Juridicum – Schriften zum
Medien-, Informations- und Datenrecht

RESEARCH

Carlo Peitz

Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen

Springer

Juridicum – Schriften zum Medien-, Informations- und Datenrecht

Reihe herausgegeben von

Matthias Cornils, Mainz, Deutschland

Louisa Specht-Riemenschneider, Bonn, Deutschland

In der Schriftenreihe erscheinen Forschungsbeiträge zum Kommunikations- und Medienrecht in seiner vollen Breite, vom Äußerungs-, Urheber- und Kunsturheberrecht über das Daten- und Informationsrecht bis zu Fragen öffentlich-rechtlicher Medien- oder Intermediärsregulierung, einschließlich ihrer theoretischen Hintergründe. Erfasst sind insbesondere innovative akademische Qualifikationsschriften, aber auch Abhandlungen und Sammelbände von herausragendem wissenschaftlichen Wert.

Weitere Bände in der Reihe http://www.springer.com/series/16165

Carlo Peitz

Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen

Springer

Carlo Peitz
Neuss, Deutschland

Zugleich Dissertation, Juristische Fakultät der Universität Passau

Erstgutachten: Prof. Dr. Louisa Specht-Riemenschneider
Zweitgutachten: Prof. Dr. Peter Bräutigam
Disputation am 21.02.2020

ISSN 2662-9488 ISSN 2662-9496 (electronic)
Juridicum – Schriften zum Medien-, Informations- und Datenrecht
ISBN 978-3-658-32049-2 ISBN 978-3-658-32050-8 (eBook)
https://doi.org/10.1007/978-3-658-32050-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Marija Kojic
Springer ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

A. Inhaltsverzeichnis

B. Einleitung

I. Bitcoins und das Potential der Blockchain-Technologie

Der Begriff „Blockchain“ ist im öffentlichen Bewusstsein vor allem verknüpft mit sog. „Kryptowährungen“ wie Bitcoin und Ether – Formen von digitalem Bargeld, bei denen die Ausgabe des Geldes nicht durch eine Zentralbank, sondern durch ein dezentrales Computernetzwerk kontrolliert wird.[1] Es handelt sich dabei um eine Art von digitaler und dezentraler Währung.[2] Die besondere Eigenschaft dieses Konzeptes liegt darin, dass die Benutzer einander virtuelle Geldbeträge überweisen können, ohne dass eine Bank an dem Transaktionsprozess beteiligt ist. Die digitale Währung liegt allein in den Händen der teilnehmenden Nutzer.[3] Eines Mittelsmannes oder Intermediärs bedarf es nicht.[4] Vielmehr wird das erforderliche Vertrauen im Wesentlichen durch Kryptographie sichergestellt.[5]

Angesichts des großen Erfolges insbesondere von Bitcoin hat sich die Erkenntnis verfestigt, dass das wirtschaftliche und technologische Potential der dem Bitcoin-Protokoll zugrundeliegenden Blockchain-Technologie bei Weitem noch

[1] Hierzu näher beispielsweise *Walport*, Distributed Ledger Technology: beyond block chain – A report by the UK Government Chief Scientific Adviser, S. 33; zum Begriff der digitalen Währung *Sixt*, Bitcoins und andere dezentrale Transaktionssysteme, 1. Aufl. 2017, S. 69 ff.
[2] *Simmchen*, MMR, 2017, 162.
[3] *Schrey/Thalhofer*, NJW, 2017, 1431.
[4] *Barth*, Legal Tech in Deutschland - zwischen Buzz Word und Anwaltsschreck, in: *Hartung/Bues/Halbleib* (Hrsg.), Legal Tech, 1. Aufl., 2018, S. 49, 49.
[5] *Blocher*, AnwBl, 2016, 612, 615.

C. Peitz, *Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen*, Juridicum – Schriften zum Medien-, Informations- und Datenrecht,
https://doi.org/10.1007/978-3-658-32050-8_1

nicht ausgeschöpft ist.[6] Tatsächlich bietet diese Technologie, die den technischen Unterbau für Bitcoins bildet, den Zugang zu weitaus komplexeren Anwendungsmöglichkeiten.[7]

Blockchains sind dezentrale digitale Transaktionsregister – sog. „Distributed Ledger" –, die den Erfolg dieser Geschäftsideen erst technisch möglich machten und im Vergleich zu anderen digitalen Technologien mehrere Vorteile aufweisen: unter anderem sind sie nachträglich unveränderlich, erfordern kein Vertrauen in einen Mittelsmann und sind nach ihrer Grundidee für jedermann öffentlich einsehbar und transparent.[8]

Zwei Aspekte machen diese neue Technologie wirtschaftlich besonders interessant:[9] einerseits die Möglichkeit, auf einen vertrauenswürdigen Mittelsmann („Gatekeeper") zu verzichten, andererseits die Verknüpfung der Blockchain-Technologie mit sog. „Smart Contracts", also Verträgen, die durch Software geprüft und ohne menschliches Eingreifen abgewickelt werden.[10] Dies veranschaulicht ein denkbarer Anwendungsfall aus dem Bereich der Versiche-

---

[6] Vgl. hierzu nur beispielhaft den Bericht des UK Government Chief Scientific Adviser für das britische Government Office of Science in: *Walport,* Distributed Ledger Technology: beyond block chain, 5 f.; s. auch *Burgwinkel*, Blockchaintechnologie und deren Funktionsweise verstehen, in: *Burgwinkel* (Hrsg.), Blockchain Technology, 1. Aufl., 2016, S. 1 f. und *Simmchen*, MMR, 2017, 162.
[7] *Bechtolf/Vogt*, Blockchain und Datenschutz - Recht technologisch, in: *Taeger* (Hrsg.), Recht 4.0 - Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 873, 874; *Quiel*, DuD, 2018, 566, 567; *Welzel/Eckert/Kirstein/Jacumeit*, Mythos Blockchain, 2017, S. 18.
[8] *Böhme/Pesch*, DuD, 2017, 473; *Bechtolf/Vogt*, ZD, 2018, 66, 67; ähnl. auch *Barth*, Legal Tech in Deutschland - zwischen Buzz Word und Anwaltsschreck, in: *Hartung/Bues/Halbleib* (Hrsg.), Legal Tech, 1. Aufl., 2018, S. 49, 49.
[9] *Swatosch/T. Hartung*, ZfV, 2018, 377; *Barth*, Legal Tech in Deutschland - zwischen Buzz Word und Anwaltsschreck, in: *Hartung/Bues/Halbleib* (Hrsg.), Legal Tech, 1. Aufl., 2018, S. 49, 49.
[10] *Söbbing*, ITRB, 2018, 43, 44.

rungswirtschaft: das Fahrzeug eines Versicherungsnehmers sendet Telemetriedaten an eine Blockchain, welche eine Smart Contract-Software wiederum ausliest und anhand der Erkenntnisse über das Fahrverhalten automatisch die Kfz-Versicherungsprämie anpasst, ohne dass ein Mittelsmann eingreifen bzw. tätig werden müsste.[11]

Vor diesem Hintergrund verwundert es nicht, dass der Blockchain-Technologie das Potential zugeschrieben wird, sämtliche Arten von Transaktionen und Registerfunktionen zu revolutionieren.[12] Zahlreiche Unternehmen im Banken- und Finanzsektor hat dies dazu bewogen, Einsatzpotentiale der Blockchain-Technologie zu eruieren,[13] jedoch zeigt bereits das obige Anwendungsbeispiel, dass das Thema Blockchain auch für verschiedenste andere Branchen interessant ist. Beispielhaft sind neben den Bereichen des Finanzmarktes („FinTech“) und des Versicherungsgeschäfts („InsurTech“) auch der Industriebereich für die Verwendbarkeit im sog. „Internet der Dinge“ oder juristische Dienstleistungen („LegalTech“) zu nennen.[14] Selbst für den öffentlichen Bereich wird die sinnvolle Eingliederung von Blockchain-Technologien im Rahmen von E-Government untersucht.[15] Die Bundesregierung plant die Erprobung von Blockchain-Technologie, um einen geeigneten Rechtsrahmen schaffen zu können,[16]

---

[11] *Swatosch/T. Hartung*, ZfV, 2018, 377, 378 f.
[12] *Guggenberger*, ZD, 2017, 49, 50.
[13] Vgl. hierzu die ausführliche Übersicht der Studie: Blockchain - Chance für Energieverbraucher?, abrufbar unter *https://www.pwc.de/de/energiewirtschaft/blockchain-chance-fuer-energieverbraucher.pdf* (Abruf am 27.10.2018).
[14] Vgl. zu diesen Begriffen beispielsweise *Zunker*, AnwBl, 2017, 1096, 1096 f.; einen Eindruck von dem hohen Interesse unterschiedlichster Wirtschaftsbranchen vermittelt auch die Auflistung bei *Glatz*, Blockchain und Smart Contracts - Eine neue Basistechnologie im Recht?, in: *Hartung/Bues/Halbleib* (Hrsg.), Legal Tech, 1. Aufl., 2018, S. 287, 292 f.
[15] *Simmchen*, MMR, 2017, 162, 163; Beispiele für Anwendungsfelder im öffentlichen Sektor bei *Welzel/Eckert/Kirstein/Jacumeit*, Mythos Blockchain, 2017, 18 ff.
[16] *Bundesregierung*, Koalitionsvertrag für die 19. Legislaturperiode, v. 14.03.2018, Rn. 2016.

die EU-Kommission hat sogar eine eigene Blockchain-Forschungsgruppe („EU-Blockchain-Beobachtungsstelle und -Forum“) ins Leben gerufen, um die neuen Herausforderungen dieser Technologie besser einzuschätzen[17].

Das starke Interesse an der Blockchain-Technologie in fast allen Bereichen der Wirtschaft und im öffentlichen Sektor legt es nahe, sich auch aus rechtlicher Sicht mit dieser neuen Technologie zu befassen und mögliche Probleme bei der weiteren Erschließung dieses technischen Gebietes zu identifizieren und zu analysieren.

Blockchain ist eine sehr junge Technologie, die naturgemäß zahlreiche rechtliche Fragen und Probleme aufwirft.[18] In der vorliegenden Bearbeitung wird aus datenschutzrechtlicher Perspektive vor allem auf einen der Aspekte eingegangen, welcher der Blockchain ihren Namen gibt und sie im Vergleich zu anderen Registern abhebt: die nahezu unabänderliche Verknüpfung von öffentlich einsehbaren und in einem Netzwerk verteilten Datenblöcken.

II. Blockchains im Spannungsfeld mit dem europäischen Datenschutz

Eine der Haupteigenschaften einer Blockchain ist, dass Transaktionen von allen anderen Netzwerkteilnehmern jederzeit einsehbar sind und zurückverfolgt

[17] *Europäische Kommission*, Pressemitteilung zur Gründung einer EU-Blockchain-Beobachtungsstelle und -Forum, v. 01.02.2018, S. 2.
[18] Vgl. zu den vordringlichen rechtlichen Fragestellungen zum Beispiel *Specht*, NJW, 2017, 3567, 3568 m.w.N.

werden können.[19] Diese vollständige Transparenz berührt potentiell datenschutzrechtlich relevante Aspekte und hat deshalb Vorgaben des einschlägigen Datenschutzrechts zu berücksichtigen und umzusetzen.[20]

Indes befindet sich nicht nur die Technologie im Umbruch; auch das Datenschutzrecht hat gravierende Neuerungen erfahren, und zwar durch die Einführung der *Datenschutz-Grundverordnung*[21] (im Folgenden kurz: *DSGVO*), welche gem. Art. 99 Abs. 2 DSGVO seit dem 25.05.2018 unmittelbar anwendbar ist[22] und die *EU-Datenschutzrichtlinie*[23] (im Folgenden kurz: *DSRL*) ablöst.

Durch die DSGVO erlebt das deutsche Datenschutzrecht erhebliche Umwälzungen, denn diese zielt als „Grund"-Verordnung[24] auf eine Vollharmonisierung

[19] *Kaulartz*, CR, 2016, 474; *Böhme/Pesch*, DuD, 2017, 473; *Hoeren*, NJW, 2017, 1587, 1592.
[20] *Lange-Hausstein*, ITRB, 2017, 93.
[21] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. Nr. L 119 v. 04.05.2016, S. 1 ff.
[22] In Kraft getreten ist die DSGVO bereits am 24.05.2016, vgl. hierzu z.B. Gola–*Piltz*, Datenschutz-Grundverordnung, 2. Aufl., 2018, Art. 99 Rn. 4; Ehmann/Selmayr–*Ehmann*, DS-GVO, 2. Aufl., 2018, Art. 99 Rn. 3; Kühling/Buchner–*Kühling/Raab*, Datenschutz-Grundverordnung/BDSG, 2. Aufl., 2018, Art. 99 Rn. 1; Sydow–*Sydow*, Europäische Datenschutzgrundverordnung, 2. Aufl., 2018, Art. 99 Rn. 1.
[23] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 v. 23.11.1995, S. 31 ff.
[24] Diese Wendung existiert an sich im Europarecht weder als Begriff noch als Normenkategorie, s. Auernhammer–*Lewinski*, DSGVO/BDSG, 6. Aufl., 2018, Einl. DSGVO Rn. 23; näher zur Bedeutung des Begriffs auch Wolff/Brink–*Wolff/Brink*, Beck'scher Online-Kommentar Datenschutzrecht, 29. Edition, 2019 [Stand: 03.03.2017], Einl. zur DS-GVO Rn. 20; Kühling/Buchner–*Kühling/Raab*, Datenschutz-Grundverordnung/BDSG, 2. Aufl., 2018, Einf. Rn. 98.

des Datenschutzrechts in der Europäischen Union.[25] Aufgrund des Prinzips des Anwendungsvorrangs sind zahlreiche nationale Regelungen neben der DSGVO nicht mehr anwendbar.[26]

Die DSGVO dehnt den räumlichen Anwendungsbereich des europäischen Datenschutzrechts massiv aus.[27] Zwar verbleibt es wie bereits zuvor in Art. 4 Abs. 1a DSRL auch gemäß Art. 3 Abs. 1 DSGVO weiterhin beim Niederlassungsprinzip, nach welchem die Datenschutz-Grundverordnung für jeden Verantwortlichen gilt, der im Rahmen der Tätigkeiten einer Niederlassung in der Union personenbezogene Daten verarbeitet; jedoch ist dieses Prinzip ausgeweitet worden, sodass die Regelung im Gegensatz zur DSRL nunmehr auch Auftragsverarbeiter umfasst, soweit sie im Rahmen einer Niederlassung in der Union tätig werden.[28] Auch wenn ein für die Verarbeitung personenbezogener Daten Verantwortlicher zwar außerhalb der EU niedergelassen, aber aufgrund Völkerrechts dem Recht eines Mitgliedsstaates unterliegt, ist die DSGVO gem. Art. 3 Abs. 3 anwendbar.

---

[25] Erw.Gr. 13 S. 1; *Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 211; Gola–*Gola*, Datenschutz-Grundverordnung, 2. Aufl., 2018, Art. 1 Rn. 24; Kühling/Buchner–*Zerdick*, Datenschutz-Grundverordnung/BDSG, 2. Aufl., 2018, Art. 1 Rn. 3; zweifelnd am Erfolg der Vollharmonisierung beispielsweise Sydow–*Sydow*, Europäische Datenschutzgrundverordnung, 2. Aufl., 2018, Einl. Rn. 22 ff.; Wolff/Brink–*Wolff/Brink*, Beck'scher Online-Kommentar Datenschutzrecht, 31. Edition, 2020 [Stand: 01.11.2019], Einl. zur DSGVO Rn. 20 m.w.N.

[26] *Hofmann/Johannes*, ZD, 2017, 221; Sydow–*Sydow*, Europäische Datenschutzgrundverordnung, 2. Aufl., 2018, Einl. Rn. 36; Ehmann/Selmayr–*Selmayr/Ehmann*, DS-GVO, 2. Aufl., 2018, Einf. Rn. 3.

[27] *Wybitul*, BB, 2016, 1077, 1078; ähnl. Ehmann/Selmayr–*Zerdick*, DS-GVO, 2. Aufl., 2018, Art. 3 Rn. 3; Kühling/Buchner–*Klar*, Datenschutz-Grundverordnung/BDSG, 2. Aufl., 2018, Art. 3 Rn. 1; Gola–*Piltz*, Datenschutz-Grundverordnung, 2. Aufl., 2018, Art. 3 Rn. 1; *Schantz/Wolff* (Hrsg.), Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 321.

[28] Sydow–*Ennöckl*, Europäische Datenschutzgrundverordnung, 2. Aufl., 2018, Art. 3 Rn. 4; Gola–*Piltz*, Datenschutz-Grundverordnung, 2. Aufl., 2018, Art. 3 Rn. 9; Kühling/Buchner–*Klar*, Datenschutz-Grundverordnung/BDSG, 2. Aufl., 2018, Art. 3 Rn. 2; Ehmann/Selmayr–*Zerdick*, DS-GVO, 2. Aufl., 2018, Art. 3 Rn. 9;*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 328.

Jedoch wird der Anwendungsbereich der DSGVO noch erweitert. Neben dem Niederlassungsprinzip führt die DSGVO in Art. 3 Abs. 2 das sog. Marktortprinzip ein, nach dem die Verordnung unter bestimmten Voraussetzungen auch für Verantwortliche oder Auftragsverarbeiter *ohne* Niederlassung in der EU Geltung beanspruchen kann.[29] Die DSGVO ist nämlich auch anwendbar auf die Verarbeitung personenbezogener Daten, wenn der Verantwortliche oder Auftragsverarbeiter zwar über keine Niederlassung in der EU verfügt, aber betroffenen Personen in der EU seine Waren oder Dienstleistungen anbietet (Art. 3 Abs. 2 lit. a) DSGVO) oder das Verhalten von betroffenen Personen in der EU beobachtet (Art. 3 Abs. 2 lit. b) DSGVO).

Es ist zu erwarten, dass die DSGVO aufgrund dieses weiten Anwendungsbereiches auch in einem großen Maße Distributed Ledger-Technologien wie zum Beispiel Blockchain betrifft: Aufgrund des Niederlassungsprinzips fallen Betreiber privater Blockchains in der EU oder im Falle einer öffentlichen Blockchain möglicherweise jeder Knotenpunkt in der EU unter die DSGVO, soweit diese als Verarbeiter personenbezogener Daten anzusehen sind.[30] Nach dem Marktortprinzip sind auch in vielen Fällen außerhalb der EU bei der Verarbeitung von Blockchain-Daten die Regeln der DSGVO zu beachten. Insbesondere in Konstellationen, in denen das Angebot von Blockchain Services – gerade bei Transaktionsleistungen, dem Hauptanwendungsbereich von Blockchains – betroffene Personen in der EU ansprechen soll, wird der Anwendungsbereich der DSGVO

[29] *Wybitul*, BB, 2016, 1077, 1079; Auernhammer–*Lewinski*, DSGVO/BDSG, 6. Aufl., 2018, Art. 3 Rn. 11; Kühling/Buchner–*Klar*, Datenschutz-Grundverordnung/BDSG, 2. Aufl., 2018, Art. 3 Rn. 3; Gola–*Piltz*, Datenschutz-Grundverordnung, 2. Aufl., 2018, Art. 3 Rn. 2; Sydow–*Ennöckl*, Europäische Datenschutzgrundverordnung, 2. Aufl., 2018, Art. 3 Rn. 1.
[30] *Berberich/Steiner*, EDPL, 2016, 422, 423; ähnl. *Finck*, EDPL, 2018, 17, 27.

entsprechend eröffnet sein.[31] Angesichts der weltweiten Verteilung von Netzwerken dürften Blockchain-Anwendungen daher regelmäßig einen grenzüberschreitenden Bezug haben.[32]

Angesichts dieses Befundes ist es nicht verwunderlich, dass die datenschutzrechtliche Situation der noch im Entwicklungsstadium befindlichen Blockchain-Technologien nicht unproblematisch ist. Ihre großen Vorteile – Transparenz, Dezentralität, Unveränderlichkeit –könnten sich für sie am Ende als ihr größter Nachteil und datenschutzrechtlich als erheblicher *„Hemmschuh"*[33] erweisen. So ließe sich argumentieren, dass Blockchain-Technologien der Verwirklichung von datenschutzrechtlichen Prinzipien *„deutlich im Weg stehen"*[34], weil sie aufgrund ihrer Unveränderlichkeit und Dezentralität die Verwirklichung von Betroffenenrechten wie Informations- (Art. 12 – 15 DSGVO), Berichtigungs- und Löschungsansprüchen (Art. 16, 17 DSGVO) sowie Widerspruchsrechten (Art. 21 DSGVO) vereiteln könnten. Andererseits könnte sich Blockchain-Technologie sogar gerade als *„eine große Chance"*[35] für die Verwirklichung des Datenschutzes mit der DSGVO und ihrer Forderung nach „Datenschutz durch Technik"[36] (Art. 25 DSGVO) herausstellen, liegt ihr als Kerngedanke doch zugrunde, durch Verschlüsselung sowie Nutzung von Anonymisierungs- und

[31] *Berberich/Steiner*, EDPL, 2016, 422, 423.
[32] *Böhme/Pesch*, DuD, 2017, 473, 478; *Finck*, EDPL, 2018, 17, 27; *Berberich/Steiner*, EDPL, 2016, 422, 423.
[33] *Schrey/Thalhofer*, NJW, 2017, 1431, 1433.
[34] *Lange-Hausstein*, ITRB, 2017, 93.
[35] *Guggenberger*, ZD, 2017, 49, 50.
[36] Erwägungsgrund 78 S. 2.

Pseudonymisierungstechniken möglichst wenige Daten über ihre Nutzer preiszugeben. Blockchain-Technologie bewegt sich im Spannungsfeld der regulatorischen Prinzipien der DSGVO.

Die Frage, inwiefern die DSGVO im Kontext von Blockchains anwendbar ist und welche Probleme sie aufwirft, ist nicht bloß theoretischer Natur und sollte auch in der Praxis keinesfalls unterschätzt werden. Schon angesichts des Umstandes, dass die DSGVO umfangreiche Pflichten auferlegt und eine Vielzahl an Verstößen sanktioniert ist, kann eine Nichtbeachtung der DSGVO zu ernsthaften Konsequenzen für datenschutzrechtlich Verpflichtete führen. Geldbußen können je nach Art des Verstoßes bis zu 20 Mio. € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres betragen, Art. 83 Abs. 5 DSGVO, sodass Verstöße empfindliche Konsequenzen für potentielle Anwender haben können.

Dies ist Grund genug, sich mit dem Spannungsfeld zwischen der noch jungen Blockchain-Technologie und der DSGVO näher auseinanderzusetzen und zu untersuchen, inwieweit sich diese neue Technologie in das neue datenschutzrechtliche Spielfeld wird einfügen können.

III. Problemaufriss

Am Beispiel der Blockchain-Technologie tritt die vermeintliche Widersprüchlichkeit zwischen Datenschutz und dezentral vernetzter Technologie besonders anschaulich zu Tage. Denn in der Regel werden auf Blockchains Daten verarbeitet, die sich technisch mit dem dahinterstehenden Nutzer verknüpfen lassen; so können beispielsweise Bitcoin-Transaktionen mit den IP-Adressen von Zahlungsauslöser bzw. -empfänger in Verbindung gebracht werden, was zeigt,

dass Blockchain-Daten nur vermeintlich anonym sind und ein relevanter, das Datenschutzrecht auslösender Personenbezug häufig nicht auszuschließen ist.[37]

Wer hat die Vorgaben der DSGVO in einem Blockchain-System einzuhalten, wenn Datenschutzrecht anwendbar ist? Wer muss insbesondere datenschutzrechtliche Betroffenenrechte wie Informations- oder Löschungsrechte erfüllen, oder kurz: wer ist in einem dezentralen System als datenschutzrechtlich Verantwortlicher anzusehen? Als eine Form der Distributed Ledger-Technologie sind Blockchains Datenbanken, die in einem Netzwerk dezentral verteilt sind.[38] Zahlreiche Stellen kommen in einem solchen Netzwerk auf unterschiedliche Weise mit Datenverarbeitungsprozessen in Berührung, während die Abstimmung eines solchen Systems größtenteils über Algorithmen abläuft, auf die ein Einzelner keinen Einfluss hat. Die technischen Abläufe machen es aus Sicht von Regulierungsbehörden wie auch Betroffenen sehr schwer, einen Regelungsadressaten und/oder Anspruchsgegner auszumachen. Unklar ist auch, inwiefern Datenschutzrecht in solchen dezentralen Netzwerken durchgesetzt werden könnte. Lässt sich kein Verantwortlicher ausmachen, drohen Blockchain-Systeme, zu einem *„datenschutzrechtliche[n] Niemandsland“*[39] zu werden. Aber auch wenn sich ein Verantwortlicher ausmachen lässt, besteht die Herausforderung, eine Verarbeitung von Blockchain-Daten rechtmäßig durchzuführen

[37] *Isler*, Datenschutz auf der Blockchain, S. 3; ähnl. z.B. auch *Finck*, EDPL, 2018, 17, 26; *Marnau*, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, in: *Eibl/Gaedke* (Hrsg.), Informatik 2017, 2017, S. 1025, 1028; *Quiel*, DuD, 2018, 566, 568.
[38] *Böhme/Pesch*, DuD, 2017, 473, Fn. 2; *Finck*, EDPL, 2018, 17; *Sixt*, Bitcoins und andere dezentrale Transaktionssysteme, 1. Aufl. 2017, S. 177.
[39] *Isler,* Datenschutz auf der Blockchain, S. 13.

und insbesondere vor dem Hintergrund der Unveränderbarkeit einen angemessenen Ausgleich zwischen dem Interesse an der Entwicklung neuer Technologien und dem Schutz von Betroffenenrechten herzustellen.

Das Grundprinzip der Blockchain-Technologie, Daten praktisch unveränderbar und öffentlich einsehbar dezentral abzuspeichern, scheint gerade hier – jedenfalls prima facie – dem Datenschutz fundamental zu widersprechen. Frei einsehbare Blockchains scheinen die *„Antipode des Datenschutzes"*[40] zu sein. Datenschutz durch ein solches System mag auf den ersten Blick sogar *„grotesk"*[41] erscheinen.

IV. Arbeitshypothese

Ist die Blockchain-Technologie eine *„große Chance"*[42] für den Datenschutz, oder könnte sie nicht sogar im Gegenteil eine Gefahr[43] für ihn bedeuten? Diese Frage soll in der folgenden Bearbeitung anhand spezifischer Problemstellungen näher beleuchtet werden. Die Relevanz der DSGVO für Blockchain-Technologien wird vor allem davon abhängen, inwiefern Daten auf einer Blockchain als personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO einzustufen sind, ob diese Daten rechtmäßig (Art. 5 Abs. 1 lit. a, Art. 6 DSGVO) und unter Wahrung der Betroffenenrechte (insbesondere der Berichtigungs- und Löschungsansprüche gem. Art. 16 und Art 17 DSGVO) verarbeitet werden können und schließlich, welche Blockchain-Akteure als Verantwortliche (Art. 4 Nr. 7, Art. 26 DSGVO)

---

[40] *Isler,* Datenschutz auf der Blockchain, S. 2.
[41] *Guggenberger*, ZD, 2017, 49.
[42] So z.B. *Guggenberger*, ZD, 2017, 49, 50; ebenso *Bechtolf/Vogt*, Blockchain und Datenschutz - Recht technologisch, in: *Taeger* (Hrsg.), Recht 4.0 - Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 873, 885.
[43] In diese Richtung z.B. *Berger*, DVBl, 2017, 1271, 1273; ähnl. *Pesch/Sillaber*, CRi, 2017, 166, 171.

anzusehen sind.[44] Vor diesem Hintergrund lohnt es sich, gerade hier mit der Untersuchung der Vereinbarkeit von technischem Prinzip und rechtlichen Rahmenbedingungen anzusetzen. In diesem Kontext stellen sich folgende Fragen, die im Folgenden der Reihe nach abgearbeitet werden sollen:

- Kann eine Verarbeitung der Daten auf einer Blockchain einen Personenbezug aufweisen?

- Bejahendenfalls: Welche Auswirkungen ergeben sich aus den Spezifika der Blockchain-Technologie?

- Wer ist datenschutzrechtlich verantwortlich?

Mit diesen zentralen Problemen befassen sich die Überlegungen im Folgenden. Dabei sei folgende These aufgestellt: in der Blockchain sind eine Reihe von Verarbeitungsvorgängen datenschutzrechtlich relevant. Die technischen Prinzipien der Blockchain-Technologie machen die Einhaltung der Vorgaben der DSGVO allerdings nahezu unmöglich, denn zum einen bereitet deren faktische Unveränderlichkeit Schwierigkeiten bei Ansprüchen auf Berichtigung und Löschung von Daten, zum anderen ist in den dezentralen Netzwerken von Blockchains in der Regel nahezu jeder Teilnehmer datenschutzrechtlich gemeinsam Verantwortlicher, ohne aber über ausreichend Einflussmöglichkeiten zu verfü-

[44] Ähnl. bereits *Berberich/Steiner*, EDPL, 2016, 422, 423 ff.; *Bechtolf/Vogt*, ZD, 2018, 66, 69 f.; *Böhme/Pesch*, DuD, 2017, 473, 478 ff.; *Quiel*, DuD, 2018, 566, 569 ff.; ausf. *Finck*, EDPL, 2018, 17, 22 ff.

gen, um die daraus erwachsenden Pflichten zu erfüllen. Der Grundsatz des Datenschutzes durch Technik verlangt daher, dass dezentrale bzw. nicht nachträglich veränderbare Blockchains nur in anonymisierter Form betrieben werden dürfen. Um dies wirksam umzusetzen, bedarf es flankierender Regelungen in der DSGVO.

Im gegenwärtigen technischen Entwicklungsstadium sind wenige verallgemeinerungsfähige Aussagen über sämtliche Blockchain-Varianten möglich, weil unterschiedlichste technische Gestaltungsmöglichkeiten denkbar sind.[45] Gleichzeitig ist die Blockchain-Technologie schnellen Entwicklungen unterworfen.[46] Die vorliegende Dissertation will daher aufzeigen, zu welchen datenschutzrechtlichen Problemen es bei der Verwendung von Blockchain-Technologien kommen kann, um einerseits technische Handlungsmöglichkeiten aufzuzeigen, andererseits aber auch rechtliche Regulierungsmöglichkeiten zu entwickeln.

V. Weiteres Vorgehen

Zunächst soll eine technisch-thematische Eingrenzung anhand der grundlegenden Prinzipien einer Blockchain erfolgen. Idealtypisch handelt es sich bei Blockchains um Datenbanktypen mit der Datenstruktur einer sog. Hash-verketteten Liste mit Arbeitsnachweis[47]. Die Registerfunktion ist die zentrale und allen Blockchain-Technologien gemeinsame Grundeigenschaft (hierzu **Kapitel C.II**), die durch verschiedene technische Komponenten unterstützt oder ergänzt

[45] *Simmchen*, MMR, 2017, 162, 163; *Gervais*, digma, 2017, 128; *Quiel*, DuD, 2018, 566, 567; *Bechtolf/Vogt*, ZD, 2018, 66, 67.
[46] *Guggenberger*, ZD, 2017, 49, 50; *Finck*, EDPL, 2018, 17, 18.
[47] *Böhme/Pesch*, DuD, 2017, 473, 475.

wird.[48] Erst durch diese technischen Komponenten ergeben sich konkrete rechtliche Probleme mit Blockchains. Dabei ist hervorzuheben, dass insbesondere die Verbindung der permanenten Speicherung von Daten mit der dauerhaften öffentlichen Einsehbarkeit des Netzwerkes (hierzu **Kapitel C.III**) große datenschutzrechtliche Probleme mit sich bringen kann, welche sodann unter **Kapitel D** näher untersucht werden sollen. In **Kapitel E** werden die identifizierten Probleme diskutiert und Lösungsansätze entworfen.

[48] *Jacobs/Lange-Hausstein*, ITRB, 2017, 10; *Marnau*, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, in: *Eibl/Gaedke* (Hrsg.), Informatik 2017, 2017, S. 1025, 1026.

C. Funktionsweise einer Blockchain

I. Einleitung

Bei der Untersuchung einer neuen Technologie unter juristischen Gesichtspunkten ist es erforderlich, sich zunächst mit den technischen Merkmalen und Eigenschaften auseinanderzusetzen, welche diese Technologie ausmachen. Da die Blockchain-Technologie mittlerweile vermehrt Gegenstand juristischer Untersuchungen ist, gibt es bereits zahlreiche Beschreibungen der technischen Merkmale.[49]

Als Grundlage der technischen Beschreibung der Blockchain-Technologie dient oft das Modell der Bitcoin-Blockchain. In diesem Zusammenhang ist es allerdings wichtig, zu verstehen, dass es nicht „die eine" Blockchain gibt.[50] Obgleich Bitcoin gleichsam *„die Wiege der Blockchain"*[51] ist, sind digitale Währungen und insbesondere Bitcoin keinesfalls der einzige Anwendungsbereich für die Blockchain-Technologie.

Es existieren zahlreiche verschiedene Blockchain-Modelle, welche jeweils auf verschiedene Art und Weise die grundsätzlichen Vorteile der Blockchain-Technologie nutzbar machen sollen. Tatsächlich gibt es viele verschiedene Gestaltungsmöglichkeiten und Varianten, etwa im Hinblick auf Speicherort, Scripting-Fähigkeiten, Zugangskontrolle und Anwendungsmöglichkeiten.[52] Insoweit

[49] Z.B. bei *Böhme/Pesch*, DuD, 2017, 473 ff.; *Kaulartz*, CR, 2016, 474 ff.; *Martini/Weinzierl*, NVwZ, 2017, 1251 ff.; *Schrey/Thalhofer*, NJW, 2017, 1431 ff.; *Isler,* Datenschutz auf der Blockchain; *Simmchen*, MMR, 2017, 162 ff.
[50] *Simmchen*, MMR, 2017, 162, 163; *Guggenberger*, ZD, 2017, 49, 50.
[51] *Isler,* Datenschutz auf der Blockchain, S. 4.
[52] Für eine beispielhafte Darstellung der Varianten s. etwa *Ploom*, Blockchains - wichtige Fragen aus IT-Sicht, in: *Burgwinkel* (Hrsg.), Blockchain Technology, 1. Aufl., 2016, S. 123, 123.

C. Peitz, *Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen*, Juridicum – Schriften zum Medien-, Informations- und Datenrecht,
https://doi.org/10.1007/978-3-658-32050-8_2

scheint es sich bei dem technischen Konzept der Blockchain-Technologie zunächst um ein im Einzelnen *„komplexes und vielschichtiges informatisches Konstrukt“* zu handeln.[53]

Der Begriff „Blockchain“ wird in verschiedenen Kontexten verwendet.[54] Blockchain-Technologie ist dabei für sich genommen nicht neu, sondern lediglich eine Kombination bereits bestehender Konzepte.[55] Daher überrascht es nicht, dass keine einheitliche – insbesondere in der rechtswissenschaftlichen Literatur anerkannte und einheitliche – Definition des Begriffes „Blockchain“ existiert.[56] Technologie und Anwendungsszenarien sind zudem einem raschen Fortschritt unterworfen.[57] Dies erschwert eine Annäherung an das Thema aus rechtlicher Sicht.

Daraus ergibt sich, dass für eine juristische Annäherung an die Blockchain-Technologie zunächst einer Auseinandersetzung mit einigen technischen Grundlagen und einer technischen Eingrenzung und Systematisierung bedarf. Dies ist vor allem auch deshalb geboten, weil Einzelheiten in den technischen Abläufen gerade im Hinblick auf Datenschutzaspekte große Unterschiede bedingen können.

---

[53] *Simmchen*, MMR, 2017, 162.
[54] Vgl. *Burgwinkel*, Blockchaintechnologie und deren Funktionsweise verstehen, in: *Burgwinkel* (Hrsg.), Blockchain Technology, 1. Aufl., 2016, S. 1, 4.
[55] *Blocher*, AnwBl, 2016, 612, 615; *Simmchen*, MMR, 2017, 162; *Böhme/Pesch*, DuD, 2017, 473 f.
[56] *Finck*, EDPL, 2018, 17, 18; in den gerichtlichen Verfahrensvorschriften des US-Bundesstaates Vermont findet sich die Legaldefinition „[…] *"blockchain technology" means a mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via Internet interaction, peer-to-peer network, or otherwise.”*, vgl. Vermont Statutes Annotated, T.12, § 1913 (a).
[57] *Lange-Hausstein*, ITRB, 2017, 93.

II. Grundeigenschaft von Blockchains: Datenbank mit Registerfunktion

Prinzipiell stellt eine Blockchain eine Datenbank[58] dar, die Soft- und Hardware in bestimmter Weise kombiniert.[59] Für die weitere Betrachtung der Blockchain-Technologie ist wichtig, dass die zentrale Grundfunktion der Blockchain-Architektur schlicht darin besteht, Daten dauerhaft und unabänderbar zu speichern.[60] Bei allen technischen Anwendungsvarianten ist allen Blockchains letztlich jedenfalls eine Grundfunktion gemein: es handelt sich um Datenbanken mit Registerfunktion.[61]

Das Besondere an diesem Datenbank-Typ ist vor allem, dass dort Einträge nur hinzugefügt, im Nachhinein aber nicht mehr gelöscht oder verändert werden können (*„append-only"*[62]) und dass in die Datenbanken neu hinzugefügte Einträge über einen Konsensmechanismus für gültig erklärt werden.[63] Sind Daten auf einer solchen Blockchain-Datenbank erst einmal gespeichert, können sie nicht mehr gelöscht oder überschrieben werden.[64] Alle Änderungen von Daten oder sonstigen Ereignissen werden chronologisch archiviert.[65]

Blockchains ermöglichen es dadurch, in verteilten Dateisystemen ohne zentrale Kontrollstelle die Integrität zu erhalten.[66] Im Grunde kann durch eine

---

[58] Im Grunde also eine *„bestimmte Art und Weise, Daten sicher zu speichern"*, s. *Schrey/Thalhofer*, NJW, 2017, 1431.
[59] *Jacobs/Lange-Hausstein*, ITRB, 2017, 10 f.
[60] Vgl. *Schrey/Thalhofer*, NJW, 2017, 1431; *Quiel*, DuD, 2018, 566, 567.
[61] *Finck*, EDPL, 2018, 17, 18; *Jacobs/Lange-Hausstein*, ITRB, 2017, 10.
[62] *„Nur-Hinzufüge-Datenspeicher"*, s. *Drescher*, Blockchain Grundlagen, 1. Aufl., 2017, S. 158; *Finck*, EDPL, 2018, 17.
[63] *Böhme/Pesch*, DuD, 2017, 473; *Quiel*, DuD, 2018, 566, 567.
[64] *Jacobs/Lange-Hausstein*, ITRB, 2017, 10; *Bechtolf/Vogt*, ZD, 2018, 66, 69.
[65] *Hoeren*, NJW, 2017, 1587, 1592.
[66] *Drescher*, Blockchain Grundlagen, 1. Aufl., 2017, S. 230.