste begrippen en het juridisch kader voor deze scriptie. Hoofdstuk II maakt een analyse van de opportuniteiten en moeilijkheden van blockchaintechnologie voor de doelstelling van controle over persoonsgegevens uit de AVG. Zowel op technisch als op juridisch vlak brengt blockchaintechnologie mogelijkheden met zich mee voor de controle door de betrokkene. Twee moeilijkheden komen aan bod: het recht op gegevenswissing en de positie van de verwerkingsverantwoordelijke. Beiden kennen een genuanceerde oplossing, via technische of juridische creativiteit. Het derde Hoofdstuk maakt een *case-study* van het SOVRIN project om de praktijk aan de theorie te toetsen. De praktijk toont gelijkaardige conclusies als de theorie, hoewel niet altijd via dezelfde middelen. Het laatste Hoofdstuk maakt een vergelijking tussen de mogelijkheden die blockchaintechnologie biedt voor de controle door de betrokkene en de conformiteitsproblemen met de AVG. Daar zien we dat de evaluatie positief is, maar gelet op de beperkte omvang van dit onderzoek en de jonge technologie moet de toekomst raad brengen. Het laatste Hoofdstuk biedt ook een aantal *best practices* voor blockchainontwikkelaars voor de facilitering van de controle door betrokkene. Als conclusie kent de centrale onderzoeksvraag een positief antwoord op basis van dit onderzoek, namelijk dat het gebruik van blockchaintechnologie opportuun is voor controle door de betrokkene over zijn persoonsgegevens in het licht van de Algemene Verordening Gegevensbescherming.

BIBLIOGRAFIE

WETGEVING

Art. 8 EVRM.

Art. 8 Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981, *BS* 30 december 1993, 29.024.

Art. 8 Handvest van de grondrechten van de europese unie, *Pb. L.* 26 oktober 2012, afl. 326, 391.

Art. 1, 11, lid 2 VEU.

Artt. 15, 16 VWEU.

Richtlijn 95/46/EG van het europees parlement en de raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb. L.* 23 november 1995, afl. 281, p. 31.

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), *Pb. L.* 27 april 2016, afl. 119, 1.

Aanbevelingen van de EDPS betreffende de opties van de EU voor hervorming van de gegevensbescherming, *Pb. L.* 12 september 2015, afl. 301, 1.

Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.

Art. 280 Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018, 68616.

RECHTSPRAAK

EHRM 7 juli 1989, nr. 10454/83, ECLI:CE:ECHR:1989:0707JUD001045483, Gaskin/Verenigd Koninkrijk.

EHRM 13 februari 2003, nr. 42326/98, ECLI:CE:ECHR:2003:0213JUD004232698, Odièvre/Frankrijk.

EHRM 28 april 2009, nr. 32881/04, ECLI:CE:ECHR:2009:0428JUD003288104, K.H. e.a./Slovakije.

EHRM 25 september 2012, nr. 3783/09, ECLI:CE:ECHR:2012:0925JUD003378309, Godelli/Italië.

HvJ 6 november 2003, C-101/01, ECLI:EU:C:2003:596, Bodil Lindqvist.

HvJ 13 mei 2014, nr. C-131/12, ECLI:EU:C:2014:317, Google Spain.

RECHTSLEER

Boeken en dergelijken

BACON, MICHELS, J. D., MILLARD, C. en SINGH, J., *Blockchain demistified*, Londen, Queen Mary University of London, 2017, 53 p.

CHANG, H., *Blockchain: disrupting data protection?*, Hong Kong, University of Hong Kong Faculty of Law Research, 2017, 5 p.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain,* Parijs, Commission Nationale de l'Informatique et des Libertés, 2018, 11 p.

DRESCHER, D., *Blockchain basics: a non-technical introduction in 25 Steps*, Frankfurt am Main, Apress, 2017, 255 p.

EDPS ETHICS ADVISORY GROUP, *Report 2018*, Brussel, Edit Directorate, 2018, 36 p.

EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, Brussel, EU Blockchain Observatory and Forum, 2018, 36 p.

EU BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain innovation in europe*, Brussel, EU Blockchain Observatory and Forum, 2018, 25 p.

EUROPEAN DATA PROTECTION SUPERVISOR, *Annual report 2016*, Luxemburg, Publications Office of the European Union, 2017, 73 p.

EUROPEAN DATA PROTECTION SUPERVISOR, *Annual report 2017*, Luxemburg, Publications Office of the European Union, 2017, 84 p.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on european data protection law*, Luxemburg, Publications Office of the European Union, 2018, 397 p.

IBÁÑEZ, D., O'HARA, K. en SIMPERL, E., *On blockchains and the general data protection regulation*, Southampton, University of Southampton, 2018, *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*.

LIMA, C., "How decentralised blockchain internet will comply with GDPR data privacy*"*, X, juni 2018, laatst geraadpleegd op 21 maart 2019, *https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf*.

LYNSKEY, O., *The foundations of EU data protection law*, New York, Oxford University Press, 2015, xxiv + 307 p.

MAXWELL, W. en SALMON, J., *A guide to blockchain*, Brussel, Hogan Lovells LLP, 2017, 24 p.

PISCINI, E., DALTON, D. en KEHOE, L., *Blockchain & cybersecurity. Let's discuss*, Dublin, Deloitte, 2017, 14 p.

SAVIN, A., *EU internet law*, Cheltenham, Edward Elgar Publishing, 2017, 360 p.

SCHRIER, D., WU, W. en PENTLAND, A., *Blockchain & infrastructure (identity, data security*), Massachusetts, Massachusetts Institute of Technology, 2016, 19 p.

SIMAL, J., *Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR*, onuitg. masterproef Rechten KU Leuven, vii + 58 p.

SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 42 p.

SUSTRONCK, O., *Praktijkboek internetrecht*, Mechelen, Wolters Kluwer, 2017, 235 p.

TREIBLMAIER, H. en BECK, R., *Business transformation through blockchain*, II, Cham, Springer, 2019, xxviii + 362.

VANDERDONCKT, L., *Decentralising the GDPR: an analysis of distributed ledger technology against ratio legis of the GDPR*, onuitg. masterproef rechten KU Leuven, 2018, vi + 51 p.

WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Guidelines on the implementation of the court of justice of the european union judgement on "Google Spain and INC v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, 26 november 2014, 14/EN WP 225, 20 p.

WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Opinion 01/2010 on the concepts of "controller" and "processor"*, 6 februari 2010, 00264/10/EN WP 169, 33 p.

WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Opinion 05/2014 on anonymisation techniques*, 10 april 2014, 0829/14/EN WP 216, 5.

WERKGROEP GEGEVENSBESCHERMING ART.29 (WP29), *Richtsnoeren inzake transparantie overeenkomstig verordening 2016/679*, 29 november 2017, 17/NL WP 260, 47 p.

WIRTH, C. en KOLAIN, M., *Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data*, Amsterdam, European Society for Socially Embedded Technologies, 2018, 7 p.

XU, X., WEBER, I. en STAPLES, M., *Architecture for blockchain applications*, Cham, Springer, 2019, xxii + 305 p.

Tijdschriftartikels

ALBRECHT, J. P., "How the GDPR will change the world", *European Data Protection Law Review* 2016, 287-289.

BERBERICH, M. en STEINER, M. “Blockchain technology and the GDPR – how to reconcile privacy and distributed ledgers”, *European Union Data Protection Law Review* 2016, 422-426.

DALMACIO POSADAS, V., “The internet of things: the GDPR and the blockchain may be incompatible”, *Journal of Internet Law* 2017-18, afl. 11, 21-29.

DE JONGHE, D. en LAAN, V. I., “Blockchain in de realiteit”, *Computerrecht* 2017, 251-260.

FINCK, M., “Blockchains and data protection in the european union”, *European Data Protection Law Review* 2017, 17-35.

FINCK, M., “Blockchains: regulating the unknown”, *German Law Journal* 2018, 665-686.

HERIAN, R., “Regulating disruption: blockchain, GDPR, and questions of data sovereignty” *Journal of Internet Law* 2018-19, afl. 2, 7-16.

HRISTOV, P. en DIMITROV, W., “The blockchain as a backbone of GDPR compliant frameworks”, *Quality-access to success* 2019, 305-310.

JO PESCH, P. en SILLABER, S., “Distributed ledger, joint control? – Blockchain and the GDPR’s transparency requirements” *Computer Law Review International* 2017, 166-172.

KROEKS-DE RAAIJ, C.C.M., WESTERDIJK, R.J.J., en ZWENNE, G.J., “De algemene verordening gegevensbescherming”, *Tijdschrift voor Internetrecht* 2016, 50-58.

LAAN, V. I. en RUTJES, A., “Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?”, *Computerrecht* 2017, 253-263.

MARIËN, S., “Blockchain en GDPR op ramkoers?”, *datanews* 2018, 32-35.

MILLARD, C., “Blockchain and law: incompatible codes?*”, Computer Law & Security Review* 2018, 843-846.

MOEREL, L., “Blockchain & data protection … and why they are not on a collision course, *European Review of Private Law* 2019, 825-851.

NOFER, M., GOMBER, P., HINZ, O. en SCHIERECK, D., “Blockchain”, *Business & Information Systems Engineering* 2017, 183-187.

OLLY, J., “Is it possible to comply with GDPR using blockchain?” *International Financial Law Review* 2 mei 2018, 1-2

POULLET, Y. en JACQUEMIN, H., “Blockchain: une révolution pour le droit?” *JT* 2018, (801) 808-809.

VAN DE MEULEBROUCKE, A., “De algemene verordening gegevensbescherming”, *RW* 2015, 1562.

VERHELST, E. W., "Blockchain aan de ketting van de algemene verordening gegevensbescherming?", *Privacy & informatie* 2017, 17-23.

ZETZSCHE, D., BUCKLEY, R., en ARNER, D., "The distributed liability of distributed ledgers: legal risks of blockchain", *University of Illinois Law Review* 2018, 1361-1406.

ZYSKIND, G., NATHAN, O. en PENTLAND, A., "Decentralising privacy: using blockchain to protect personal data", *Security and Privacy Workshops* 2015, 180-184.

Internetartikels en blogs

ARCHER SOFT, "The right to be forgotten (GDPR) vs blockchain technology, New York, 7 juni 2018, laatst geraadpleegd op 26 november 2018, *http://www.archer-soft.com/en/blog/right-be-forgotten-gdpr-vs-blockchain-technology*.

AUTORITEIT PERSOONSGEGEVENS, "Controle over je data", Den Haag, 2018, laatst geraadpleegd op 1 november 2018, *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/controle-over-je-data*.

BLOCKCHAINHUB, "Identity as a bottleneck for blockchain, Berlijn, 17 oktober 2017, laatst geraadpleegd op 2 november 2018, *https://blockchainhub.net/blog/blog/decentralized-identity-blockchain/*.

BURCHETT, C., "How to fight the coming quantum decryption threat", San Diego, 12 juli 2018, laatst geraadpleegd op 9 april 2019, *https://www.enterprisetech.com/2018/07/12/how-to-fight-the-coming-quantum-data-decryption-threat/*.

CALLAHAN, M. A., "How blockchain can be used to secure sensitive data storage", State City, 7 november 2017, laatst geraadpleegd op 30 oktober 2018, *http://www.dataversity.net/blockchain-can-used-secure-sensitive-data-storage/*.

COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, "Duiding bij de privacywet", Brussel, 2018, laatst geraadpleegd op 27 maart 2018, *https://www.privacycommission.be/nl/duiding-bij-de-privacywet*.

CZARNECKI, J., "Blockchain and personal data protection regulations explained", New York, 26 april 2017, laatst geraadpleegd op 22 november 2018, *https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained*.

EUR-LEX, "Document 32016R0679", Brussel, s.d., laatst geraadpleegd op 6 februari 2019, *https://eur-lex.europa.eu/legal-content/NL/HIS/?uri=celex:32016R0679*.

GEGEVENSBESCHERMINGSAUTORITEIT, “Behoud de controle over jouw gegevens!”, Brussel, 2018, laatst geraadpleegd op 21 november 2018, *https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-burger*.

JENSEN, G., “Reconciling GDPR rightbs to erasure and rectification of personal data to blockchain”, Californië, 16 juli 2018, laatst geraadpleegd op 17 november 2018, *https://blogs.oracle.com/cloudsecurity/reconciling-gdpr-rights-to-erasure-and-rectification-of-personal-data-with-blockchain*.

MEYER, D. “Blockchain technology is on a collision course with EU privacy law, Porthsmouth, 27 februari 2018, laatst geraadpleegd op 11 november 2018, *https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/*.

Andere

DUTCH LAW ENCYCLOPEDIC DICTIONARY, “Encryptie”, X, 2018, laatst geraadpleegd op 9 april 2019, *https://www.juridischwoordenboek.nl/zoek/encryptie*.

EUROPESE COMMISSIE, “Blockchain technologies”, Brussel, 2018, laatst geraadpleegd op 11 maart 2019, *https://ec.europa.eu/digital-single-market/en/blockchain-technologies*.

FRANKENFIELD, J., “Off-chain transactions (cryptocurrency)”, New York City, 10 april 2018, laatst geraadpleegd op 9 april 2019, *https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp*.

HUYGHEBAERT, P., “Groot Facebooklek: bedrijf van bannon maakte gegevens van 50 miljoen mensen buit”, Brussel, 17 maart 2018, laatst geraadpleegd op 24 maart 2018, *https://www.vrt.be/vrtnws/nl/2018/03/17/facebook--schorst--bedrijf-cambridge-analytica-dat-voor-trump-ca/*.

LEE, T.B., “Facebook’s cambridge analytica scandal, explained”, Californië, 20 maart 2018, laatst geraadpleegd op 22 maart 2018, *https://arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained/*.

MARR, B., “30+ real examples of blockchain technology in practice”, Jersey City, 14 mei 2018, laatst geraadpleegd op 17 maart 2019, *https://www.forbes.com/sites/gradsoflife/2019/03/04/to-end-the-ever-growing-skills-gap-employers-must-change-their-outdated-hiring-practices/#44329de62d16*

MEYER, R. “My facebook was breached by cambridge analytica. Was yours?”, Washington D.C., 10 april 2018, laatst geraadpleegd op 30 april 2018,

https://www.theatlantic.com/technology/archive/2018/04/facebook-cambridge-analytica-victims/557648/.

SOVRIN FOUNDATION, "Sovrin governance framework V2 master document", Provo, 31 oktober 2018, laatst geraadpleegd op 15 maart 2019, *https://docs.google.com/document/d/1WqUOqdTBc3JACIlRviJoWJRcJHTNTNzk9_As9v-jwrY/edit*.

SOVRIN FOUNDATION, *Sovrin: a protocol and token for self-sovereign identity and decentralised trust*, Provo, Sovrin Foundation, 2018, 42 p.

SOVRIN FOUNDATION, *The technical foundations of sovrin*, Provo, Sovrin Foundation, 2016, 25 p.

SOVRIN FOUNDATION, *Sovrin: what goes on the ledger*, Provo, Sovrin Foundation, 2018, 11 p.

VAN DALE UITGEVERS, "Controle", Utrecht, 2018, laatst geraadpleegd op 1 november 2018, *https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/controle#.W9sXI5NKhPY*.

WINDLEY, P., "How sovrin works", 3 oktober 2016, laatst geraadpleegd op 15 maart 2019, *http://www.windley.com/archives/2016/10/how_sovrin_works.shtml*.

ZYSKIND, G., "2018: When privacy and decentralization collided", New York, 8 januari 2019, laatst geraadpleegd op 17 maart 2019, *https://www.coindesk.com/2018-when-privacy-and-decentralization-collided*.