Decentralized Web – Vom Spannungs- zum Komplementaritätsverhältnis zwischen (Datenschutz-)Recht und Code

Urheber: NicoElNino | Quelle: shutterstock.com

Nadine Rinderknecht

Mehr als 10 Jahre

12. Februar 2020

Web 3.0, Datenautonomie, Pathetic Dot Theory, Privacy Paradox, Schutz vor sich selbst, Selbstverantwortung, Smart Privacy Contract, Zensur

Die Welt, so wie wir sie kennen, ist eine Welt des Datenmissbrauchs. Webgiganten wie Google, Amazon, Facebook und Apple sammeln die Daten ihrer sorglosen Nutzer und speichern sie in abgeriegelten Datensilos. In nicht wenigen Fällen werden Daten monetarisiert und missbraucht; die europäische Datenschutz-Grundverordnung wirkt sich auf die informationelle Selbstbestimmung der betroffenen Personen im Cyberspace nur wenig aus. Denn wer auch immer den Speicherort der Daten beherrscht, der kontrolliert den Datenzugang und damit auch die Daten selber.

Diese Feststellung ist Problem und Lösung zugleich: Bestimmen nicht mehr die Unternehmen sondern die Nutzer über Speicherort und Datenzugang, so wandert die Datenautonomie zu den Nutzern. Das Decentralized Web (DWeb) versucht genau dies zu erreichen, sodass das aktuelle Spannungsverhältnis zwischen der Technik (Code), welche Datenmissbräuche überhaupt ermöglicht, und dem (Datenschutz-)Recht, welche diese unterbinden möchte, zu einem Komplementaritätsverhältnis gemeinsamer Verhaltensregulierung werden könnte. Doch (wie) soll das DWeb **reguliert** werden? Welche Fragen ergeben sich für das Recht wie das **Wettbewerbsrecht**, das **Urheberrecht** und – besonders – das **Datenschutzrecht**? Und wird allein die technische Architektur des DWebs einen Datenmissbrauch verhindern können?

Inhaltsverzeichnis

1 Zentralisierung des Webs und Decentralized Web 5
2 Definition des (D)Webs 7
2.1 Allgemeine Definition des Webs 7
2.2 Drei Web-Generationen 7
2.3 Decentralized Web 8
2.3.1 Heutiges und zukünftiges DWeb 8
2.3.2 Dezentralisiertes Speicher- und Kontrollsystem 9
2.3.3 Weitere dezentralisierte Systeme 10
2.3.4 Solid und Inrupt Inc. 10
2.3.5 Blockchain-Technologien 12
2.4 Zwischenfazit 12
3 Regulierung des DWebs 13
3.1 Ist das DWeb zu regulieren? 13
3.2 Wie ist das DWeb zu regulieren? 13
3.2.1 Pathetic Dot Theory 13
3.2.2 Problematik der Durchsetzbarkeit 14
3.3 Zwischenfazit 15
4 Das Wettbewerbsrecht 16
4.1 (D)Web und (D)Apps 16
4.2 Privacy Paradox 16
4.3 Re-Zentralisierung des Webs 18
4.4 Spezifische (Blockchain-)Problemfälle 18
4.5 Zwischenfazit 19
5 Das Urheberrecht 20
5.1 Digital Rights Management 20
5.1.1 Begriff 20
5.1.2 Anonymität, Zensur und endgültige Löschung 20
5.1.3 Digitale Rechteminderung 21
5.1.4 Zwischenfazit 21
5.2 Smart Contracts 21
5.3 Nicht-automatisierte Datenautonomie 22

5.4 Zwischenfazit 23
6 Das Datenschutzrecht 24
6.1 Code und Recht 24
6.1.1 Code als Ursprung der Datenautonomie 24
6.1.2 Hüter der Datenautonomie 25
6.1.2.1 Datenschutzrecht 25
6.1.2.2 Datenschutzcode 25
6.1.3 Zwischenfazit 26
6.2 Machtverhältnisse, Schutz vor sich selbst und Paternalismus 26
6.2.1 Veränderung der Machtverhältnisse 26
6.2.2 Schutz vor anderen und vor sich selbst 27
6.2.3 Paternalistischer Regelungsbedarf 27
6.2.4 Zwischenfazit 28
6.3 Verantwortlicher Dateninhaber 28
6.3.1 Verantwortlichkeit in der Blockchain 28
6.3.2 Datenschutzrechtliche Selbstverantwortung 29
6.3.3 Zwischenfazit 30
6.4 Sachlicher Anwendungsbereich (Art. 2 DSGVO) 30
6.5 Grundsätze der Datenverarbeitung (Art. 5 DSGVO) und Smart Privacy Contract .31
6.5.1 Grundsatz der Transparenz 31
6.5.2 Grundsatz der Zweckbindung 32
6.5.3 Grundsatz der Datenminimierung 32
6.5.4 Grundsatz der Richtigkeit 32
6.5.5 Grundsatz der Speicherbegrenzung 33
6.5.6 Grundsatz der Integrität und Vertraulichkeit 33
6.5.7 Rechenschaftspflicht 34
6.5.8 Smart Privacy Contract 34
6.5.8.1 Begriff 34
6.5.8.2 Voraussetzungen des Privacy by Design 34
6.5.8.3 Smart Contracts im Vertragsrecht 35
6.5.9 Zwischenfazit 36
6.6 Verbotsprinzip mit Erlaubnisvorbehalt (Art. 6 DSGVO) 36

6.6.1 Begriff und Einwilligung 36
6.6.2 Ausschliessliche faktische Datenautonomie 37
6.6.3 Zwischenfazit 38
6.7 Recht auf Löschung (Art. 17 DSGVO) 38
6.7.1 Begriff, Löschungsgrund und Erforderlichkeit 38
6.7.2 Zuweisung der Zensurpflicht 39
6.7.2.1 Zum Dateninhaber 39
6.7.2.2 Zum Kollektiv 39
6.7.2.3 Zu einer zentralen Stelle 39
6.7.3 Zwischenfazit 40
6.8 Recht auf Datenübertragbarkeit (Art. 20 DSGVO) 40
6.8.1 Begriff 40
6.8.2 Disruption durch Recht und Technologie 41
6.8.3 Entgegenstehende öffentliche Interessen 42
6.8.4 Entgegenstehende Interessen Dritter 42
6.8.5 Zwischenfazit 43
6.9 Datenübermittlung an Drittländer (Art. 44 ff. DSGVO) 43
6.10 Zwischenfazit 44
7 Schlussfazit 45

1 Zentralisierung des Webs und Decentralized Web

1 *~ Dieses erste Bit Programmcode von Enquire [Vorgängerversion des World Wide Webs] führte mich zu etwas viel größerem: zu einer Vision, die einen dezentralisierten […] Fortschritt von Ideen, Technologien, ja der Gesellschaft einschließt.*[1] *~*

2 1999 stellt Sir *Tim Berners-Lee*, der Begründer des World Wide Webs 1989 ("WWW" oder auch nur "Web"), seinen Report vor, in dem er die Entstehungsgeschichte des WWW darstellt. 20 Jahre später sieht er die Potentiale des Webs aber zunehmend als gefährdet an.[2] Dies ist besonders dem Umstand geschuldet, dass die Kommunikation zwischen Webnutzern nicht mehr auf direkte Art und Weise erfolgt. Im Gegenteil werden meist Plattformen (z.B. Gmail, AmazonPay, Facebook, FaceTime) bzw. Server zwischengeschaltet, die von einigen wenigen Unternehmen gehostet werden (z.B. GAFA-Unternehmen[3]).[4] Eine solche geringe Anzahl an Webgiganten steht jedoch in einem krassen Missverhältnis zu den weltweit rund 4,5 Milliarden aktiven Internetnutzern (Stand Januar 2020)[5] und damit auch zu der Vision des WWW-Begründers, durch die dezentralisierte Architektur des Webs zentrale Instanzen zu überwinden.[6]

3 Die daraus ergehenden Folgen sind mannigfaltig: Nicht nur lagern die Webgiganten die Daten in grossen, abgeriegelten Datensilos, sondern sie missbrauchen diese, dringen in die Privatsphäre der Webnutzer ein und erleichtern die staatliche Überwachung und Zensur wie etwa im Falle des Sozialkredit-Systems in China.[7] Denn: "The web is already decentralized. The problem is the dominance of one search

---

[1] *Tim Berners-Lee/Mark Fischetti*, Der Web-Report: Der Schöpfer des World Wide Webs über das grenzenlose Potential des Internets, München 1999, S. 9.

[2] *Berkman Klein Center for Internet & Society at Harvard University*, The future of the decentralized web, in: Medium vom 31. Juli 2019, o.S.

[3] Der Oberbegriff "GAFA-Unternehmen" erfasst (neben Microsoft) die Unternehmen **G**oogle, **A**mazon, **F**acebook und **A**pple; siehe *Marc Kowalsky*, Warum die Internetgiganten zu mächtig sind, in: Handelszeitung vom 20. März 2018, o.S.; siehe auch die Vielzahl an Ökosystemen der (GAFA-)Unternehmen.

[4] *Zoë Corbyn*, Decentralisation: the next big step for the world wide web, in: The Guardian vom 8. September 2018, o.S.

[5] *Statista GmbH*, Global digital population as of January 2020; es ist daran zu erinnern, dass die Begriffe "Web" und "Internet" auseinanderzuhalten sind (siehe auch unten Rz. 6). Da das Web jedoch einer der wichtigsten Internetdienste ist und meines Wissens die aktuelle Anzahl an Webnutzern nicht auffindbar ist, wird hier die Statistik über die Anzahl an *Internet*nutzern aufgeführt.

[6] *Berners-Lee/Fischetti*, S. 32.

[7] *Chelsea Barabas/Neha Narula/Ethan Zuckerman*, Defending Internet Freedom through Decentralization: Back to the Future?, The Center for Civic Media & The Digital Currency Initiative MIT Media Lab, Cambridge 2017, S. 15 ff.; *Edina Harbinja/Vasileios Karagiannopoulos*, Web 3.0: the decentralised web promises to make the internet free again, in: The Conversation vom 11. März 2019, o.S.; *FAQ des Decentralized Web Summit 2018*, Antwort zu Frage 3 (nachfolgend "FAQ-DWeb").

engine, one big social network, one Twitter for microblogging. We don't have a technology problem; we have a social problem."[8]

4 Gemäss den von *Berners-Lee* initiierten 9 Prinzipien im "Contract for the Web" ist der zunehmenden Zentralisierung des Webs und den daraus entstehenden Problemen besonders durch die Selbstverpflichtung seitens der Staaten (Prinzipien 1-3), der Unternehmen (Prinzipien 4-6) sowie der Bürger (Prinzipien 7-9) entgegenzutreten.[9] Doch das Problem der Web-Zentralisierung könnte auch durch die technische Modifikation der Webarchitektur selbst gelöst werden.[10] "[In the traditional web] we are pointing to this location and pretending [the information] exists in only one place, […] And from this comes this whole monopolisation that has followed... because whoever controls the location controls access to the information."[11]

Abbildung 1: Sir *Tim Berners-Lee*

[8] *Quentin Hardy*, The Web's Creator Looks to Reinvent It, in: The New York Times vom 7. Juni 2016, o.S. (Zitat von *Berners-Lee*); siehe auch unten Rz. 31 zur Re-Zentralisierung des Webs.

[9] *Representatives from over 80 organizations*, Contract for the Web, November 2019, S. 3 ff. (nachfolgend "Web-Contract").

[10] *Hardy*, o.S.

[11] *Corbyn*, o.S. (Zitat von *Matt Zumwalt*).

2 Definition des (D)Webs

5 In diesem Kapitel wird zunächst die allgemeine Funktionsweise des Webs definiert (siehe sogleich Rz. 6). Nach einem kurzen Überblick über die drei Webgenerationen (siehe unten Rz. 8) wird sodann die dritte Webgeneration – das Decentralized Web – in vertiefter Weise dargestellt (siehe unten Rz. 9).

2.1 Allgemeine Definition des Webs

6 Das WWW ist eine Nutzungsart – neben etwa Internettelefonie und E-Mail – des Internets, das die Struktur eines Netzes aufweist. Die Knoten des Netzes sind elektronische Hypertext-Dokumente (z.B. Webseiten), die untereinander durch Hyperlinks verknüpft sind.

7 In diesem Netz kommt den Standards URI, HTTP und HTML eine grundlegende Bedeutung zu.[12] Der Uniform Resource Identifier (URI) ist eine Zahlenfolge zur eindeutigen Bezeichnung einer Ressource (z.B. abzurufende Webseite).[13] Mit dem Hypertext Transfer Protocol (HTTP) werden Daten übertragen (z.B. Laden einer Webseite in den Webbrowser).[14] Und die Hypertext Markup Language (HTML) ist eine Auszeichnungssprache bzw. maschinenlesbare Sprache zur Gliederung und Formatierung eines Hypertextes (z.B. Anzeigen von Text und Bildern einer Webseite im Webbrowser).[15]

2.2 Drei Web-Generationen

8 1989 begründete *Berners-Lee* das WWW, angeregt durch seine eigenen Vorarbeiten zu "Enquire"[16] sowie diejenigen von Vannevar Bush zu "Memex" und Ted Nelson zu "Xanadu".[17] Diese erste Generation des Webs (Web 1.0) lässt sich dadurch charakterisieren, dass eine kleine Anzahl an Produzenten Hypertext-Dokumente erstellt und so einen "globalen Informationsraum"[18] schafft, worauf die Konsumenten zugreifen (sog. Hypertext Web).[19] Ab 2005 verbreitete sich sodann der Begriff "Web 2.0" (sog. Social Web). Dieser beschreibt die zweite Generation des Webs als eine Plattform, auf welcher die Webnutzer (sog. Prosumenten) als Kon*sumenten* und infolge nutzerfreundlicherer Verwendungsmöglichkeiten neu auch als *Pro*duzenten

---

12 *Berners-Lee/Fischetti*, S. 61; mit der Zeit kamen jedoch noch weitere Standards hinzu (z.B. HTTPS, CSS).

13 *Tim Berners-Lee et al.*, RFC 3986, Uniform Resource Identifier (URI), 2005, S. 4.

14 *Tim Berners-Lee et al.*, RFC 1945, Hypertext Transfer Protocol, 1996, S. 4.

15 *Tim Berners-Lee/Dan Connolly*, RFC 1866, Hypertext Markup Language, 1995, S. 2 f.

16 Siehe oben auch das Zitat bei Rz. 1.

17 *Berners-Lee/Fischetti*, S. 13 ff.; siehe auch "home of the first website" beim CERN.

18 *Berners-Lee/Fischetti*, S. 14.

19 *Berners-Lee/Fischetti*, S. 32.

aktiv werden, woraus eine kollektive Intelligenz hervorgeht (z.B. Wikipedia, YouTube).[20] Sodann beschreibt das Web 3.0 die dritte Generation des Webs (sog. Semantic Web). Die von den Prosumenten erzeugten Daten werden derart in Relation zu anderen Daten gesetzt, dass dadurch ein semantisches Datennetz entsteht (sog. Linked Data). Die Bedeutung der Daten soll damit maschinenlesbar werden und so etwa die Web-Kommunikation zwischen Maschinen oder verbesserte Suchergebnisse ermöglichen.[21] [22]

2.3 Decentralized Web

2.3.1 Heutiges und zukünftiges DWeb

9 Das Decentralized Web[23] (oder auch nur "DWeb") ist ein Unterfall des Web 3.0, wobei Linked Data dezentralisiert gespeichert wird.[24] Auch wenn bereits heute auf dem Peer-to-Peer-Netzwerk laufende Apps (sog. DApps) angeboten werden (z.B. ZeroNet, DTube, OpenBazaar oder Matrix), wird das DWeb gemäss dem aktuellen Gartner Hype Cycle for Emerging Technologies voraussichtlich erst in mehr als 10 Jahren das Plateau der Produktivität (Mainstream) erreichen.[25]

10 Doch bereits heute geht das *Decentralized* Web über die Dezentralisierung, welche mit den Webgenerationen 1.0 bis 2.0 eingesetzt hat, hinaus: Nach der Dezentralisierung des Zugriffs (Web 1.0) und der Produktion (Web 2.0) der Daten erfolgt mit dem DWeb primär eine Dezentralisierung ihres *Speicherorts*.[26] Das DWeb basiert unter anderem auf der Distributed-Ledger-Technologie (DLT) bzw. auf einer ihren Unterformen wie den Blockchain-Technologien. Zum jetzigen Zeitpunkt ist die konkrete Ausgestaltung der DLT jedoch noch unklar.[27] Wahrscheinlich ist aber, dass

---

[20] *Tim O'Reilly*, What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, in: Communications & Strategies, no. 65, 1st quarter 2007, S. 18 f., 22 f.

[21] *Berners-Lee/Fischetti*, S. 259 ff.; siehe auch *Tim Berners-Lee*, The next web, TED Talk vom Februar 2009 zur Linked Data.

[22] Vgl. zum Ganzen *Nupur Choudhury*, World Wide Web and Its Journey from Web 1.0 to Web 4.0, in: International Journal of Computer Science and Information Technologies, Vol. 5 (6), 2014, S. 8096 ff. sowie *B. K. Hiremath/Anand Y Kenchakkanavar.*, An Alteration of the Web 1.0, Web 2.0 and Web 3.0: A Comparative Study, in: Imperial Journal of Interdisciplinary Research, Vol-2, Issue-4, 2016, S. 705 ff.; siehe auch Die Evolution des Webs.

[23] Von der dezentralisierten Struktur ist neben der zentralisierten auch die distribuierte zu unterscheiden. Siehe dazu die 3 Network Topologies (unter Berücksichtigung ihrer Angriffsanfälligkeit bzw. Point of Failure). Das Titelbild dieses Sheets ist im Kontext des DWebs insofern nicht ganz zutreffend (aber schön).

[24] *Harbinja/Karagiannopoulos*, o.S.; *Nick Vogel*, The Great Decentralization: How Web 3.0 Will Weaken Copyrights, in: John Marshall Review of Intellectual Property Law, Vol. 15, No. 1, 2016, S. 137 ff.

[25] *Gartner Inc.*, Gartner Hype Cycle for Emerging Technologies, 29. August 2019, o.S.; siehe auch *FAQ-DWeb*, Antwort zu Frage 14: "Some apps and programs, built on the decentralized model, are already available […]. But the Decentralized Web, as an envisioned ecosystem, might not be fully functional and integrated for another five or ten years."

[26] Vgl. FAQ-DWeb, Antwort zu Frage 2; siehe unten Rz. 13 zu den weiteren dezentralisierten Systemen.

[27] *FAQ-DWeb*, Antworten zu Frage 6 und 12.

auch das Blockchain-Protokoll auf der Web-Struktur Verwendung finden wird.[28] Im Folgenden werden deshalb zuerst das DWeb (siehe sogleich Rz. 11), das Solid-Protokoll und das Unternehmen Inrupt Inc. (siehe unten Rz. 15) sowie kursorisch die Blockchain dargestellt (siehe unten Rz. 16).

2.3.2 Dezentralisiertes Speicher- und Kontrollsystem

Faktische Datenautonomie:

Autonomie über Speicherort und Zugang zu den eigenen Daten

11 Im DWeb werden verschiedene Web-Komponenten dezentralisiert. Da jedem Datum ein URL zugeteilt wird, wird ein Datum nicht mehr – wie bei den ersten zwei Webgenerationen – aufgrund seines Speicherorts auf einem bestimmten Server identifiziert, sondern aufgrund seines URLs.[29] Anstatt auf einem einzelnen Server (eines GAFA-Unternehmens) können Daten deshalb auf einer Vielzahl von Servern gespeichert werden (dezentralisiertes Speichersystem). Die Speicherung kann sodann auf verschlüsselte Weise erfolgen, sodass nur der Inhaber des privaten Schlüssels auf ***seine*** Daten zugreifen kann. Der Dateninhaber kontrolliert so den Speicherort derjenigen Daten, die er generiert hat, und den Zugriff darauf (faktische Datenautonomie). Damit erlangt er die (ausschliessliche)[30] faktische Herrschaft über seine Daten (zurück).[31]

12 Doch die Server bieten nicht nur Dienste an, sondern können sie wie Clients auch in Anspruch nehmen. Dazu kommt, dass die Clients (z.B. Smartphones) infolge Anreizmechanismen wie Tokens oder Coins gleichzeitig auch als Server fungieren können. Diese Identität von Server und Client führt zu einer Verschiebung vom Client-Server-Modell zum Peer-to-Peer-Modell (P2P-Modell): Das DWeb basiert auf einem Netzwerk von Peers (sog. Nodes), welche direkt miteinander kommunizieren und so die Einflussmöglichkeiten von Intermediären im DWeb einschränken oder gar zerschlagen können (dezentralisiertes Kontrollsystem).[32]

---

[28] *Danielle Robinson*, o.T., in: Press Kit des Decentralized Web Summit 2018, Ziff. 7 (nachfolgend "Press Kit-DWeb").

[29] *Solid*, Linked Data Fundamentals, Introduction to Linked Data, o.J., o.S.

[30] Siehe unten Rz. 93 zum nicht durchsetzbaren Datenzugriff.

[31] *Corbyn*, o.S. sowie *Tom Simonite*, The Decentralized Internet Is Here, With Some Glitches, in: Wired vom 3. Mai 2018, o.S.; vgl. auch *Hans Bechtolf/Niklas Vogt*, in: Datenschutz in der Blockchain – Eine Frage der Technik, Technologische Hürden und konzeptionelle Chancen, ZD 2018, S. 71 mit Verweis auf *Guy Zyskind/Oz Nathan/Alex 'Sandy' Pentland*, Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015, S. 2 ff.

[32] Vgl. zum Ganzen *Marco Alessi/Alessio Camillò/Enza Giangreco et al.*, A Decentralized Personal Data Store based on Ethereum: Towards GDPR Compliance, in: Journal of Communications Software and Systems, 2019, S. 79 ff.

2.3.3 Weitere dezentralisierte Systeme

13 Um mit anderen Nodes kommunizieren zu können, muss sich der User zunächst mit seinem DWeb-Password (Private Key) als Dateninhaber einloggen (dezentralisiertes Loginsystem).[33] Der Inhalt der Transaktion kann sodann eine Zugangsgewährung zu seinen Daten (z.B. Fotos) oder ein Zahlungsfluss von Kryptowährungen (dezentralisiertes Zahlungssystem) sein.[34] Die Kommunikation erfolgt dabei direkt zwischen den Peers. Um eine sichere Kommunikation zu ermöglichen, kann nur der rechtmässige Empfänger die kryptographisch verschlüsselte Kommunikation entschlüsseln (dezentralisiertes Authentifizierungssystem).[35] Transaktionen werden sodann gespeichert bzw. archiviert, sodass auch ältere Versionen des DWebs angefordert werden können (z.B. Abrufen einer gelöschten Website). Dies führt im Hinblick auf die Speicherung der DWeb-Versionen zu einer Ausweitung von der neuesten Version auf alle älteren Versionen (zeitlich dezentralisiertes Versionensystem).[36]

Dezentralisierte Systeme:

- Speichersystem
- Kontrollsystem
- Loginsystem
- Zahlungssystem
- Authentifizierungssystem
- Versionensystem

14 Bezüglich dieser dezentralisierten Systeme hat sich scheinbar ein gewisser Konsens herausgebildet. Allerdings steht die Technologie des DWebs noch am Anfang ihrer Entwicklungsphase, sodass sich der Konsens nicht verhärten und sich deshalb in Zukunft auch noch verändern könnte. Im Folgenden wird vom gegenwertigen Konsens ausgegangen.[37]

2.3.4 Solid und Inrupt Inc.

15 Da zurzeit lediglich die Konturen des DWebs ersichtlich sind, wird sich dieses Sheet besonders auch mit einer seiner möglichen Ausprägungsformen (hinsichtlich der Datenspeicherung) beschäftigen: Solid ist ein von *Berners-Lee* geleitetes Open Source Projekt zur Verwirklichung des DWebs. Inrupt Inc. ist ein von *Berners-Lee* und *John Bruce* geführtes Unternehmen, das die Solid-Technologie auf dem Markt

---

[33] *Barabas/Narula/Zuckerman*, S. 47; *Corbyn*, o.S.; vgl. auch *Solid*, Solid Explained, o.J., o.S. sowie *Solid*, Introduction to the solid specification, o.J., o.S.

[34] *FAQ-DWeb*, Antwort zu Frage 2.

[35] Die Authentifizierung des Empfängers kann etwa durch Public Key Encryption erfolgen. Dabei kommt nur derjenige Node als Empfänger in Betracht, der mit seinem Public Key die Transaktion entschlüsseln kann. Siehe *Jeff Kaplan*, Locking the Web Open: A Call for a Decentralized Web, in: Brewster Kahle's Blog vom 11. August 2015, o.S. m.w.H.

[36] *Klint Finley*, The Inventors of the Internet Are Trying to Build a Truly Permanent Web, in: Wired vom 20. Juni 2016, o.S. (nachfolgend "*Finley*, Permanent Web"); *Hardy*, o.S.; *Brewster Kahle*, o.T., in: Press Kit-DWeb, Ziff. 1 ff.; vgl. auch die heute (nicht umfassend archivierende) Wayback Machine.

[37] Vgl. zum Ganzen *FAQ-DWeb*, Antwort zu Frage 2 sowie *Corbyn*, o.S.

umsetzen soll.[38] Die Abbildung 2 von Inrupt Inc. stellt die wichtigste Neuerung des DWebs, sprich die faktische Datenautonomie, bildlich dar. Dabei werden die eigenen Daten in einem "**P**ersonal **O**nline **D**ata (Store)" (POD) auf dem P2P-Netzwerk gespeichert; wohlgemerkt nicht in einer Blockchain.[39] "Solid empowers users and organizations to separate their data from the applications that use it. It allows people to look at the same data with different apps at the same time."[40] Und "Think of your Solid POD as your own private website, except that your data interoperates with all your apps."[41] Der Dateninhaber kann so Apps oder Personen den Zugang zu seinen Daten gewähren – oder auch nicht.[42] Da damit das dezentralisierte Speichersystem (etwa in Gestalt von Solid) eine zentrale Sammlung und Verwaltung der Daten ermöglicht, kann es als eine Ausprägungsform der Personal Information Management Systems (PIMS) angesehen werden.[43] Das DWeb geht als ganzes Ökosystem allerdings weit über diese üblichen Aufgaben einer PIMS hinaus.

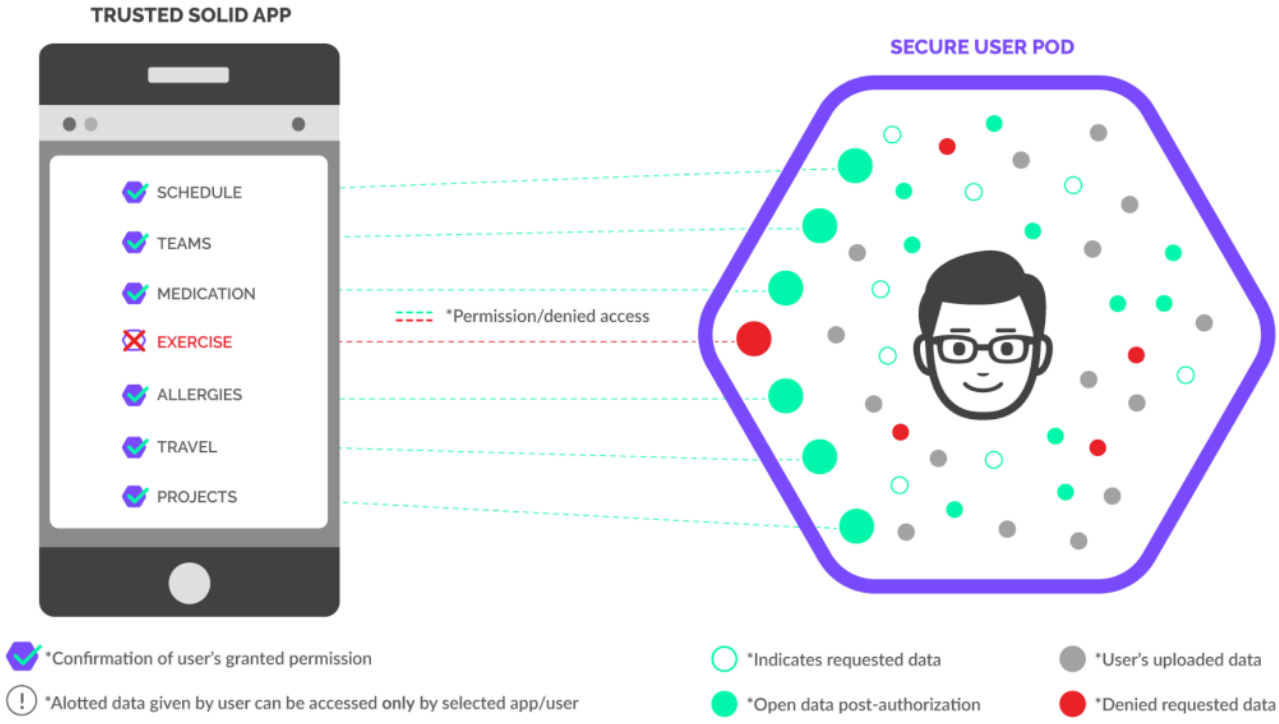

Abbildung 2: "Trusted Solid App" und Datenzugang zum "POD"

---

[38] *K.G Orphanides*, How Tim Berners-Lee's Inrupt project plans to fix the web, in: Wired vom 15. Februar 2019, o.S. m.w.H.

[39] *Ruben Verborgh*, Paradigm shifts for the decentralized Web, in: Ruben Verborgh (Blog) vom 20. Dezember 2017, o.S.; *Shermin Voshmgir*, Blockchains, Smart Contracts und das Dezentrale Web, Berlin 2016, S. 10 f.

[40] *Solid*, This is for everyone, o.J., o.S.

[41] *Solid*, Solid Explained, o.J., o.S.

[42] *Solid*, Solid Explained, o.J., o.S.; *Verborgh*, o.S.; *Barabas/Narula/Zuckerman*, S. 69 ff.; vgl. auch *Berkman Klein Center for Internet & Society at Harvard University*, o.S.

[43] Vgl. *Rolf H. Weber/Florent Thouvenin*, Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS), S. 7 (zuletzt besucht: 16. Januar 2021).

2.3.5 Blockchain-Technologien

16 Die Blockchain-Technologien sind ein Unterfall der DLT, die sich dadurch auszeichnen, dass die Transaktionsdaten in Blöcken ("Block") gespeichert werden. Dabei beinhaltet jeder Block typischerweise drei Grundinformationen: die soeben erwähnten Transaktionsdaten, einen Zeitstempel sowie den Hashwert des zeitlich vorangehenden Blocks (sog. digitaler Fingerabdruck). Daraus ergibt sich eine chronologische Kette ("Chain") von durch Hashwerte verbundenen Blöcken. Die Hashwerte werden von Nodes (Minern) errechnet, da sie eine Belohnung wie Tokens oder Coins (z.B. Bitcoins) erhalten.[44]

2.4 Zwischenfazit

17 Nach der Dezentralisierung des Zugriffs (Web 1.0) und der Produktion (Web 2.0) der Daten setzt mit dem DWeb primär eine Dezentralisierung ihres Speicherorts ein (Web 3.0). Dadurch könnten die für die Webuser negativen Auswirkungen der Zentralisierung, die mit dem Web 2.0 eingesetzt haben, beschränkt oder gar beseitigt werden. Konkrete Technologien dazu sind beispielsweise Solid und die Blockchain.

[44] Vgl. zum Ganzen *Albert Schlund/Hans Pongratz*, Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung, in: DStR 2018, S. 598 f. sowie *Joachim Schrey/Thomas Thalhofer*, Rechtliche Aspekte der Blockchain, in: NJW 2017, S. 1431 f.; vgl. auch *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 1 ff.

3 Regulierung des DWebs

18 Von der Frage, mit welcher Technik dem Handeln der Webgiganten im Web Einhalt geboten werden kann, ist nun zu den Fragen überzugehen, ob (siehe sogleich Rz. 19) und wie (siehe unten Rz. 21) das DWeb zu regulieren ist.

3.1 *Ist* das DWeb zu regulieren?

19 Die Beantwortung der Frage "Ist das DWeb zu regulieren?" setzt voraus, dass das DWeb überhaupt *rechtlich* regulierbar[45] ist. Dagegen scheint besonders die Unabhängigkeitserklärung des Cyberspace von 1996 zu sprechen: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. […] You have no sovereignty where we gather. […] You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."[46] Doch diese (naive) Auffassung der Digital Libertarians gilt heute als weitestgehend überholt. Der Cyberspace ist – mitsamt dem Web – *regulierbar*.[47]

20 Dies entspricht auch der überwiegenden Meinung der Teilnehmer des Decentralized Web Summit 2018: "It's our belief that technology alone cannot change society; it takes laws, policies, market forces, and the right set of values to make meaningful change. So we are convening people from many sectors to consider how to build the Web we want, and the Web we deserve."[48]

3.2 *Wie* ist das DWeb zu regulieren?

3.2.1 Pathetic Dot Theory

21 Wie der DWeb Summit erläutert hat, sind neben der Technologie weitere Elemente für einen gesellschaftlichen Wandel erforderlich (siehe soeben Rz. 20). Ähnliches beschreibt die sog. Pathetic Dot Theory von *Lawrence Lessig*, mit der die Verhaltenssteuerung einer Person ("Pathetic Dot") mittels vier Kräften beschrieben wird: soziale Normen, Architektur (z.B. Hard- und Software), Markt und Recht.[49] Die Schwerpunktsetzung dieses Sheets liegt auf dem Recht sowie der Hard- und

---

[45] Im Folgenden bezeichnet der Begriff "Regulierung" eine *rechtliche* Regulierung soweit nichts anderes angegeben wird.

[46] *John Perry Barlow*, A Declaration of the Independence of Cyberspace, 8. Februar 1996, o.S. Interessant ist auch anzumerken, dass *Barlow* 1996 primär in den Regierungen eine Gefahr für den Cyberspace sah, während heute eine Unabhängigkeitserklärung auch an die Internetgiganten adressiert werden müsste. Dies verdeutlicht die weitreichenden Auswirkungen der Transition vom Web 1.0 zum Web 2.0 (siehe auch oben Rz. 8).

[47] *Primavera De Filippi/Samer Hassan*, Blockchain Technology as a Regulatory Technology, From Code is Law to Law is Code, in: First Monday, Volume 21, Number 12 - 5. Dezember 2016, o.S.

[48] *FAQ-DWeb*, Antwort zu Frage 4; siehe auch *Kahle*, in: Press Kit-DWeb, Ziff. 1.

[49] *Lawrence Lessig*, CODE version 2.0, 2. Aufl., New York 2006, S. 123; für einen kurzen Überblick siehe auch "iLaw 2004: Lawrence Lessig on Regulation".

Software.[50] Nun kommen im Bereich des DWebs als zu regulierende Pathetic Dots die Nutzer und Entwickler des DWebs bzw. der DApps in Betracht.

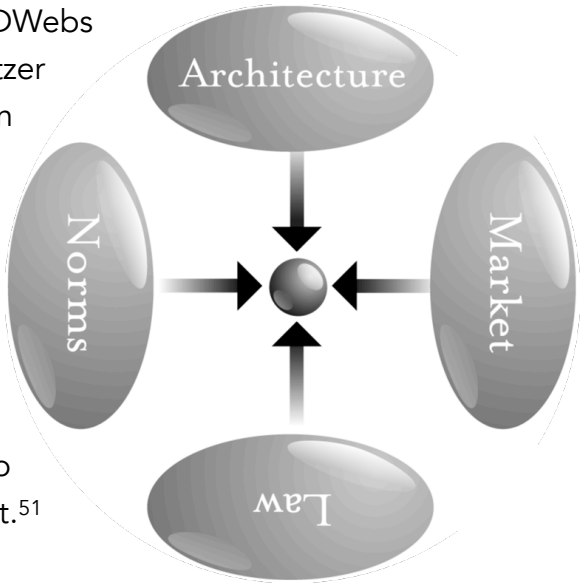

Abbildung 3: Auf einen Pathetic Dot einwirkende Kräfte

22 Greift die regulierende Hand des Staates über die Entwickler in den Cyberspace ein, so reguliert er damit das Verhalten der Entwickler, indem er sie zur technischen Umsetzung rechtlicher Normen verpflichtet oder sie dabei unterstützt. Zudem wird so auch das Verhalten der Nutzer reguliert.[51] *Lessig* spricht in diesem Zusammenhang prägnant von "Code is Law". Damit meint er allerdings nicht, dass der Programmcode zu einer Rechtsvorschrift oder der Programmierer gar zu einem Gesetzgeber wird.[52] Vielmehr versteht er unter "Code" diejenige Architektur der Hard- und Software, die im Cyberspace das Verhalten der Pathetic Dots faktisch reguliert.[53] Wird aber Recht in Code überführt, so ist die Bezeichnung "Law is Code" geläufig.[54] Ein prominentes Beispiel für Letzteres ist das Digital Rights Management zum Urheberrechtsschutz, das eine urheberrechtswidrige Verhaltensweise durch technische Massnahmen unterbinden soll.[55]

3.2.2 Problematik der Durchsetzbarkeit

23 Problematisch bei der Regulierung des DWebs ist jedoch, dass sie einen Adressaten (Nutzer oder Entwickler) voraussetzt, der zum rechtmässigen Verhalten gezwungen werden kann. Dies setzt wiederum voraus, dass der Staat die Identität des Adressaten kennt und er im Falle der Zuwiderhandlung Zwangsmassnahmen durchsetzen kann.[56] Allerdings kann die Identität eines Nutzers oder Entwicklers auch anonym sein. Dies verdeutlicht etwa das Tor-Netzwerk oder der Bitcoin-Erfinder "Satoshi Nakamoto",

---

[50] *Lessig*, S. 120 ff. m.w.H. zu den übrigen Kräften; siehe auch *Bart Jansen*, Towards a Hermeneutics of Pathetic Dots: Finding the Gap Between Law and Reality, in: Yuridika, Volume 34 No. 3, September 2019, S. 421 ff. m.w.H.

[51] Vgl. *Köndgen*, Privatisierung des Rechts: Private Governance zwischen Deregulierung und Rekonstitutionalisierung, in: Archiv für die civilistische Praxis, 206. Bd., H. 2/3 (2006), S. 502 f.

[52] *Felix Gantner*, «Code Is Law» aber «Is Law Code»?, in: Jusletter IT 22. Februar 2018, Rz. 2, 6 f.

[53] *Lessig*, S. 5 ff.; siehe auch *Gantner*, Rz. 1 ff.

[54] *De Filippi/Hassan*, o.S.; *Gantner*, Rz. 37.

[55] *De Filippi/Hassan*, o.S. m.w.H.; siehe eingehend unten Rz. 36 zum Digital Rights Management.

[56] Vgl. *Harbinja/Karagiannopoulos*, o.S. sowie *Köndgen*, S. 503.

dessen Identität seit 2008 unbekannt ist.[57] Zudem können die Adressaten dermassen entwurzelt agieren, dass sie sich der Zwangsgewalt eines Staates entziehen.[58] Dadurch könnte besonders die strafrechtliche Verfolgung von Cyberkriminalität erschwert werden.[59] Schliesslich kann der Staat die Zwangsmassnahmen nicht durchsetzen, weshalb sie ihre abschreckende Wirkung auf die Adressaten verlieren. Insofern kommt dem Recht seine regulatorische Kraft abhanden.[60]

3.3 Zwischenfazit

24 Während die Frage nach dem "ob" der Regulierung des DWebs klar bejaht werden muss, wird die Frage nach dem "wie" mit der Pathetic Dot Theory beantwortet. Demgemäss wird das Verhalten der Entwickler und Nutzer mittels vier Kräften reguliert, wobei in diesem Sheet der Code und das Recht von wichtiger Bedeutung sein werden. Als besonderer Problempunkt hat sich herausgestellt, dass das Recht im Cyberspace infolge der anonymen oder entwurzelten Adressaten nur schwer durchsetzbar ist.

---

[57] Siehe *FAQ von bitcoin.org*, Antwort zu Frage 2 "Wer hat Bitcoin erfunden?": "[…] Genau wie bei gegenwärtigen Entwicklern, war Satoshis Einfluss auf jene Veränderungen begrenzt, die von anderen angenommen wurden und demzufolge kontrollierte er Bitcoin nicht. Deshalb ist die Identität des Erfinders von Bitcoin mittlerweile wahrscheinlich so relevant wie die Identität der Person, die das Papier erfunden hat."Das Beispiel von *Nakamoto* sollte eigentlich nur verdeutlichen, dass eine langjährige Anonymität eines Entwicklers durchaus möglich ist. Doch die hier abgedruckte Antwort eröffnet auch einen Blick auf die Schwierigkeiten der Verantwortungszuweisung zu einer bestimmten Person(-engruppe), die sich in einem dynamischen Personengeflecht (anonymer) Entwickler befindet.

[58] *Köndgen*, S. 503.

[59] *Harbinja/Karagiannopoulos*, o.S.; ein Beispiel eines (nahezu) rechtsfreien Raums ist das Darkweb mit einer entsprechend hohen Kriminalitätsrate.

[60] Vgl. *Lessig*, S. 124.

4 Das Wettbewerbsrecht

25 Dieses Kapitel führt in die möglichen wettbewerbsrechtlichen Grundsatzfragen ein, die sich im Bereich des DWebs ergeben könnten. Denn um die Wirkungen einer Technologie verstehen zu können, muss zuerst der Kontext, in der sie gehandelt wird, verstanden werden. Zuerst soll deshalb das Verhältnis zwischen dem aktuellen Web und dem DWeb beleuchtet werden (siehe sogleich Rz. 26), um sodann zum Privacy Paradox überzugehen (siehe unten Rz. 28). Schliesslich werden die Möglichkeit einer Re-Zentralisierung des Webs (siehe unten Rz. 31) sowie altbekannte, spezifischere Blockchain-Problematiken behandelt, die auch im Kontext des DWebs auftreten könnten (siehe unten Rz. 32).

4.1 (D)Web und (D)Apps

26 Es fragt sich, wie das Wettbewerbsverhältnis zwischen dem DWeb und dem aktuellen Web auf lange Sicht ausfallen wird. Gemäss dem Decentralized Web Summit 2018 sind drei Fallkonstellationen denkbar: Das DWeb wird integriert, steht neben oder ersetzt das aktuelle Web.[61] Es gilt also abzuwarten, welche Fallkonstellation die Bedürfnisse der Verbraucher besser wird bedienen können.[62]

27 Weiter ist fraglich, ob nach den (auf dem DWeb laufenden) DApps überhaupt eine Nachfrage seitens der Marktgegenseite bestehen würde. Bereits der Umstand, dass schon heute (auf dem aktuellen Web laufende) DApps auf dem Markt angeboten werden, indiziert nicht nur das allgemein fehlende Vertrauen in die Webgiganten und den Wunsch nach einer vergrösserten Datenautonomie, sondern auch eine gewisse Offenheit gegenüber dezentralisierten Technologien wie dem DWeb und den DApps.[63] Allerdings spiegelt der Wunsch nach mehr Privatsphäre nicht immer das Verhalten der Verbraucher wieder.

4.2 Privacy Paradox

28 Der Unterschied zwischen einer zentralisierten App (z.B. YouTube) und einer *de*zentralisierten App (z.B. DTube) liegt nicht nur in ihrer begriffsimmanenten (De-)Zentralität, sondern auch in einer Vielzahl daran anknüpfender Punkte. Als wohl bedeutendster Nachteil des DWebs gegenüber dem heutigen Web ist infolge der grösseren Datenautonomie – paradoxerweise – die geringere Monetarisierung der Nutzerdaten zu nennen.[64] Denn anstatt mit Daten zu bezahlen

---

[61] *FAQ-DWeb*, Antwort zu Frage 10; vgl. auch *FAQ-DWeb*, Antwort zu Frage 8.

[62] Vgl. *Corbyn*, o.S.; siehe aber auch unten Rz. 114 zur Fragmentierung des Internets.

[63] *Barabas/Narula/Zuckerman*, S. 28; vgl. auch die *FAQ von Inrupt Inc.*, Antwort zu Frage 3.

[64] Vgl. *FAQ-DWeb*, Antwort zu Frage 13.

("gratis") müssen im DWeb Micropayments in Kryptowährungen geleistet werden, um den Zugang zu Content wie Musikstücken oder Zeitungsartikeln erhalten zu können.[65]

29 In diesen Kontext der Monetarisierung ist nun das sog. Privacy Paradox zu setzen, sprich der "Widerspruch zwischen sorglosem Verhalten und Sorgen über mangelnde Privatsphäre"[66]. Auch wenn der Datenschutz für viele Verbraucher an Wichtigkeit gewonnen hat und damit zu einem bedeutenden Wettbewerbsfaktor geworden ist,[67] so gefährden die Verbraucher – selbst bei einem geringen Vorteil wie einem Rabatt – ihre Privatsphäre durch das Offenlegen ihrer Daten im Web.[68] Um jedoch den Schritt vom aktuellen Web zum DWeb gehen zu können, bedarf es nicht nur der Technologie des DWebs, sondern auch der Aufklärung und Sensibilisierung der Gesellschaft hinsichtlich der Wichtigkeit des Datenschutzes und – überhaupt – der Datenautonomie. **"A tipping point could be reached where people will realize ‚that data belongs to me'"**.[69] Denn letztlich ist der Aufstieg der Webgiganten kein technologisches sondern ein soziales Problem,[70] das mit der technischen Lösung des DWebs nur dann beseitigt werden kann, wenn sie auf die soziale Lösung des gesellschaftlichen Wandels trifft.[71]

30 Doch auch die Vorteile des DWebs, welche besonders die Benutzerfreundlichkeit ansprechen, könnten den Verbrauchern zu diesem Schritt Anreize bieten. So etwa der unwahrscheinlichere Datenverlust mangels eines sog. Single Point of Failure, ein praktischeres Login-System, Verdienen von Coins für das Speichern fremder Daten sowie die sichere, direkte Zahlung zwischen Peers.[72] Doch auch wenn das DWeb in einem ersten Schritt von den Verbrauchern bevorzugt werden sollte, könnte es sich in einem zweiten Schritt immer noch re-zentralisieren.

---

[65] *Corbyn*, o.S.; siehe aber auch die Möglichkeit zur Monetarisierung der Daten im Kontext der PIMS: *Weber/Thouvenin*, S. 16.

[66] *Barbara Engels/Mara Grunewald*, Das Privacy Paradox: Digitalisierung versus Privatsphäre, in: IW Kurzberichte 57. 2017, o.S.

[67] Vgl. *Torsten Körber*, „Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht – Teil 2, in: NZKart 2016, S. 349.

[68] *Engels/Grunewald*, o.S. m.w.H.

[69] *Klint Finley*, Tim Berners-Lee, Inventor of the Web, Plots a Radical Overhaul of His Creation, in: Wired vom 4. April 2017, o.S. (Zitat von *Berners-Lee*).

[70] *Hardy*, o.S. (Zitat von *Berners-Lee*).

[71] Anderer Ansicht eher *Hardy*, o.S.

[72] Vgl. *FAQ-DWeb*, Antwort zu Frage 1 und 2; vgl. auch *Corbyn*, o.S.

4.3 Re-Zentralisierung des Webs

31 Trotz der dezentralisierten Struktur ist auch im DWeb eine erneute Machtkonsolidierung möglich.[73] Denn auch eine technisch dezentralisierte Technologie wie das DWeb kann durch Zentralisten in eine politisch zentralisierte Technologie überführt werden und möglicherweise auch zu wettbewerbswidrigen Zwecken genutzt werden.[74] Ein paradigmatisches Beispiel für eine politische Zentralisierung lässt sich in der ersten Webgeneration finden, da sie von Anfang an technisch dezentral konzipiert war, dann aber mit den Webgiganten eine politische Zentralisierung erfahren hat.[75] Als weiteres Beispiel ist die Bitcoin-Blockchain zu nennen: Zwar ist sie als öffentliche Blockchain technisch dezentral in Miners organisiert, doch hat sie sich in dem Sinne zentralisiert, als dass sich ein Grossteil der Rechenleistung des Bitcoin-Netzwerks (Hashrate) unter wenigen, grossen Mining-Pools verteilt hat.[76] Abgesehen von diesen allgemeinen Ausführungen sind aber auch spezifische (Blockchain-)Problemfälle denkbar.

4.4 Spezifische (Blockchain-)Problemfälle

32 Bereits heute sind spezifische, wettbewerbsrechtliche Problemfälle im Kontext der Blockchain anzutreffen: So etwa der Gebrauch von Smart Contracts in (privaten[77]) Blockchains zur Einhaltung wettbewerbsbeschränkender Vereinbarungen (Art. 101 AEUV),[78] der Missbrauch der marktbeherrschenden Stellung bei einer Gatekeeper-Stellung in (privaten) Blockchains (Art. 102 AEUV)[79] oder die Beurteilung einer Blockchain als ein (materiell) beteiligtes Unternehmen an einem Zusammenschluss (Art. 3 FKVO)[80].

---

[73] *Corbyn*, o.S.; *Harbinja/Karagiannopoulos*, o.S.; *Juan Ortiz Freuler/Rosemary Leith*, Three reflections regarding the re-decentralization of the web, in: Medium vom 3. Juli 2019, o.S.

[74] *Vitalik Buterin*, The Meaning of Decentralization, in: Medium vom 6. Februar 2017, o.S.; *Freuler/Leith*, o.S.; siehe dazu auch die graphische Darstellung der technischen, politischen und logischen (De-)Zentralisierung.

[75] *Barabas/Narula/Zuckerman*, S. 8 ff.; vgl. *Hardy*, o.S.

[76] *blockchain.com*, Hashrate Verteilung, Eine Abschätzung der Hashrate-Verteilung unter den größten Mining-Pools., o.J., o.S.

[77] Zum Unterschied zwischen der öffentlichen und der privaten Blockchain siehe *Peter Preuss*, Blockchain-Technologie – Funktionsweise und ausgewählte Anwendungsbeispiele in der Finanzindustrie, in: Marcel Seidel (Hrsg.), Banking & Innovation 2018/2019, Ideen und Erfolgskonzepte von Experten für die Praxis. Mit Sonderteil China, Wiesbaden 2019, S. 76 ff.

[78] *Raoul Hoffer/Kristina Mirtchev*, Erfordert die Blockchain ein neues Kartellrecht?, in: NZKart 2019, S. 242 m.w.H.; *Giovanna Massarotto*, From Digital to Blockchain Markets: What Role for Antitrust and Regulation, 26. Januar 2019, S. 14 ff. m.w.H.

[79] *Hoffer/Mirtchev*, S. 243 ff. m.w.H.; *Thibault Schrepel*, Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox, in: Georgetown Law Technology Review / 3 Geo. L. Tech. Rev. 281 (2019), S. 302 ff. m.w.H.

[80] *Hoffer/Mirtchev*, S. 246 m.w.H.

33 Es treten damit besonders bei privaten Blockchains wettbewerbsrechtliche Problematiken auf, da sich die faktische Kontrolle über die Blockchain weitestgehend bei einem Wettbewerber (oder im Falle einer Consortium Blockchain bei wenigen koordinierten Wettbewerbern) konzentriert.[81] So wird ihnen die Möglichkeit einer wettbewerbswidrigen Nutzung "ihrer" Blockchain eröffnet. Es muss aber unterstrichen werden, dass die blosse Kontrolle einer Blockchain noch kein wettbewerbswidriges Verhalten darstellt, denn dazu bedarf es eines qualifizierenden Umstands wie eines erfüllten Missbrauchstatbestands.[82]

4.5 Zwischenfazit

34 Das aktuelle Web und das DWeb stehen in einem Wettbewerbsverhältnis zueinander. Zurzeit besteht zwar eine (Nischen-)Nachfrage nach dezentralisierter Technologie, allerdings ist fraglich, ob und wie das Privacy Paradox in diesem Kontext überwunden werden kann. Denn die Zentralisierung des aktuellen Webs ist ein soziales Problem. Aus diesem Grund kann auch wieder eine politische Zentralisierung des (D)Webs erfolgen. Spezifischere, wettbewerbsrechtliche Problematiken sind sodann im Bereich der (privaten) Blockchain bereits heute anzutreffen und könnten sich mit dem DWeb weiter fortsetzen.

---

[81] *Hoffer/Mirtchev*, S. 241, 243 und 245.

[82] *Hoffer/Mirtchev*, S. 244.

5 Das Urheberrecht

35 Da im Web neben dem Datenschutzrecht auch dem Urheberrecht eine grosse Bedeutung zukommt, soll es der Vollständigkeit halber in diesem Sheet auch behandelt werden. Entsprechend befasst sich dieses Kapitel nur kursorisch mit den Grundsatzfragen des Urheberrechts, die sich im Rahmen des Digital Rights Managements (siehe sogleich Rz. 36), der Smart Contracts (siehe unten Rz. 40) sowie der Datenautonomie (siehe unten Rz. 43) ergeben könnten.

5.1 Digital Rights Management

5.1.1 Begriff

36 Zur Durchsetzung des Urheberrechts kommt im (D)Web das Digital Rights Management (oder auch "DRM" und "digitale Rechteverwaltung") in Betracht. Mittels technischer Sicherheitsmassnahmen schränkt es im digitalen Bereich den Zugang und die Nutzung von urheberrechtlich geschützten Werken auf das lizenzvertraglich vereinbarte Mass ein, sodass eine Verletzung des Urheberrechts technisch verunmöglicht wird.[83] Die Durchsetzung des Urheberrechts erfolgt insofern auf technische Art und Weise. Jedoch kann der Programmcode des DRM auch durch andere Programmcodes umgangen werden, sodass die Durchsetzung letztlich wieder auf den Staat zurückfällt.[84]

5.1.2 Anonymität, Zensur und endgültige Löschung

37 Im Kontext des DWebs sind der Urheberrechtsdurchsetzung besonders die Anonymität der Urheberrechtsverletzer hinderlich.[85] Sodann kommt hinzu, dass das DWeb die Möglichkeit (staatlicher) Zensur, etwa eines im DWeb veröffentlichten Plagiats, gerade einschränken oder gar verunmöglichen will.[86] Und zuletzt kann in einem dezentralisierten Speichersystem auch das endgültige Löschen, etwa des Plagiats, von allen Peers problematisch sein.[87]

---

[83] *Lessig*, S. 116 f.; *Tassilo Pellegrini*, Digital Rights Management - Technologien, Anwendungsbereiche und Entwicklungsperspektiven, in: Jan Krone/Tassilo Pellegrini (Hrsg.), Handbuch Medienökonomie, Wiesbaden 2016, S. 2.

[84] *Pellegrini*, S. 2 f.; siehe auch *Simonite*, o.S. zum DRM in DTube: "It's a clever design but one that illustrates how decentralized systems might face legal and governance problems. Some parts of the IPFS network support copyright takedowns, but they can be worked around."

[85] *Vogel*, S. 146 ff.

[86] *Verborgh*, o.S.; vgl. *Vogel*, S. 141; siehe auch unten Rz. 98 zur Zuweisung der Zensurpflicht.

[87] *FAQ-DWeb*, Antwort zu Frage 12; *Corbyn*, o.S.

5.1.3 Digitale Rechte*minderung*

38 Bereits in den 1990er-Jahren wurde kritisiert, dass für die digitale Rechteverwaltung die Bezeichnung digitale Rechte*minderung* zutreffender sei. Die unflexiblen, technischen Schutzmassnahmen verunmöglichen neben Urheberrechtsverletzungen auch rechtlich zulässige Nutzungshandlungen wie die Nutzung zu privaten, schulischen oder parodistischen Zwecken.[88] Auch wenn diese Kritik infolge toleranterer DRM zurzeit an Bedeutung verloren hat,[89] zeigt sie dennoch die Auswirkungen einer Technologie auf, die urheberrechtlichen Schrankenbestimmungen nicht gerecht werden kann und so ein Spannungsverhältnis zwischen Urheberrecht und Code schafft. Doch diese Problematik des allzu starren DRM lässt sich besonders mit den Smart Contracts – vorausgesetzt, sie lassen sich überhaupt auf der DWeb-Architektur aufsetzen – sowie mit der Datenautonomie entschärfen.

5.1.4 Zwischenfazit

39 Das DRM ermöglicht eine automatisierte Durchsetzung des Urheberrechts im (D)Web. Problematisch könnten im DWeb allerdings die Anonymität, die Zensur und das endgültige Löschen werden. Zuletzt könnte der digitalen Rechteminderung aber mit der Flexibilität der Smart Contracts und Datenautonomie begegnet werden.

5.2 Smart Contracts

40 Smart Contracts sind auf einer Blockchain laufende Protokolle, welche beim Auftreten eines zuvor festgelegten Ereignisses eine zuvor festgelegte Aktion ausführen und so die Vertragsabwicklung automatisieren.[90] Gegenstand eines Smart Contracts ist etwa eine Lizenz an einem urheberrechtlich geschützten Werk.[91] Da eine Vielzahl an Wenn-Dann-Logiken programmiert werden kann, erweisen sich Smart Contracts tendenziell flexibler als die klassischen DRM.[92] Doch auch hier ergeben sich verschiedene Problematiken.

41 Das Problem des anonymen Urheberrechts- bzw. Vertragverletzers spielt zwar auch im Bereich der Smart Contracts mit, doch verliert es hier erheblich an Bedeutung, wenn der Smart Contract bereits die Folgen der Pflichtverletzung regelt und sie auch selbst

---

[88] *De Filippi/Hassan*, o.S.; *Pellegrini*, S. 2.

[89] *Pellegrini*, S. 2.

[90] *Robert Wilkens/Richard Falk*, Smart Contracts, Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden 2019, S. 3 f.

[91] *Nicolas Hohn-Hein/Günter Barth*, Immaterialgüterrechte in der Welt von Blockchain und Smart Contract, in: GRUR 2018, S. 1093.

[92] Vgl. auch *Zhaofeng Ma/Ming Jiang/Hongmin Gao/Zhen Wang*, Blockchain for digital rights management, in: Future Generation Computer Systems 89 (2018), S. 746 ff. zum blockchainbasierten "paradigm of the DRM for content protection".

vollziehen kann.[93] Insofern braucht der Verletzer weder für den Staat noch für den Vertragspartner identifizierbar zu sein; es genügt die Identifizierbarkeit gegenüber dem Smart Contract bzw. den darunter liegenden dezentralisierten Systemen. Sollen allerdings die Folgen der Pflichtverletzung ausserhalb des Smart Contracts vollzogen werden, bestehen die oben angesprochenen Probleme der Anonymität, der Zensur und des dezentralisierten Speichersystems indes weiter (siehe oben Rz. 37). Darüberhinaus ergeben sich weitere Problemfelder.

42 So können nicht alle lizenzvertraglich relevanten Umstände, besonders unbestimmte Rechtsbegriffe wie Werkänderung oder -verwendung,[94] in einen Programmcode überführt werden.[95] Im Übrigen kann ein Fall der fehlerhaften Softwaregestaltung vorliegen.[96] Auch in diesen beiden letzten Konstellationen erweist sich als problematisch, dass der Smart Contract das Problem nicht selbst lösen kann, sondern Hilfe "von aussen" durch den Menschen bedarf. Als Lösung wird in der Literatur etwa der Einsatz von programmierten Schiedsstellen diskutiert,[97] sprich einer "Streitbeilegung unter ausschliesslicher bzw. unterstützender Verwendung von Software"[98]. Dies erscheint im Hinblick auf einen Artikel der Zeitschrift Sciencemag mit dem Titel "Artificial intelligence prevails at predicting Supreme Court decisions"[99] zumindest ein interessanter Lösungsansatz, ist der Schritt vom Vorhersagen zum Urteilen doch nicht gross.

5.3 Nicht-automatisierte Datenautonomie

43 Im DWeb gewährt die Datenautonomie dem Dateninhaber die faktische Autonomie über die Speicher- und Zugangsmodalitäten zu seinen Daten (siehe oben Rz. 11). Somit kann ein Urheber als Dateninhaber im Rahmen der Datenautonomie über seine Werke als Daten verfügen, beispielsweise indem er die Werkexemplare einem Lizenznehmer zugänglich macht. Neben dem Verwenden eines Smart Contracts (siehe oben Rz. 40) kann der Urheber in jedem Einzelfall auch manuell (d.h. nicht-automatisiert) entscheiden, ob und in welchem Ausmass eine Person Zugang zu seinen Werkexemplaren erhalten soll. Im Vergleich zu den klassischen DRM und Smart Contracts besteht insofern eine weitergehende, wenn auch mangels

---

[93] *Hohn-Hein/Barth*, S. 1093; *Schawe*, S. 220 f.

[94] *Sandra Brändli*, Die Flexibilität urheberrechtlicher Schrankensysteme, Eine rechtsvergleichende Untersuchung am Beispiel digitaler Herausforderungen, Bern 2017, S. 45.

[95] *Hohn-Hein/Barth*, S. 1093.

[96] *Hohn-Hein/Barth*, S. 1095; *Schawe*, S. 221.

[97] So etwa *Eduard Hofert*, Regulierung der Blockchains: Hoheitliche Steuerung der Netzwerke im Zahlungskontext, Tübingen 2018, S. 35 ff. sowie *Schawe*, S. 222.

[98] *Schawe*, S. 222.

[99] *Matthew Hutson*, Artificial intelligence prevails at predicting Supreme Court decisions, in: Sciencemag vom 2. Mai 2017, o.S. m.w.H.

Automatisierung umständlichere, Flexibilität. Da sich die Problematiken der Anonymität, Zensur und vollständigen Löschung überhaupt erst aufgrund der DWeb-Architektur ergeben, wird auf die entsprechenden Ausführungen zu den Smart Contract bzw. zum DRM verwiesen (siehe oben Rz. 37).

44 Die Datenautonomie strahlt jedoch nicht nur auf die Stellung der Dateninhaber sondern auch auf diejenige der Intermediäre aus. Denn besonders das dezentralisierte Speicher- und Zahlungssystem schränken den Einfluss von Intermediären auf den Urheber ein. Demgemäss wird angenommen, dass das DWeb der Unabhängigkeit der Künstler von Intermediären wie Plattenfirmen oder Verlagen förderlich sein kann.[100] Das urheberrechtliche Ausschliesslichkeitsrecht bzw. die Autonomie, die einem Urheber *rechtlich* zusteht, wird durch die *faktische* Datenautonomie unterstützt und ergänzt.

5.4 Zwischenfazit

45 Die drei Konstellationen der klassischen DRM, der Smart Contracts sowie der nicht-automatisierten Datenautonomie weisen die Grundprobleme der Anonymität, Zensur und vollständigen Löschung auf, da sie auf dem gemeinsamen Nenner des DWebs basieren. Daneben ergeben sich spezifische Problempunkte, etwa die unvollständige oder fehlerhafte Programmierung eines Smart Contracts. Allerdings nimmt die Flexibilität der Technologie zur Durchsetzung des Urheberrechts vom klassischen DRM über die Smart Contracts bis hin zur nicht-automatisierten Datenautonomie tendenziell zu. Infolgedessen kann die Urheberrechtsdurchsetzung technisch gesehen rechtskonformer ausgestaltet werden, sodass sich das Spannungsverhältnis zwischen Urheberrecht und Code auf ein Komplementaritätsverhältnis zubewegen könnte.

[100] Vgl. *Corbyn*, o.S.; so schon *Hohn-Hein/Barth*, S. 1093.

6 Das Datenschutzrecht

46 Die folgenden Ausführungen befassen sich mit den Auswirkungen des DWebs auf die europäische Datenschutz-Grundverordnung (DSGVO[101]). Nach den allgemeinen Überlegungen zum Verhältnis zwischen DWeb und Datenschutzrecht (Rz. 47 bis Rz. 61) wird auf ausgewählte Artikel der DSGVO eingegangen (Rz. 62 bis Rz. 117). Die Ausführungen werden aufzeigen, dass aufgrund des DWebs ein Paradigmenwechsel im Datenschutzrecht stattfinden kann.

6.1 Code und Recht

6.1.1 Code als Ursprung der Datenautonomie

47 *~ [Solid is] the platform that turns the privacy world upside down – or, should I say, right side up.*[102] ~

48 Die betroffene Person hat mit den Betroffenenrechten (Art. 12 ff. DSGVO) zwar eine gewisse Vergrösserung ihrer rechtlichen Autonomiesphäre über Daten, die sich auf ihre Person beziehen, erhalten. Angesichts der Datenmissbräuche, die aufgrund der jetzigen Web-Architektur in Verbindung mit dem sorglosen Verhalten der Nutzer überhaupt erst auftreten konnten, kann selbst nach der strengen Reform des Datenschutzrechts durch die DSGVO aber kaum von einem effektiven Datenschutz oder gar von einem "Dateninhaber" und "seinen" Daten gesprochen werden. Zwar gewährt die DSGVO der betroffenen Person weitergehende Rechte, doch trägt die Architektur des heutigen Webs bzw. die darauf aufbauenden Dienste der Verantwortlichen vergleichsweise wenig zur Verwirklichung des Privacy by Design (Art. 25 Abs. 1 DSGVO) und des Privacy by Default (Art. 25 Abs. 2 DSGVO) bei. Doch gerade das Privacy by Design ist von grundlegender Bedeutung für die Gewährung einer weitreichenden Datenautonomie zum Dateninhaber.[103] Es besteht so ein Spannungsverhältnis zwischen dem aktuellen Web, das Datenmissbräuche technisch ermöglicht, und dem Datenschutzrecht.

49 Das DWeb könnte nun einen entscheidenden Beitrag zum Datenschutz leisten: "Solid essentially solves today's privacy conundrum, more effectively than any single piece of legislation can hope. It's putting data back into the hands of users, not service

---

[101] 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 (Datenschutz-Grundverordnung), ABl. L 119 vom 4. Mai 2016, S. 1 ff.

[102] *Inrupt Inc.*, Turning the Privacy World "Right Side Up", 12. Dezember 2018, o.S. (Zitat von *Berners-Lee*) (nachfolgend "Inrupt-Privacy World").

[103] *Schawe*, S. 221; vgl. *Norbert Nolte/Christoph Werkmeister*, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, VO (EU) 2016/679: Kommentar, 2. Aufl., München 2018, Art. 25 N 2.

providers."[104] Im DWeb kommt damit nicht dem Recht sondern dem Code eine starke regulatorische Kraft im Hinblick auf die Gewährung der Datenautonomie zu.[105]

6.1.2 Hüter der Datenautonomie

6.1.2.1 Datenschutzrecht

50 Zwar ermöglicht der Code in einem ersten Schritt eine weitreichende Datenautonomie "putting data back into the hands of users". Doch soll in einem zweiten Schritt diese neu gewonnene Autonomie in den Händen auch *fest ergriffen und festgehalten* werden, sodass sie nicht wieder verloren geht. Diese Aufgabe kommt besonders dem Datenschutzrecht infolge seiner Schutzziele zu: Diese sind erstens der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen (Art. 1 Abs. 2 DSGVO) und zweitens der freie Verkehr von Personendaten (Art. 1 Abs. 3 DSGVO).

51 Zentraler Bestandteil des ersten Schutzziels ist gemäss h.L. das Recht auf informationelle Selbstbestimmung: "Das Grundrecht [der informationellen Selbstbestimmung] schützt den Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten, indem es ihn ermächtigt, selbst über die Verwendung seiner Daten zu entscheiden."[106] Für die Verwirklichung dieses Rechts und den freien Datenverkehr ist die Datenautonomie jedoch derart grundlegend, dass das Datenschutzrecht sie nicht bloss den Bestimmungen de lege lata unterstellen sollte. Vielmehr sollte das Datenschutzrecht de lege ferenda zu ihrem Erhalt beitragen, sodass eine "offene Hand", so wie sie heute vorliegt, nicht mehr datenschutzkonform sein kann. Denn mit der Datenautonomie steht oder fällt das Gebäude des effektiven Datenschutzes mitsamt des intensiven, freien Datenverkehrs.

6.1.2.2 Datenschutzcode

52 Zum Erhalt der Datenautonomie kann zum Recht auch der Datenschutz durch Code (Privacy by Design und Privacy by Default) hinzutreten. Beispielsweise könnte der Code eine umfassende Datenzugangsgewährung an ein Unternehmen technisch

---

[104] *Inrupt-Privacy World*, o.S.

[105] Zur Erforderlichkeit eines Dateneigentums sei auf die einschlägige Literatur verwiesen: siehe grundlegend *Rolf H. Weber/Florent Thouvenin*, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, in: ZSR 2018, I Heft 1, S. 43 ff. Siehe zustimmend *Jutta Stender-Vorwachs/Hans Steege*, Wem gehören unsere Daten?, in: NJOZ 2018, S. 1362 ff. sowie ablehnend *Karl-Heinz Fezer*, Dateneigentum der Bürger, in: ZD 2017, S. 99 ff. Vgl. auch *Peter Georg Picht*, Dateneigentum und Datenzugang, in: Jusletter IT Flash 11. Dezember 2017, Rz. 1 ff. zum Schutz von Geschäftsgeheimnissen als Ordnungsrahmen für die Datenwirtschaft. Im DWeb könnte allerdings die *Datenautonomie* als Ordnungsrahmen fungieren, da sie die eigentümerähnliche Position der betroffenen Person über ihre Daten weiter verstärken und so die Notwendigkeit eines – bereits heute überwiegend abgelehnten – Dateneigentums in noch weitere Ferne rücken könnte.

[106] *Jens Ambrock*, in: Silke Jandt/Roland Steidle (Hrsg.), Datenschutz im Internet, Rechtshandbuch zu DSGVO und BDSG, Baden-Baden 2018, Rechtliche Grundlagen N 18.

unterbinden. Doch wie genau sollen alle rechtlich relevanten Sachverhaltselemente vom Code bewertet werden? Und wie sind die aus dem Datenschutzrecht fliessenden Rechte gegenüber anderen Rechten wie der Meinungs-, Informations- oder Forschungsfreiheit durch Algorithmen abzuwägen?[107]

53 Diese Fragen verdeutlichen die regulatorische Ungeeignetheit des Datenschutzcodes in komplexen Konstellationen, sodass sich neben der Gefahr einer allzu starren Regulierung wie im Falle des klassischen DRM (siehe oben Rz. 38) auch Smart Contracts-Probleme ergeben könnten (siehe oben Rz. 41).[108] In weniger komplexen Fällen kann dem Datenschutzcode aber besonders infolge seiner Durchsetzungskraft ex ante eine das Recht unterstützende Wirkung zukommen.[109]

6.1.3 Zwischenfazit

54 Der Code ist zwar der Ursprung der Datenautonomie, doch das Recht ist ihr Hüter. Vorerst wird der Datenschutzcode aber wohl nur in weniger komplexen Fällen zum Datenschutzrecht unterstützend hinzutreten.

6.2 Machtverhältnisse, Schutz vor sich selbst und Paternalismus

6.2.1 Veränderung der Machtverhältnisse

55 Die Datenautonomie führt zu einer Veränderung der Machtverhältnisse zwischen Dateninhaber sowie Staaten und Unternehmen. Die DSGVO trat allerdings in einem Kontext in Kraft, dem ein krasses Missverhältnis zwischen den Autonomiebereichen der betroffenen Person und des Verantwortlichen immanent war. Entsprechend versucht die DSGVO die Rechte und Pflichten dergestalt zu verteilen, dass dadurch das Missverhältnis im Machtverhältnis ausgeglichen oder mindestens doch abgeschwächt werden kann.[110]

56 Mit dem DWeb vollzieht sich jedoch ein gewisser Ausgleich *faktischer* Natur: Die Datenautonomie des Dateninhabers weitet sich so aus, dass sie Teile der Datenautonomie des Verantwortlichen einnimmt. Insofern aktualisiert sich die

---

[107] Vgl. *Benedikt Buchner*, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG: Kommentar, 2. Aufl., München 2018, Art. 1 N 15; vgl. auch 4. Erwägungsgrund der DSGVO; die Lösung dieser Probleme wird auch grundlegend für die Anwendbarkeit des Smart Privacy Contracts sein (siehe unten Rz. 86).

[108] Mit der Zeit könnte der Datenschutzcode jedoch auch zu einem geeigneteren Regulator als das Datenschutzrecht avancieren.

[109] Vgl. *Panel for the Future of Science and Technology (STOA)* des Europäischen Parlaments, Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, Brüssel 2019, S. 91 ff. (nachfolgend "STOA-DLT"); *Bechtolf/Vogt*, S. 71.

[110] *Stefan Ernst*, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018, Art. 1 N 7; vgl. auch 11. Erwägungsgrund der DSGVO.

Notwendigkeit einer "Kalibrierung" der datenschutzrechtlichen Schutzbedürftigkeit der Akteure mitsamt der Verteilung ihrer Rechte und Pflichten.[111]

6.2.2 Schutz vor anderen und vor sich selbst

57 Es ist daran zu erinnern, dass das Recht die Datenautonomie erhalten und schützen soll (siehe oben Rz. 50). Im DWeb kommt dem Dateninhaber mit der Datenautonomie jedoch eine wesentlich grössere Handlungsfreiheit als im aktuellen Web zu, sodass der Dateninhaber von einer primär passiven Figur zu einem aktiven Akteur wird. Infolge dieser neuen, weitreichenden Datenautonomie in Verbindung mit dem Privacy Paradox geht die Gefahr ihres Verlustes aber nicht mehr nur vom Staat oder von Unternehmen aus, sondern verstärkt auch vom aktiven "Öffnen der Hand" durch den Dateninhaber selbst. Steht heute also noch der Schutz *vor anderen* im Zentrum des Datenschutzrechts,[112] so könnte im DWeb der Schutz des Dateninhabers *vor sich selbst* an Bedeutung gewinnen.[113]

6.2.3 Paternalistischer Regelungsbedarf

58 Dadurch schränkt das Datenschutzrecht aber das ein, was es zu erhalten versucht: die Datenautonomie. Allerdings wäre eine paternalistische Intervention dem Datenschutzrecht nicht fremd, enthält die DSGVO doch ein "vielfältiges Spektrum paternalistischer Elemente"[114] wie das Verbot mit Erlaubnisvorbehalt oder das Gebot des Privacy by Default.[115] Der Schutz vor sich selbst liesse sich somit in diesen sog. Datenpaternalismus einfügen.[116] Da die grundlegende Neuerung der Datenautonomie die (meist) auf einem Vertrag beruhende Zugangsgewährung zu den eigenen Daten ist, gewinnt zudem die Dimension des Vertragsrechts im DWeb an

---

[111] Vgl. *Verborgh*, o.S.; siehe besonders unten Rz. 64 zum verantwortlichen Dateninhaber.

[112] *Ernst*, in: Paal/Pauly, Art. 1 N 7; vgl. 6. Erwägungsgrund der DSGVO; vgl. auch Art. 28 des Schweizerischen Zivilgesetzbuchs vom 10. Dezember 1907 (ZGB).

[113] Vgl. auch *Barbara Sandfuchs*, Privatheit wider Willen? Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht, Tübingen 2015, S. 165 ff., 169 ff.; vgl. auch Art. 27 ZGB.

[114] *Christoph Krönke*, Datenpaternalismus: Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, in: Der Staat, Vol. 55, No. 3 (2016), S. 322.

[115] *Krönke*, S. 325 und 329.

[116] Auf die Frage nach der Daseinsberechtigung des Datenpaternalismus wird hier nicht eingegangen. Siehe hierzu *Krönke*, S. 330 ff.

Bedeutung.[117] Darin lebt freilich eine "paternalistische[n] Tradition"[118], die sich beispielsweise im Schutz vor übermässiger Bindung äussert.[119]

59 Des weiteren müssen auch die spezifischen Umstände, in denen der Schutz vor sich selbst greifen soll, berücksichtigt werden. Zum einen ist im DWeb die Fallhöhe der Autonomie derart hoch, dass diese neue, grosse Datenautonomie den Dateninhaber auch überfordern könnte.[120] Und zum anderen wird das Privacy Paradox selbst durch Aufklärungsarbeit wohl nicht so schnell zu überwinden sein, hat sich in der heutigen Zeit der sorglose Umgang mit den "eigenen" Daten doch bereits zur Gewohnheit verhärtet.[121]

60 Aufgrund rechtlicher Überlegungen und spezifischer Umstände ist ein Paternalismus zumindest nicht per se abzulehnen, sondern in engen Grenzen zuzulassen. Ein paternalistischer Regelungsbedarf besteht etwa dann, wenn ein Dateninhaber einem Staat oder Unternehmen jegliche Datenautonomie über seine (besonders schützenswerten) Daten durch die Übergabe seines privaten Schlüssels abgeben und so auf einen autonomielosen Boden herabfallen würde.

6.2.4 Zwischenfazit

61 Das DWeb führt zu einer Veränderung der Machtverhältnisse, in denen der Dateninhaber als aktiver Akteur auftritt. Angesichts rechtlicher Überlegungen sowie spezifischer Umstände ist ein Schutz vor sich selbst in engen Grenzen zuzulassen.

6.3 Verantwortlicher Dateninhaber

6.3.1 Verantwortlichkeit in der Blockchain

62 Der Verantwortliche ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO). Dieser Begriff soll

---

117 Vgl. allgemein auch RL (EU) 2019/770 des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und Dienstleistungen, ABl. L 136 vom 22. Mai 2019, S. 1 ff.; siehe auch unten Rz. 89 zu den Smart Contracts im Vertragsrecht.

118 *Axel Metzger*, Mehr Freiheit wagen auf dem Markt der Daten: Voraussetzungen und Grenzen eines Marktmodells für „big data", in: Anatol Dutta/Christian Heinze (Hrsg.), Mehr Freiheit wagen – Symposium zur Emeritierung von Jürgen Basedow, Tübingen 2018, S. 2.

119 Siehe etwa Art. 27 ZGB. Hierbei gilt es anzumerken, dass im Schweizer Recht über Art. 1 (Schutz der Persönlichkeit) des Bundesgesetzes über den Datenschutz (DSG) *und* über Art. 19/20 (persönlichkeitswidriger Vertragsinhalt) des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) zu Art. 27 ZGB gelangt wird. In diesem Sinne: Alle Wege führen zu Art. 27 ZGB.

120 *STOA-DLT*, S. 50; vgl. *Harbinja/Karagiannopoulos*, o.S.; vgl. aber auch *Web-Contract*, 8.c Prinzip und 9.a Prinzip.

121 *Yoan Hermstrüwer*, Informationelle Selbstgefährdung: Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, Tübingen 2016, S. 231 ff.

dazu dienen, die Verantwortung für eine datenschutzkonforme Datenverarbeitung einem bestimmten Adressaten zuzuweisen (Art. 24 DSGVO), sodass die betroffene Person *durch ihn* ihre Betroffenenrechte verwirklichen kann (z.B. Löschen der Daten *durch* den Verantwortlichen).[122]

63 Bereits im Kontext der (öffentlichen) Blockchain haben sich erhebliche Probleme bei der Suche nach einem solchen Adressaten ergeben, geht mit ihrer dezentralisierten Struktur doch auch eine Dezentralisierung der Verantwortung einher. Die Verantwortung wird auf das gesamte Netzwerk dermassen verteilt, dass einem einzelnen Node nur ein Quäntchen Verantwortung verbleibt, das aber so klein ist, dass es die Betroffenenrechte alleine nicht durchzusetzen vermag.[123] Doch gerade dieser Umstand trägt zur Sicherheit und Stabilität der Blockchain-Architektur bei.[124]

6.3.2 Datenschutzrechtliche Selbstverantwortung

64 Infolge der weiten Datenautonomie kann der Dateninhaber die Betroffenenrechte im DWeb hinsichtlich der Daten in seinem Autonomiebereich – wie unten allgemein noch zu zeigen sein wird – eigenständig durchsetzen (z.B. Daten selber löschen). Gleichzeitig verunmöglicht die DWeb-Architektur dem Verantwortlichen diese Rechte für den Dateninhaber durchzusetzen. Auf diese Weise beseitigt das DWeb einen weiteren "Intermediären": den Verantwortlichen.[125] Ein Teil der datenschutzrechtlichen Verantwortung wandert so vom Verantwortlichen zum verantwortlichen Dateninhaber (datenschutzrechtliche Selbstverantwortung).[126]

65 Ausserhalb des Autonomiebereichs des Dateninhabers – als Paradebeispiel bietet sich die Datenerhebung durch Personen an, auf welche sich die Daten *nicht* beziehen (z.B. Videoüberwachung im öffentlichen Raum) an – sollte im allgemeinen aber derjenige zur Durchsetzung der Betroffenenrechte verantwortlich sein, der dazu im Einzelfall auch geeignet ist. Jedenfalls kann eine im Hinblick auf die Durchsetzbarkeit der Betroffenenrechte "blinde" Subsumtion, die lediglich auf die Begriffe "Zwecke" und "Mittel" abstellt, nicht zielführend sein, wenn sie dadurch der Durchsetzungsfunktion des Verantwortlichen nicht genügend Rechnung trägt.[127]

---

[122] *Jürgen Hartung*, in: Kühling/Buchner, Art. 4 Nr. 7 N 1 und 6; *STOA-DLT*, S. 37.

[123] Auch die Konstruktion der gemeinsamen Verantwortlichkeit der Nodes (Art. 26 DSGVO) hilft hier nicht viel weiter. Siehe dazu *Mario Martini/Quirin Weinzierl*: Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: NVwZ 2017, S. 1253 ff.

[124] *Bechtolf/Vogt*, S. 69; *Thomas Janicki/David Saive*, Privacy by Design in Blockchain-Netzwerken, Verantwortlichkeit und datenschutzkonforme Ausgestaltung von Blockchains, in: ZD 2019, S. 252 ff.; *Martini/Weinzierl*, S. 1253 ff.

[125] Vgl. *STOA-DLT*, S. 49 f.

[126] Vgl. auch *Web-Contract*, 7., 8. und 9. Prinzip.

[127] *STOA-DLT*, S. 37 ff. und 52; vgl. *Bechtolf/Vogt*, S. 69.

6.3.3 Zwischenfazit

66 Während in der Blockchain verschiedenste Probleme bei der Verantwortungszuweisung auftreten, eröffnet das DWeb dem Dateninhaber neue Autonomiesphären. Diese ermöglichen ihm seine Rechte selber zu verwirklichen, ohne auf die Mitwirkung eines "Verantwortlichen" zurückgreifen zu müssen. Der Dateninhaber wird so zum verantwortlichen Dateninhaber, dem eine datenschutzrechtliche Selbstverantwortung zukommt.

6.4 Sachlicher Anwendungsbereich (Art. 2 DSGVO)

67 Der sachliche Anwendungsbereich der DSGVO wird eröffnet, wenn personenbezogene Daten verarbeitet werden (Art. 2 Abs. 1 DSGVO). Erstens müssen sich die Daten auf eine identifizierte oder identifizierbare Person beziehen, sodass das Herstellen eines Personenbezugs im Einzelfall für den Verantwortlichen mit verhältnismässigen Mitteln möglich ist (Art. 4 Nr. 1 DSGVO).

68 Besonders problematisch ist im DWeb das Speichern der Daten auf dem P2P-Netzwerk *in verschlüsselter Form*.[128] In einer Vielzahl der Fälle wird das Datenschutzrecht aufgrund der verschlüsselten, anonymen Daten also gar nicht erst anwendbar sein: Erst die Entschlüsselung der Daten öffnet Tür und Tor zum Datenschutzrecht.[129] Im DWeb kommt – neben einer eher unwahrscheinlichen Entschlüsselung durch Hacker – jedoch nur eine Entschlüsselung durch den Dateninhaber oder durch einen Dritten, dem der Dateninhaber Zugriffsrechte eingeräumt hat, in Betracht.[130] Dem Dateninhaber kommt demnach eine Schlüsselposition im Hinblick auf die Anwendbarkeit des Datenschutzrechts zu, wobei dies einen massgeblichen Einfluss auf die Grundsätze der Datenverarbeitung aufweisen wird (siehe unten Rz. 70).

69 Als zweites Erfordernis müssen Personendaten verarbeitet werden, wobei jeder Vorgang im Zusammenhang mit Daten erfasst wird (Art. 4 Nr. 2 DSGVO).[131] Hinsichtlich dieser Voraussetzung bestehen im DWeb wohl keine erwähnenswerten Probleme.[132]

---

[128] Siehe auch den Datenschutz im Kontext der (Post-)Quanten-Kryptografie: *ZD-Aktuell*, Datensicherheit bei Anwendungen durch Quantencomputer, in: ZD-Aktuell 2018, S. 06325.

[129] Sollten Daten im semantischen und nicht im syntaktischen Sinne verstanden werden, so würden hier nicht nur keine personenbezogenen Daten vorliegen, sondern infolge der verschlüsselten, bedeutungslosen Zeichenfolge überhaupt keine Daten.

[130] *STOA-DLT*, S. 29; vgl. *Annika Selzer*, Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit, Eine Betrachtung unter Anwendung der Datenschutz-Grundverordnung, Wiesbaden 2020, S. 23.

[131] *Alexander Rossnagel*, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019, Art. 4 Nr. 2 N 11.

[132] Vgl. auch *STOA-DLT*, S. 8 ff. zum räumlichen Anwendungsbereich (Art. 3 DSGVO).

6.5 Grundsätze der Datenverarbeitung (Art. 5 DSGVO) und Smart Privacy Contract

70 Im Folgenden werden die Auswirkungen des DWebs auf die Grundsätze der Datenverarbeitung (Art. 5 DSGVO) aufgezeigt (siehe sogleich Rz. 71). Sodann wird auf die automatisierte Kontrolle (und Durchsetzung) ihrer Einhaltung durch den Smart Privacy Contract eingegangen (siehe unten Rz. 86).

6.5.1 Grundsatz der Transparenz

71 Zunächst muss die Datenverarbeitung rechtmässig sein (Art. 5 Abs. 1 lit. a 1. Halbsatz DSGVO), wobei Art. 6 DSGVO und Art. 9 DSGVO anzurufen sind.[133] Diese beiden Artikel werden weiter unten behandelt (siehe unten Rz. 91). Dem Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a 2. Halbsatz DSGVO) wird hier nicht weiter nachgegangen.

Grundsätze der Datenverarbeitung:

- Grundsatz der Rechtmässigkeit, Treu und Glauben sowie Transparenz
- Grundsatz der Zweckbindung
- Grundsatz der Datenminimierung
- Grundsatz der Richtigkeit
- Grundsatz der Speicherbegrenzung
- Grundsatz der Integrität und Vertraulichkeit

72 Zuletzt ist der Grundsatz der Transparenz zu untersuchen. Alle Informationen und Mitteilungen zur Datenverarbeitung müssen für die betroffene Person leicht zugänglich, verständlich sowie in klarer und einfacher Sprache abgefasst werden (Art. 5 Abs. 1 lit. a 3. Halbsatz DSGVO). Die betroffene Person muss besonders über Risiken, Vorschriften, Garantien, Rechte sowie deren Geltendmachung informiert werden.[134] Hierfür interessant wäre im DWeb – soweit technisch möglich – ein im Smart Contract implementiertes elektronisches Register, das die Informationen, welche zur Einhaltung des Grundsatzes der Transparenz vonnöten sind, beinhaltet.[135] Der Smart Contract könnte so die Verarbeitung laufend kontrollieren oder gar selbst darauf reagieren (z.B. Zugangssperre). Darauf wird zurückzukommen sein (siehe unten Rz. 86).

---

[133] *Stephan Pötters*, in: Gola, Art. 5 N 6.

[134] 39. Erwägungsgrund der DSGVO; *Philipp Reimer*, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. Aufl., Baden-Baden 2018, Art. 5 N 12 ff.

[135] Vgl. *Weber/Thouvenin*, S. 17 f.

6.5.2 Grundsatz der Zweckbindung

73 Der Grundsatz der Zweckbindung besagt, dass Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen (Art. 5 Abs. 1 lit. b DSGVO).

74 Sollte der Datenzugang zu einem der Zwecke in Art. 6 Abs. 1 lit. b-f DSGVO oder Art. 9 Abs. 2 lit. b-j DSGVO rechtlich nicht durchsetzbar sein (siehe eingehend unten Rz. 93), so kann der Dateninhaber den Datenzugang zu für ihn unerwünschten Zwecken auch verweigern. Mithin kann er den Zweck festlegen, seine konkrete Weite ("eindeutig") und den Zugriff auf legitime Zwecke beschränken. Ohne die Einwilligung des Dateninhabers kann der Zugriffswillige somit gar nicht erst auf die Daten zugreifen, weshalb letztlich nicht mehr der Verantwortliche sondern der Dateninhaber den Verarbeitungszweck festlegt.[136]

6.5.3 Grundsatz der Datenminimierung

75 Im Lichte der Zweckbindung ist sodann der Grundsatz der Datenminimierung zu sehen. Demgemäss muss eine Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Mass beschränkt sein (Art. 5 Abs. 1 lit. c DSGVO). Der Grundsatz gebietet damit eine Reduktion der Anzahl an verarbeiteten Daten sowie der Anzahl ihrer Nutzungen.[137]

76 Wird durch den Dateninhaber dem Zugangsberechtigten Zugang zu den Daten verschafft, könnten auch die Anzahl der verarbeiteten Daten und die Anzahl ihrer Nutzungen in einem Smart Contract festgelegt werden. Mit dem DWeb lässt sich der Grundsatz der Datenminimierung somit besser verwirklichen als im aktuellen Web.[138]

6.5.4 Grundsatz der Richtigkeit

77 Des weiteren besagt der Grundsatz der Richtigkeit, dass die Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen (Art. 5 Abs. 1 lit. d DSGVO).

78 Da im DWeb der Speicherort eines Datums durch einen Zugriff nicht verändert wird, kann der Dateninhaber ungeachtet der Zugangsgewährung die Richtigkeit seiner Daten kontrollieren und sie nötigenfalls löschen (siehe aber unten Rz. 98). Fraglich ist jedoch, wo genau das personenbezogene Ergebnis einer Datenverarbeitung gespeichert wird. Sollte es sich *ausserhalb* der Autonomiesphäre des Dateninhabers befinden, so besteht ein mit heute vergleichbares Machtverhältnis, weshalb das

---

[136] Vgl. *Weber/Thouvenin*, S. 15.

[137] *Pötters*, in: Gola, Art. 5 N 22 f.

[138] Vgl. *Schawe*, S. 221; zu beachten ist jedoch, dass in einer Blockchain die Daten eines Blocks als "Anhängsel" aller neueren Blöcke mitverarbeitet werden. Siehe dazu *STOA-DLT*, S. 65 f. m.w.H.

aktuelle Datenschutzrecht als Ausgleich zur fehlenden Datenautonomie heranzuziehen wäre. Sollte es sich hingegen *innerhalb* seiner Autonomiesphäre befinden, so wird dem Zugangsberechtigten seine Pflichterfüllung technisch verunmöglicht, sodass ihm hinsichtlich der Richtigstellung keine Verantwortung mehr zukommen kann. Vielmehr gilt hier die datenschutzrechtliche Selbstverantwortung des Dateninhabers.

79 Ist die Unrichtigkeit der Daten zum Nachteil des Dateninhabers, so *kann* er sie selbst beheben. Ist sie jedoch (auch) zum Nachteil des Zugangsberechtigten, so fragt sich, ob der Dateninhaber sie beheben *muss*. Dies ist höchstens dann vorstellbar, wenn der Zugangsberechtigte für den Datenzugriff eine angemessene Gegenleistung erbracht hat (z.B. Coins) und sein wirtschaftlicher Erfolg und seine pflichtgemässe Aufgabenerfüllung von der Richtigkeit der Daten abhängt.[139]

6.5.5 Grundsatz der Speicherbegrenzung

80 Der Grundsatz der Speicherbegrenzung besagt, dass die Identifizierung der betroffenen Person nur so lange möglich sein darf, wie es für die Verarbeitungszwecke erforderlich ist (Art. 5 Abs. 1 lit. e DSGVO). Da die Daten nicht länger als nötig gespeichert werden dürfen, müssen sie nach dem Erfüllen des Verarbeitungszwecks gelöscht oder anonymisiert werden.[140]

81 Bezüglich der Daten im Autonomiebereich des Dateninhabers wird dem Grundsatz der Speicherbegrenzung besonders durch eine Zugriffssperre bzw. eine Anonymisierung der Daten Rechnung getragen.[141] Dies durch den Dateninhaber oder den Smart Contract beim Erfüllen eines in ihm festgelegten Verarbeitungszwecks. Bezüglich der Daten ausserhalb seines Autonomiebereichs ist wie beim Grundsatz der Richtigkeit auf das aktuelle Datenschutzrecht zurückzugreifen (siehe oben Rz. 78).

6.5.6 Grundsatz der Integrität und Vertraulichkeit

82 Gemäss dem Grundsatz der Integrität und Vertraulichkeit müssen die Daten derart verarbeitet werden, dass eine angemessene Sicherheit der Daten durch geeignete technische und organisatorische Massnahmen gewährleistet werden kann (Art. 5 Abs. 1 lit. f DSGVO).

83 Im DWeb wird die angemessene technische Sicherheit der Daten weitestgehend durch die DWeb-Architektur geleistet (z.B. Verschlüsselung der Daten).[142] Zudem ist der Dateninhaber zur (organisatorischen) Sicherung seiner Daten selbst

---

[139] Vgl. *Rossnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 5 N 137.

[140] 39. Erwägungsgrund der DSGVO; *Tobias Herbst*, in: Kühling/Buchner, Art. 5 N 66.

[141] Vgl. *Verborgh*, o.S.; vgl. auch *STOA-DLT*, S. 67.

[142] Vgl. auch *Weber/Thouvenin*, S. 15.

verantwortlich, etwa durch eine sichere Aufbewahrung seines privaten Schlüssels.[143] Für die Daten ausserhalb seiner Autonomiesphäre ist der Zugangsberechtigte zur Einhaltung des Grundsatzes der Integrität und Vertraulichkeit verantwortlich.

6.5.7 Rechenschaftspflicht

84 Zuletzt ist auf die Rechenschaftspflicht einzugehen. Der Verantwortliche ist für die Einhaltung der Grundsätze in Art. 5 Abs. 1 lit. a-f DSGVO verantwortlich und muss ihre Einhaltung nachweisen können (Art. 5 Abs. 2 DSGVO).

85 Im DWeb ist der Zugangsberechtigte für die Einhaltung dieser Grundsätze und damit für eine rechtmässige Verarbeitung der Daten des Dateninhabers *in- und ausserhalb* der Autonomiesphäre des Dateninhabers verantwortlich. Allerdings kann er die Folgen ihrer Verletzung bei Daten innerhalb der Autonomiesphäre des Dateninhabers nicht mehr selbständig beheben (z.B. unrichtige Daten), sodass der Dateninhaber die Folgen beheben kann bzw. muss. Um schliesslich die Einhaltung dieser Grundsätze nachweisen zu können, könnte dem Verantwortlichen das Register im Smart Privacy Contract behilflich sein.

6.5.8 Smart Privacy Contract

6.5.8.1 Begriff

86 Die obigen Ausführungen zu den Grundsätzen der Datenverarbeitung haben verdeutlicht, dass eine Datenverarbeitung durch den Zugangsberechtigten grundsätzlich nur dann erfolgen kann, wenn ihm der Dateninhaber Zugriff auf seine Daten gewährt. Damit kann der Dateninhaber über die Modalitäten der Datenverarbeitung entscheiden bzw. den Datenzugriff für ihm unerwünschte Modalitäten verweigern. Ihre Einhaltung könnte durch einen Smart Contract überwacht und durchgesetzt oder aber ein Verstoss dem Dateninhaber gemeldet werden (Smart Privacy Contract).[144] Dies würde nicht nur dem Transparenz- (Art. 12 DSGVO), dem Informations- (Art. 13 f. DSGVO) und dem Auskunftsrecht (Art. 15 DSGVO) des Dateninhabers sondern auch dem Gebot des Privacy by Design Rechnung tragen.

6.5.8.2 Voraussetzungen des Privacy by Design

87 Es fragt sich, ob der Zugriffswillige infolge des Gebots des Privacy by Design (Art. 25 Abs. 1 DSGVO) einen Smart Privacy Contract benutzen müsste, wenn er auf die Daten zugreifen möchte. Die Beantwortung dieser Frage hängt gemäss Art. 25 Abs. 1

---

[143] Vgl. *Bericht des [Schweizer] Bundesrates*, Rechtliche Grundlagen für *Distributed Ledger*-Technologie und Blockchain in der Schweiz, Eine Auslegeordnung mit Fokus auf dem Finanzsektor, Bern 2018, S. 32.

[144] Vgl. *Bechtolf/Vogt*, S. 71.

DSGVO vom Stand der Technik, den Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen ab. Neben diesen Kriterien ist auch die Wirksamkeit der Umsetzung der Datenschutzgrundsätze zu beurteilen. Es dürfen daher keine Probleme oder besondere Schwierigkeiten durch eine automatisierte Kontrolle (und Durchsetzung) der Modalitäten der Datenverarbeitung durch einen Smart Privacy Contract auftreten.[145] Dabei gilt es besonders auch die bereits beschriebenen Problematiken hinsichtlich der Smart Contracts im Auge zu behalten (siehe oben Rz. 41).

88 Vorstellbar ist jedenfalls, dass ohne eine laufende, automatisierte Verarbeitungskontrolle durch einen Smart Privacy Contract die weit gefasste Datenautonomie wohl nur bei der Ausgestaltung der Verarbeitungsmodalitäten ausgeschöpft würde, sodass *nach* der Zugangsgewährung die Kontrolle über den weiteren Bearbeitungsvorgang – wie heute – faktisch aufgegeben würde. Doch möchte die Datenautonomie gerade das verhindern.[146] Sollten deshalb Smart Privacy Contracts verwendet werden können, so könnten das Datenschutzrecht und der Code näher zusammengeführt werden, sodass sie nicht mehr in einem Spannungsverhältnis stehen würden, sondern in einem Komplementaritätsverhältnis gemeinsamer Verhaltensregulierung im Dienste des Datenschutzes.

6.5.8.3 Smart Contracts im Vertragsrecht

89 Sollte ein Smart Privacy Contract technisch umsetzbar sein, so ist seine rechtliche Beurteilung fraglich. Ein Smart Contract ist nur dann ein Vertrag im Rechtssinne, wenn er auch rechtlich zustande gekommen ist. In vielen Fällen ist er daher bloss eine Software, welche die Einhaltung eines Vertrags kontrolliert und/oder vollzieht.[147] Ist ein Smart Privacy Contract aber als Vertrag zu qualifizieren, so stellen sich die folgenden (nicht abschliessenden) Fragen: Mutieren die Grundsätze der Datenverarbeitung bzw. ihre konkreten Ausgestaltungen zu den essentialia negotii dieses Vertragstypus (z.B. Bestimmung des zulässigen Zwecks, Aufhebung oder Reduzierung bestimmter Grundsätze wie der Datenminimierung)? Welche Bestimmungen der DSGVO können vertraglich wegbedungen werden? Wie weit soll der Schutz gegen sich selbst in die Vertragsfreiheit eingreifen dürfen? Und ist der Grundsatz der jederzeitigen Widerrufbarkeit der Einwilligung (Art. 7 Abs. 3 DSGVO) angesichts eines (zweiseitigen) Vertragsverhältnisses in dem Sinne einzuschränken, als dass die Einwilligung nur noch unter bestimmten Umständen widerrufen werden

---

[145] Vgl. *Marit Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 25 N 30.

[146] Vgl. auch 7. und 78. Erwägungsgrund der DSGVO.

[147] *Schrey/Thalhofer*, S. 1431.

kann? Es ergeben sich damit spannende Fragen an der Schnittstelle zum Vertragsrecht, welche hier jedoch nur angesprochen, aber nicht beantwortet werden sollen. Nichtsdestotrotz wird bereits durch das Stellen der Fragen deutlich, dass die Datenautonomie als Triebkraft die zwei bislang nur wenig miteinander interagierenden Rechtsgebiete – das Datenschutzrecht und das Vertragsrecht – näher zusammenführen wird.

6.5.9 Zwischenfazit

90 Sollte der Dateninhaber den Datenzugriff gewähren, so könnten gemäss Art. 25 Abs. 1 DSGVO die Verarbeitungsmodalitäten in einen Smart Privacy Contract aufgenommen werden. Dabei werden die Modalitäten durch den Smart Privacy Contract oder den Dateninhaber kontrolliert und durchgesetzt. Der Zugangsberechtigte trägt aber auch im DWeb noch die Verantwortung zur Einhaltung dieser Grundsätze. Daran ändert nichts, dass er die Folgen bei einer Verletzung der Grundsätze hinsichtlich derjenigen Daten, die sich innerhalb der Autonomiesphäre des Dateninhabers befinden, nicht mehr selbständig beheben kann. Dies ist Ausdruck der neuen Datenautonomie des Dateninhabers.

6.6 Verbotsprinzip mit Erlaubnisvorbehalt (Art. 6 DSGVO)

6.6.1 Begriff und Einwilligung

91 Gemäss dem sog. Verbotsprinzip mit Erlaubnisvorbehalt (Art. 6 DSGVO) ist eine Datenverarbeitung grundsätzlich verboten, ausser es besteht ein Erlaubnistatbestand i.S.v. Art. 6 Abs. 1 DSGVO.[148] Zwar ist bereits heute die Einwilligung i.S.v. Art. 6 Abs. 1 lit. a DSGVO der weitaus bedeutendste Erlaubnistatbestand,[149] doch wird sich seine Wichtigkeit mit der Datenautonomie voraussichtlich noch weiter akzentuieren.

92 Da nur der Dateninhaber entscheiden kann, wer auf seine Daten zugreifen darf, kann eine Datenverarbeitung durch einen Dritten überhaupt nur dann erfolgen, wenn der Dateninhaber seine Einwilligung dazu abgibt. Ein "selbständiges" Tätigwerden, etwa durch ein Unternehmen, gestützt auf einen Erlaubnistatbestand i.S.v. Art. 6 Abs. 1 lit. b-f DSGVO ist zumindest rein technisch wohl nicht mehr möglich. Hat der Dateninhaber auch kein Interesse an einer Zugangsgewährung zu den Zwecken in Art. 6 Abs. 1 lit. b-f DSGVO[150], so fragt sich, wie eine solche Datenverarbeitung

---

[148] Die folgenden Ausführungen gelten entsprechend auch für die Verarbeitung besonders schutzwürdiger Daten (Art. 9 DSGVO).

[149] *Alessi/Camillò/Giangreco et al.*, S. 79.

[150] Ein mangelndes Interesse an der Datenverarbeitung zu den Zwecken in Art. 6 Abs. 1 lit. b/d DSGVO scheint unwahrscheinlich. Theoretisch kann der Dateninhaber den Datenzugriff aber auch zu diesen Zwecken verweigern.

rechtlich durchgesetzt werden kann, zumal der Dateninhaber auch anonym sein kann.[151]

6.6.2 Ausschliessliche faktische Datenautonomie

93 Sollte ein Datenzugang rechtlich nicht durchzusetzen sein, wandert der Datenschatz in die *ausschliessliche* faktische Herrschaft des Dateninhabers und wird so den "anerkennenswerten Interessen"[152] des Dritten oder gar der Gesellschaft entzogen, sodass die Daten nicht mehr "im Dienste der Menschheit stehen"[153] würden. Es erfolgt damit eine Transition von den (allgemein zugänglichen) Daten als öffentliche Güter[154] zu den Daten als faktische Ausschliesslichkeitspositionen. Nicht nur könnten Daten so dem Staat entzogen werden, sondern sie könnten als "wertvollste Ressource der Welt"[155] auch vom Wirtschaftsverkehr abgekoppelt werden. Es könnten deshalb Anreize wie Coins oder "kostenlose" Dienste gesetzt werden, um Zugriffsmöglichkeiten auf die Datenschätze zu den Zwecken in Art. 6 Abs. 1 lit. b-f DSGVO erhalten zu können.

94 Auf der anderen Seite unterscheidet sich diese Ausnahmekonstellation, in der die Daten nicht im Dienste der Menschheit stehen, kaum von den grundsätzlichen Begebenheiten der heutigen Datenwirtschaft, in der einige wenige Unternehmen über grosse Datenschätze herrschen. Ihre (nahezu) ausschliessliche faktische Datenautonomie umfasst grosse, meist abgeriegelte Datensilos, von denen ein entsprechend geringer Nutzen für die Menschheit und ein ebenso beschränkter Datenhandel ausgehen.[156] Verwalten aber 4,5 Milliarden Internetnutzer ihre Daten, ergeben sich daraus beträchtliche Potentiale für den Datenhandel und letztlich auch für die Menschheit. Dies gilt besonders im Hinblick auf die enormen Datenmengen, die im "Internet of Things" bzw. im "Internet of Everything" generiert werden. Die Problematik der ausschliesslichen faktischen Datenautonomie ist im DWeb also von verschwindend geringer Bedeutung. Problematisch ist vielmehr, dass die Dateninhaber im Sinne des wohl nicht so schnell zu überwindenden Privacy Paradox zu sorglos mit der Zugangsgewährung zu ihren Daten umgehen werden. Deshalb soll besonders in diesem Falle der Schutz vor sich selbst greifen.

---

[151] Vgl. *STOA-DLT*, S. 35 f.

[152] *Sebastian Schulz*, in: Gola, Art. 6 N 10.

[153] 4. Erwägungsgrund der DSGVO.

[154] *Gianni Fröhlich-Bleuler*, Eigentum an Daten?, in: Jusletter 6. März 2017, Rz. 6 f.

[155] *The Economist*, The world's most valuable resource, in: The Economist vom 6. Mai 2017, o.S.

[156] *Tekla S. Perry*, The Fathers of the Internet Revolution Urge Today's Software Engineers to Reinvent the Web, in: IEEE Spectrum vom 13. Juni 2016, o.S.

6.6.3 Zwischenfazit

95 Die Datenautonomie gewährt dem Dateninhaber eine faktische Datenherrschaft über seine Daten. Kann eine Datenverarbeitung rechtlich nicht durchgesetzt werden, wird sie zu einer *ausschliesslichen* faktischen Datenherrschaft. In Anbetracht der heutigen Datenwirtschaft ist diese Fallkonstellation allerdings von vergleichsweise geringer Bedeutung.

6.7 Recht auf Löschung (Art. 17 DSGVO)

6.7.1 Begriff, Löschungsgrund und Erforderlichkeit

96 Die betroffene Person kann vom Verantwortlichen die Löschung der sie betreffenden Daten verlangen, wenn ein Löschungsgrund i.S.v. Art. 17 Abs. 1 lit. a-f DSGVO vorliegt und die Verarbeitung *nicht* erforderlich i.S.v. Art. 17 Abs. 3 lit. a-e DSGVO ist.[157] Als Löschungsgründe kommen besonders das Erreichen des Verarbeitungszwecks (Art. 17 Abs. 1 lit. a DSGVO) und der Widerruf der Einwilligung (Art. 17 Abs. 1 lit. b DSGVO) in Betracht. Im DWeb könnte der Datenzugriff mit dem Eintritt eines Löschungsgrunds durch den Smart Privacy Contract oder den Dateninhaber verweigert werden, sodass die Daten für den Zugangsberechtigten wieder verschlüsselt werden (siehe auch oben Rz. 81). Um den Zweck des Rechts auf Löschung – das Beschränken der negativen Auswirkungen der offengelegten Daten auf die betroffene Person[158] – erreichen zu können, *könnte* also eine Verschlüsselung der Daten genügen.

97 Als zweite Voraussetzung darf die Verarbeitung nicht erforderlich für einen der Fälle in Art. 17 Abs. 3 lit. a-e DSGVO sein. Diese Einschränkung des Rechts auf Löschung ist Ausdruck einer Interessenabwägung zwischen den kollidierenden Interessen der betroffenen Person sowie denjenigen des Verantwortlichen bzw. der ganzen Gesellschaft.[159] Massgeblich sind im DWeb vor allem die im öffentlichen Interesse liegenden Archivzwecke (Art. 17 Abs. 3 lit. d DSGVO) in der Form des zeitlich dezentralisierten Versionensystems (siehe oben Rz. 13).[160] Demgemäss sollen die früheren Versionen des DWebs archiviert werden, sodass das Wissen auch für die Nachwelt erhalten werden kann.

---

[157] Auf die Informationspflicht i.S.v. Art. 17 Abs. 2 DSGVO wird hier nicht eingegangen; die folgenden Gedanken zum Recht auf Löschung können weitestgehend auch auf das Recht auf Berichtigung (Art. 16 DSGVO) übertragen werden.

[158] *Boris P. Paal*, in: Paal/Pauly, Art. 17 N 6.

[159] *Nolte/Werkmeister*, in: Gola, Art. 17 N 43 ff.

[160] Vgl. *Alexander Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 17 N 34.

6.7.2 Zuweisung der Zensurpflicht

6.7.2.1 Zum Dateninhaber

98 Die soeben vorgeschlagene Lösung der Verschlüsselung (siehe oben Rz. 96) kann insofern nicht zielführend sein, als dass sie lediglich in der aktuellen DWeb-Version ihre Wirkungen entfalten würde und nicht auch in den Vorgängerversionen. Die oben angesprochene Interessenabwägung manifestiert sich hier in einer Kollision zwischen der individuell geprägten Datenautonomie und dem kollektiven Interesse am Erhalt der Daten. Um die Datenautonomie in diesem Bereich nicht zu unterminieren, wird etwa die Notwendigkeit einer Erlaubnis zur Archivierung der eigenen Website vorgeschlagen.[161] Zudem könnte eine Löschung einer bereits archivierten Information durch den Dateninhaber in Betracht kommen.[162] Zwar stärken diese beiden Ansätze die Datenautonomie, doch überlassen sie allein dem Dateninhaber den Entscheid für oder gegen eine Archivierung – ohne dass er die entgegenstehenden kollektiven Interessen zu berücksichtigen hätte.

6.7.2.2 Zum Kollektiv

99 Eine Berücksichtigung der Kollektivinteressen kann wie im Falle von DTube auch in der Zuweisung der Lösch- bzw. Zensurpflicht zum Kollektiv selber bestehen: "DTube's operators say they can't censor videos on the service, and that content will only disappear if the site's users overwhelmingly down-vote it."[163] Ein solches Down-Voting ist besonders bei disruptiven, innovativen Inhalten problematisch, da sie ihrer Zeit meist voraus sind und deshalb eher auf Unverständnis oder gar Ablehnung in der Gesellschaft stossen.[164] Im Allgemeinen könnten so Minderheitsmeinungen durch die Mehrheit ausgeschlossen werden, sodass infolge der sich kontinuierlich ausbreitenden Mehrheitsmeinung kaum noch Raum für Minderheitsmeinungen zurückbleiben würde.

6.7.2.3 Zu einer zentralen Stelle

100 Im Hinblick auf den Minderheitenschutz wäre eine Zuordnung der Löschpflicht zu einer zentralen Stelle (z.B. Google,[165] Staat) zielführender. Doch dann würde die klassische Gefahr des Missbrauchs der Zentralgewalt bestehen, sodass letztlich nicht

---

[161] *Klint Finley*, Pied Piper's New Internet Isn't Just Possible – It's Almost Here, in: Wired vom 1. Juni 2017, o.S.; *Finley*, Permanent Web, o.S.; die Problematik der Veränderungsresistenz des DWebs tritt hier also gar nicht erst auf. *Martini/Weinzierl*, S. 1254 ff. m.w.H. zur Veränderungsresistenz der Blockchain. Siehe dazu auch *ZeroNet*: "No censorship: After something is published there is no way to remove it."

[162] Vgl. *Martini/Weinzierl*, S. 1254 ff.

[163] *Simonite*, o.S.

[164] Vgl. *Finley*, Permanent Web, o.S. sowie *Verborgh*, o.S.

[165] Siehe etwa *Herbst*, in: Kühling/Buchner, Art. 17 N 67 ff. zum *"Google Spain"-Urteil*.

nur die Meinungen der Minderheit sondern die Meinungen *aller* (umfassend) zensiert werden könnten.[166]

101 Wird die Pflicht zur Zensur also dem Dateninhaber zugeordnet, so werden die gemäss Art. 17 Abs. 3 lit. a-e DSGVO zu berücksichtigenden Interessen des Verantwortlichen oder der Gesellschaft gefährdet. Wird sie aber der Mehrheit oder einer Zentralstelle zugewiesen, so könnten im ersten Fall die Interessen der Minderheit oder im zweiten Fall gar diejenigen der ganzen Gesellschaft übergangen werden.[167] Wem auch immer die Pflicht zur Zensur zugeteilt wird; es bedarf hier einer sorgfältigen Abwägungen der damit verbundenen Vor- und Nachteile. Denn die Pflichtzuweisung strahlt nicht nur auf die Gegenwart hinaus, sondern durch das zeitlich dezentralisierte Versionensystem auch weit in die Zukunft.

6.7.3 Zwischenfazit

102 Das Recht auf Löschung gilt nicht uneingeschränkt: Während das Vorliegen eines Löschungsgrunds im DWeb kaum Probleme bereiten dürfte, erweist sich die Abwägung zwischen den Individualinteressen des Dateninhabers an der Löschung und den Kollektivinteressen am Erhalt der Daten als besonderes Problemfeld, das es sorgfältig zu lösen gilt.

6.8 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

6.8.1 Begriff

103 Mit dem Recht auf Datenübertragbarkeit (sog. Datenportabilität) kann die betroffene Person vom Verantwortlichen erstens verlangen, die sie betreffenden und von ihr bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Zweitens hat die betroffene Person das Recht, diese Daten ohne Behinderung vom exportierenden Verantwortlichen zu einem importierenden Verantwortlichen zu übermitteln (Art. 20 Abs. 1 DSGVO). Drittens kann die betroffene Person erwirken, dass diese Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden (Art. 20 Abs. 2 DSGVO).

---

[166] Vgl. *Finley*, Permanent Web, o.S.

[167] Die gleiche Missbrauchsproblematik ergibt sich auch dann, wenn die Daten *entgegen* des Willens des Dateninhabers gelöscht werden sollen (z.B. Hate Speech, illegale Bilder). Siehe dazu *Harbinja/Karagiannopoulos*, o.S.

6.8.2 Disruption durch Recht und Technologie

104 "Dieses – im positiven Sinne – ‚disruptive' Recht ist eines der modernen Elemente in der DSGVO".[168] "But it's a legal prescription, and not the technical reality".[169] Diese beiden Zitate verdeutlichen die heutige Diskrepanz zwischen Recht und Code, vermag das "disruptive Recht" die informationelle Selbstbestimmung der betroffenen Person doch kaum zu stärken. Dies auch im Hinblick auf die Lock-in-Effekte, für die es überhaupt erst geschaffen wurde.[170] Derzeit fehlt es somit nicht an einem disruptiven Recht sondern an einer disruptiven *Technologie*. Das DWeb ist aber umso disruptiver, als dass es dieses moderne Element des Rechts bereits wieder obsolet macht. Denn im DWeb wird jedem Datum ein URL zugeteilt, sodass es aufgrund dessen identifiziert werden kann (siehe oben Rz. 11). Oder in anderen Worten: "Things saved through one app are available in another: you never have to sync, because your data stays with you."[171] Damit entspricht die Datenportabilität im DWeb also der Zugangsgewährung für einen anderen Anbieter.

105 Folglich ist im DWeb weder eine indirekte Datenübermittlung i.S.v. Art. 20 Abs. 1 DSGVO noch eine direkte Datenübermittlung i.S.v. Art. 20 Abs. 2 DSGVO erforderlich. Hinsichtlich des Erfordernisses der Verarbeitung aufgrund einer Einwilligung (oder eines Vertrags) nach Art. 20 Abs. 1 lit. a DSGVO würden zwar kaum Probleme im DWeb auftreten. Jedoch wäre für das dezentralisierte Speichersystem irrelevant, ob eine Verarbeitung mit oder ohne automatisierte Verfahren (Art. 20 Abs. 1 lit. b DSGVO) erfolgen würde.[172] Doch letztlich sind dies bloss hypothetische Überlegungen über Erfordernisse, die aufgrund des Speichersystems ohnehin nicht mehr erfüllt werden müssten bzw. umgangen werden könnten.

106 Diese faktischen Umgehungsmöglichkeiten, welche auf der Eigeninitiative des Dateninhabers basieren, sind besonders deshalb problematisch, weil das Recht auf Datenportabilität nicht absolut gilt. Vielmehr wird es im Falle der Datenverarbeitung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art. 20 Abs. 3 Satz 2 DSGVO) oder aber bei Beeinträchtigung der Rechte und Freiheiten anderer Personen infolge der Geltendmachung eines Portabilitätsrechts (Art. 20 Abs. 4 DSGVO) ausgeschlossen.[173]

---

[168] *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 20 N 1.

[169] *Arnav Bansal*, An introduction to SOLID, Tim Berners-Lee's new, re-decentralized Web, 29. Oktober 2018, o.S.

[170] *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 20 N 1.

[171] *Solid*, Solid Explained, o.J., o.S.

[172] Da der Gesetzgeber mit diesem Erfordernis besonders die Portabilität der in Papierform gespeicherten Daten ausschliessen wollte, wäre dieses Erfordernis im DWeb freilich nicht von Bedeutung. *Herbst*, in: Kühling/Buchner, Art. 20 N 13 m.w.H.

[173] *Gernot Sydow/Maria Wilhelm*, in: Sydow, Art. 20 N 18 f.

6.8.3 Entgegenstehende öffentliche Interessen

107 Im ersten Fall ist massgeblich, dass die Daten von den betroffenen Personen bereitgestellt wurden, um für im öffentlichen Interesse liegende Aufgaben verwendet zu werden.[174] Die Bestimmung will damit verhindern, dass die Erfüllung der öffentlichen Aufgabe durch die Datenübertragung bzw. den Datenentzug erschwert wird.[175]

108 Infolge des dezentralisierten Speichersystems können im DWeb aber auch mehrere Zugangsberechtigte gleichzeitig auf den gleichen Datensatz zugreifen, sodass ein Hinzutreten eines neuen Zugangsberechtigten den Datenzugang des alten Zugangsberechtigten unberührt lässt.[176] Tritt der Staat zudem als Dienstleister in Erscheinung (z.B. Bürgerportale), so ist eine Datenportabilität aufgrund der wettbewerbsrechtlichen Prägung[177] des Rechts auf Datenportabilität ohnehin denkbar.[178] In Bezug auf das DWeb gilt hier anzumerken, dass die Datenautonomie aufgrund der geringeren Lock-in-Effekte den Wettbewerb zwischen den (staatlichen und/oder privaten) Anbietern von DApps ohnehin intensiviert.[179] Damit ist das dezentralisierte Speichersystem mit Art. 20 Abs. 3 Satz 2 DSGVO kompatibel.

6.8.4 Entgegenstehende Interessen Dritter

109 Im zweiten Fall der Beeinträchtigung der Rechte und Freiheiten anderer Personen ist relevant, dass eine betroffene Person nur diejenigen Daten portieren kann, die sich *ausschliesslich* auf ihre Person beziehen, da die Daten ansonsten ohne eine Rechtsgrundlage (insbesondere Einwilligung der anderen betroffenen Personen) portiert werden könnten.[180]

110 Da im DWeb die Portierung einer Zugangsgewährung für einen anderen Anbieter gleichkommt, müsste der Dateninhaber zusammen mit all den anderen betroffenen Personen über die erneute Zugangsgewährung entscheiden. Sollte im DWeb allerdings nur der Inhaber des datenerzeugenden Mittels (z.B. Fotokamera bei einem Gruppen-Selfie) auf die damit erzeugten Daten *alleine* zugreifen können, so wäre eine

---

174 *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 20 N 17.

175 *Wulf Kamlah* (kein Link), in: Kai-Uwe Plath (Hrsg.), BDSG/DSGVO, Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen von TMG und TKG, 2. Aufl., Köln 2016, Art. 20 N 14.

176 Technisch gesehen kann der Dateninhaber den Datenzugang des alten Zugangsberechtigten aber auch aufheben, weshalb zur Zweckerreichung von Art. 20 Abs. 3 Satz 2 DSGVO eine solche Zugangssperre rechtlich verboten und gegebenenfalls auch technisch erschwert werden sollte.

177 *Hans-Georg Kamann/Martin Braun*, in: Eugen Ehmann/Michael Selmayr (Hrsg.), DS-GVO: Kommentar, 2. Aufl., München 2018, Art. 20 N 3 m.w.H.

178 *Sydow/Wilhelm*, in: Sydow, Art. 20 N 16.

179 *Barabas/Narula/Zuckerman*, S. 31; *Harbinja/Karagiannopoulos*, o.S.

180 *Carlo Piltz*, in: Gola, Art. 20 N 40.

gemeinsame Ausübung der Datenautonomie ein interessanter Gedanke.[181] Denn die auf eine Zugangsgewährung folgende Datenverarbeitung kann neben den Grundrechten und Grundfreiheiten des Inhabers der Fotokamera in unserem Beispiel genauso die Grundrechte und Grundfreiheiten aller anderen betroffenen Personen verletzen.[182] Eine Reduktion der Rechte dieser betroffenen Personen auf die heutigen (weniger effektiven) Betroffenenrechte erscheint im Lichte des DWebs, das anders als die DSGVO eine weitreichende Datenautonomie zu gewähren vermag, nicht angezeigt.[183]

6.8.5 Zwischenfazit

111 Das DWeb ist umso disruptiver, als dass es das moderne Portabilitätsrecht bereits wieder obsolet macht. Zudem ist das dezentralisierte Speichersystem mit Art. 20 Abs. 3 Satz 2 DSGVO kompatibel. Letztlich sollte die Datenautonomie hinsichtlich eines Datums, das sich auf mehrere Personen bezieht, von diesen *gemeinsam* ausgeübt werden.

6.9 Datenübermittlung an Drittländer (Art. 44 ff. DSGVO)

112 In diesem letzten Unterkapitel soll der Blick von der EU auf den restlichen Teil der Welt ausgeweitet werden. Ein Drittlandtransfer von Daten kann aber nur dann erfolgen, wenn die Bestimmungen in Art. 44 ff. DSGVO eingehalten werden, sodass das hohe Datenschutzniveau der EU auch auf Drittländer ausgedehnt werden kann (sog. Transborder Data Flow).[184]

113 Da das (D)Web samt des in ihm implementierten Privacy by Design einen internationalen Charakter aufweist, fragt sich, ob dadurch ein weltweit ähnlich hohes Datenschutzniveau erreicht werden kann, sodass die Bestimmungen in Art. 44 ff. DSGVO weitestgehend obsolet werden würden. Dies wäre zumindest dann vorstellbar, wenn die DWeb-Architektur weltweit keine zu grossen Unterschiede hinsichtlich der Ausgestaltung des Privacy by Design aufweisen würde und auch keine sonstigen Gefahrenquellen (besonders im Bereich der organisatorischen Massnahmen) die Rechte der Dateninhaber – mehr als es die DSGVO zulässt – gefährden würden.

---

[181] Vgl. *Solid*, Take a Look under the Hood, o.J., o.S. wo bei "Shared Things" mehrere Personen als "Owner" aufgeführt sind.

[182] Problematisch ist in Anbetracht der (vorherrschenden) relativen Theorie über das Herstellen eines Personenbezugs allerdings, dass sich mit dem Zugriffswilligen auch die Gruppe der zur Zugriffsentscheidung befugten Personen ändern würde. Solid scheint dahingegen eher von einer Gruppe ähnlich einer Whatsapp-Gruppe auszugehen (wozu nicht alle betroffenen Personen gehören).

[183] Vgl. *Martin Munz*, in: Jürgen Taeger/Detlev Gabel (Hrsg.), DSGVO - BDSG: Kommentar, 3. Aufl., Frankfurt am Main 2019, Art. 20 N 53.

[184] 101. Erwägungsgrund der DSGVO.

114 In diesem Kontext ist jedoch die sog. Fragmentierung des Internets zu setzen. Die heutige nationale Regulierung bewirkt auf der Ebene der Internet-Dienste wie dem Web eine bloss oberflächliche Fragmentierung des Internets.[185] Dies etwa durch Zensur oder gar die Internet-Verfassung "Marco Civil da Internet" in Brasilien.[186] Wird die Fragmentierung in Zukunft aber auch die Internetinfrastruktur wie Standards oder Protokolle treffen, so besteht die Gefahr einer Vielzahl an Internet***s***, welche jeweils durch einen Gatekeeper kontrolliert und beherrscht werden.[187] Ob durch eine Dezentralisierung dieser Art die Vision eines "[…] dezentralisierten Fortschritt[s] von Ideen, Technologien, ja der Gesellschaft […]"[188] verwirklicht werden kann?

6.10 Zwischenfazit

115 Wie bereits einleitend zum Kapitel des Datenschutzrechts antizipiert, könnte das DWeb einen Paradigmenwechsel im Datenschutzrecht einläuten. Das Recht sollte daher als Hüter der Datenautonomie fungieren, verändert es doch die Machtverhältnisse zugunsten des Dateninhabers. Dies führt für den Dateninhaber neben einem verstärkten Schutz vor sich selbst auch zu einer grösseren Verantwortung (datenschutzrechtliche Selbstverantwortung) sowie zu seiner Schlüsselposition im Hinblick auf die Anwendbarkeit des Datenschutzrechts im Kontext des sachlichen Anwendungsbereichs.

116 Darüberhinaus könnte der Dateninhaber mit dem Zugriffswilligen die Modalitäten der Datenverarbeitung in einem Smart Privacy Contract festsetzen, sodass er die Datenverarbeitung besser kontrollieren und wenn nötig auch eingreifen kann. Allerdings könnte der Dateninhaber auch von einer solchen Zugangsgewährung absehen und bei einem rechtlich nicht durchsetzbaren Datenzugang seine Daten in ausschliessliche Positionen überführen.

117 In Bezug auf das Recht auf Löschung wird abzuwarten sein, wem die Zensurpflicht zugewiesen wird. Nicht auszuschliessen ist immerhin, dass der Dateninhaber seine Daten eigenständig (auch im Versionensystem) löschen könnte. Darüberhinaus wird das primäre Ziel des Portabilitätsrechts – der Anbieterwechsel – durch das dezentralisierte Speichersystem selbst erreicht. Interessant wäre hierbei die Konstellation der gemeinsamen Ausübung der Datenautonomie. Letztens wurde im Zusammenhang mit der Datenübermittlung in Drittländer auch auf die

---

185 *Daniel Voelsen*, Risse im Fundament des Internets: Die Zukunft der Netz-Infrastruktur und die globale Internet Governance, SWP-Studie, Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit, 12/2019, S. 27.

186 So bereits *Hannes Grassegger*, Staaten steigen aus dem Web aus, in: NZZ vom 9. Februar 2014, o.S.

187 *Voelsen*, S. 27 ff.

188 Siehe oben das Zitat bei Rz. 1.

Fragmentierung des Internets hingewiesen, welche die Potentiale des (D)Webs erheblich eindämmen könnten.

7 Schlussfazit

118 Das DWeb gewährt dem Dateninhaber eine weitreichende Autonomie hinsichtlich Speicherort und Zugang zu seinen Daten (Datenautonomie). Je nachdem wie die DWeb-Architektur aber technisch reguliert wird, ist sie Fluch oder Segen für die Durchsetzbarkeit des Rechts. Doch das DWeb wirkt sich speziell auch auf das Wettbewerbsrecht, das Urheberrecht und das Datenschutzrecht aus.

119 In Bezug auf das Wettbewerbsrecht wird von entscheidender Bedeutung sein, ob sich das DWeb samt DApps überhaupt gegenüber dem aktuellen Web und Apps wird durchsetzen können. Dabei ist besonders das Privacy Paradox zu berücksichtigen. Doch selbst wenn sich das DWeb durchsetzen sollte, könnte in Zukunft immer noch eine politische Re-Zentralisierung des Webs erfolgen.

120 Die Durchsetzung des Urheberrechts erfolgt im DWeb – neben dem DRM und den Smart Contracts – auch mit der Datenautonomie. Probleme bereiten dabei die Anonymität des Urheberrechtsverletzers, die erschwerten Löschmöglichkeiten nach einer Urheberrechtsverletzung und das vollständige Löschen in einem dezentralisierten Speichersystem. Als vorteilhaft erweist sich besonders die grössere Unabhängigkeit des Dateninhabers bzw. des Urhebers gegenüber Intermediären wie Verlagen.

121 Zum Schluss wurde in diesem Sheet in vertiefter Weise auf das Datenschutzrecht eingegangen. Der Datenautonomie kommt auch hier eine zentrale Wichtigkeit zu, stosst sie doch einen Paradigmenwechsel im Datenschutzrecht infolge der veränderten Machtverhältnisse zwischen betroffener Person bzw. Dateninhaber und Verantwortlicher bzw. Zugangsberechtigter an. Indem die Datenautonomie der betroffenen Person eine grössere Autonomiesphäre gewährt, vergrössert sich auch ihre Verantwortung mitsamt der Notwendigkeit eines Schutzes vor sich selbst. Ausdruck ihres Autonomiebereichs ist besonders der Smart Privacy Contract. Die Datenautonomie könnte so das aktuelle Spannungsverhältnis zwischen dem Code, der Datenmissbräuche infolge der praktisch unbeschränkten Datenzugriffe überhaupt erst ermöglicht, und dem Datenschutzrecht, das solche Missbräuche gerade unterbinden will, durchaus entspannen. Letztlich könnte es sich so zu einem Komplementaritätsverhältnis wandeln, denn Code und Recht sollten gemeinsam – zwecks Datenschutz – regulieren. Ausserhalb ihrer Autonomiesphäre muss die betroffene Person zur Durchsetzung ihrer Betroffenenrechte allerdings wie heute über das Datenschutzrecht auf die Datenautonomie des Verantwortlichen zurückgreifen.

Dadurch kommt nicht dem Code sondern dem Recht eine ausgleichende Wirkung im Machtverhältnis zwischen der betroffenen Person und dem Verantwortlichen zu.

122 Indem sich der Autonomieraum der betroffenen Person ausweitet, nimmt er auch einen Teil des Autonomiebereichs des Verantwortlichen ein. Da Letzterer im Rahmen des Datenschutzrechts die Daten in seinem eigenen Interesse *und* im öffentlichen Interesse der Gesellschaft bearbeiten darf, könnten beide Interessen durch die Datenautonomie, die auch auf egoistische Weise ausgeübt werden kann, unterminiert werden. Die Architektur des DWebs ermöglicht dem Dateninhaber somit nicht nur seine Daten vor dem Staat zu verbergen, sondern sie bietet ihm auch die Gelegenheit, seine Daten als wertvollste Ressource der Welt vom Wirtschaftsverkehr abzukoppeln. Daten sind jedoch keine Güter des ausschliesslichen persönlichen Gebrauchs, sondern sie sollen im Dienste der Menschheit stehen. In Anbetracht des Privacy-Paradox liegt der Problempunkt aber gerade nicht in einer Zugangsverweigerung sondern in einer sorglosen Zugangs*gewährung*, die schlimmstenfalls zur Autonomielosigkeit des Dateninhabers führt. Im Sinne des Schutzes vor sich selbst soll ein solches autonomiezerstörendes Verhalten durch das Datenschutzrecht bis zu einem gewissen Grad unterbunden werden.

123 **Die Datenautonomie löst damit nur die technische Seite des Datenmissbrauchs, übrig bleibt das soziale Problem des sorglosen Handelns.** Nach dem Spannungsverhältnis zwischen Datenschutzrecht und Code gilt es nun dasjenige zwischen Datenschutz und sorglosem Handeln zu entschärfen.

~ The future is still so much bigger than the past.[189] *~*

[189] *Tim Berners-Lee*, One Small Step for the Web…, in: Medium vom 29. September 2018, o.S.

Abbildungsverzeichnis

Abbildung 1: Sir *Tim Berners-Lee* (siehe Rz. 4).
Quelle: Wikimedia Commons (*Paul Clarke*).

Abbildung 2: "Trusted Solid App" und Datenzugang zum "POD" (siehe Rz. 15).
Quelle: www.inrupt.com/solid.

Abbildung 3: Auf einen Pathetic Dot einwirkende Kräfte (siehe Rz. 21).
Quelle: *Lessig*, S. 123.

Letzter Abruf der Quellen

Die Quellen wurden zuletzt am 12. Februar 2020 abgerufen. Ausnahmen wurden in der jeweiligen Fussnote gekennzeichnet.

Version

2.0.