UHASSELT
KNOWLEDGE IN ACTION

KU LEUVEN

Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

Blockchain en GDPR

Nathalie Cornelis

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Ken ANDRIES

2022
2023

De transnationale Universiteit Limburg is een uniek samenwerkingsverband van twee universiteiten in twee landen: de Universiteit Hasselt en Maastricht University.

UHASSELT
KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

Faculteit Rechten

master in de rechten

Masterthesis

Blockchain en GDPR

Nathalie Cornelis

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Ken ANDRIES

Samenvatting

Deze masterscriptie onderzoekt het belang van persoonsgegevensbescherming en de uitdagingen en kansen die de blockchaintechnologie in dit kader biedt. Gegevensbeheer heeft een donkere historische achtergrond, met name tijdens de Tweede Wereldoorlog toen de gegevens van Joden werden bijgehouden en misbruikt. De snel evoluerende digitale maatschappij en de globalisering zorgen ervoor dat we met z'n allen massaal veel data genereren. *Big data* die ook *big business* zijn met een grote economische waarde. Daarom is het essentieel om negatieve gevolgen te vermijden en het recht op controle en bescherming van persoonsgegevens te waarborgen. De GDPR legt de autonomie voor de controle over diens persoonsgegevens bij het individu zelf.

Het eerste hoofdstuk legt de werking van blockchaintechnologie uit, alsook de toepassingen ervan in de maatschappij. Eveneens wordt de blockchaintechnologie gesitueerd in het recht en kijken we naar de plaats van de technologie in de juridische context. Het belicht de uitdagingen waarmee wet- en regelgevers toekomstig mee geconfronteerd zullen worden.

Het tweede hoofdstuk gaat dieper in op het recht op bescherming van persoonsgegevens zoals vastgelegd in de GDPR en meer in het bijzonder het recht op controle van het individu over zijn persoonsgegevens. Het onderzoekt de verenigbaarheid van blockchaintechnologie met de GDPR en identificeert belangrijke problemen, waaronder het identificeren van de verwerkingsverantwoordelijke, het recht om vergeten te worden, en de strijdigheid met het beginsel van minimale gegevensverwerking en opslagbeperking.

Het derde hoofdstuk verkent hoe blockchaintechnologie meer GDPR-conform kan worden gemaakt. Het suggereert dat er meerdere creatieve, juridische en technische mogelijkheden zijn om blockchains te verenigen met de eisen van de GDPR, waardoor individuen hun recht op controle over hun persoonsgegevens kunnen behouden.

Tot slot wordt de conclusie geformuleerd waarin de centrale onderzoeksvraag beantwoord kan worden. Het veronderstelde spanningsveld tussen blockchain technologie en de GDPR blijkt uiteindelijk een paradox te zijn. Door het gebruik van blockchain technologie kunnen de gegevensbeschermingswaarborgen die de GDPR voorziet nageleefd of zelfs gefaciliteerd worden. Beiden zijn verzoenbaar met elkaar ondanks dat GDPR uitgaat van centraal gegevensbeheer en blockchaintechnologie net decentraal gegevensbeheer behelst. Zo dient het benadrukt dat beide systemen streven naar dezelfde doelen van gegevensbescherming en -privacy, maar verschillende methoden en andere structuren gebruiken om deze te bereiken. Deze scriptie benadrukt het potentieel voor een innovatieve verzoening van deze systemen ten gunste van gegevensbeheer en -bescherming.

Dankwoord

In 2015 verliet ik door omstandigheden de UHasselt zonder masterdiploma, op een zucht van de eindmeet. Ik vatte het werkleven aan, weliswaar niet in de juridische wereld – wel in de medische en transportwereld- en ging steeds vol overtuiging en enthousiasme voor mijn jobs. Ik probeer(de) een meerwaarde te zijn voor de organisatie en de collega's. Dat ik mijn masterdiploma niet had behaald, is altijd al een los eindje geweest dat ik vooral verdrong totdat ik op 1 juli 2021 mijn huidige functie van consulent juridische dienst bij politiezone Limburg Regio Hoofdstad opnam. Wat een TOPJOB! Ik ben enorm dankbaar dat ik zo goed ben terecht gekomen in een dynamische werkomgeving met een arsenaal aan juridische vraagstukken allerhande. Geen enkele dag is hetzelfde op de juridische dienst van PZ LRH! Ik was onmiddellijk weer gebeten door het juridische, leerde zoveel bij en groeide hierdoor ook als mens. Mijn job en collega's gaven me na 7 jaar (eindelijk!) de moed om dat los eindje trachten vast te knopen.

Het was allerminst evident om mijn masteropleiding af te ronden. Het was een moeilijke oefening, in een (academie)jaar waarin alles lijkt samen te vloeien. De combinatie van een nieuw (samen gesteld) gezin, een voltijdse job met regelmatige deadlines, twee opleidingsonderdelen met bijhorende taken, presentaties, voorbereidingen en papers volbrengen, het schrijven van een masterscriptie en een beetje zorgen voor de (schoon) mama's wiens gezondheid even minder was.

Het vroeg doorzettingsvermogen en het offer van mijn sociaal leven maar ondertussen neem ik de laatste horde in de Masteropleiding Rechten waarbij ik aan verschillende mensen een oprecht woord van dank wens te richten.

Vooreerst wens ik prof. dr. Ken Andries te bedanken voor zijn begrip en geduld, zijn heldere inzichten, bijsturing en het delen van zijn vakkennis.

Vervolgens wil ik mijn werkgever PZ LRH en in het bijzonder, aan korpschef Philip Pirard, bedanken voor de stimulans en het duwtje in de goede richting, alsook voor het vertrouwen dat ik elke dag opnieuw krijg.

Uiteraard verdienen mijn mama en Jo ook een warm woord van dank, voor hun steun, hun geloof in mij en na de ontgoocheling van het niet behalen van mijn masterdiploma toch ook de trots dat ik de spreekwoordelijke "bretellen" aantrok om dit losse eindje trachten vast te knopen.

Ook mijn collega's die meeleefden, mijn metekindje Jolien die me voorzag van bemoedigende tekeningen, iedereen die me heeft bijgestaan verdient een dankjewel.

Als laatste maar daarom zeker niet de minste, wil ik mijn vriend Stefaan bedanken. Bedankt om mij altijd dat niveau hoger te tillen, voor je onuitputtelijke positiviteit om mijn +1 te zijn, te fungeren als veilige haven, om mijn onvoorwaardelijke steun en toeverlaat te zijn, voor al je hulp en nalezen, om mijn klankbord en rots in de branding te zijn. Maar ook bedankt om mij te verdragen op mijn aller slechtste (humeurige) momenten en daarover te kunnen kijken.

Graag sluit ik dit dankwoord af met 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."

Nathalie Cornelis

Hasselt, 15 mei 2023

Inhoudsopgave

1. Inleiding: onderzoeksopzet

1.1. Probleemstelling

1. We maakten afgelopen jaren al kennis met *artificial intelligence*, *virtual reality* en verschillende *cryptocurrencies* waarvan de *bitcoins* het best gekend zijn bij het bredere publiek.

2. De technologische vooruitgang zorgt nogmaals voor een nieuw concept in onze samenleving dat niet, of niet volledig door onze bestaande rechtsregels wordt gereguleerd. En zelfs ertegen lijkt in te gaan. De blockchain technologie vindt razendsnel toepassing in onze samenleving en maakt zelfs alsmaar meer deel uit van eenieders dagdagelijks leven. Auteurs Iansiti en Lakhani beweren zelfs in de "Harvard Business Review" dat de blockchain technologie een grondleggende technologie is, vergelijkbaar met die van het internet en de elektriciteitsvoorziening.[1]

3. Een blockchain kan omschreven worden als een digitale werkwijze die het mogelijk maakt om delicate gegevens op een veilige en transparante manier bij te houden. Hierbij wordt de rol van een centrale tussenpersoon die nodig is bij bepaalde handelingen of transacties zoals bijvoorbeeld een bankinstelling, de notaris, een overheid, of dossierbeheerders overgenomen door een gedecentraliseerd netwerk dat handelt op basis van consensus en vertrouwen. Naast het overbodig maken van tussenpersonen kan de blockchain technologie dus ook allerlei commerciële, industriële en praktische processen transparanter maken. Deze transparantie maakt dat fraude plegen een stuk complexer en moeilijker wordt.

4. Aan de blockchain technologie wordt veel potentieel toegeschreven.[2] Als de blockchain technologie haar beloftes waarmaakt, zal ze een grote impact hebben op meerdere domeinen in onze samenleving. Toch zal het nog jaren duren vooraleer de blockchain technologie zich standvastig en effectief in onze maatschappelijke structuren zal wortelen. Krijgt deze nieuwe digitale technologie wel de beleidsaandacht die ze verdient?

5. De snel evoluerende digitale evolutie van onze maatschappij en een steeds meer globaliserende wereld heeft er voor gezorgd dat mensen anders zijn gaan leven. Alles is maar een muisklik of *swipe* veraf. We zijn permanent altijd online en shoppen online met onze smartphone… Hierdoor genereren wij enorme hoeveelheden data. *Big data* die in het huidig maatschappelijk klimaat *big business* zijn. Niet verwonderlijk dat de meest invloedrijke bedrijven op mondiaal vlak momenteel technologiebedrijven zijn zoals Facebook, Apple, Microsoft en Amazon. De vermeende privacy schendingen van Facebook en Cambridge Analytica nog indachtig, waarbij de gegevens van 86 miljoen facebookgebruikers onrechtmatig verzameld zouden zijn.[3] Dit maakt meteen duidelijk dat een krachtig gegevensbeschermingssysteem en het belang van controle door betrokkenen over diens persoonsgegevens noodzakelijk zijn. Hiertoe zal de General Data Protection Regulation (hierna:

[1] M. IANSITI en R. LAKHANI, "The Truth About Blockchain", *Harvard Business Review* 2017, januari-februari 2017, https://hbr.org/2017/01/the-truth-about-blockchain.
[2] B. VUYLSTEKE, "Blockchain - Wat is het? Wat kan het betekenen voor het notariaat?", *T.Not.* 2018, 207; H. JACQUEMIN en Y. POULLET, "Blockchain: une révolution pour le droit?", JT 2018, 803; I. VAN GIEL, S. EGAMBERDIEV en A. APPELMANS, "Blockchain in vastgoedtransacties", *TBO* 2019, nr. 2, 166; M. VAN DE LOOVERBOSCH, "Crypto-effecten: tussen droom en daad", *TRV-RPS* 2018, 195.
[3] P. HUYGHEBAERT, *Groot Facebooklek: bedrijf van Bannon maakte gegevens van 50 miljoen mensen buit*, 2018, www.vrt.be/vrtnws/nl/2018/03/17/facebook--schorst--bedrijf-cambridge-analytica-dat-voor-trump-ca.

GDPR) als waakhond van gegevensbescherming van individuen als uitgangspunt genomen worden voor dit onderzoek. De GDPR beoogt enerzijds om de veiligheid en vertrouwelijkheid van persoonsgegevens te beschermen en de controle van zijn/haar persoonsgegevens aan het individu toe te kennen. Dit onderzoek zal handelen over de relatie tussen blockchaintechnologie en het Europese gegevensbeschermingssysteem.

6. Heikel punt voor de privacyjuristen is of de vele persoonsgegevens die zich in de blockchains bevinden, voldoende gewaarborgd worden door de gegevensbescherming die de GDPR vastlegt.

7. De relevantie van dit onderzoek ligt in de ontwikkelingen van de steeds verdere digitalisering van de maatschappij, waarbij mensen voortdurend met nieuwe digitale concepten worden geconfronteerd en er alsmaar meer data wordt gegenereerd en verwerkt, komen naast nieuwe mogelijkheden mogelijk ook negatieve gevolgen. Nieuwe digitale ontwikkelingen behelzen mogelijk een bedreiging voor de bescherming van persoonsgegevens aangezien het niet vanzelfsprekend is om als individu te weten hoe je persoonsgegevens worden verwerkt in digitale toepassingen. Hiertoe wil de GDPR individuen meer controle geven over hun persoonsgegevens.

8. Maar gelukkig impliceren nieuwe en nog vrij onbekende nieuwigheden ook opportuniteiten. De blockchain technologie is nog steeds redelijk recent en niet afgelijnd ingebed in het recht. Het staat als een paal boven water dat als de blockchain technologie opmars maakt in onze maatschappelijke structuren zij ook een verandering van de bestaande regelgeving noodzaakt. Een ideale gelegenheid dus om voor de nog onbestaande onduidelijkheden een juridische interpretatie te geven om trachten oplossingen aan te reiken.

1.2. Onderzoeksvragen

9. De centrale onderzoeksvraag van dit onderzoek luidt: "Bestaat er een spanningsveld tussen de blockchain technologie en de GDPR, en zo ja, hoe kan de symbiose tussen beiden gefaciliteerd worden?" (Analytisch)

10. Om een antwoord te kunnen formuleren op de centrale onderzoeksvraag, zal eerst geantwoord worden op onderstaande subonderzoeksvragen:

- Kan het bestaande recht (GDPR) de bescherming van persoonsgegevens die zich in blockchains bevinden, voldoende waarborgen? (beschrijvend)
- Wat zijn mogelijkheden om de technologie van blockchains verenigbaar te maken met de GDPR. (beschrijvend)
- Kan blockchain technologie aangewend worden om GDPR-conforme gegevensverwerkingen na te streven? (evaluatief)

1.3. Gehanteerde onderzoeksmethode

11. Deze masterscriptie beoogt het kritisch schetsen van een transparant beeld van de stand van zaken en mogelijkheden op vlak van verenigbaarheid tussen de blockchain technologie en de GDPR.

Door een tweeledige benadering van het probleem beoogt het onderzoek een brede theoretische analyse.

12. Een eerste pijler is de overwegend juridische visie over het probleem. De tweede pijler stoelt overwegend op de theoretische benadering van het probleem.

13. Ondanks dat er vanuit juridisch oogpunt veel aandacht bestaat over deze nieuwe blockchain technologie, beperkt dit onderzoek zich tot de gegevensbeschermingswet van de Europese Unie. Met een mondiaal fenomeen als blockchaintechnologie verdient een studie van Europese wetgeving dan ook de voorkeur ten opzichte van een studie in lidstatelijke context. De Europese context is in dit onderzoek van essentieel belang aangezien blockchaintechnologie zal worden beoordeeld in het licht en de waarborgen die de GDPR biedt.

14. Door toepassing van de juridische dogmatische methode zullen vooreerst de gevestigde rechtsbronnen worden onderzocht. Vervolgens zal het geldende recht en de onderliggende beginselen en middelen worden geanalyseerd vanuit het perspectief van en met betrekking tot het digitale tijdperk dat we momenteel verkennen.

15. Er wordt onderzoek gevoerd naar de rechtsgeldigheid van de gegevensverwerking via blockchains. Vooreerst zal het bestaand wettelijk kader, met name de GDPR, beschreven worden om vervolgens afgetoetst te worden aan de werking van de blockchain technologie op vlak van de bescherming en verwerking van persoonsgegevens.

16. Het onderzoek bestaat er tevens in initiatieven te beschrijven die het eventuele spanningsveld tussen de blockchain technologie en de GDPR kunnen ontmijnen. Om nadien de evaluatieve denkoefening in omgekeerde richting te maken. Er wordt geconcludeerd welke oplossing de voorkeur geniet en dit zal eveneens afgetoetst worden in het licht van de privacy waarborgen die de rechtsonderhorigen minimaal dienen te genieten. Zo zal dit onderzoek in het eerste deel beschrijvend zijn, het tweede evaluatief.

17. Toekomstvoorspellingen over de blockchain technologie en hoe de uitwerking hiervan toekomstig zou zijn in verscheidene domeinen zijn geen onderdeel van dit onderzoek. Ook ligt er geen nadruk op de technische, ICT-matige benadering en constructie van de blockchain technologie, evenmin als de potentiële economische doorwerking in de maatschappij. De sociologische insteek, waaronder bijvoorbeeld het vertrouwen (of wantrouwen) in centrale tussenpersonen, die resulteren in een positieve dan wel een negatieve houding ten aanzien van de blockchain technologie wordt evenzeer buiten beschouwing gelaten in dit onderzoek.

18. Het tijdsbestek en de omvang zijn ook te krap om(alle mogelijke toepassingen van de blockchain technologie te bespreken. Het is dus van belang dat het onderzoeksveld krap wordt gehouden en zich beperkt tot het aspect van de gegevensbeschermingswaarborgen van de GDPR die betrokkenen meer controle biedt over hun persoonsgegevens.

19. Er zal geen diepte-onderzoek gebeuren naar de virtuele munten en de smart-contracts bijvoorbeeld. De focus ligt echter wel op het juridisch onderzoek naar de werkingsprincipes van blockchains en hun verenigbaarheid met de GDPR, waarbij het vertrekpunt concrete en in praktijk bestaande euvels onder de loep genomen worden om zo een realistische aanbeveling te kunnen formuleren rond de verenigbaarheid van de blockchain technologie en de GDPR.

20. Zowel de selectieve als de sneeuwbalmethode worden gebruikt voor de bronnenanalyse in dit onderzoek. Een selectieve bronnenanalyse laat toe in om in een kort tijdsbestek relatief veel bronnen te bekijken. De sneeuwbalmethode daarentegen maakt het vinden van de belangrijkste bronnen mogelijk.

1.4. Opbouw onderzoek

21. Het eerste hoofdstuk zal de werking van blockchaintechnologie en haar toepassingen in de maatschappij verduidelijken alsook de situering van deze relatief nieuwe technologie in het recht. In het tweede hoofdstuk wordt onderzocht of de waarborgen voor gegevensbescherming zoals vervat in de GDPR gevrijwaard zijn bij het gebruik van blockchaintechnologie. Een derde hoofdstuk spitst zich toe op initiatieven om blockchaintechnologie meer GDPR-conform te maken. Tot slot wordt in de conclusie antwoord gegeven op de hoofdonderzoeksvraag.

2. Algemeen kader

2.1. Wat is blockchain technologie?

22. "Een blockchain is zoals een boek. De pagina's zijn genummerd. Het boek is gepubliceerd en iedereen kan het inkijken. Aangezien het bewaard wordt op vele plaatsen tegelijkertijd, is niemand in staat om de rest te overtuigen van een vervalste versie." [4] Hoger genoemd citaat uit het boek *Tradition in motion* tracht op bevattelijke en begrijpbare wijze blockchain technologie te definiëren. Er is immers geen universeel aangenomen definitie van het begrip blockchain, daar er geen eensgezindheid bestaat over welke gedistribueerde digitale grootboeken nu precies onder de noemer van blockchain technologie vallen vanwege hun grote verscheidenheid. Echter, voor een goed begrip van dit onderzoek is het noodzakelijk een uitgebreidere begripsomschrijving te hanteren. Meer uitgebreid kan blockchain technologie omschreven worden als een digitale werkwijze om communicatie, informatieopslag en het faciliteren van transacties tussen veel actoren (gedistribueerd in de zin van afzonderlijke participanten van het computernetwerk, ook wel *nodes* genoemd) mogelijk maakt op basis van consensus zonder de tussenkomst van een centrale derde partij (gedecentraliseerd). De transacties, die onveranderbaar zijn eenmaal ze zijn opgenomen in een block, worden door middel van encryptie aan een reeks van bestaande blokken toegevoegd. Aldus wordt de centrale en vaak verplichte tussenpersoon, zoals bijvoorbeeld een bank, vervangen door een gedecentraliseerd netwerk van *nodes*. Zodoende wordt een bepaalde transactie niet louter beheerd of is zij slechts afhankelijk van één entiteit. Evenwel is het noodzakelijk het netwerk van *nodes* zekerheid te verschaffen dat zij allen over dezelfde historiek van transacties beschikken om te kunnen beslissen. Blockchain technologie faciliteert dus het vastleggen van het verloop van transacties, die onveranderlijk zijn en niet slechts afhankelijk zijn van één autoriteit.

2.2. Ontstaan en doel van blockchain technologie

23. Tijdens de creatie van een digitaal betalingssysteem in 2008 deed de blockchain technologie haar intrede, als onderdeel van de ontwikkeling van *cryptocurrencies*. Het doel was om een digitale werkwijze te ontwikkelen waarbij een gedecentraliseerd netwerk van deelnemers (via hun via het internet aangesloten computers, *nodes* genoemd) de touwtjes in handen heeft.

24. Sinds de opmars van de digitale valuta waarvan Bitcoins het meest gekend zijn bij het bredere publiek, heeft blockchain technologie zich aanzienlijk verder ontwikkeld. Blockchain technologie wordt nu in verschillende sectoren gebruikt en kent een veelvoud aan toepassingsgebieden waaronder *supply chain management*, identiteitsbeheer, *smart contracts*, … Kortom deze digitale werkwijze sijpelde reeds door in verschillende segmenten van de samenleving en zullen hoe langer hoe meer ingebed worden in ons dagdagelijks functioneren.

[4] K. AUDENAERT, F. BARY, E. BEGUIN, B. BLONDE, P.BOSSELER, L. CHABOT, P.DANNEELS, H. DE DECKER, C. DENOYELLE, B. DOOLAEGE, J. GANSEMAN, M. HUDSON, E. JANSSENS, I. LEUNCKENS, P. MERLEYDE, B. PRINS, K. SEPP, M. VAN MOURIK, E. VAN VOOREN, B. VERHEYE, K. VERSLEYPE en N. WATTILLON, *Tradition in motion : notarieel congres Antwerpen 2019*, Brussel, Larcier, 2019, 127.

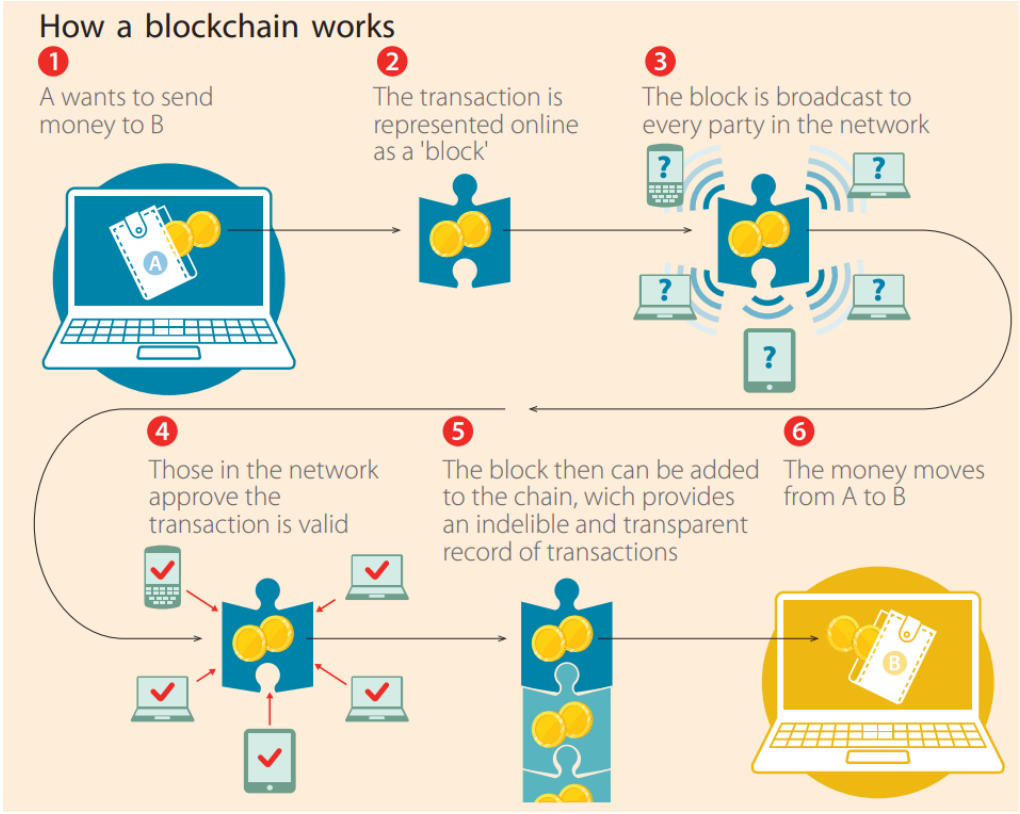
25. Het doel van blockchain technologie bestaat erin om transacties tussen verschillende actoren op transparante, veilige en efficiënte wijze te faciliteren door de creatie van een database waarin transacties gedecentraliseerd kunnen worden opgeslagen en geverifieerd. Het wegvallen van de centrale tussenpersoon zorgt ervoor dat partijen sneller hun transacties kunnen vervolmaken, hetgeen op zijn beurt dan weer lagere transactiekosten impliceert. Hierdoor wordt de vertrouwelijkheid en integriteit van data gewaarborgd alsook het vertrouwen tussen partijen. Blockchain technologie is hierdoor zowaar fraudebestendig.[5]

2.3. De werking en beveiliging van blockchain technologie

26. Ondanks het bestaan van allerlei soorten blockchains met verschillende specificaties en functies, afhankelijk van het doel en de sector waarvoor en -waarin zij gebruikt worden, kan de algemene chronologische basiswerking als volgt worden omschreven:

27. Wanneer een gebruiker een transactie initieert, zal deze transactie gecontroleerd en gevalideerd worden door de vertegenwoordigers van het netwerk, ook wel knooppunten of *nodes* genoemd. *Nodes* vervangen de centrale tussenpersoon en handelen op basis van consensus. Gevalideerde transacties worden samengevoegd en opgenomen in een *block* om vervolgens toegevoegd te worden aan de keten. Elke transactie wordt omgezet in een unieke code, ook *hash* (verwijzing) genoemd, die wordt opgeslagen in het blok. Elk *block* heeft bevat een *hash*, die verwijst naar alle voorgaande *blocks*, waardoor er dus een ketting of reeks van *blocks* ontstaat. Blockchain ontleent haar benaming dan ook aan een keten van *blocks*. De *blocks* worden opgeslagen in het distributieregister of het grootboek, het geen een kopie is van de blockhain en die door elke node in het netwerk wordt bijgehouden. Het toevoegen van nieuwe *blocks* kan slechts wanneer er consensus via complexe consensus-algoritmen zoals *proof-of-work* of *proof-of-stake* wordt bereikt over de geldigheid van die nieuwe *blocks*. Eenmaal een block is vastgeketend aan de keten is zij onveranderbaar en kan zij niet meer gewijzigd of verwijderd worden. Dit garandeert de integriteit van de gegevens op de blockchain. De *hash* naar de voorgaande *blocks* waarborgt evenzeer de integriteit en vertrouwelijkheid van de blockchain wanneer een nieuwe *block* en dus nieuwe transacties worden toegevoegd aan de bestaande blockchain. De beveiliging van de blockchain wordt bewerkstelligd doordat de gegevens van de transacties versleuteld zijn. Bijgevolg is het niet meteen duidelijk welke gegevens nu precies binnen de gedane transacties kaderen. Bovendien is de werking van blockchain gestoeld op consensus waardoor zij betrouwbaar is. De *hashes* leggen de herkomst van de transacties bloot, hetgeen transparantie bewerkstelligt. De transacties opgeslagen in *blocks* zijn onveranderbaar, waardoor het werken met blockchain technologie als veilig wordt ervaren.[6]

[5] R. BELEN-SAGLAM, E. ALTUNCU, Y. LU en S. LI, *A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems*, 2022, https://arxiv.org/abs/2210.04541, 6.
[6] S. HAN en A. PARK, "A gap between blockchain and general data protection regulation: A systematic review", *IEEE* 2022, https://ieeexplore.ieee.org/abstract/document/9906064, 103889.

28. 

[7]

29. Dit is hoe blockchain-technologie in algemene zin werkt. Er zijn veel verschillende soorten blockchains met verschillende specificaties en functies, dus deze beschrijving is algemeen van aard. De werking van een blockchain kan voor een goed begrip ervan best uitgelegd en gevisualiseerd worden aan de hand van een praktijkvoorbeeld. Hieronder een weergave van hoe blockchain technologie werkt aan de hand van *cryptovaluta bitcoin*.

30. Om transacties te doen via een blockchain, zoals het verzenden, ontvangen én ontgrendelen van cryptocurrency, wil men zeker zijn van de gebruiker die deze opdracht geeft. Hetzelfde voor de *node*-beheerders die in de blockchain de transacties valideren. Men zal zich dienen te identificeren in de softwaretoepassing door het gebruik van twee 'sleutels'. Enerzijds zijn publieke sleutel (*public key*) en anderzijds zijn private sleutel (*private key*).

31. Een publieke sleutel is openbaar in de toepassing en zichtbaar voor iedereen. Donatiepagina's delen maar al te graag hun publieke sleutel met de vraag om *cryptocurrency* ernaar over te schrijven. Het is je adres of een pseudoniem, maar het kan wel leiden naar je persoon waardoor ook de GDPR-wetgeving er op van toepassing is.[8]

32. Je private sleutel is geheim en deel je nooit. Je hebt deze sleutel nodig om te beschikken over je eigendommen van waarde waarvan je eigenaar bent. Een privé-sleutel is een soort van zeer lang paswoord omwille van veiligheidsredenen, gemakkelijk bestaande uit 61 tot 256 tekens.

---

[7] R. BOONE, "Smart contracts: evolutie, geen revolutie", *Juristenkrant* 2020, afl. 416, 6.
[8] EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Blockchain and the General Data Protection Regulation : Can Distributed Ledgers Be Squared with European Data Protection Law?*", 2019, www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, 49.

33. Beide sleutels worden asymmetrisch geëncrypteerd. Ze zijn door een algoritme aan elkaar verbonden waarbij dat men van de private sleutel de publieke sleutel kan afleiden. Maar uiteraard niet omgekeerd.[9]

34. Een openbare sleutel is steeds aan iemand toegewezen. Alhoewel men meestal een pseudoniem gebruikt, kan met behulp van aanvullende gegevens de identiteit van de openbare sleutel achterhalen. Als men anoniem is, kan men nooit teruggaan naar iemands oorspronkelijke gegevens. Bij pseudonimisering bestaat er steeds een risico om de oorspronkelijke gegevens, iemands identiteit, te achterhalen. Toch bestaat er bij gegevensbeschermingsautoriteiten consensus dat geavanceerde pseudonimiseringstechnieken garanties kunnen bieden. Dit door encryptie, het gebruik van extra codes en het vertroebelen (*obfuscation*) van gegevens.[10]

2.4. Vormen

35. Publieke en private blockchains zijn twee soorten gedistribueerde grootboeken die in verschillende contexten worden gebruikt. Hoewel ze op technologisch niveau vergelijkbaar zijn, zijn er enkele belangrijke verschillen in hun doelen, toegankelijkheid en beheer. De werking van de blockchain zoals oorspronkelijk bedacht door Nakamoto is een publieke of "*permissionless*" blockchain: open en toegankelijk voor iedereen die wil deelnemen zonder voorafgaande toestemming. Deze blockchain is "*open-source*" en "*open-acces*". Deelnemers aan een publieke blockchain kunnen de transacties in het grootboek bekijken, nieuwe transacties initiëren en bijdragen aan het consensusproces om nieuwe blokken te valideren.

36. Een variant op de publieke blockchain is de private blockchain of "permissioned" blockchain, die zich bevindt op een privaat netwerk. Niet iedereen kan deel uitmaken van deze blockchain aangezien de toegang tot het netwerk wordt afgeschermd en voorbehouden tot een selecte groep deelnemers. Toegangsrechten, beheer en regels worden vastgelegd door een centrale autoriteit. Alzo is er een hoger niveau van gegevensbescherming in een private blockchain omdat de toegang tot de transactiegegevens is beperkt tot de geautoriseerde deelnemers. Bovendien is in private blockchains het consensusmechanisme minder van belang omdat men hier doorgaans vertrouwt op het goede gedrag van de *nodes* of omdat bepaalde *nodes* verantwoordelijk gesteld zijn voor het verifiëren van transacties.

37. Samengevat zijn publieke blockchains open, gedecentraliseerd en transparant, terwijl private blockchains beperkte toegang, centraal beheer en meer privacy bieden. Publieke blockchains zijn door hun gedecentraliseerde aard "vernieuwd" ten aanzien van de GDPR wetgeving en behelzen dan ook het merendeel aan privacy-uitdagingen.

[9] CRYPTOPEDIA STAFF, *What are public and private keys*?, 2022, www.gemini.com/cryptopedia/public-private-keys-cryptography#section-public-and-private-keys-control-your-crypto
[10] C. PEHLIVAN en I. READ, "Blockchain and data protection", *Global Privacy Law Review* 2020, Volume I, issue I, https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2020005.pdf

2.5. Belang van blockchain technologie in de samenleving

38. Heden wordt de blockchain technologie samen met *artificial intelligence* (kunstmatige intelligentie) genoemd als de twee disruptieve technologische ontwikkelingen die de huidige samenleving, op een hopelijk goede manier, zullen 'ontwrichten'. Zij zullen een grote impact hebben op de samenleving en het leven van personen.[11]

39. De blockchain technologie heeft vandaag evenveel potentie zoals het huidige internet had aan de vooravond van haar doorbraak. De mogelijkheden die de blockchain technologie vandaag biedt, zijn enorm.

40. Internet werd revolutionair omdat informatie over heel de wereld kon worden uitgewisseld en men overal ter wereld met elkaar kon communiceren. Blockchain is vandaag de revolutie in 'vertrouwen' waardoor 'waarde' kan worden uitgewisseld over het internet.[12]

41. Door blockchain kunnen transacties tussen personen gebeuren zonder dat er een centrale partij (intermediair of tussenpersoon) nodig is. Een klassieke geldtransactie naar een andere persoon gebeurt vandaag via een bankoverschrijving. De bank zorgt voor het vertrouwen tussen twee vreemde partijen. Maar een transactie met Bitcoins, die ook de blockchain technologie gebruikt, gebeurt zonder tussenpersoon. De blockchain technologie zorgt voor het vertrouwen. De duizenden aangesloten computers (*nodes*) op de Bitcoin blockchain technologie gaan na of de Bitcoin-transactie voldoet aan de spelregels en zo ja, valideren de transactie. Deze transactie wordt onmiddellijk opgeslagen in de duizenden aangesloten computers. Het is dus niet één centrale entiteit die de transactie valideert, wel een collectief van computers die allen valideren dat aan de spelregels is voldaan waardoor de transactie kan plaatsvinden en allemaal vele kopies van de transactie in een blockchain bewaren. Blockchain staat aldus voor gedecentraliseerd, onveranderlijk, transparant en betrouwbaar.[13]

42. Blockchain zal in de toekomst nog meer de werking van ondernemingen ondersteunen en verbeteren. Ze realiseert een enorme efficiëntiewinst en automatisering van werkingsprocessen. Door het alsmaar meer gebruik van de blockchain technologie in de samenleving, zal ze zorgen voor een toegevoegde waarde van $ 360 miljard in 2026 en $ 3,1 biljoen in 2023.[14]

43. Maar waar wordt blockchain vandaag voor gebruikt of waar zou ze voor kunnen worden gebruikt? We sommen hieronder een aantal mogelijkheden op. Uiteraard zijn de blockchain mogelijkheden onbeperkt om op te sommen en halen we hier louter enkele concrete voorbeelden aan. Uiteraard is het aan de aandachtige lezer om zijn gedachten hiermee de vrije loop te laten gaan en zelf te bedenken waarvoor in zijn dagelijks-, professioneel- of vrije tijdsleven blockchains allemaal nuttig kunnen zijn.

---

[11] O. ZABOLOTNYY, *How AI and blockchain are changing business*, https://firstbridge.io/blog/blockchain/how-ai-and-blockchain-are-changing-businesses.
[12] J. GOOSSENS, K. VERSLYPE en E. TJONG TJIN TAI, *Blockchain en smart contracts: Herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving*, 2020, https://library.oapen.org/handle/20.500.12657/53282, 9.
[13] P. JOOSTEN, *Blockchain. Definitie, werking, kansen & 6 voorbeelden*, www.peterjoosten.net/blockchain/
[14] B. BHIDE, *Blockchain and its future in 2023: What is blockchain?*, 2023, www.projectcubicle.com/blockchain-and-its-future-in-2023.

44. Van het één in het ander moeilijk woord. Ook *smart contracts* maken gebruik van blockchain technologie. *Smarts contracts* zijn automatische transacties die gebruikmaken van deterministische software. Eenmaal het proces met een bepaalde input gestart, moet er een output komen. Indien aan bepaalde voorwaarden wordt gedaan, volgt een bepaalde handeling.[15]

Een *smart contract* is een zelfuitvoerend proces dat onveranderlijk is. Daarbij wordt de weg die het *smart contract* tijdens haar werkingsproces aflegt, bepaald door de software. Ook wel *code is law* genoemd. De uitvoering van hetgeen werd overeengekomen als aan een bepaalde voorwaarde is voldaan is automatisch en gegarandeerd. Waardoor zelfs rechterlijke tussenkomst niet meer nodig kan zijn.[16]

Belangrijke nuance is dat *smart contracts* hun naam niet verdienen. Het zijn helemaal geen contracten of een opgestelde overeenkomst tussen partijen zoals wij dat kennen, noch is het slim want het proces verloopt louter zoals de software het heeft voorgeschreven.

Smart contracts worden bijvoorbeeld gebruikt bij *supply chain management*, het betalen en openen van een Cambiowagen[17], de afhandeling van een verzekeringsdossier[18] of het ontvangen van een koffievoucher van de vliegmaatschappij als tegemoetkoming voor een vlucht met vertraging.[19]

45. Twee onbekende partijen die een financiële transactie willen doen via het internet, kunnen dit doen via software die gebruikmaakt van blockchain technologie. Een dure en trage klassieke bank als tussenpersoon is niet meer nodig om vertrouwen te creëren. Want blockchain zorgt voor vertrouwen om waarde te kunnen overmaken aan een andere partij. Bovendien kan dit ook in zelfgekozen cryptocurrency, waarvan de meest bekende de Bitcoin is. In de media komt deze recent aan bod omwille van de woekerwinsten die men er mee kan maken door erin te investeren.[20] Maar een cryptocurrency is en blijft een alternatief betaalmiddel in concurrentie met de klassieke betalingen via de bank en in een officiële valuta.[21]

Maar ook voor andere toepassingen die vandaag bij de bank gebeuren, kan dit via een *smart contract*. Zoals de vrijgave van een huurwaarborg als aan bepaalde voorwaarden is voldaan. Als de spelregels van de blockchain zijn gevolgd, zullen de *nodes* de transactie valideren waardoor de huurwaarborg vrijkomt.[22]

---

[15] J. GOOSSENS en K. VERSLYPE, *Blockchain en smart contracts: het einde van de vertrouwde tussenpersoon*, 2019, https://pure.uvt.nl/ws/portalfiles/portal/32111708/EHBR19_blockchain_en_smartcontracts.pdf, 7.
[16] R. LEENES, W. KAUFMANN, M. SCHELLEKENS, F. SCHEMKES en E. TJONG TJIN TAI, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, 2019, www.stibbe.com/sites/default/files/2022-07/tk_bijlage_blockchain_en_het_recht_def_8316.pdf, 7.
[17] R. BOONE, "Smart contracts: evolutie, geen revolutie", *Juristenkrant* 2020, afl. 416, 6.
[18] D. DOBBELAERE en J. VERCAUTEREN, "Smart contracts en verzekeringen" in P. AERTS, F. HOOGENDIJK en N. VANDEZANDE (eds.), *Smart contracts. Een overzicht vanuit juridisch perspectief*, Antwerpen, Intersentia, 2020, 297.
[19] M. KORZ, *Vier redenen waarom blockchain de toekomst gaat veranderen*, www.rabobank.nl/bedrijven/groei/marktontwikkeling/vier-voordelen-van-blockchain.
[20] H. RENIER, Tiener (19) die rijk werd met bitcoin: "Eigen schuld als je binnen 10 jaar geen miljonair bent", 2018, www.hln.be/geld/tiener-19-die-rijk-werd-met-bitcoin-eigen-schuld-als-je-binnen-10-jaar-geen-miljonair-bent~af3d1b82.
[21] B. BHIDE, *Blockchain and its future in 2023: What is blockchain?*, 2023, www.projectcubicle.com/blockchain-and-its-future-in-2023.
[22] J. GOOSSENS, K. VERSLYPE en E. TJONG TJIN TAI, *Blockchain en smart contracts: Herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving*, 2020, https://library.oapen.org/handle/20.500.12657/53282, 13.

46. In het *supply chain management* wordt al gretig gebruik gemaakt van de voordelen van blockchain technologie omwille van haar eigenschappen. Een concreet voorbeeld is de bevoorrading van geneesmiddelen en daarbij het voorkomen van namaakgeneesmiddelen.[23] Door het gebruik van blockchain technologie kan de volledige distributie van het geneesmiddel worden gevolgd en is er geen plaats voor namaakgeneesmiddelen. De blockchain technologie voor een waterdichte opvolging waar geen fouten kunnen gebeuren en zodus namaakgeneesmiddelen onmiddellijk ontdekt worden. Een ander voorbeeld van het waterdicht systeem dat blockchain technologie biedt, is het voorkomen van fraude bij het doorverkopen van toegangstickets voor concerten. Elk toegangsticket heeft maar één eigenaar. Bij het doorverkopen ervan dient in een blockchain de nieuwe eigenaar te worden bepaald.[24]

47. In het notariaat is de notaris het vertrouwen tussen twee voor elkaar onbekende partijen. Maar ook hier staat de blockchain technologie met haar vertrouwen te springen om het werk van de notaris over te nemen. Toch is men er ook realistisch in. Net zoals indertijd computers met tekstverwerkers en databanken de pen en het typemachine hebben overgenomen, ziet het notariaat het gebruik van de blockchain technologie als prioriteit die ervoor kan zorgen dat de notaris door blockchain net een betere dienstverlening aan zijn cliënt kan aanbieden. Minder formaliteiten en administratie en dankzij de blockchain technologie minstens zo zeker dat bij de overdracht van het goed de akte volledig correct is.[25]

48. Het werk van de notaris en het bijhouden van de registratie van onroerende goederen in het registratiekantoor zijn door de blockchain technologie misschien bijna verleden tijd. Blockchain kan hier beter en gemakkelijker voor zorgen. In het blockchain registratiekantoor registreren koper en verkoper zelf hun akte. Elk onroerend goed kan maar één eigenaar hebben. Daarvoor kunnen we de blockchain technologie vertrouwen. De registratiegegevens zijn onwijzigbaar en kunnen daarna alleen nog maar veranderen als aan de spelregels om te veranderen is voldaan. Zoals een nieuwe akte met daarin een nieuwe eigenaar. Onroerend goed zal rechtstreeks kunnen overgaan van verkoper naar koper dankzij de blockchain technologie. En de *smartcontract*-technologie zorgt ervoor dat de kwaliteit van de aktes wordt gewaarborgd. Pas als alle gegevens overeenkomstig de koop-verkoopregels correct in de *smart contract* toepassing zijn ingebracht, zal dit leiden tot een akte die in het blockchain registratiekantoor kan worden ingegeven.

Een notaris en de registratiekantoren zullen we, als we volop gebruik gaan maken van blockchain technologie, binnenkort niet meer nodig hebben voor de overdracht van een onroerend goed.[26]

Zelfs zeer klassieke beroepen worden gemakkelijk bedreigd door de blockchain technologie.

49. Door de transparantie die blockchain biedt, kan het perfect gebruikt worden voor een samenwerking tussen verschillende onbekende partijen. Zoals voor het beheer van een gedeelde

[23] B. BHIDE, *Blockchain and its future in 2023: What is blockchain?*, 2023, www.projectcubicle.com/blockchain-and-its-future-in-2023.
[24] M. KORZ, *Vier redenen waarom blockchain de toekomst gaat veranderen*, www.rabobank.nl/bedrijven/groei/marktontwikkeling/vier-voordelen-van-blockchain.
[25] S. CLOET, *Blockchain en het notariaat*, 2018, www.linkedin.com/pulse/blockchain-en-het-notariaat-match-made-heaven-stephaan-cloet.
[26] J. GOOSSENS, K. VERSLYPE en E. TJONG TJIN TAI, *Blockchain en smart contracts: Herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving*, 2020, https://library.oapen.org/handle/20.500.12657/53282, 12.

eigendom. De eigenaars kunnen in de blockchain transparant nagaan welke inkomsten het samen verhuurde goed elke maand heeft opgebracht en welke beheerskosten er zijn. Een andere concrete toepassing voor de transparantie van de blockchain technologie is de ingave van de kokosproductie- en prijzen van elke kokosteler in een blockchain voor fairtrade handel zodat men van elkaar weet dat iedereen de correcte prijs toepast.[27]

50. Overheden kunnen uiteraard ook gebruikmaken van blockchain om hun overheidstaken nog efficiënter en beter uit te voeren. Zoals het innen van belastingen die wordt *berekend* voor elke persoon aan de hand van vooraf bepaalde regels. In een blockchain zullen de nodes bepalen of er aan de regels is voldaan, waarna de berekening en inning van de belasting automatisch gebeurt. Daarbij zorgt de blockchain ook voor de nodige transparantie over de berekeningswijze.[28]

2.6. Blockchain technologie en wetgeving

2.6.1. Blockchain en privaat recht

51. Toepassingen die gebruik maken van blockchain gaan over transacties van of voor personen. Personen mogen vrij handelen met elkaar, binnen de contouren die het privaatrecht vastlegt. Eenmaal verbintenissen aangegaan, dient men die na te leven. En ingeval van niet-naleving van de aangegane verbintenis is een schadevergoeding verschuldigd.

52. Verder, gelet op de mondiale werkwijze van blockchain technologie, dient het internationaal privaatrecht bepalen welk recht van toepassing is alsook welke rechter. Tenslotte blijft de blockchain als nieuwe technologie toch nog steeds voer voor discussie. Hoe moet het concept blockchain met haar eigen werkwijze worden gekwalificeerd en ingepast in het bestaande privaatrecht? Net zoals met elke innovatie in de samenleving loopt het recht achter de feiten aan. Maar dit is niet abnormaal en is zelfs de normale evolutie van regels in de samenleving.[29]

2.6.2. Toezicht op de transacties 'met waarde' op de blockchain-cryptocurrency

53. Op de klassieke financiële sector in ons land wordt er toezicht gehouden ter voornamelijk bescherming van de consument en het voorkomen van fraude. O.a. de Belgische bankinstellingen zijn onderworpen aan deze toezichtswetgeving[30] met als financiële waakhonden (toezichtshouders) de Nationale Bank van België en de Autoriteit voor Financiële Diensten en Markten (beter gekend onder haar Engelstalige naam Financial Services and Markets Authority, afgekort FSMA)[31].

---

[27] M. KORZ, *Vier redenen waarom blockchain de toekomst gaat veranderen*, www.rabobank.nl/bedrijven/groei/marktontwikkeling/vier-voordelen-van-blockchain.
[28] J. GOOSSENS, K. VERSLYPE en E. TJONG TJIN TAI, *Blockchain en smart contracts: Herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving*, 2020, https://library.oapen.org/handle/20.500.12657/53282, 13.
[29] R. LEENES, W. KAUFMANN, M. SCHELLEKENS, F. SCHEMKES en E. TJONG TJIN TAI, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, 2019, www.stibbe.com/sites/default/files/2022-07/tk_bijlage_blockchain_en_het_recht_def_8316.pdf, 30.
[30] Wet 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, *BS* 4 september 2002.
[31] Art. 84 e.v. wet 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, *BS* 4 september 2002; AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN, *Wat is de FSMA?*, www.fsma.be/nl/wat-de-fsma.

54. Cryptomunten waren onderworpen aan regelgeving die niet voor cryptomunten was bedoeld. Ze werden gekwalificeerd als financieel instrument en zodus onderworpen aan de regeling voor de effectenmarkten.[32]

55. Maar ook in een blockchain-*cryptocurrency* gebeuren er transacties met cryptomunten met een bepaalde waarde. Daarom werd in 2022 de wet betreffende de toezicht op de financiële sector gewijzigd door de invoeging van een bepaling waarbij de FSMA ook bevoegd wordt om regels op te leggen inzake de commercialisering van virtuele munten en het toezicht te organiseren op de naleving ervan. Hierbij worden 'virtuele munten' toch wel door de wetgever vaag en onzeker omschreven als 'een digitale weergave van waarde die niet door een centrale bank of een overheid wordt uitgegeven of gegarandeerd, die niet noodzakelijk aan een wettelijk vastgestelde valuta is gekoppeld en die niet de juridische status van valuta of geld heeft, maar die door natuurlijke of rechtspersonen als ruilmiddel wordt aanvaard en die elektronisch kan worden overgedragen, opgeslagen en verhandeld.'[33]

56. De waakhond FSMA kreeg daardoor op 1 mei 2022 de bevoegdheid om aanbieders van cryptomunten te verplichten te voldoen aan een aantal voorwaarden die onder andere verband houden met hun professionele betrouwbaarheid, een inschrijving bij de FSMA en de naleving van de anti-witwaswetgeving.[34]

57. En terwijl vanaf 17 mei 2023 de FSMA van de federale regering de bijkomende bevoegdheid krijgt om de consument extra te beschermen tegen de risico's verbonden aan reclame voor cryptomunten[35], ging begin mei 2023 nog een grote Belgische *cryptocurrency*-aanbieder Bit4You failliet. De FSMA kan al onmiddellijk met haar nieuwe bevoegdheid aan de slag en stelt alvast een onderzoek in[36]. Het zal niet het eerste en niet de laatste cruptocurrency-aanbieder zijn die failliet gaat, waardoor overheidsregulering zich opdringt ter bescherming van de consument in de zeer lucratieve maar nog meer risicovolle wereld van de cryptomunten.

58. Maar toch is het vooral van de Europese Unie dat we rechtsregels mogen verwachten over een materie die totalitair en mondiaal, maar allerminst fysiek zich laat tegenhouden door landsgrenzen.

59. De Europese Commissie wil Europa geschikt maken voor het digitale tijdperk en om een toekomstbestendige economie uit te bouwen. Om de verdere innovatie van deze nieuwe technologie te verhogen en risico's te beperken, zette de Europese Commissie een proefregeling op poten voor marktstructuren die willen proberen transacties in financiële instrumenten in cryptoactiva te

[32] EUROPESE COMMISSIE, *Wettelijk en regelgevingskader voor blockchain*, https://digital-strategy.ec.europa.eu/nl/policies/regulatory-framework-blockchain.
[33] Art. 4 wet 5 juli 2022 houdende diverse financiële bepalingen, *BS* 19 juli 2022.
[34] AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN, *Cryptomunten: nieuwe regels voor bepaalde aanbieders van diensten*, 2022, www.fsma.be/nl/news/cryptomunten-nieuwe-regels-voor-bepaalde-aanbieders-van-diensten.
[35] AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN, *Virtuele munten: de FSMA zet in op de bescherming van de consument*, 2023, www.fsma.be/nl/news/virtuele-munten-de-fsma-zet-op-de-bescherming-van-de-consument.
[36] P. VAN MAELE, *Beurswaakhond maakt dossier tegen Belgische cryptobeurs Bit4You over aan het parket*, 2023, www.standaard.be/cnt/dmf20230509_95826573.

verhandelen en af te wikkelen. Blockchainontwikkelaars kunnen daardoor genieten van vrijstellingen van bepaalde regels en krijgen speelruimte om innovatieve oplossingen te testen.[37]

60. En ondertussen werd zopas ook de langverwachte en belangrijke Europese MiCA-verordening gestemd in het Europees Parlement[38]. Deze wil de innovatie van cryptocurrencies ondersteunen, de cryptoactivasector aantrekkelijker maken. Maar ook de consumenten en de integriteit van de crypto-uitwisselingen beschermen en witwassen tegengaan. Crypto-diensten worden voortaan verplicht om de identiteit van de gebruikers vast te leggen.[39]

61. Maar de Europese Commissie zit niet stil. In februari 2023 werd het initiatief genomen om een *sandbox* voor innovatieve toepassingen die gebruikmaken van *distributed ledger*, zoals de blockchain technologie dat doet. In deze *sandbox* gaan regelgevers en blockchain ontwikkelaars met elkaar in overleg, wordt juridisch advies en regelgevende begeleiding voorzien in een veilige en vertrouwelijke omgeving. Met als doel dat op basis hiervan goede regelgeving wordt bedacht die effectief tegemoetkomt aan de blockchain technologie.[40]

[37] Voorstel (Comm.) voor een richtlijn van het Europees Parlement en de raad betreffende een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie, 24 september 2020, COM(2020)594 final - 2020/0267 (COD).
[38] Voorstel (Comm.) voor een verordending van het Europees Parlement en de raad betreffende markten voor cryptoactiva en tot wijziging van de Richtlijn (EU) 2019/1937, 24 september 2020, COM(2020)593 final - 2020/0265(COD).
[39] W. VAN DEN BERGH, *Langverwachte MiCA wetgeving wordt goedgekeurd*, 2023, https://digitalcurrencyacademy.be/langverwachte-mica-wetgeving-wordt-goedgekeurd.
[40] EUROPEAN BLOCKCHAIN SANDBOX, *European blockchain regulatory sandbox for distribued ledger technologies*, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Sandbox+Project#:~:text=The%20European%20Blockchain%20Regulatory%20Sandbox,for%20innovative%20blockchain%20technology%20solutions.

3. Blockchain technologie en GDPR

3.1. General Data Protection Regulation (doel – belang)

3.1.1. Stijgende aandacht in de samenleving voor de bescherming van persoonsgegevens

62. Met de registratie van persoonsgegevens (ras, bevolkingsgroep, ..) tijdens de Tweede Wereldoorlog begon het besef dat een registratie ook heel wat risico's inhoudt. En door toedoen van de technologische evolutie zijn er elke dag nieuwe en ongekende mogelijkheden om op oneindig grote schaal verwerkingen te doen van persoonsgegevens. En van verbanden te leggen tussen deze gegevens. Tegenwoordig kunnen moeiteloos en supersnel enorme hoeveelheden persoonsgegevens voor zeer lange tijd worden opgeslagen. Met steeds verfijndere technieken kunnen verbanden tussen de persoonsgegevens worden gelegd die ook worden verzameld zonder medeweten van personen. En de verspreiding ervan naar vele bestemmelingen kan met enkele muisklikken. In de wereld waar kennis gelijk staat aan macht, kan het bezitten van persoonsgegevens grote risico's inhouden voor het individu. Daarom almaar meer de noodzaak om persoonsgegevens beter te beschermen.[41]

3.1.2. Doel van de GDPR

63. De bescherming van persoonsgegevens (personal data) van de onderdanen van de Europese Unie en van wie zich op het Europees grondgebied bevindt, gebeurt door het Handvest van de grondrechten van de Europese Unie[42]. Het recht op gegevensbescherming heeft de status van een grondrecht. Maar specifieker beschermt vooral de Algemene Verordening Gegevensbescherming van de Europese Unie[43] die rechtstreekse werking heeft in al haar EU-lidstaten. Op 25 mei 2018 trad de GDPR in werking. Deze verordening wordt veelal afgekort door AVG, maar nog meer genoemd met de Engelstalige afkorting GDPR van haar Engelstalige benaming *General Data Protection Regulation*. De GDPR legt de regels vast inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en over het vrije verkeer van persoonsgegevens.[44]

64. Ook het Europees Verdrag voor de Rechten van de Mens erkent impliciet het recht op bescherming van persoonsgegevens op grond van de grondwettelijke en mensenrechtelijke bescherming van de persoonlijke levenssfeer. Het Europees Hof voor de Rechten van de mens heeft in de loop der jaren een ruime interpretatie toegekend aan het begrip persoonlijke levenssfeer. Zij erkennen een ruime toepassing van dit recht inclusief de bescherming van de informationele privacy.[45] Ook het Verdrag betreffende de werking van de Europese Unie legt het recht op

[41] F. SCHRAM, *Privacy en persoonsgegevens*, Brussel, Politeia, 2019, 59.
[42] Artikel 8 Handvest van de grondrechten van de Europese Unie van 7 december 2000, *Pb.L*. 18 december 2000, afl. 346, 1-22.
[43] Verord. EP en Raad nr. 2016/679, 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, *PB.L.* 4 mei 2016, afl. L 119, 1. (= GDPR)
[44] Art. 1(1) GDPR.
[45] R. MORGAN en R. BOARDMAN, *Data Protection Strategy. Implementation data protection compliance,* Londen, Sweet & Maxwell Limited, 2012, 33-34.

bescherming van persoonsgegevens vast in artikel 16. Dit primair unierecht vormt de juridische grondslag voor de GDPR.[46]

65. De GDPR wil elke natuurlijke persoon meer controle geven over wat er gebeurt met zijn persoonsgegevens. Natuurlijke personen hebben hiervoor nu rechten die ze rechtstreekse kunnen uitoefenen tegenover eenieder die persoonsgegevens verwerkt.

66. De GDPR beschermt persoonsgegeven door te bepalen hoe we moeten omgaan met persoonsgegevens, welke procedures we moeten volgen om ze te gebruiken en hoe we ze moeten afschermen.[47]

67. De GDPR harmoniseert nationale wetten op het gebied van informatiebescherming en beoogt de privacy rechten van burgers met betrekking tot hun persoonsgegevens te waarborgen, te beschermen, te optimaliseren en te verruimen. Dit is essentieel in een tijdperk waarin de gegevenseconomie uitgaat van "*platform power*", waarbij grote spelers zoals Google, Facebook, Amazon,… over gigantische hoeveelheden gegevens beschikken die zij digitaal verwerken en opslaan.[48] Bijgevolg verplicht de GDPR om centraliseerde beheerders van grote hoeveelheden persoonsgegevens om op een verantwoorde wijze de verwerking van de persoonsgegevens waarover zij beschikken, te voltrekken. Organisaties worden verantwoordelijk gesteld voor de bescherming van de persoonsgegevens die zij verwerken. Zij moeten zorgen voor transparantie en inzicht in hoe ze deze gegevens verwerken, en moeten burgers het recht geven om hun gegevens op te vragen, te bekijken, te verbeteren en te verwijderen. Wanneer organisaties verzaken aan deze verplichtingen kunnen zij gesanctioneerd worden met een boete. Of nog erger, leiden tot imago- en reputatieschade.[49]

3.1.3. Draagwijdte van de GDPR

68. De draagwijdte van de GDPR is groot, ook inzake blockchain-technologie, omdat een verordening rechtstreekse toepassing en doorwerking vindt in de nationale rechtsordes. Een verordening is dan ook het meest opportuun om de bescherming van een grondrecht, meer bepaald het recht op bescherming van persoonsgegevens te waarborgen opdat op Unieniveau een krachtig, consistent en coherent beschermingsniveau wordt uitgewerkt. Een gefragmenteerde bescherming van het recht op gegevensbescherming zou leiden tot rechtsonzekerheid en aanzienlijke risico's inhouden voor de rechten van natuurlijke personen. Bovendien is het normaal in het huidige digitale tijdperk dat gegevensverwerking al snel over de landsgrenzen heengaat, daar internet een mondiaal verschijnsel is. De impact van de GDPR is groot aangezien zij een handhavingsmechanisme hanteert dat in grote sancties voorziet waardoor de naleving van de verplichtingen die erin zijn opgenomen strikt moeten worden nageleefd.

[46] A. SAVIN, *EU Internet Law*, Cheltenham, Edward Elgar Publishing, 2017, 283.
[47] D. VERHULST en K. ZADORA, *Blockchain technologie en controle over persoonsgegevens uit de GDPR*, 2021, https://monardlaw.be/nl/verhalen/blockchain technologie-en-controle-over-persoonsgegevens-uit-de-gdpr.
[48] O. LYNSKEY, *Regulating 'platform power'*, 2017, https://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf, 9.
[49] O. SUSTRONCK*, Praktijkboek internetrecht,* Mechelen, Wolters Kluwer, 2017, 140.

3.1.4. Enkele belangrijke begrippen en rollen binnen de GDPR

69. Om de raakpunten tussen GDPR en blockchain goed in kaart te brengen, is het belangrijk om enkele belangrijke begrippen uit de GDPR te duiden.

70. Verwerker :

Een (gegevens)verwerker is een derde die instaat voor de verwerking van persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke.[50]

71. Verwerkingsverantwoordelijke :

De verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking van de persoonsgegevens. Hij heeft de macht om te bepalen wat er met de persoonsgegevens gebeurt, maar draagt wel de eindverantwoordelijkheid. [51]

72. Verwerkers en verwerkersverantwoordelijken zijn gebonden aan de GDPR beschermings-en verantwoordingsbeginselen. Zij moeten persoonsgegevens[52]:

- Verwerken op een rechtmatige, behoorlijke en transparante wijze. (*lawfulness, fairness & transparency*)
- Verwerken voor een duidelijk welomschreven legitiem doel. (*purpose limitation*)
- Ter zake *dienend verwerken, enkel het minimale dat nodig is om het doel te bereiken. (data mimimization*)
- Steeds actualiseren en corrigeren. (*accuracy*)
- Niet langer te bewaren dan nodig is. (*storage limitation*)
- Beveiligen door technische en organisatorische maatregelen. (*security*)

De verwerkingsverantwoordelijke moet aantonen dat hij voldoet aan deze principes. Niet pas nadat zich bij hem een incident heeft voorgedaan, wel al vanaf dag één dat hij persoonsgegevens verzamelt. (*accountability*)

73. Het mag duidelijk zijn dat eenieder op EU grondgebied een aantal verregaande verplichtingen op zich draagt vanaf het moment dat hij persoonsgegevens verwerkt. Willen of niet willen, de GDPR-regels en vooral verplichtingen zijn van rechtswege op hem van kracht.

3.1.5. Toepassingsgebied van de GDPR

74. De blockchain technologie biedt een quasi onuitputtelijk potentieel om enorme hoeveelheden gegevens te verwerken. Voor zowel private organisaties als overheden lijken er alleen maar voordelen te bestaan door het gebruik van blockchain technologie. Maar evenzeer kunnen die gegevens ook persoonsgegevens zijn waar privacyregels aan gebonden zijn.[53]

[50] Art. 4(8) GDPR.
[51] Art. 4(7) GDPR.
[52] Art. 5 GDPR.
[53] J. SIMAL, *Blockchain en privacy : een onderzoek naar de verzoenbaarheid van blockchain technologie en GDPR*, 2018, www.scriptiebank.be/sites/default/files/thesis/2018-09/SIMAL_J_masterproef_privacy_en_blockchain.pdf, 1.

75. De GDPR regels zijn op de blockchain technologie van toepassing vanaf het moment dat we spreken over de verwerking van persoonsgegevens. Dus eenieder die door gebruik van de blockchain technologie dergelijke handelingen verricht met persoonsgegevens, dient de GDPR na te leven.

76. Een oplossing lijkt onmiddellijk om de GDPR te snel af te zijn door deze persoonsgegevens te encrypteren of te pseudonimiseren, waardoor enkel degene die de versleutelingscode kent de persoonsgegevens kan zien. Maar ook hierover is de GDPR zeer duidelijk : "Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.[54]"

77. Uiteraard volgt hieruit dat anonimisering van persoonsgegevens in een blockchain wel is toegestaan. Want dan bestaat er geen gevaar dat er nog naar de oorspronkelijke persoonsgegevens kan worden teruggekeerd.

78. Artikel 2.1 GDPR bepaalt het materieel toepassingsgebied waarop de verordening uitwerking vindt: "is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen." De Europese wetgever hanteerde hierbij een technologieneutrale formulering, waarbij de bescherming van persoonsgegevens niet afhankelijk mag zijn van de gebruikte technologie om alzo een neutraal, coherent en consistent niveau van bescherming voor persoonsgegevens te waarborgen.

79. Territoriaal is zij toepasbaar op de verwerking van persoonsgegevens wanneer deze gegevens worden verwerkt door een organisatie die zich bevindt binnen de EU[55] of die persoonsgegevens van EU-onderdanen verwerkt ongeacht de locatie waar deze verwerking gebeurt.[56] Aldus dient gevolg te worden gegeven aan de vereisten van de GDPR wanneer er persoonsgegevens van EU-burgers worden verwerkt, ongeacht of de fysieke locatie van het bedrijf zich al dan niet in de EU bevindt, ongeacht de locatie van de verwerkingsverantwoordelijke of verwerker. Een blockchain buiten de EU gevestigd kan aldus gehouden zijn aan de naleving van de GDPR indien zij persoonsgegevens verwerkt van klanten die EU-onderdaan zijn. De GDPR zal van toepassing zijn op de verwerkingsactiviteiten ongeacht de locatie van de blockchain *nodes* of de ontwikkelaars die het systeem hebben opgezet.

80. Elke *node* (computer) die zich bevindt binnen de EU is onderworpen aan de GDPR. Maar ook de persoonsgegevens van een persoon die zich op het grondgebied van de EU bevindt die zich op een node bevindt ergens ter wereld, is beschermd door de GDPR.

[54] Artikel 4(5) GDPR.
[55] Art. 3, eerste lid GDPR.
[56] Art. 3, tweede lid GDPR.

81. Maar de realiteit is dat *nodes* van elkaar niet weten waar ze zich bevinden waardoor de kans zeer groot is dat de GDPR wel steeds van toepassing zal zijn. Maar zekerheid is er niet.[57]

3.2. Toetsing van de kenmerkende eigenschappen van de blockchain technologie aan de waarborgen die de GDPR biedt

82. De GDPR legt een dwingend kader vast van de manier waarop persoonsgegevens verwerkt, opgeslagen en gebruikt moeten worden teneinde EU-onderdanen te beschermen tegen misbruik van hun persoonsgegevens door overheidsinstanties of onafhankelijke bedrijven. Om tot een regulering te komen die de verwerking van persoonsgegevens beschermt hanteert zij zes essentiële beginselen. (i) Het beginsel van rechtmatigheid, behoorlijkheid en billijkheid, (ii) finaliteitsbeginsel, (iii) het beginsel van minimale gegevensverwerking, (iv) nauwkeurigheidsprincipe (v) de opslag beperking, (vi) integriteit en vertrouwelijkheid. In dit hoofdstuk zal de relatie tussen blockchain technologie en het Europese gegevensbeschermingssysteem onderzoeken. Zijn er gegevensbeschermingswaarborgen die onder druk staan bij het gebruik van blockchain technologie?

3.2.1. Versleuteld

83. Zoals hoger uiteen gezet worden gegevens in een blockchain opgeslagen in 'blokken' die aan elkaar gekoppeld zijn door middel van cryptografie. De gegevens opgeslagen in een *block* zijn aldus op een bepaalde wijze gecodeerd, zodat zij alleen toegankelijk en leesbaar zijn voor diegenen die de juiste 'sleutel' (hash) hebben om het te ontcijferen. Versleuteling draagt alzo bij aan de veiligheid en de integriteit van de blockchain doordat de gegevens opgeslagen in een blok niet raadpleegbaar zijn voor iedereen. Versleuteling is in het gedecentraliseerde netwerk een instrument om vertrouwen tussen de deelnemers te creëren en kwaadwillende partijen het moeilijk te maken om gegevens te manipuleren.

3.2.1.1. De verwerking van persoonsgegevens

84. De GDPR vindt maar toepassing wanneer er persoonsgegevens worden verwerkt. In hoe verre hebben we te maken met de verwerking van persoonsgegevens in het geval van blockchain technologie?

85. Persoonsgegevens worden gedefinieerd als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon." [58] Denk hierbij dus aan elk soort van informatie waarmee we iemand (*data subject*) mee kunnen identificeren: een

[57] J. SIMAL, *Blockchain en privacy : een onderzoek naar de verzoenbaarheid van blockchain technologie en GDPR*, 2018, www.scriptiebank.be/sites/default/files/thesis/2018-09/SIMAL_J_masterproef_privacy_en_blockchain.pdf, 30.
[58] Art. 4(1) GDPR.

naam, adres, telefoonnummer, leeftijd, rijksregisternummer, e-mailadres, foto op de website, bankrekeningnummer, medische gegevens, gebruikersnaam, tweets, IP-adres, locatiebepaling, biometrische data, web cookies, ..

86. Verwerken van persoonsgegevens is het 'verwerken van gegevens' (*data processing*). Deze term slaat op het geautomatiseerd of handmatig 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[59] of gewoonweg op eender wat men met die persoonsgegevens doet.

87. Het is duidelijk dat transacties die plaatsvinden op een blockchain vallen onder het begrip "verwerking", doch is het evenwel niet steeds duidelijk of de gegevens die in de blockchain worden verwerkt ook steeds aangemerkt kunnen worden als persoonsgegevens zoals bedoeld door de GDPR.

3.2.1.2. Pseudonimisering

88. Pseudonimisering is een gegevensbeschermingstechniek waarbij persoonsgegevens op een zodanige manier worden verwerkt dat gegevens niet langer rechtstreeks aan een specifieke persoon kunnen worden gelinkt zonder het gebruik van aanvullende informatie.[60] Dit wordt bewerkstelligd door bepaalde identificeerbare elementen in de gegevens te vervangen door pseudoniemen zoals willekeurige reeksen letters of cijfers. Deze aanvullende gegevens dienen apart te worden bewaard met inachtname van technische en organisatorische maatregelen om ervoor te zorgen dat de persoonsgegevens niet aan geïdentificeerde of identificeerbare natuurlijke personen kunnen worden gekoppeld. Doch vallen persoonsgegevens die gepseudonomiseerd zijn, maar die kunnen dienen om iemand opnieuw te identificeren niet buiten het toepassingsgebied van de GDPR.[61] Dit omdat gepseudonomiseerde persoonsgegevens, persoonsgegevens blijven en herleid kunnen worden met de nodige aanvullende informatie naar de betrokkene erachter. Aldus biedt de techniek van pseudonimisering geen absolute garantie voor de bescherming van persoonsgegevens. Dit in tegenstelling tot de techniek van anonimisering waarbij persoonsgegevens onomkeerbaar zijn losgekoppeld van de betrokkene en het op geen enkele wijze mogelijk is om terug te keren naar de oorspronkelijke gegevens met als gevolg dat de betrokkene niet (langer) kan worden geïdentificeerd.[62] Toch is pseudonimisering een waardevolle techniek om enerzijds de persoonsgegevens van betrokkene beter te beschermen en het risico op onbedoelde weergave of gegevensinbreuken van persoonsgegevens die tot hun identiteit leiden te verminderen. Anderzijds kunnen gegevensverwerkende organisaties deze techniek inroepen als een passende technische en organisatorische maatregel[63] die aantoont dat zij de nodige acties hebben ondernomen om op een verantwoorde wijze persoonsgegevens te verwerken en te beschermen. Ook bij het gebruik van blockchain technologie worden gegevens pseudoniem overgedragen tussen de verschillende

[59] Art. 4(2) GDPR.
[60] Art. 4(5) GDPR.
[61] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Advies 4/2007 over het begrip persoonsgegevens*, 20 juni 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_nl.pdf, 18.
[62] Overweging 26 GDPR; GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Advies 05/2014 over anonimiseringstechnieken*, 10 april 2014, https://docplayer.nl/amp/422750-Groep-gegevensbescherming-artikel-29.html, 6.
[63] Art. 31, eerste lid, a) GDPR.

deelnemers in de *chain* (keten). Dit doordat de blockchain wordt versleuteld door asymmetrische encryptie waarvoor een "sleutel" nodig is, die eveneens wordt beschouwd als een persoonsgegeven en fungeert als pseudoniem om terug te leiden naar de betrokkene. De houder van de sleutel kan de betrokkene opnieuw identificeren door de dataset te ontsleutelen. Een tweede manier waarop blockchain technologie pseudonimisering gebruikt is bij het opslaan van de transactiegegevens als een *hash*. Dit omdat een *hash* nog steeds kan terugleiden naar de oorspronkelijke transactiegegevens in de blockchain. Aldus zijn gegevens die opgeslagen zijn onder de vorm van een *hash* ook persoonsgegevens.[64]

89. Versleuteling door assymetrische encryptie en cryptografische hashfuncties zijn beiden inherente eigenschappen van blockchain technologie. Dit impliceert dat een blockchain steeds een pseudoniem is, wat op zijn beurt dan weer in hoge mate verzoenbaar is met de GDPR. Meer nog, de GDPR moedigt zelfs pseudonimiseringsmaatregelen sterk aan.[65] Doch dient benadrukt dat sterke versleuteling geen inherente eigenschap is van blockchain technologie daar er verschillende types blockchains bestaan. Het zal van blockchain tot blockchain afhangen hoe sterk de ontwikkelaar ervan in de versleuteling voorzag. Zo bestaan er reeds geavanceerde versleutelingstechnieken die tot een zeer hoog niveau van bescherming of zelfs tot, weliswaar in mindere mate, tot anonimisering leiden. Zolang de oorspronkelijke gegevens of de sleutel bestaan is de mogelijkheid tot identificatie niet uitgesloten. Echter is een individuele beoordeling per concreet geval opportuun om uit te maken of de hoge norm van anonimisering werd bereikt en waardoor er geen sprake meer is van persoonsgegevens en de GDPR aldus niet langer van toepassing is.

3.2.2. Gedecentraliseerd en gedistribueerd

90. Zoals hoger al uiteengezet behelst blockchain technologie het gebruik van een soort database die gedistribueerd wordt over alle nodes, zonder dat een centrale autoriteit daarbij het beheer voert. In het bijzonder rijzen problemen met de permissionless of publieke blockchains. De GDPR werd immers geschreven op maat van gecentraliseerde databases waarbij de uitgewerkte verplichtingen en vereisten voor een verantwoorde persoonsgegevensverwerking en de bescherming ervan voorbijging aan gedecentraliseerde databases. In dat opzicht was de GDPR reeds achterhaald voordat ze in werking trad. Het ontbreken van een heldere juridische methode in de verordening voor gedecentraliseerde en universele databases doet het aantal gegevensbeschermingsinbreuken en privacy kwesties onvermijdelijk toenemen.[66]

91. Blockchaintechonologie wordt mijn inziens alzo te snel afgeschilderd als strijdig met de GDPR, doch kunnen *permissioned* of private blockchains grosso modo voldoen aan de verplichtingen en verantwoordelijkheden van organisaties om de rechten van betrokkenen m.b.t. hun persoonsgegevens te waarborgen en zoals omschreven in de GDPR. Conflict met de GDPR ontstaat

[64] R. BELEN-SAGLAM, E. ALTUNCU, Y. LU en S. LI, *A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems*, 2022, https://arxiv.org/abs/2210.04541, 15.
[65] Overweging 28 GDPR.
[66] O. AL MASHHOUR, A. AZIZ en N. MOHD NOR, "Blockchain and its entire eco-system: A legal consideration to an international cross-border technology", *International Journal of Multidisciplinary Sciences and Advanced Technology* 2022, vol 3, no 3, www.researchgate.net/publication/363645357_Blockchain_and_its_Entire_Eco-System_A_Legal_Consideration_to_an_International_Cross-Border_Technology/link/63273e180a70852150036b90/download, 21.

aldus voornamelijk bij publieke blockchains, maar is dat zo gek? Blockchains worden immers ingepast in een regelgeving die daar niet voor is gemaakt. De GDPR heeft geen rekening gehouden met gedecentraliseerd gegevensbeheer, waardoor het niet abnormaal is dat blockchain niet compliant lijkt te zijn met de GDPR. Eenzelfde vergelijking is een cakebeslag kloppen in een vierkante mengkom. Dan weten we op voorhand dat het droge deeg in de hoeken blijft kleven en het beslag nooit optimaal zal zijn.

3.2.2.1. De verwerkingsverantwoordelijke

92. Artikel 4, zevende lid GDPR definieert de verwerkingsverantwoordelijke als "de natuurlijke persoon of de rechtspersoon, overheidsinstantie, dienst of een ander orgaan die, alleen of samen met anderen het doel en de middelen van de verwerking van persoonsgegevens vastlegt." Opvallend is dat de GDPR in haar definitie van verwerkingsverantwoordelijke het enkelvoud hanteert, hetgeen mogelijk doelt op slechts één centrale entiteit die de rol van verwerkingsverantwoordelijk opneemt.

93. Op de schouders van de verwerkingsverantwoordelijke rust de verantwoordingsplicht, met andere woorden hij draagt de eindverantwoordelijkheid voor het volledige proces van de verwerking van persoonsgegevens.[67] Dit behelst onder andere de wijze waarop persoonsgegevens opgeslagen, beveiligd en overgedragen zullen worden, op welke manier de persoonsgegevens gebruikt zullen worden voor marketingdoeleinden en het verstrekken van informatie aan betrokkenen. Daarnaast staat hij in voor het waarborgen van de rechten toegekend door de GDPR aan te betrokkenen, te vrijwaren en te waarborgen. De verwerkingsverantwoordelijke beslist hoe en op welke wijze persoonsgegevens verwerkt zullen worden, waarbij het zijn taak is toezicht te houden op een met de GDPR conforme interne en eventuele externe verwerking van persoonsgegevens. Bij een niet-conforme verwerking van persoonsgegevens zal de verwerkingsverantwoordelijke aansprakelijk zijn voor de schade die, die niet-conforme verwerking teweeg bracht.

94. Het behoeft geen verder betoog dat de gedecentraliseerde aard van blockchain technologie hier een struikelblok vormt wanneer de verwerkingsverantwoordelijke aangeduid dient te worden. Bij een private blockchain kan er relatief eenvoudig de verwerkingsverantwoordelijke aangeduid worden daar het beheer en de toegang gecontroleerd wordt door één centrale autoriteit én de deelnemers beperkt en met toestemming tot de blockchain toetreden.[68] Het identificeren van een verwerkingsverantwoordelijke in een publieke *permissionless* blockchain is problematisch aangezien hier geen sprake is van centraal beheer en de GDPR de verantwoordingsplicht van de verwerkingsverantwoordelijke enkel in centrale organisaties benadrukt. Het is dus onduidelijk wie deze taak op zich neemt in een gedecentraliseerde blockchainomgeving. Publieke blockchains berusten op peer-to-peer netwerken, iedereen die zich bij dit netwerk aansluit wordt een knooppunt (*node*).[69] Niemand heeft de volledige controle over het systeem. Er ontbreekt dus een entiteit om een *block* te wijzigen of te corrigeren zodra het in de keten is opgenomen, vanwege de

[67] Art. 5, tweede lid GDPR.
[68] M. FINCK, *Blockchains and data protection in the European Union*, 2017, https://theblockchaintest.com/uploads/resources/Michele%20Finck%20-%20Blockchain%20and%20data%20Protection%20in%20the%20European%20Union%20-%20na.pdf, 16.
[69] J. RIPOSO, "Diffusion on the Peer-to-Peer Network." *Journal of Risk and Financial Management* 2022, 15:47, www.mdpi.com/1911-8074/15/2/47, 2.

decentralisatie. Iedereen in de keten kan als gegevensbeheerder worden aangemerkt en alle persoonsgegevens publiceren die hij wil. Omdat het moeilijk is één verwerkingsverantwoordelijke te identificeren bij publieke *permissionless* blockchains maakt dit een directe schending uit van de GDPR omdat zij in strijd is met artikel 5 GDPR, dat gericht is op het bevorderen van eerlijkheid, integriteit, privacy en veiligheid.[70]

95. Recente rechtswetenschappelijke literatuur omschrijft meerdere hypothesen om de verwerkingsverantwoordelijke te bepalen bij publieke *permissionless* blockchains.

96. Een eerste hypothese bestaat erin alle *nodes* te kwalificeren als verwerkingsverantwoordelijke omdat elke node vrij en onafhankelijk handelt, niet geïnstrueerd wordt door externe bevelen maar zelf bepaalt wat zij onderneemt in de blockchain. Doch loopt deze hypothese al snel tegen haar grenzen enerzijds omdat men bij toepassing van deze hypothese elke node kan aanmerken als een verwerkingsverantwoordelijke, hetgeen impliceert dat de in de verordening vastgelegde wettelijke verplichtingen op elk afzonderlijke node van toepassing is. Een extra hindernis voor de betrokkene om zijn rechten te kunnen uitoefenen in dit scenario is het uitzoeken wie hij moet aanspreken. Anderzijds omdat *nodes* geen inspraak hebben over de werkwijze en het functioneren van het blockchainsysteem. Bovendien zien alle *nodes* hetzelfde in de blockchain, met name de *gehashte* data waaraan zij geen wijzigingen kunnen aanbrengen door de onveranderlijke aard als wezenlijke eigenschap van een blockchain. *Nodes* bepalen dus niet de procedure hoe persoonsgegevens behandeld moeten worden, hetgeen een verwerkingsverantwoordelijke wel als kerntaak heeft.[71]

97. Een tweede hypothese bestaat erin de *nodes* te kwalificeren als een gezamenlijke verwerkingsverantwoordelijke. Het begrip "gezamenlijke verwerkingsverantwoordelijke" wordt in artikel 26 GDPR omschreven als " Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast (…) door middel van een onderlinge regeling (…)." In casu bepalen de nodes niet "gezamenlijk de doeleinden en de middelen van de verwerking" en evenmin op transparante wijze "hun respectieve verantwoordelijkheden bepalen", maar zij acteren onafhankelijk of zij zich al dan niet aansluiten bij een *permissionless* blockchain.[72]

98. De twee eerste hypotheses brengen geen soelaas voor de omschrijving van een concreet begrip van wie als de verwerkingsverantwoordelijke aangeduid kan worden in het geval van een publieke *permissionless* blockchain.

99. Een derde hypothese gaat de mogelijkheid na om *miners* te kwalificeren als gezamenlijke verwerkingsverantwoordelijke. Deze kwalificatie stoelt op het feit dat *miners* bepaalde *nodes* zijn die transacties valideren en blokken van gegevens aan elkaar vastmaken of toevoegen waardoor de

[70] R. BELEN-SAGLAM, E. ALTUNCU, Y. LU en S. LI, *A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems*, 2022, https://arxiv.org/abs/2210.04541, 7.
[71] M. FINCK, *Blockchains and data protection in the European Union*, 2017, https://theblockchaintest.com/uploads/resources/Michele%20Finck%20-%20Blockchain%20and%20data%20Protection%20in%20the%20European%20Union%20-%20na.pdf, 16.
[72] Art 26, eerste lid GDPR.

gegevens op permanente wijze worden opgeslagen in de blockchain.[73] Ook deze hypothese loopt al snel tegen haar grenzen op, daar de handelingen die *miners* stellen, grotendeels automatisch, computergestuurd en passief gebeuren, zonder dat zij daarin een eigen beslissingsrecht hebben met betrekking tot wijze waarop persoonsgegevens worden verwerkt. Hun rol is grotendeels technisch waarbij eigen beslissingsrecht ondergeschikt is. Het kan dan ook moeilijk aanvaard worden om *miners* te identificeren als gezamenlijke verwerkingsverantwoordelijke.

100. Een vierde hypothese is om de gebruikers, de betrokkenen zelf, aan te merken als verwerkingsverantwoordelijke. Het lijkt aanvaardbaar dat betrokkenen zelf zich ervan vergewissen welke risico's het toetreden tot een blockchain inhoudt voor hun persoonsgegevens. Men moge ervan uitgaan dat de betrokkene goede redenen heeft om toe te treden tot een blockchain. Het is aan de betrokkene zelf om te bepalen welke middelen zoals bijvoorbeeld hardware en software hij hiervoor gebruikt. In deze hypothese zal de betrokkene zijn eigen persoonsgegevens *hashen* en toevoegen aan de blockchain, hetgeen hem betrokkene én verwerkingsverantwoordelijke maakt.[74] Deze hypothese vergt enig inzicht en kennis van het individu. Bij een foute inschatting zijn de nefaste gevolgen dan ook voor eigen rekening. Het is te kort door de bocht om elke betrokkene ook aan te merken als verwerkingsverantwoordelijke, dit zal om gangbaar en werkbaar te worden in praktijk, geval per geval beoordeeld moeten worden.

101. Een vijfde hypothese is om de gebruiker, de betrokkene zelf, voor wat betreft de essentie, het doel, samen met de *nodes* voor wat betreft de niet-essentiële elementen zoals de middelen van de verwerking, samen aan te duiden als verwerkingsverantwoordelijke.[75] Deze hypothese kent voor- en tegenstanders. Het EU Blockchain Observatory and Forum en de Franse gegevensbeschermingsautoriteit (Commission Nationale de l'Informatique et des Libertés, hierna : CNIL) maken de inschatting aan de hand van de toets of gebruikers uit commerciële of professionele overwegingen persoonsgegevens aan de block toevoegen.[76] Zij die hun persoonsgegevens uit commerciële of professionele overwegingen toevoegen aan de block kunnen hun inziens dan ook aangemerkt worden als verwerkingsverantwoordelijke. Natuurlijke personen die zonder commerciële of professionele intenties persoonsgegevens toevoegen aan de block, vallen onder de uitzondering van zuiver persoonlijk of huishoudelijk gebruik[77], waardoor de GDPR geen toepassing vindt en zij dus ook niet aangemerkt kunnen worden als verwerkingsverantwoordelijke.[78] Een andere strekking meent dat de toepassing van deze vijfde hypothese logisch is en aldus dient te worden toegepast daar de gebruiker zelf beslist toe te treden tot de blockchain om alzo persoonsgegevens toe te voegen aan de block en de controle over zijn persoonsgegevens uit te oefenen aan de hand van

[73] J. CZARNECKI, *Blockchains and Personal Data Protection Regulations explained*, 2017, www.coindesk.com/markets/2017/04/26/blockchains-and-personal-data-protection-regulations-explained/.
[74] M. FINCK, *Blockchains and data protection in the European Union*, 2017, https://theblockchaintest.com/uploads/resources/Michele%20Finck%20-%20Blockchain%20and%20data%20Protection%20in%20the%20European%20Union%20-%20nhidea.pdf, 16.
[75] S. MARIEN, "Blockchain en GDPR op ramkoers?", *DataNews* 2018, (32) 35.
[76] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain*, 2018, www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, 2; THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, 2018, www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, 18.
[77] Art. 2, tweede lid 2, c) GDPR
[78] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain*, 2018, www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, 3; THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, 2018, www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, 18.

decryptiesleutel.[79] Ook de vijfde hypothese biedt geen duidelijk uitsluitsel over wie er nu als verwerkingsverantwoordelijke aangemerkt dient te worden in het voorliggende geval van een publieke *permissionless* blockchain.

102. Persoonlijk sluit ik me aan bij de visie van CNIL en het EU Blockchain Observatory and Forum, om vooraleer een gebruiker, de betrokkene aldus aan te merken als verwerkingsverantwoordelijke het toetsend criterium of de betrokkene persoonsgegevens vanuit commerciële of professionele overwegingen toevoegt aan een block, in aanmerking te nemen. Mijn inziens hangt de waarborging van de toegekende rechten inzake persoonsgegevens door de GDPR niet enkel af van de gegevensverwerker, maar dient ook het individu zelf ook een zekere behoedzame, aandachtige en weloverwogen keuzes te maken m.b.t. tot de doorgifte van zijn persoonsgegevens. Vanuit deze redenering ben ik hypothese 4 het meest genegen. Als men gebruik wenst te maken van nieuwe technologieën waarvoor er nog een juridisch privacyvacuüm bestaat, is het gebruik op eigen risico. De gebruiker dient een afweging te maken of een mogelijke inbreuk op persoonsgegevens opweegt tegen het voordeel dat hij bekomt door het gebruikmaken van de blockchain technologie.

103. Het is duidelijk dat het identificeren van de verwerkingsverantwoordelijke moeilijk is bij een publieke *permissionless* blockchain. De GDPR, noch haar overwegingen, vermelden geen "tussenoplossing" voor het geval dat er geen verwerkingsverantwoordelijke bestaat of deze niet geïdentificeerd kan worden. De niet-identificatie van een verwerkingsverantwoordelijke noopt automatisch tot een schending van de GDPR aangezien twee pertinente vragen over de "core business" van de GDPR zo onbeantwoord blijven. Tot wie moet de betrokkene zich wenden om zijn rechten uit te oefenen? Wie is aansprakelijk in geval van sancties? In het volgende hoofdstuk worden mogelijke oplossingen voor dit euvel aangereikt.

3.2.2.2. Recht van inzage

104. De veruitwendiging van het transparantiebeginsel in een afdwingbaar recht voor de betrokkene vertaalt zich in praktijk in het recht van inzage, omschreven in artikel 15 GDPR. De betrokkene heeft het recht te weten of zijn persoonsgegevens verzameld, verwerkt of opgeslagen worden en in voorkomend geval kan hij om nadere informatie en inzage verzoeken met betrekking tot het doeleinde van de verwerking, de categorieën van persoonsgegevens die verwerkt worden, de duurtijd dat zijn persoonsgegevens opgeslagen zullen worden of minstens de hoe de bewaartermijn berekend wordt en welke partijen ontvanger zijn van zijn persoonsgegevens.[80]

105. Bovendien bepaalt de GDPR dat wanneer persoonsgegevens van betrokkenen worden doorgegeven aan landen buiten de EU of aan internationale organisaties, de betrokkenen hiervan voorafgaand geïnformeerd moeten worden.[81] Blockchain technologie overschrijdt de grenzen van verschillende jurisdicties, wat betekent dat persoonsgegevens in blokken over de hele wereld aan elkaar worden geketend, meer precies, daar waar de *nodes* zich bevinden. Zelfs als de verwerking van persoonsgegevens van een EU-onderdaan buiten de grenzen van de EU gebeurt, zal de GDPR

[79] M. FINCK, *Blockchains and data protection in the European Union*, 2017, https://theblockchaintest.com/uploads/resources/Michele%20Finck%20-%20Blockchain%20and%20data%20Protection%20in%20the%20European%20Union%20-%20na.pdf, 7.
[80] Art. 15, eerste lid GDPR.
[81] Art. 15, tweede lid GDPR.

van toepassing zijn. Afhankelijk van de locatie van de *nodes*, die overal ter wereld kunnen zijn, kent blockchain technologie geen territoriale beperking in draagwijdte, in tegenstelling tot de GDPR.

106. Het is moeilijk om de verwerkingsverantwoordelijke te identificeren waaraan de betrokkene zijn recht van inzage kan richten, te meer omdat er geen sprake is van één centrale verwerkingsverantwoordelijke die dergelijke verzoeken kan en dient te behandelen, maar dat de betrokkene zich bij het gebruik van blockchain technologie bevindt in een systeem waarbij heel veel *nodes* transacties moeten verifiëren. Als *nodes* al aangemerkt kunnen worden als verwerkingsverantwoordelijke blijft betrokkene vooralsnog in het duister tasten over welke *node* nu zijn aanspreekpunt is om zijn recht op inzage te doen gelden, aangezien de gegevens opgeslagen in een *block* beveiligd zijn door pseudonimisering. Bij gebreke aan een duidelijk aanspreekpunt vervalt eveneens de mogelijkheid voor betrokkene om zekerheid te krijgen of zijn persoonsgegevens al dan niet verwerkt worden. In de veronderstelling dat de betrokkene er toch in slaagt de "juiste" *node* aan te spreken, die zijn persoonsgegevens heeft geverifieerd en toegevoegd, ziet enkel een versleutelde of *gehashte* versie van de persoonsgegevens in de blockchain, waardoor het verzoek tot inzage nog steeds geen bevredigend gevolg zal kennen voor betrokkene.[82] Hieruit vloeit voort dat ook andere waarborgen van rechten zoals het recht op beperking van verwerking[83], het recht op rectificatie[84] en het recht op gegevenswissing[85] op losse schroeven komen te staan.

3.2.2.3. Gegevensbescherming door ontwerp en door standaardinstellingen

107. *Privacy by desgin and default* zijn al jaren een gekend concept als procedurele vereiste om gegevensbescherming te bewerkstelligen. Dit beginsel wil ontwikkelaars, verwerkers en verwerkingsverantwoordelijken van meet af aan stimuleren om na te denken over gegevensbescherming als een kerngedachte van waaruit men start voor het ontwikkelen van een bepaalde technologie en niet als toevoeging. Niettegenstaande is gegevensbescherming door ontwerp op zich geen absolute verplichting voor de verwerkingsverantwoordelijke, maar (alleen) een aanmoediging om rekening te houden met het aspect van gegevensbescherming bij het ontwikkelen, ontwerpen, selecteren en gebruiken van instrumenten voor de verwerking van persoonsgegevens.[86] Een schoolvoorbeeld van *privacy by design* is de integratie van gegevensbeschermingssoftware in de (nieuwe) technologie, reeds bij de ontwikkeling en het ontstaan ervan.[87] De verordening verplicht evenwel geen enkele ontwikkelaar om een besturingsmechanisme op deze manier te creëren.[88]

108. Evenwel vereist artikel 25 GDPR dat de verwerkingsverantwoordelijke de relevante organisatorische en technische maatregelen te treffen zowel in het bepalen van de verwerkingsmiddelen als bij de verwerking zelf. Met andere woorden vereist men van de

[82] M. FINCK, *Blockchains and data protection in the European Union*, 2017, https://theblockchaintest.com/uploads/resources/Michele%20Finck%20-%20Blockchain%20and%20data%20Protection%20in%20the%20European%20Union%20-%20na.pdf, 22.
[83] Art. 18 GDPR.
[84] Art. 16 GDPR.
[85] Art. 17 GDPR.
[86] Overweging 78 GDPR.
[87] INTERSOFT CONSULTING, *GDPR Privacy by Design*, https://gdpr-info.eu/issues/privacy-by-design.
[88] M. BERBERICH en M. STEINER, "Practitioner's Corner - Blockchain Technology and The GDPR - How to reconcile Privacy and Distributed Ledgers?", *European Data Protection Law Review* 2016, volume 2, issue 3, (422) 423.

verwerkingsverantwoordelijke dat hij de relevante, organisatorische en technische maatregelen die hij nodig acht, effectief toepast om aan de vereisten van de verordening te voldoen en de rechten van betrokkenen te beschermen en te waarborgen.[89]

109. De bedoelde maatregelen hebben betrekking op gegevensminimalisatie, waarbij de gegevens die men verzamelt, verwerkt en bewaart beperkt tot datgene dat noodzakelijk is voor hun specifieke doeleinden, ook omschreven als gegevensbescherming door standaardinstellingen.[90] Zo kan een bedrijf alleen maar persoonsgegevens verwerken die nodig zijn voor hun legitieme en zakelijke doelen en niet langer dan nodig. Doel hierbij is om ongeautoriseerde toegang en gebruik van persoonsgegevens te voorkomen. Persoonsgegevens kunnen in beginsel enkel mits menselijke tussenkomst toegankelijk gemaakt worden voor een onbeperkt aantal natuurlijke personen.[91]

110. Blockchain technologie deed mondiaal zijn intrede in 2008, bij de publicatie van het witboek van Bitcoin door Satoshi Nakamoto, toen er nog geen sprake was van de GDPR. Bij de ontwikkeling van de bitcoinblockchain werd dus allerminst rekening gehouden met gegevensbescherming door ontwerp en standaardinstelling, omdat blockchain technologie de eerstgeborene is, nog voordat de GDPR uitwerking vond. Het behoeft geen uitgebreid betoog dat blockchain technologie dan ook moeilijk te rijmen valt met het beginsel van gegevensbescherming door ontwerp en door standaardinstelling. Het kenmerkende gedistribueerde karakter van blockchain technologie waardoor alle informatie met het hele netwerk wordt gedeeld druist dan ook in tegen het principe van gegevensbescherming door ontwerp. Het doel dat de maatregelen beogen in hoofde van gegevensbescherming door standaardinstelling en meer in het bijzonder: "*persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt*" [92] blijken erg problematisch bij blockchain. Wanneer toepassing wordt gemaakt van de blockchain technologie gebeuren meerdere processen automatisch zonder menselijke tussenkomt. Transactievalidatie gebeurt wanneer een gebruiker een transactie initieert zoals het verzenden van cryptovaluta naar een andere gebruiker, dan wordt deze transactie automatisch gecontroleerd door het netwerk om te bevestigen dat de gebruiker de benodigde fondsen heeft en dat de transactie niet eerder is uitgevoerd. Ook blokcreatie gebeurt automatisch, transacties worden automatisch gegroepeerd tot blokken door *miners* en deze worden vervolgens toegevoegd aan de *chain*. Door de automatische toevoeging van een *block* aan de *chain* worden de opgeslagen, weliswaar geëncrypteerde persoonsgegevens, zichtbaar voor iedereen aanwezig in de keten.

3.2.3. Onwijzigbaar en onverwijderbaar (permanent)

111. Daar waar GDPR gegevensbescherming (en afscherming) beoogt, hanteert blockchain technologie de werkwijze dat gegevens onveranderlijk, permanent en transparant zijn. De blockchain is in weze een *append-only* gedecentraliseerde database die door consensus algoritmen wordt onderhouden en op verschillende computers wordt opgeslagen.[93] Het permanente karakter ontstaat

[89] Art. 25 lid 1 GDPR.
[90] Art. 25, lid 2 GDPR.
[91] Art. 25, lid 2, in fine GDPR.
[92] Ibid.
[93] K. HEINES, "The risks and rewards of blockchain technology", *Risk management* 2016, afl. 4, p 6-7.

doordat gegevens, gecreëerd via cryptografische *hash*functies, eenmaal in een blok zijn verankerd en zijn vastgekoppeld aan het vorige blok, er nog zeer moeilijk wijzigingen kunnen gebeuren. Dus eenmaal iets opgeslagen in de blockchain impliceert in feite dus een definitieve opslag van die gegevens, met in principe de onmogelijkheid om dit nog te wijzigen. In theorie bestaat deze mogelijkheid wel, al is deze erg onrealistisch om toe te passen in praktijk. De enige mogelijkheid om alsnog gegevens opgeslagen in de *block* en toegevoegd aan de keten, te wijzigen is wanneer de meerderheid van de *nodes* consensus bereiken over de desbetreffende transactie.[94] Bijgevolg is er eveneens consensus nodig om de omgekeerde beweging uit te voeren, waarbij de hele blockchain moet worden losgekoppeld tot aan het desbetreffende block om het nadien terug vast te maken.[95]

112. Naast een samenwerking van meer dan de helft van de *nodes*, zou dit ook een immense computerkracht vergen waarbij de hele blockchain bovendien geblokkeerd blijft en nieuwe transacties verhinderd worden.[96] Deze optie is praktisch en operationeel niet wenselijk en bovendien onhaalbaar.

3.2.3.1. Recht op het wissen van gegevens

113. Artikel 17 GDPR, ook omschreven als het recht om vergeten te worden of het recht op vergetelheid is de concretisering van het beginsel van minimale gegevensverwerking zoals vervat in artikel 5,1., c) GDPR en het beginsel van opslagbeperking. Het recht van betrokkene om de verwerkingsverantwoordelijke te verzoeken zijn persoonsgegevens te wissen werd erkend door het Hof van Justitie in de *Google-Spain* zaak.[97] Het Hof oordeelde dat een inmenging op de rechten van betrokkene ter bescherming van zijn persoonsgegevens niet louter gerechtvaardigd kan worden door het economisch belang van de exploitant van de zoekmachine. Het hof stelt dat er een afweging gemaakt dient te worden tussen de rechten van betrokkene en de rechtmatige belangen van de onderneming, hetgeen impliceert dat het recht op vergetelheid geen absoluut recht is en het afhankelijk is van de concrete omstandigheden, die geval per geval beoordeeld moeten worden, welk recht zal prevaleren.

114. De verwerkingsverantwoordelijke zal in zes situaties verplicht gevolg dienen te geven aan de vraag tot wissing van persoonsgegevens. Met name indien (i)de persoonsgegevens niet langer nodig zijn in verband met de doeleinden waarvoor ze verwerkt worden, (ii) wanneer betrokkene zijn toestemming intrekt en er geen andere rechtsgrond bestaat voor de verwerking, (iii) wanneer betrokkene zijn recht op bezwaar uitoefent en bij afwezigheid van dwingende rechtvaardigingsgronden, (iv) in geval dat de persoonsgegevens onrechtmatig worden verwerkt, (v) om te kunnen voldoen aan een wettelijke verplichting en ten slotte, (vi) wanneer persoonsgegevens

[94] D. MEYER, *Blockchain technology is on a collision course with EU privacy law*, 2018, https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law.
[95] M. BERBERICH en M. STEINER, "Practitioner's Corner - Blockchain Technology and The GDPR - How to reconcile Privacy and Distributed Ledgers?", *European Data Protection Law Review* 2016, volume 2, issue 3, (422) 425.
[96] J. TENNISON, *What is the impact of blockchains on privacy?*, 2015, www.theodi.org/article/what-is-the-impact-of-blockchains-on-privacy.
[97] HvJ 13 mei 2014, nr. C-131/12, ECLI:EU/C:2014:317, Google Spain.

verzameld zijn met betrekking tot een aanbod van diensten van de informatiemaatschappij aan kinderen zoals vermeld in art. 8, eerste lid GDPR.[98]

115. Wanneer de verwerkingsverantwoordelijke een verzoek ontvangt om persoonsgegevens te wissen, neemt hij "*rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen* (…)"[99] Deze bepaling lijkt enige speelruimte te bieden voor een alternatieve oplossing, rekening houdend met de "beschikbare technologie" die van nature uit een onveranderlijk karakter heeft waardoor het wissen van persoonsgegevens technisch niet haalbaar is of onevenredige inspanningen zou vergen. Bijgevolge kan de verwerkingsverantwoordelijke niet verplicht worden tot het behalen van een gunstig resultaat dat ze realistisch gezien niet kunnen garanderen.

116. De blockchain technologie komt hier in conflict met het recht op gegevenswissing en dit door de architectuur van de technologie. Blockchain is niet in staat om gegevens die erin zijn opgeslagen te vergeten. In theorie blijven de gegevens definitief en permanent op de blockchain staan, doordat *hashes* verwijzen naar de voorgaande *blocks* die gegevens bevatten. Gedistribueerde grootboektechnologie staat haaks op het recht op gegevenswissing voortvloeiend uit het principe van minimale gegevensverwerking zoals opgelegd door de GDPR.

117. Blockchain technologie hanteert daarentegen het omgekeerde principe, namelijk een *append-only* mechanisme waarin gegevens aanpassen zeer moeilijk tot onmogelijk is met als doel bestand te zijn tegen censuur.[100] De kerneigenschappen van blockchain technologie zijn de onveranderlijkheid van gegevens en de daaruit voortvloeiende onwisbare of permanente opslag van die gegevens. Het recht op gegevenswissing in haar zuivere vorm zal dus geen toepassing kunnen vinden bij het gebruik van blockchain technologie.

3.2.3.2. Recht op rectificatie

118. Artikel 16 GDPR kent aan betrokkenen het recht van rectificatie toe in navolging van het nauwkeurigheidsprincipe dat vereist dat gegevens actueel en relevant zijn voor het doel waarvoor zij worden verwerkt. Het is aan de verwerkingsverantwoordelijke om een procedure uit te schrijven om onvolledige of onjuiste informatie onmiddellijk te kunnen corrigeren of zelfs te wissen.[101] Om de accuraatheid van gegevens te kunnen waarborgen dienen zij regelmatig bijgewerkt te worden zodat ze steeds relevant zijn voor de huidige situatie van betrokkene.

119. In de doelstelling van de Europese Unie om betrokkene meer controle over hun persoonsgegevens te geven voorziet de regelgeving in een tweeledig recht op rectificatie.

120. Enerzijds het recht aan de betrokkene verschaffen om (i) onjuiste gegevens te corrigeren, (ii) alsook de mogelijkheid om op elk moment onvolledige gegevens aan te vullen onder meer door het verstrekken van een aanvullende verklaring.[102] De verwerkingsverantwoordelijke is belast met een kennisgevingsplicht van de rectificatie aan andere partijen, tenzij dat onmogelijk of onevenredig veel inspanning vergt. Om het recht op rectificatie bij blockchain technologie te handhaven dient

[98] Art. 17, eerste lid GDPR; Overweging 65 GDPR.
[99] Art. 17, tweede lid GDPR.
[100] S. NAKOMOTO, *Bitcoin: A peer-to-peer electronic cash system*, 2008, https://bitcoin.org/bitcoin.pdf, 1.
[101] Art. 5, eerste lid, (d) GDPR.
[102] Art. 16 GDPR.

opnieuw gezegd dat het voor de betrokkene moeilijk is om te bepalen wie zijn aanspreekpunt is als verwerkingsverantwoordelijke. In de hypothese dat hij succesvol de *node* kan aanspreken die toegang heeft tot zijn persoonsgegevens, kunnen de gegevens op de blokchain vooralsnog niet gewijzigd worden door de onveranderlijke en permanente aard van de transacties in blockchain technologie. Doch zou het recht op rectificatie conflictloos toepassing vinden indien door toevoeging van correcte en aanvullende informatie, opgenomen in een nieuwe *block*, de foutieve (en onvolledige) gegevens corrigeert. Het *apply only* mechanisme staat de toevoeging van een nieuwe *block* met aanvullende informatie ter correctie van reeds bestaande gegevens in de blockchain niet in de weg, maar wel dient opgemerkt dat hierdoor de incorrecte gegevens daarom niet verwijderd zijn van de blockchain. De blijvende aanwezigheid van incorrecte gegevens kan mogelijk nadelig zijn voor de betrokkene. Een volledige waarborg van het recht op rectificatie blijft aldus uit in het kader van blockchain technologie aangezien gegevenscorrectie door vervanging van onjuiste gegevens onrijmbaar is met het permanente karakter van de blockchain.

3.2.3.3. Recht op beperking van de gegevensverwerking

121. Het principe van opslagbeperking houdt in dat de persoonsgegevens die verwerkt worden niet langer mogen worden opgeslagen dan nodig is voor de doeleinden waarvoor zij verwerkt wordt.[103] Dit ter bescherming van de identiteit van de betrokkene, die niet langer achterhaald kan worden. De verwerkingsverantwoordelijke dient een doeltreffend bewaarbeleid te voeren om te voorkomen dat gegevens langer bewaard worden dan nodig. Hoe lang gegevens bewaard worden moet gebaseerd zijn op een specifiek doel, waarvoor de verwerking nodig is en de toepasselijke wetgeving. Een bewaarbeleid kan bijvoorbeeld een bewaartermijn van 5 jaar na het aflopen van de verzekeringspolis vastleggen omdat op die manier eventuele geschillenbeslechting mogelijk blijft. Na het verstrijken van de bewaartermijn dient de verwerkingsverantwoordelijke de persoonsgegevens te anonimiseren of definitief te verwijderen.

122. Artikel 18 van de GDPR omschrijft het recht op beperking van de verwerking en verplicht de verwerkingsverantwoordelijke om de verwerking van de persoonsgegevens van betrokkene te beperken op diens vraag in vier voorkomende situaties: (i) de correctheid van de persoonsgegevens wordt betwist, (ii) de verwerking onrechtmatig is en waarbij de betrokkene zich verzet tegen het wissen van deze persoonsgegevens, (iii) indien de verwerkingsverantwoordelijke de gegevens niet meer nodig heeft maar betrokkene inzake het voeren of zich verweren in een rechtsvordering, (iv) indien de betrokkene bezwaar maakte tegen de verwerking en wachtende is op een antwoord op de vraag of er rechtvaardigingsgronden zijn in hoofde van de verwerkingsverantwoordelijke die zwaarder doorwegen.[104]

123. Opnieuw botst een gegevensbeschermingsrecht tegen het permanente karakter van de blockchain door haar *apply only* mechanisme, zodat gegevens niet gewist kunnen worden, zelfs niet wanneer de verwerkings- en bewaartermijnen verlopen zijn. In het geval dat foutieve persoonsgegevens zijn opgeslagen in de blockchain heeft de betrokkene het recht om de beperking van de verwerking te vragen aan de verwerkingsverantwoordelijke. De foutieve gegevens opgeslagen

[103] Art. 5, eerste lid, e) GDPR.
[104] Art. 18, eerste lid GDPR.

in de blockchain mogen *an sich* blijven bestaan, op voorwaarde dat er verder niets mee gebeurt. Opnieuw blijkt het waarborgen van een gegevensbeschermingsrecht van betrokkene problematisch aangezien blockchain technologie gebruikmaakt van meerdere automatische processen. *Miners* groeperen automatisch transacties in blokken, die worden toegevoegd aan de keten, waarbij automatisch een nieuwe kopie wordt gegenereerd voor de laatste deelnemer in het netwerk. Maar ook het toevoegen van een nieuwe *block* aan de blockchain maakt dat een update automatisch verspreid wordt naar alle *nodes* in het netwerk. *Nodes* beschikken over een kopie van de volledige blockchain, die voortdurend wordt bijgewerkt. Deze werkwijze impliceert dat persoonsgegevens blijvend opnieuw worden verwerkt. Vervolgens lopen we opnieuw tegen het permanente karakter van de blockchain doordat het onmogelijk is de desbetreffende persoonsgegevens er uit te halen en te verwijderen om een verdere verwerking ervan te voorkomen. De persoonsgegevens die een beperking van de verwerking rechtvaardigen blijven alzo blijvend verwerkt doordat ze in de keten blijvend gekopieerd en geüpdatet worden in functie van het berekenen van de *hash*waarden. Het recht op beperking van verwerking kan niet gewaarborgd worden bij blockchain technologie.[105]

3.2.3.4. Recht op overdraagbaarheid

124. Betrokkenen hebben recht op overdraagbaarheid van hun persoonsgegevens waardoor zij een kopie in een digitaal leesbaar en gangbaar formaat van de verwerkingsverantwoordelijke kunnen vragen, om hun gegevens te kopiëren of over te dragen van het ene elektronische verwerkingssysteem naar een ander op een veilige manier zonder dat de bruikbaarheid ervan wordt aangetast.[106] Betrokkene kan de verwerkingsverantwoordelijke eveneens verzoeken zijn persoonsgegevens rechtstreeks over te maken aan een andere verwerkingsverantwoordelijke. Zo kan gegevensoverdracht gebeuren zonder het moeizame proces de persoonsgegevens van de oorspronkelijke eigenaar te krijgen.[107] Voornoemd recht stelt individuen in staat om controle uit te oefenen over hun persoonsgegevens en deze te kunnen verplaatsen tussen aanbieders.[108] Het recht van overdraagbaarheid is van toepassing op alle gegevens die de betrokkene heeft verstrekt aan de verwerkingsverantwoordelijke. Het recht op overdraagbaarheid van persoonsgegevens lijkt gewaarborgd te zijn doordat de uitoefening ervan verenigbaar is met de technische eigenschappen van de blockchain. Zowel de controle als de overdracht van persoonsgegevens zijn gewaarborgd door de blockchain doordat zij gegevens die op het grootboek staan beschermt door pseudonimisering en zij in het geval ze geregistreerd zijn in een openbare blockchain ook beschikbaar zijn voor het grote publiek.

---

[105] R. LEENES, W. KAUFMANN, M. SCHELLEKENS, F. SCHEMKES en E. TJONG TJIN TAI, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, 2019, www.stibbe.com/sites/default/files/2022-07/tk_bijlage_blockchain_en_het_recht_def_8316.pdf, 24.
[106] Art. 20 GDPR.
[107] M. GODDARD, "The EU General information protection regulation (GDPR): European regulation that has a global impact, *International Journal of Market Research* 2017, vol. 59, issue 6, https://eclass.upatras.gr/modules/document/file.php/CULTURE110/goddard2017.pdf, (703) 703.
[108] L. MARELLI en G. TESTA, "Scrutinizing the EU general information protection regulation", *Science* 2018 , vol. 360, issue 6388, https://lastatalenews.unimi.it/sites/default/files/attachments/Marelli%20and%20Testa%20Science%202018.pdf, (496) 498.

125. CNIL bevestigt dat er geen probleem is met de uitoefening van het recht van overdraagbaarheid van persoonsgegevens in blockchains.[109] Doch blijkt een mogelijke moeilijkheid bij het ten gelde maken van het recht op overdraagbaarheid, m.n. de kopie van de gegevens vereist in een gebruiksvriendelijk formaat. Dit kan problematisch zijn omdat verschillende blockchainplatforms incompatibel zijn met elkaar door het ontbreken van standaardisatie tussen verschillende blockchains waardoor overdracht in een gebruiksvriendelijk formaat moeilijk kan zijn.[110]

3.3. Tussenbesluit: gedetecteerde privacy conflicten bij het gebruik van blockchain technologie

126. Een toetsing van de kenmerkende eigenschappen van blockchain technologie aan de waarborgen geboden door de GDPR resulteert onomstotelijk in enkele conflicten. Ondanks dat de GDPR een technologie neutrale opvatting hanteert, de bescherming van persoonsgegevens mogen immers niet afhankelijk zijn van het soort technologie dat gebruikt wordt, is het duidelijk dat de GDPR is geschreven vanuit de opvatting van gecentraliseerd gegevensbeheer. Er werd geen rekening gehouden met systemen die persoonsgegevens op decentrale wijze verwerken, derhalve moet de GDPR evenzeer toepassing vinden wanneer deze nieuwe technologieën persoonsgegevens verwerken. Doordat de wetgeving zich niet leent voor decentraal gegevensbeheer zijn er automatisch meer inbreuken op gegevensbescherming zoals voorzien door de GDPR. Het is alsof de GDPR ingrediënten verstrekt om het gerecht konijn met pruimen klaar te maken maar dan wel eist dat je met die ingrediënten een appelcake zou bakken? Een tweeledig gegevensbeschermingsconflict wordt vastgesteld. Ten eerste zorgt het decentrale en gedistribueerde karakter van een blockchain voor een uiterst moeilijke identificatie van de verwerkingsverantwoordelijke. Meerdere hypotheses werden besproken, doch kon geen enkele volledige overtuiging bieden voor de waarborging van de rechten op gegevensbescherming. De identificatie van de verwerkingsverantwoordelijke hangt af van de gebruikte blockchain. In private *permissioned* blockchains is het mogelijk een centrale entiteit te identificeren die het doel en de middelen voor de verwerking van persoonsgegevens vastlegt. Het zijn voornamelijk publieke *permissionless* blockchains die problematisch zijn voor het aanduiden van de verwerkingsverantwoordelijke. Indien deze niet aangeduid kan worden of kenbaar is voor de betrokkene komen meerdere waarborgen zoals bijvoorbeeld het recht op inzage onder druk te staan.

127. Ten tweede botst het permanent karakter van blockchain technologie met de uitoefening van belangrijke rechten van betrokkenen. Het *apply only* mechanisme behelst dat er alleen gegevens kunnen worden toegevoegd maar niet kunnen worden gewijzigd. Dit leidt ertoe dat het recht om vergeten te worden en het recht op rectificatie alsook het recht op beperking van verwerking niet gewaarborgd kan worden bij het gebruik van blockchain technologie. De werkwijze van blockchain technologie waarbij persoonsgegevens permanent bewaard blijven zijn strijdig met het algemeen

[109] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Solutions for a responsible use of the blockchain in the context of personal data*, 2018, www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.
[110] T. KUSBER, S. SCHWALM, K. SHAMBURGER, U. KORTE, "Criteria for trustworthy digital transactions - Blockchain/DLT between eIDAS, GDPR, data and evidence preservation" in H. ROßNAGEL, C. SCHUNCK, S. MÖDERSHEIM, D. HÜHNLEIN (eds.) *Open identity summit 2020, Lecture notes in informatics (LNI)*, 2020, https://dl.gi.de/bitstream/handle/20.500.12116/33181/proceedings-04.pdf?sequence=1&isAllowed=y, (49) 56.

beginsel van minimale gegevensverwerking en opslagbeperking evenals met het principe gegevensbescherming door ontwerp en standaardinstelling. Concluderend kan men vaststellen dat de zuiverste vorm van GDPR voor wat betreft het aangehaalde tweeledige conflict niet compatibel is met blockchain, terwijl blockchain technologie niet compatibel is met de GDPR.[111] Daar waar de GDPR, EU onderdanen voorziet van een arsenaal aan rechten om de controle over hun persoonsgegevens te kunnen voeren, zijn blockchains ontworpen om er voor te zorgen dat gegevens niet worden gewijzigd zonder het compromitteren van de integriteit van de volledige keten. In praktijk kunnen gegevens slechts worden bijgewerkt door een extra blokcreatie. Het gedecentraliseerd karakter vereist dan ook dat een hoog niveau van transparantie noodzakelijk is om het consensusmechanisme te kunnen bewerkstelligen. In een blockchain zijn dus alle gegevens zichtbaar voor iedereen in het netwerk, hetgeen vanuit gegevensbeschermingsoogpunt niet wenselijk is in het licht van de GDPR.

128. Toch kan de gemeenschappelijke noemer van gegevensbeveiliging onderscheiden worden tussen blockchain technologie en de waarborgen die de GDPR vooropstelt. Het versleutelde karakter van blockchain technologie is volledig verenigbaar met de vereiste dat verwerkingsverantwoordelijken de passende organisatorische en technische maatregelen moet voorzien om persoonsgegevens te beveiligen. Pseudonimisering wordt door de GDPR zelfs sterk aangemoedigd. Blockchain technologie mag dan niet voldoen aan de letter van de wet, toch streeft zij evenwel de geest van de GDPR na, met name het waarborgen van vertrouwen, traceerbaarheid en de veiligheid van transacties, waarin persoonsgegevens verwerkt worden. GDPR en blockchain technologie mogen dan wel wezenlijk verschillen in gehanteerde architectuur, hun doel ligt op één lijn.

129. Het feit dat GDPR en *distributed ledger* technologie op bepaalde vlakken diametraal tegenover elkaar staan behelst niet dat er in navolging van eventuele aangepaste wetgeving geen initiatieven genomen kunnen worden om blockchain technologie meer GDPR conform te maken. Totdat er nieuwe wettelijke richtlijnen vastgelegd zijn is het aan blockchainontwikkelaars om creatieve oplossingen te zoeken en is het roeien met de spreekwoordelijke riemen om vooralsnog te kunnen voldoen aan de gegevensbeschermingsverplichtingen zoals opgenomen in de GDPR. In het volgende hoofdstuk bespreken we mogelijke oplossingen om GDPR-conformiteit te bewerkstelligen bij het gebruik van blockchain technologie.

4. Initiatieven tot het verzoenen van de blockchain en de GDPR

130. In dit hoofdstuk wordt nagegaan welke juridische en technische middelen aangewend kunnen worden in blockchaintechnologie om te kunnen voldoen aan de GDPR en om het hoofd te bieden aan de vastgestelde moeilijkheden uit het vorige hoofdstuk. De twee belangrijkste problemen, eveneens omschreven door het *EU Blockchain Observatory and Forum* zijn de identificatie van de verwerkingsverantwoordelijke en het recht op het wissen van persoonsgegevens.[112] Vooreerst worden de mogelijkheden met betrekking tot de identificatie van de verwerkingsverantwoordelijke besproken om nadien een algemeen overzicht te geven van creatieve, technische of juridische middelen die blockchains meer GDPR conform maken.

4.1. Identificatie van de verwerkingsverantwoordelijke

131. Zoals reeds besproken is de identificatie van de verwerkingsverantwoordelijke problematisch en allerminst vanzelfsprekend bij blockchaintechnologie. Het is van belang om een onderscheid te maken tussen *private permissioned* en *public permissionless* blockchains. De problemen doen zich voornamelijk voor bij het laatste soort van blockchains omdat iedereen kan toetreden tot de blockchain en waarbij *nodes*, die vaak onbekend zijn voor de gebruikers, het systeem besturen. Een interessante mogelijkheid bestaat erin dat regelgevers met normen en minimumvereisten komen die vervolgens in een *code* vertaald en geïmplementeerd wordt in het protocol van een blockchain om GDPR regelgeving van meet af aan te bevorderen. Doch blijkt Europa niet geneigd om minimumnormen uit te vaardigen. Dit zou immers raken aan het hoge beschermingsniveau dat de GDPR vereist en rechtsonzekerheid bewerkstelligen. IBANEZ, O'HARA en SIMPERL stellen twee mogelijkheden voor om de verwerkingsverantwoordelijke te kunnen identificeren bij *public permissionless* blockchains.

132. In een eerste scenario wordt er gekeken of er een direct dan wel een indirect contact tussen de gebruiker en de blockchain bestaat. Bij een rechtstreeks contact tussen beiden zal de verwerkingsverantwoordelijke aangeduid worden als verwerkingsverantwoordelijke, bij gebrek aan een andere mogelijke verwerkingsverantwoordelijke. Voormelde auteurs opperen om in dit geval de blockchain zodanig te ontwikkelen dat de conformiteit met de gegevensbeschermingsregels verzekerd is door haar technische eigenheid.[113] Auteurs wijzen op het belang van twee elementen bij het ontwikkelen van blockchains. Ten eerste dat de blockchain moet verhinderen dat gebruikers bepaalde soorten van persoonsgegevens aan de blockchain toevoegen. Ten tweede, dat de blockchain de invoer van een rechtmatige verwerkingsgrond zoals bepaald in artikel 6 GDPR vereist voordat gebruikers persoonsgegevens aan de blockchain kunnen toevoegen. Betrokkene wordt hier zelf verwerkingsverantwoordelijke, hetgeen in schril contrast staat met hoe de GDPR de verschillende rollen van de betrokkene en verwerkinsverantwoordelijke strikt afbakent, mogelijk komt de bescherming van de betrokkene in het gedrang, daar hij zelf verantwoordelijk is voor de verwerking

[112] THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, 2018, www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, 5.
[113] L.-D. IBANEZ, K. O'HARA en E. SIMPERL, *On blockchains and the general data protection regulation*, 2018, www.researchgate.net/publication/326913146_On_Blockchains_and_the_General_Data_Protection_Regulation, 8.

van zijn persoonsgegevens.[114] De GDPR legt de verwerkingsverantwoordelijke verplichtingen op, maar het is aan hem om een inschatting te maken of de blockchain voldoet aan de vereisten van de GDPR.

133. In een tweede scenario heeft de gebruiker indirect contact met de blockchain en fungeert de blockchain als communicatiemiddel. Dit scenario veronderstelt het gebruik van een applicatie die de persoonsgegevens van betrokkene off-chain opslaat. In deze situatie zullen de eigenaars van de applicatie waarin de persoonsgegevens verwerkt worden aangeduid worden als verwerkingsverantwoordelijke. Zij bepalen immers het doel en de middelen voor de verwerking van de persoonsgegevens die erin worden verwerkt. Als verwerkingsverantwoordelijke kan eveneens aangeduid worden de persoon achter de applicatie of het *smart contract*, wanneer deze persoon identificeerbaar is.[115] Ook de Franse toezichthoudende autoriteit CNIL is de mening toegedaan dat gebruikers van de blockchain die een schrijfrecht hebben op de keten en die besluiten om gegevens ter validatie aan te bieden door *miners* kunnen aangeduid worden als verwerkingsverantwoordelijke.[116] Hieruit vloeit voort dat de CNIL elke rechtspersoon die namens een natuurlijke persoon persoonsgegevens registreert in een blockchain identificeert als verwerkingsverantwoordelijke.

4.2. Off-chain opslag

134. Off-chain opslag betekent dat persoonsgegevens verhuizen naar een andere locatie, buiten de blockchain.[117] Uiteraard is het van belang dat de andere locatie voldoende waarborgen biedt voor gegevensbescherming.

135. Off-chain opslag van persoonsgegevens, dus het opslaan van persoonsgegevens buiten de blockchain biedt een oplossing aan meerdere conflicten die zich voordoen door de fundamentele verschillen in hoe beide systemen zijn ontwerpen en functioneren. Het conflict ontstaat door de onveranderlijke aard van gegevens die in een blockchain zijn opgeslagen.

136. In de eerste plaats biedt off-chain opslag een oplossing voor het conflict met het recht op wissen of het recht om vergeten te worden alsook het recht op rectificatie. Betrokkenen hebben het recht om hun persoonsgegevens te laten verwijderen. Gegevens die vervat zijn in een block en toegevoerd worden aan de keten kunnen niet gewijzigd of verwijderd worden.[118] Door persoonsgegevens off-chain op te slaan kunnen deze wel gewijzigd of verwijderd worden wanneer

[114] R. TEPERDJIAN, ''The puzzle of squaring blockchain with the general data protection regulation,'' *Forthcoming in jurimetrics* 2020, vol. 60, issue no. 3, https://ssrn.com/abstract=3638736, (1) 6.
[115] M. POPPE en T. VERBIEST, "Quelle relation entre la protection des données à caractère personnel et la blockchain?", *Revue Lamy Droit des Affaires* 2017, no. 129, www.degaullefleurance.com/wp-content/uploads/2017/10/Dossier-Blockchain-RLDA.pdf, (38) 39.
[116] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain*, 2018, www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, 2.
[117] J. EBERHARDT en S. TAI, *On or off the blockchain? Insights on off-chaining computation and data*, 2017, www.researchgate.net/publication/319416136_On_or_Off_the_Blockchain_Insights_on_Off-Chaining_Computation_and_Data, 3.
[118] B. VARGHESE, M. VILLARI, O. RANA, P. JAMES, T. SHAH, M.FAZIO en R. RANJAN, ''Realizing edge marketplaces: Challenges and opportunities,'' *IEEE Cloud Computing* 2018, vol. 5, no. 6, 2018, https://ieeexplore.ieee.org/document/8552630, (9) 11.

nodig. On-chain wordt dan enkel een *hashwaarde* in de blockchain opgeslagen.[119] Echter dient men voor ogen te houden dat de persoonsgegevens die de *gehashte* data koppelen aan de betrokkene *off-chain* worden bewaard en in een latere fase worden gewist. Pas na verwijdering van de persoonsgegevens zal de *gehashte* data als voldoende anoniem beschouwd worden.[120] Feit blijft wel dat de *hash* die verwijst naar de data die *off-chain* is opgeslagen in een specifieke inhoudsversie van een bepaald tijdstip bestond en dus aanwezig blijft in de blockchain. Desalniettemin zal na verwijdering van de persoonsgegevens *off-chain* de *hash on-chain* louter nog verwijzen naar gegevens die verwijderd zijn.

137. Ten tweede biedt de off-chain opslag soelaas voor het conflict met het beginsel van minimale gegevensverwerking. Onder de GDPR mag men slechts die persoonsgegevens verwerken die noodzakelijk zijn voor een legitiem of zakelijk doel en waarbij de persoonsgegevens niet op onverenigbare wijze met dat doel worden verwerkt.[121] De gedecentraliseerde en gedistribueerde aard van blockchaintechnologie maakt dat een hoog niveau van transparantie tussen de verschillende *nodes*, die op basis van een consensusmechanisme transacties valideren en groeperen in *blocks*, die vervolgens worden toegevoegd aan de keten, is vereist. Elke *node* bewaart een kopie van de gegevens in de keten, die bovendien telkens een nieuwe *block* toevoegen en updaten.[122] Ook de onveranderlijkheid van de blockchain maakt dat opgeslagen gegevens voor onbepaalde tijd deel uitmaken van de keten, terwijl er steeds meer *blocks* aan de keten worden toegevoegd. Ontwikkelingen in dit verband waarbij blockchains kunnen voldoen aan het beginsel van minimale gegevensverwerking is wanneer persoonsgegevens *off-chain* worden geregistreerd en geminimaliseerd om binnen het gegevensbeschermingskader van de GDPR te blijven. Slechts overdraagbare gegevens (transactiegegevens) kunnen *off-chain* opgeslagen worden. *Public keys* daarentegen kunnen niet *off-chain* opgeslagen worden omdat zij noodzakelijk zijn om transacties van gegevens in de *block* te laten plaatsvinden.[123] Doordat *public keys* alleen op de blockchain opgeslagen kunnen worden, kunnen de gegevens die erop geregistreerd staan, niet gewist worden.

138. Ten derde kan de methode van *off-chain* opslag de waarborg van gegevensbescherming door ontwerp en standaardinstelling, die voorop stelt dat gegevensbescherming vanaf het begin in nieuwe systemen en technologieën moet worden ingebouwd, faciliteren. Potentieel kan de blockchain zo ontwikkeld worden dat gevoelige gegevens bijvoorbeeld steeds *off-chain* opgeslagen moeten worden. De betrokkene wiens persoonsgegevens *off-chain* opgeslagen zijn, wordt eigenaar van de *private key*, die toegang geeft tot de gegevens opgeslagen in het off-chain gedeelte. Hierdoor wordt aan de betrokkene meer controle gegeven over zijn persoonsgegevens.

---

[119] C. LIMA, *How decentralized blockchain internet will comply with GDPR data privacy*, 2018, https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf, 3.
[120] N. EICHLER, N. JONGERIUS, S. McMULLEN, O. NAEGELE, L. STEININGER en K. WAGNER, *Blockchain, data protection, and the GDPR*, 2018, www.crowdfundinsider.com/wp-content/uploads/2018/06/GDPR_Position_Paper_v1.0.pdf, 4.
[121] Art. 5, lid 1, onder b) GDPR.
[122] J. HALAMKA, A. LIPPMAN en A. EKBLAW, *The potential for blockchain to transform electronic health records*, 2017, https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.
[123] M. FINCK, *Blockchains and data protection in the European Union*, 2017, https://theblockchaintest.com/uploads/resources/Michele%20Finck%20-%20Blockchain%20and%20data%20Protection%20in%20the%20European%20Union%20-%20na.pdf, 14 en 21.

139. Ten slotte kan *off-chain* opslag ook tegemoet komen aan het recht van inzage en aan het recht van overdraagbaarheid van persoonsgegevens. De GDPR geeft aan individuen het recht om hun persoonsgegevens in een gestructureerd, algemeen gangbaar en machinaal leesbaar formaat te ontvangen en over te dragen. Dit kan moeilijk te realiseren zijn doordat vele blockchainplatfora niet compatibel zijn met elkaar en bovendien een complexe technische aard van gegevensstructuur hanteren. Off-chain opslag van persoonsgegevens kan hieraan tegemoet komen.

140. In de meeste van bovengenoemde gevallen zal de *off-chain* opslag eerder de gebiedende wijs dan een vrijblijvende optie uitmaken om te kunnen voldoen aan de verplichtingen van gegevensbescherming in de GDPR. *Off-chain* opslag zorgt voor wat betreft overdraagbare transactiegegevens voor een oplossing. *Off-chain* opslag maakt het mogelijk om beperking van verwerking van persoonsgegevens te realiseren of om persoonsgegevens na een bepaalde termijn te wissen of te anonimiseren. Belangrijk om in het achterhoofd te houden is dat wanneer er geopteerd wordt voor *off-chain* opslag, de fundamentele eigenschappen die blockchaintechnologie biedt niet uitgehold wordt opdat er geen vertrouwen in anderen noodzakelijk is om toch veilig gebruik te kunnen maken van het systeem.[124]

141. Er wordt dan ook aanbevolen om enkel als het noodzakelijk is persoonsgegevens op de blockchain op te slaan en zo veel als mogelijk te opteren voor een *off-chain* opslag van persoonsgegevens. Bovendien wordt het sterk afgeraden om gevoelige gegevens zoals medische gegevens in een *public permissionless* blockchain op te slaan.

4.3. Encryptietechnieken

142. Door persoonsgegevens te encrypteren kunnen enkel personen met een decryptiesleutel ze ontcijferen. Wanneer de betrokkene zijn recht op vergetelheid wil laten gelden, kan het vernietigen van de decryptiesleutel volstaan opdat niemand de gegevens nog kan lezen waardoor ze in feite als gewist aanschouwd kunnen worden, ondanks dat ze niet fysiek van de blockchain verwijderd zijn maar niet langer leesbaar zijn.[125] Bijgevolg kunnen de gegevens de betrokkene niet meer identificeren waardoor de GDPR niet langer van toepassing is.[126]

143. Geavanceerde encryptietechnieken kunnen zorgen voor een toenemende mate van pseudonimiteit en in bepaalde gevallen ook anonimiteit. De vraag blijft echter, in een snel evoluerend en veranderend digitaal tijdperk, waarin nieuwe decryptiemogelijkheden zoals *quantum decryption*[127] worden ontwikkeld, het vernietigen van de decyrptiesleutel zal volstaan om persoonsgegevens werkelijk anoniem te maken. De Artikel 29 Werkgroep benadrukt dat het feit of een encryptietechniek

[124] Idem 102.
[125] P. HRISTOV en W. DIMITROV, *The blockchain as a blackbone of GDPR compliant frameworks*, 2018, www.researchgate.net/publication/328576742_The_blockchain_as_a_backbone_of_GDPR_compliant_frameworks, 7.
[126] Overweging 26 GDPR; GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Advies 05/2014 over anonimiseringstechnieken*, 10 april 2014, https://docplayer.nl/amp/422750-Groep-gegevensbescherming-artikel-29.html, 5.
[127] C. BURCHETT, *How to fight the coming quantum decryption treath?*, 2018, www.enterpriseai.news/2018/07/12/how-to-fight-the-coming-quantum-data-decryption-threat.

nu al dan niet tot anonimisering leidt, geval per geval beoordeeld moet worden.[128] Geëncrypteerde gevoelige gegevens of persoonsgegevens die lange tijd op de blockchain blijven opgeslagen vormen een schat aan informatie voor kwaadwillende cyberdieven die beschikken over *quantum decryption*.[129] Mits aangepaste methodes en blijvende opvolging en vernieuwing van de evolutie lijkt het mogelijk om encryptie te garanderen. *Double encryption* en *Crypto-agility*, respectievelijk het versleutelen van gegevens op verschillende niveaus en het wijzigen van de versleutelingswijze bieden al het hoofd tegen het probleem van *quantum decryption*.[130]

4.4. *Obfuscation*

144. Door encryptie worden persoonlijke gegevens in de blockchain vertroebeld. De persoonsgegevens worden omgezet in bijvoorbeeld een getal of een andere code die enkel door degene die de encryptiesleutel heeft kan worden gelezen. Soms kan daarbij ook gebruik worden gemaakt van een derde partij die de encryptiecode kent, maar daardoor kan de blockchain haar doel voorbijgaan omdat ze net pretendeert dat er geen derde partijen nodig zijn.[131]

145. Daarnaast bestaan er ook nog andere technieken die blockchain technologie meer compliant maken met de GDPR zoals, *data protection by design*, het gebruik van *smart contracts…*

4.5. Tussenbesluit

146. Dit onderzoek toont aan dat er heel wat creatieve, juridische maar vooral technische technieken bestaan die gebruikt kunnen worden binnen de blockchain technologie om gegevensbeschermingsconflicten met de GDPR te voorkomen. Het gebruik van blockchain technologie raakt daardoor niet aan gegevensbeschermingswaarborgen die de GDPR voorziet in het recht op controle over persoonsgegevens van betrokkenen. Het gebruik van blockchain technologie kan zelfs opportuun zijn voor de controle van persoonsgegevens van de betrokkene.

[128] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Advies 05/2014 over anonimiseringstechnieken*, 10 april 2014, https://docplayer.nl/amp/422750-Groep-gegevensbescherming-artikel-29.html, 4.
[129] C. BURCHETT, *How to fight the coming quantum decryption treath?*, 2018, www.enterpriseai.news/2018/07/12/how-to-fight-the-coming-quantum-data-decryption-threat.
[130] Ibid.
[131] THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, 2018, www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, 20.

5. Conclusie

147. Dit onderzoek gaat over het veronderstelde spanningsveld tussen blockchaintechnologie en de bescherming van persoonsgegevens zoals vervat in de GDPR. De knelpunten voor de uitoefening van de rechten van een betrokkene over zijn persoonsgegevens worden omschreven in het kader van het gebruik van blockchaintechnologie en in het licht van de GDPR.

148. Een eerste hoofdstuk geeft een beschrijving van de werking en toepassingen van blockchaintechnologie alsook van de belangrijkste begrippen. In een tweede hoofdstuk worden de rechten van betrokkene met betrekking tot de bescherming van zijn persoonsgegevens uiteen gezet bij het gebruik van blockchaintechnologie en de wettelijke vereisten van de GDPR. Hiertoe kunnen we besluiten dat het gebruiken van blockchaintechnologie bepaalde rechten van gegevensbescherming niet kan waarborgen zoals het recht om vergeten te worden en het recht op rectificatie. Ook blijkt blokchaintechnologie niet conform het beginsel van minimale gegevensverwerking en opslagbeperking.

149. In het derde hoofdstuk gaan we na op welke manieren blockchaintechnologie meer GDPR-conform aan gegevensverwerking kan doen. Er kunnen meerdere initiatieven onderscheiden worden die blockchaintechnologie doen overeenstemmen met de vereisten van de GDPR. In een vierde hoofdstuk worden opportuniteiten besproken die blockchaintechnologie kan hebben bij de verwerking van persoonsgegevens. Tot slot wordt geëvalueerd wat wenselijk is om blockchaintechnologie en GDPR met elkaar te verzoenen.

150. Van oudsher is technologie het recht voor, dit is niet anders bij blockchaintechnologie. Over deze nieuwe technologie liggen nog veel juridische vraagstukken open op verschillende rechtsdomeinen.

151. Het zwaar bekritiseerde spanningsveld tussen blockchaintechnologie en de waarborgen van gegevensbescherming zoals vervat in de GDPR mogen m.i. dan ook herleid worden naar een verondersteld spanningsveld, aangezien er zelfs zonder Europese *lex specialis*, een arsenaal aan mogelijkheden op basis van creatieve, technische en juridische middelen blijken om blockchaintechnologie verzoenbaar te maken met GDPR. Echter is het roeien met de riemen die voorhanden zijn en is daarbij de minst slechte oplossing ook een oplossing. Een sterk coherent accuraat en wetgevend kader blijven hierdoor voorlopig achterwege. Dit leidt tot rechtsonzekerheid en een gefragmenteerde aanpak op lidstatelijk niveau om het hoofd te bieden aan de gevolgen en de uitwerking die blockchaintechnologie met zich meebrengt.

152. Een zoveelste weerspiegeling van technologie versus wetgeving waarbij de technologie het onderspit delft omdat het wetgevend proces op Europees niveau in het bijzonder, traag en log verloopt. Zo was de GDPR al achterhaald voordat deze uitwerking vond. Eenmaal er dan Europese regelgeving voorhanden is, is ze niet geneigd snel te wijzigen. Een gemiste kans voor Europa waarbij dat onaangepaste en rigide regelgeving mogelijk de technologische innovatie fnuikt doordat de toepassing van onaangepaste wetgeving of het te lang achterwege blijven van voorspelbare, heldere en conforme regelgeving noopt tot onvermijdelijke inbreuken op de waarborgen van gegevensbescherming die de GDPR biedt. Inbreuken die door het handhavingsmechanisme van de GDPR met omvangrijke sancties beteugeld (kunnen) worden enerzijds.

153. Anderzijds doordat nieuw ontwikkelde technologieën aanpassingen moeten doen aan hun (technisch) opzet en werkwijze om te kunnen voldoen aan de verplichtingen van persoonsgegevensbescherming. Hierdoor behaalt blockchaintechnologie niet haar volledig potentieel met bovendien het gevaar op uitholling van hun doelstellingen en krachtlijnen. De kracht en impact van blockchaintechnologie wordt afgezwakt en dat terwijl deze onstuitbaar is en steeds meer toepassing vindt in verschillende sectoren en zich zo reeds in de maatschappelijke structuren van de samenleving verankert.

154. Juridische bescherming is een historische constructie die steeds onderhevig is aan de maatschappelijke evoluties. Daarbij gebeurt geleidelijk aan een conceptuele modernisering van de afweging van enerzijds innovatie en anderzijds het waarborgen van het (grond)recht op bescherming van persoonsgegevens. Bovendien dient gezegd dat gegevensbeschermingswaakhond GDPR een erg hoog niveau van gegevensbescherming en de daartoe behorende verplichtingen voor de verwerkingsverantwoordelijke hanteert. Voldoen aan alle vereisten die de GDPR vooropstelt impliceert in praktijk vaak dat andere werkprocessen uitgehold en gefnuikt worden. Heeft het nut wetgeving met een bovengemiddeld hoog beschermingsniveau door en dito verplichtingen af te dwingen als blijkt dat de onderlat niet eens nageleefd kan worden? Het is niet omdat de specifieke vereisten in de GDPR ter waarborging van gegevensbescherming niet voldaan zijn, dit eveneens zou impliceren dat er geen of onvoldoende gegevensbescherming is voorzien. Blockchain technologie is opportuun om de doelstellingen vervat in de GDPR te behalen, maar niet op dezelfde wijze als het wettelijke kader van de GDPR vastlegt. Blockchain technologie zal naar de letter van de GDPR niet voldoen aan alle vereisten van gegevensbescherming. Maar in wezen streeft zij wel dezelfde doelstelling na. Blockchain technologie is evenwel in overeenstemming met de geest van de GDPR. Zij faciliteert digitale transacties die veilig, transparant en tegen misbruik en censuur bestand zijn. Blockchain technologie werd ontworpen om gegevensintegriteit en beveiliging te waarborgen door middel van cryptografie en gedistribueerde consensusmechanismen. Als zodanig zijn datalekken die rechtstreeks voortvloeien uit het gebruik van blockchain technologie zeldzaam. Dit maakt dat zij een betrouwbare technologie is om te gebruiken in verschillende sectoren en toepassingen.

155. Eveneens dient opgemerkt dat individuen ook een zekere *Bonus Pater Familias*-plicht hebben in de omgang met hun persoonsgegevens. Er mag m.i. een zekere verantwoordelijkheid van de betrokkene verwacht worden daar hij zelf beslist gebruik te maken van blockchain technologie. De afweging tussen het voordeel dat het gebruik van blockchain technologie en een mogelijke inbreuk op de bescherming van persoonsgegevens zijn voor zijn rekening. Al is hierbij vereist dat de betrokkene een duidelijk en helder beeld heeft van hoe blockchain technologie werkt en wat de mogelijke risico's behelzen voor de bescherming van zijn persoonsgegevens. Hierbij dient aangestipt te worden dat blockchaintechnologie *an sich* niet strijdig is met de vereisten van de GDPR, maar wel het gebruik ervan. Dit is opnieuw de vertaling van het feit dat blockchain technologie niet steeds conform is volgens de letter van de GDPR maar wel volgens de geest van de GDPR. Dat zij in hetzelfde spreekwoordelijke schuitje zitten op "geestelijk" niveau blijkt uit de opportuniteiten die blockchain technologie biedt in het kader van GDPR. Zij heeft het potentieel opportuniteiten te bieden in gegevensbescherming op vlak van transparantie en traceerbaarheid, toestemmingsbeheer, gegevensintegriteit en het vergroten van de autonomie van betrokkenen. Het is dus waarschijnlijk dat oude veronderstelde vijanden nieuwe vrienden worden.

156. Als men als uitgangspunt neemt, datgene dat zowel door de GDPR als door blockchain technologie wordt nagestreefd is dit mogelijk de sleutel om blockchain technologie en GDPR met elkaar te verzoenen en de brug tussen beide te slaan voor wat betreft de letter van de wet.

157. De centrale onderzoeksvraag kan negatief beantwoord worden, daar het slechts gaat om een verondersteld spanningsveld.

6. Bibliografie

I. WETGEVING EN VOORBEREIDENDE DOCUMENTEN

a. Wetgeving

i. Europese wetgeving

Handvest van de grondrechten van de Europese Unie van 7 december 2000, *Pb.L*. 18 december 2000, afl. 346, 1-22.

Verordening EP en Raad nr. 2016/679, 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, *PB.L.* 4 mei 2016, afl. L 119, 1-88.

ii. Belgische wetgeving

Wet 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, *BS* 4 september 2002.

Wet 5 juli 2022 houdende diverse financiële bepalingen, *BS* 19 juli 2022.

b. Voorbereidende werken en beleidsdocumenten

Europese wetgeving

EUROPEAN BLOCKCHAIN SANDBOX, *European blockchain regulatory sandbox for distribued ledger technologies*, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Sandbox+Project#:~:text=The%20European%20Blockchain%20Regulatory%20Sandbox,for%20innovative%20blockchain%20technology%20solutions.

EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Blockchain and the General Data Protection Regulation : Can Distributed Ledgers Be Squared with European Data Protection Law?*", 2019, www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, 120 p.

EUROPESE COMMISSIE, *Wettelijk en regelgevingskader voor blockchain*, https://digital-strategy.ec.europa.eu/nl/policies/regulatory-framework-blockchain.

GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Advies 4/2007 over het begrip persoonsgegevens*, 20 juni 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_nl.pdf, 28 p.

GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Advies 05/2014 over anonimiseringstechnieken*, 10 april 2014, https://docplayer.nl/amp/422750-Groep-gegevensbescherming-artikel-29.html, 43 p.

Voorstel (Comm.) voor een verordending van het Europees Parlement en de raad betreffende markten voor cryptoactiva en tot wijziging van de Richtlijn (EU) 2019/1937, 24 september 2020, COM(2020)593 final - 2020/0265(COD).

Voorstel (Comm.) voor een richtlijn van het Europees Parlement en de raad betreffende een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie, 24 september 2020, COM(2020)594 final – 2020/0267 (COD).

II. RECHTSPRAAK

Europa

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

III. RECHTSLEER

a. Boeken

AUDENAERT, K., BARY, F., BEGUIN, E., BLONDÉ, B., BOSSELER, P., CHABOT, L., DANNEELS, P., DE DECKER, H., DENOYELLE, C., DOOLAEGE, B., GANSEMAN, J., HUDSON, M., JANSSENS, E., LEUNCKENS, I., MERLEYEDE, P., PRINS, B., SEPP, K., VAN MOURIK, M., VAN VOOREN, E., VERHEYE, B., VERSLYPE, K. en WATTILLON, N., *Tradition in motion : notarieel congres Antwerpen 2019,* Brussel, Larcier, 2019, xxi + 321 p.

BELEN-SAGLAM, R., ALTUNCU, E., LU, Y. en LI, S., *A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems*, 2022, https://arxiv.org/abs/2210.04541, 64 p.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Premiers éléments d'analyse de la CNIL sur la blockchain*, 2018, www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, 11 p.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Solutions for a responsible use of the blockchain in the context of personal data*, 2018, www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf, 10 p.

FINCK, M., *Blockchains and data protection in the European Union*, 2017, https://theblockchaintest.com/uploads/resources/Michele%20Finck%20-%20Blockchain%20and%20data%20Protection%20in%20the%20European%20Union%20-%20na.pdf, 32 p.

FINCK, M., *Blockchain: regulation and governance in Europe, Cambridge*, Cambridge University Press, 2018, 214 p.

GOOSSENS, J. en VERSLYPE, K., *Blockchain en smart contracts: het einde van de vertrouwde tussenpersoon*, 2019, https://pure.uvt.nl/ws/portalfiles/portal/32111708/EHBR19_blockchain_en_smartcontracts.pdf, 7 p.

GOOSSENS, J. en VERSLYPE, K. en TJONG TJIN TAI, E., *Blockchain en smart contracts: Herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving*, 2020, https://library.oapen.org/handle/20.500.12657/53282, 159 p.

LEENES, R., KAUFMANN, W., SCHELLEKENS, M., SCHEMKES, F. en TJONG TJIN TAI, E., *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, 2019, www.stibbe.com/sites/default/files/2022-07/tk_bijlage_blockchain_en_het_recht_def_8316.pdf, 137 p.

MORGAN, R. en R. BOARDMAN, R., *Data Protection Strategy. Implementation data protection compliance,* Londen, Sweet & Maxwell Limited, 2012, 450 p.

SAVIN, A., *EU Internet Law*, Cheltenham, Edward Elgar Publishing, 2017, 384 p.

SCHRAM, F., *Privacy en persoonsgegevens*, Brussel, Politeia, 2019, 760 p.

SMITS, G., *Blockchain is WTF (Waarschijnlijk Toch Fundamenteel)*, Brugge, die Keure, 2018, 206 p.

SUSTRONCK, O.*, Praktijkboek internetrecht,* Mechelen, Wolters Kluwer, 2017, 284 p.

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR*, 2018, www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, 36 p.

VERSLYPE, K. en VERHEYE, B., *Blockchain en smart contracts: het einde van de vertrouwde tussenpersoon?*, Brussel, Intersentia, 2019, 109 p.

VOIGT, P. en VON DEM BUSSCHE, A., *The EU general data protection regulation (GDPR): a practical guide*, New York City, Springer International Publishing, 2017, 383 p.

WEYTS, L., *De notariswet*, Mechelen, Wolters Kluwer, 2023, 598 p.

b. Bijdragen in boeken

DELFORGE, A. en POULLET, Y., "Les blockchains : un défi et/ou un outil pour le RGPD ? " in COTIGA-RACCAH, A. (eds.), *Les blockchains et les smart contracts à l'épreuve du droit*, Brussel, Larcier, 2020, 97-133.

DOBBELAERE, D. en VERCAUTEREN, J. "Smart contracts en verzekeringen" in AERTS, P., HOOGENDIJK, F. en VANDEZANDE, N. (eds.), *Smart contracts. Een overzicht vanuit juridisch perspectief*, Antwerpen, Intersentia, 2020, 297-327.

KUSBER, T., SCHWALM, S., SHAMBURGER, K., KORTE, U., "Criteria for trustworthy digital transactions - Blockchain/DLT between eIDAS, GDPR, data and evidence preservation" in ROßNAGEL, H., SCHUNCK, C., MÖDERSHEIM, S., HÜHNLEIN, D. (eds.), *Open identity summit 2020, Lecture notes in informatics (LNI)*, 2020, https://dl.gi.de/bitstream/handle/20.500.12116/33181/proceedings-04.pdf?sequence=1&isAllowed=y, 49-60.

c. Bijdragen in tijdschriften

AL-ABDULLAH, M., ALSMADI, I., ALABDULLAH, R. en FARKAS, B., "Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR", *Digital Policy, Regulation and Governance* 2020, Vol. 22, 5/6, 389-411.

AL MASHHOUR, O., AZIZ, A. en MOHD NOR, N., "Blockchain and its entire eco-system: A legal consideration to an international cross-border technology", *International Journal of Multidisciplinary Sciences and Advanced Technology* 2022, vol 3, no 3, www.researchgate.net/publication/363645357_Blockchain_and_its_Entire_Eco-System_A_Legal_Consideration_to_an_International_Cross-Border_Technology/link/63273e180a70852150036b90/download, 14 – 24.

BELL, T. W., "Copyrights, Privacy, and the Blockchain", *Ohio Northern University Law Review* 2016, Afl. 2, 439-470.

BERBERICH, M. en STEINER, M., "Practitioner's Corner - Blockchain Technology and The GDPR - How to reconcile Privacy and Distributed Ledgers?", *European Data Protection Law Review* 2016, volume 2, issue 3, 422-426.

BOONE, R., "Smart contracts: evolutie, geen revolutie", *Juristenkrant* 2020, afl. 416, 6-7.

DE JONGHE, D. en LAAN, V., "Blockchain in de realiteit", *CR* 2017, afl. 6, 347-354.

GIANNOPOULOU, A., "Putting data protection by design on the blockchain", *EDPL* 2021, vol. 3, 388-399.

GODDARD, M., "The EU General information protection regulation (GDPR): European regulation that has a global impact, *International Journal of Market Research* 2017, vol. 59, issue 6, https://eclass.upatras.gr/modules/document/file.php/CULTURE110/goddard2017.pdf, 703-705.

HAQUE, A., ISLAM, A., HYRYNSALMI, S., NAQVI, B. en SMOLANDER, K., "GDPR Compliant Blockchains–A Systematic Literature Review," *IEEE Access* 2021, vol. 9, 50593-50606.

JACQUEMIN, H., en POULLET, Y., "Blockchain: une révolution pour le droit?", *JT* 2018, 801–819.

LAAN, V., "Privacy en blockchain: wanneer is er voor wie privacywerk aan de winkel?", *IR* 2017, afl. 1, 4 – 11.

LAAN, V. en RUTJES, A., "Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?", *CR* 2017, afl. 6, 364-371.

LINNEMANN, J., "Juridische aspecten van (toepassingen van) blockchain", *CR* 2016, afl. 6, 319-324.

MARIËN, S., "Blockchain en GDPR op ramkoers?", *DataNews* 2018, 32-35.

MARELLI, L. en TESTA, G., "Scrutinizing the EU general information protection regulation", *Science* 2018, vol. 360, issue 6388,

https://lastatalenews.unimi.it/sites/default/files/attachments/Marelli%20and%20Testa%20Science%202018.pdf, 496-498.

MIRCHANDANI, A., "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR", *Fordham Intellectual Property, Media and Entertainment Law Journal* 2019, vol. 29, 1201-1241.

POPPE, M. en VERBIEST, T., "Quelle relation entre la protection des données à caractère personnel et la blockchain?", *Revue Lamy Droit des Affaires* 2017, no. 129, www.degaullefleurance.com/wp-content/uploads/2017/10/Dossier-Blockchain-RLDA.pdf, 38-40.

SEL, M., "Blockchain, een functionele introductie", *TBO* 2019, afl. 2, 150 - 155.

STRUYF, P. en OOSTVOGELS, R., "Blockchaintechnologie als wondermiddel voor hedendaagse politionele informatieinefficiënties?", *Panopticon* 2021, afl. 2, 149-160.

TEPERDJIAN, R., ''The puzzle of squaring blockchain with the general data protection regulation,'' *Forthcoming in jurimetrics* 2020, vol. 60, issue no. 3, https://ssrn.com/abstract=3638736, 1-61.

VALGAEREN, E. en LINNEMANN, J.J., "Inleiding: "Blockchain ontketend", *CR,* 2017, afl. 6, 343 – 346.

VAN DE LOOVERBOSCH, M., "Crypto-effecten: tussen droom en daad", *TRV-RPS* 2018, 193 – 207.

VAN GIEL, I., EGAMBERDIEV, S. en APPELMANS, A., "Blockchain in vastgoedtransacties", *TBO* 2019, nr. 2, 165 – 179.

VAN HUMBEECK, A., "The Blockchain-GDPR paradox," *Journal of Data Protection & Privacy* 2019, 208-212.

VUYLSTEKE, B., "Blockchain - Wat is het? Wat kan het betekenen voor het notariaat?", *T.Not.* 2018, 205 – 211.

d. Onlinebronnen

ABD ALI, S., YUSOFF, M. en FALAH HASAN, H., "Redactable Blockchain: Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions", *Future Internet* 2023, https://www.researchgate.net/publication/367157229_Redactable_Blockchain_Comprehensive_Review_Mechanisms_Challenges_Open_Issues_and_Future_Research_Directions.

BERKE, A., "How safe are blockchains? It depends", *Harvard Business Review*, 2017, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends.

BUTERIN, V., "Privacy on the blockchain", 15 januari 2016, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain.

CARIDE, C. en SCHRODER, M., *Helios final legal report*, 2021, https://helios-h2020.eu/wp-content/uploads/2022/01/D1.4_Final-Legal-Report.pdf, 83 p.

CLOET, S., *Blockchain en het notariaat*, 2018, http://www.linkedin.com/pulse/blockchain-en-het-notariaat-match-made-heaven-stephaan-cloet.

CZARNECKI, J., *Blockchains and Personal Data Protection Regulations explained*, 2017, www.coindesk.com/markets/2017/04/26/blockchains-and-personal-data-protection-regulations-explained.

DE FILIPPI, P., "The interplay between decentralization and privacy: the case of blockchain technologies", *Journal of Peer Production* 2016, https://ssrn.com/abstract=2852689.

EBERHARDT, J. en TAI, S., *On or off the blockchain? Insights on off-chaining computation and data*, 2017, www.researchgate.net/publication/319416136_On_or_Off_the_Blockchain_Insights_on_Off-Chaining_Computation_and_Data, 14 p.

EICHLER, N., JONGERIUS, N., McMULLEN, S., NAEGELE, O., STEININGER, L., en WAGNER, K., *Blockchain, data protection, and the GDPR*, 2018, www.crowdfundinsider.com/wp-content/uploads/2018/06/GDPR_Position_Paper_v1.0.pdf, 9 p.

GEORGIEV, N., *Old foes becoming friends : Blockchain and the GDPR*, 2020, www.law.kuleuven.be/citip/blog/old-foes-becoming-friends-blockchain-and-the-gdpr.

GODYN, M., KEDZIORA, M., REN. Y., LIU, Y. en SONG, H., *Analysis of solutions for a blockchain compliane with GDPR*, 2022, www.nature.com/articles/s41598-022-19341-y, 11 p.

HAN, S. en PARK, A., "A gap between blockchain and general data protection regulation: A systematic review", *IEEE* 2022, https://ieeexplore.ieee.org/abstract/document/9906064, 103888-103905.

HAQUE, A., ISLAM, A., HYRYNSALMI, S., NAQVI, B., "Towards a GDPR-compliant blockchain-based COVID vaccination passport," *Applied Sciences* 2021, vol. 11, www.mdpi.com/2076-3417/11/13/6132.

HRISTOV, P. en DIMITROV, W., *The blockchain as a blackbone of GDPR compliant frameworks*, 2018, www.researchgate.net/publication/328576742_The_blockchain_as_a_backbone_of_GDPR_compliant_frameworks, 7 p.

HU, W., "Juridische eisen aan de betrouwbaarheid van digitale toestemming in de AVG", *Computerrecht* 2022, afl. 2, 86-96.

IANSITI, M. en LAKHANI, R., "The Truth About Blockchain", *Harvard Business Review* 2017, januari-februari 2017, https://hbr.org/2017/01/the-truth-about-blockchain.

IBANEZ, L.-D., O'HARA, K. en SIMPERL, E., *On blockchains and the general data protection regulation*, 2018, www.researchgate.net/publication/326913146_On_Blockchains_and_the_General_Data_Protection_Regulation, 13 p.

LIMA, C., *How decentralized blockchain internet will comply with GDPR data privacy*, 2018, https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf, 5 p.

LYNSKEY, O., *Regulating 'platform power'*, 2017, https://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf, 31 p.

MEYER, D., *Blockchain technology is on a collision course with EU privacy law*, 2018, https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law.

MIRCHANDANI, A., *The GDPR-blockchain paradox: Exempting permissioned blockchains from the GDPR*, 2019, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj, 43 p.

PEHLIVAN, C. en READ, I., "Blockchain and data protection", *Global Privacy Law Review* 2020, Volume I, issue I, https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2020005.pdf

SAVA, N. en DRAGOS, D., *The legal regime of smart contracts in public procurement*, 2022, https://rtsa.ro/tras/index.php/tras/article/view/698/693.

SIMAL, J., *Blockchain en privacy : een onderzoek naar de verzoenbaarheid van blockchain technologie en GDPR*, 2018, www.scriptiebank.be/sites/default/files/thesis/2018-09/SIMAL_J_masterproef_privacy_en_blockchain.pdf, 58 p.

TENNISON, J., *What is the impact of blockchains on privacy?*, 2015, www.theodi.org/article/what-is-the-impact-of-blockchains-on-privacy.

VERHULST, D. en K. ZADORA, K., *Blockchain technologie en controle over persoonsgegevens uit de GDPR*, 2021, https://monardlaw.be/nl/verhalen/blockchain technologie-en-controle-over-persoonsgegevens-uit-de-gdpr.

WIRTH, C., KOLAIN, M., "Privacy by Blockchain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data, Reports of the European Society for Socially Embedded Technologies 2018, https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf.

IV. OVERIGE BRONNEN EN NIET-JURIDISCHE BRONNEN

ABERER, K. en HAUSWIRTH, M., "An Overview of Peer-to-Peer Information Systems", *WDAS* 2002, 171-188.

AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN, *Wat is de FSMA?*, www.fsma.be/nl/wat-de-fsma.

AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN, *Cryptomunten: nieuwe regels voor bepaalde aanbieders van diensten*, 2022, www.fsma.be/nl/news/cryptomunten-nieuwe-regels-voor-bepaalde-aanbieders-van-diensten.

AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN, *Virtuele munten: de FSMA zet in op de bescherming van de consument*, 2023, www.fsma.be/nl/news/virtuele-munten-de-fsma-zet-op-de-bescherming-van-de-consument.

BHIDE, B., *Blockchain and its future in 2023: What is blockchain?*, 2023, www.projectcubicle.com/blockchain-and-its-future-in-2023.

BURCHETT, C., *How to fight the coming quantum decryption treath?*, 2018, www.enterpriseai.news/2018/07/12/how-to-fight-the-coming-quantum-data-decryption-threat.

CRYPTOPEDIA STAFF, *What are public and private keys*?, 2022, www.gemini.com/cryptopedia/public-private-keys-cryptography#section-public-and-private-keys-control-your-crypto.

HALAMKA, J., LIPPMAN, A. en EKBLAW, A., *The potential for blockchain to transform electronic health records*, 2017, https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.

HEINES, K., "The Risks and Rewards of Blockchain Technology", *Risk Management* 2016, Afl. 4, 6-7.

HOFMAN, D., LEMIEUX, V.L., JOO, A., BATISTA, D. A., ""The margin between the edge of the world and infinite possibility": Blockchain, GDPR and information governance", *Records Management Journal* 2019, vol. 29, 1/2, 240-257.

HOOFNAGLE, C.J., VAN DER SLOOT, B., ZUIDERVEEN BORGESIUS, F., "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law* 2019, vol. 28, 1, 65-98

HUYGHEBAERT, P., *Groot Facebooklek: bedrijf van Bannon maakte gegevens van 50 miljoen mensen buit*, 2018, www.vrt.be/vrtnws/nl/2018/03/17/facebook--schorst--bedrijf-cambridge-analytica-dat-voor-trump-ca.

INTERSOFT CONSULTING, *GDPR Privacy by Design*, https://gdpr-info.eu/issues/privacy-by-design.

JOOSTEN, P., *Blockchain. Definitie, werking, kansen & 6 voorbeelden*, http://www.peterjoosten.net/blockchain.

KARASEK-WOJCIECHOWICZ, I., "Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces", *Journal of Cybersecurity* 2021, vol. 7, 1-28.

KARISMA, K., TEHRANI, P. M., "Data protection governance framework: A silver bullet for blockchain-enabled applications", *Procedia Computer Science* 2023, vol. 218, 2480-2493.

KORZ, M., *Vier redenen waarom blockchain de toekomst gaat veranderen*, http://www.rabobank.nl/bedrijven/groei/marktontwikkeling/vier-voordelen-van-blockchain.

NAKOMOTO, S., *Bitcoin: A peer-to-peer electronic cash system*, 2008, https://bitcoin.org/bitcoin.pdf, 9 p.

POELMAN, M. en IQBAL, S., "Investigating the compliance of the GDPR: Processing personal data on a blockchain"*, IEEE* 2021, 38–44.

RENIER, H., *Tiener (19) die rijk werd met bitcoin: "Eigen schuld als je binnen 10 jaar geen miljonair bent"*, 2018, www.hln.be/geld/tiener-19-die-rijk-werd-met-bitcoin-eigen-schuld-als-je-binnen-10-jaar-geen-miljonair-bent~af3d1b82.

RIPOSO, J., "Diffusion on the Peer-to-Peer Network." *Journal of Risk and Financial Management* 2022, 15:47, www.mdpi.com/1911-8074/15/2/47, 1-47.

SEDLMEIR, J., LAUTENSCHLAGER, J., FRIDGEN, G. en URBACH, N., "The transparency challenge of blockchain in organizations", *Electronic Markets* 2022, 32, 1779–1794.

TATAR, U., GOKCE, Y. en NUSSBAUM, B., "Law versus technology: Blockchain, GDPR, and tough tradeoffs", *Computer Law & Security Review* 2020, www.sciencedirect.com/science/article/pii/S026736492030059 5?casa_token=PhJ5T9lBATsAAAAA:IqtdeS4KyvtIevY-R7uQFkWcQ2f1sI00TET0wmKSoOEguuwlUyZy6LDqcC1zBt2JUaLLBKFCLw.

TRUONG, N. B., SUN, K., LEE, G. M. en GUO, Y., "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution", *IEEE Transactions on Information Forensics and Security 2020*, vol. 15, 1746-1761.

VARGHESE, B., VILLARI, M., RANA, O., JAMES, P., SHAH, T., FAZIO, M. en RANJAN, R., ''Realizing edge marketplaces: Challenges and opportunities,'' *IEEE Cloud Computing* 2018, vol. 5, no. 6, 2018, https://ieeexplore.ieee.org/document/8552630, 9-20.

VAN DEN BERGH, W., *Langverwachte MiCA wetgeving wordt goedgekeurd*, 2023, https://digitalcurrencyacademy.be/langverwachte-mica-wetgeving-wordt-goedgekeurd.

VAN MAELE, P., *Beurswaakhond maakt dossier tegen Belgische cryptobeurs Bit4You over aan het parket*, 2023, www.standaard.be/cnt/dmf20230509_95826573.

ZABOLOTNYY, O., *How AI and blockchain are changing business*, https://firstbridge.io/blog/blockchain/how-ai-and-blockchain-are-changing-businesses.