AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.10
www.austrian-law-journal.at

# Digitalisierung und Selbstbestimmung

**Iris Eisenberger,*** Universität für Bodenkultur Wien

***Kurztext**: Der Beitrag beleuchtet das Verhältnis von Digitalisierung und Recht. Am Beispiel der Blockchain-Technologie wird aufgezeigt, wie neue Formen und Räume der Selbstbestimmung geschaffen werden können. In distribuierten Systemen ist die Tendenz erkennbar, dass sich die rechtliche hin zu einer technologischen Steuerung verlagert. Wenn Funktionen, die für gewöhnlich der demokratisch legitimierte Gesetzgeber wahrnimmt, auf andere Systeme übergehen, führt dies zu Herausforderungen für rechtsstaatliche Demokratien. Fundamentale Fragen von Kontrolle und Machtbeschränkung iZm Digitalisierung stehen im Fokus. Der Beitrag plädiert schließlich für „legal foresight"-Forschung im Bereich neuer Technologien.*

***Schlagworte:** Blockchain-Technologie; distribuierte Systeme; dezentralisierte Systeme; zentralisierte Systeme; natürliche Person; juristische Person; elektronische Person; Verantwortung und Zurechnung; Demokratie.*

## I. Einleitung[1]

Seit Jahrzehnten ist in den Rechtswissenschaften davon die Rede, dass durch Digitalisierung Selbstbestimmung verloren gehe.[2] Die Antithese, nämlich dass Digitalisierung neue Formen und Räume der Selbstbestimmung eröffnet, ließe sich ebenso begründet aufstellen. Die Frage, wie selbst- oder fremdbestimmt wir sind, adressiert das Kernproblem der Digitalisierung mE jedoch nicht. Digitalisierung führt dazu, dass Funktionen, die in rechtsstaatlichen Demokratien für gewöhnlich der demokratisch legitimierte Gesetzgeber und das Recht übernehmen,[3] zunehmend

* Univ.-Prof. Dr. Iris *Eisenberger*, MSc (LSE) ist Universitätsprofessorin und Leiterin des Instituts für Rechtswissenschaften der Universität für Bodenkultur Wien.

1 Für zahlreiche wertvolle Diskussionen danke ich Tina *Ehrke-Rabel*, Elisabeth *Hödl* und Konrad *Lachmayer*. Für die Unterstützung bei der Recherche und Ergänzung des Fußnotenapparats danke ich Franziska *Bereuter*, Sophie *Schmidt* und Lisa *Schranz*.

2 Siehe *Helbing et al*, Digitale Demokratie statt Datendiktatur, in *Könneker* (Hrsg), Unsere digitale Zukunft (2017) 3; *Spiecker,* Steuerung im Datenschutzrecht – Ein Recht auf Vergessen wider Vollzugsdefizite und Typisierung? Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaften 2014, 28; *Thiesse,* Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung, in *Fleisch/Mattern* (Hrsg), Das Internet der Dinge (2005) 363.

3 Vgl *I. Eisenberger*, Zwischen Rechtswissenschaften und Life Sciences (in Druck); Zur Konfliktkanalisierungsfunktion des Rechts im Bereich von Risikotechnologien siehe *Stelzer*, Sicherheit durch Recht oder Rechtssicherheit? FORUM 1993, 56; Zur Steuerungsfunktion des Rechts siehe *Mayntz*, Soziale Dynamik und politische Steuerung: Theoretische und methodische Überlegungen (1997); Zur Funktion des Rechts als Ordnungs- und Friedenstifter siehe nur *Kelsen*, Reine Rechtslehre[2] (1960) 38 f.

**Fundstelle:** *Eisenberger*, Digitalisierung und Selbstbestimmung, ALJ 2/2017, 140–149 (http://alj.uni-graz.at/index.php/alj/ article/view/112).

durch andere Systeme wahrgenommen werden.[4] Die idR verfassungsrechtlich etablierte Kontrolle von Macht und die Vorbeugung von Machtmissbrauch[5] laufen damit zunehmend ins Leere.[6] Neue „Eliten", wie beispielsweise Software-EntwicklerInnen, etablieren mit ihren technologischen Innovationen gesellschaftliche Ordnungssysteme,[7] in denen sich regelmäßig die Werthaltungen der Programmierer widerspiegeln[8] und nicht die eines im demokratischen System errungenen gesellschaftlichen Konsenses. Dieser Beitrag zeichnet daher zunächst die Digitalisierung als eine recht(swissenschaft)liche Verlustgeschichte nach (II.), in weiterer Folge zeigt er anhand der Blockchain-Technologie, dass Digitalisierung auch neue Formen und Räume der Selbstbestimmung ermöglicht (III.), bevor er erörtert, ob digitalisierte, distribuierte Systeme von rechtlicher zu technologischer Steuerung führen (IV.) und vor welche Herausforderungen dieser Wandel demokratische Rechtssysteme stellt (V.) sowie schließlich, was daraus folgt (VI.).

## II. Digitalisierung: Eine recht(swissenschaft)liche Verlustgeschichte der Selbstbestimmung

Die Frage, wie sich die Digitalisierung auf die Selbstbestimmung auswirkt, lässt sich leicht als recht(swissenschaft)liche Verlustgeschichte der Selbstbestimmung erzählen. Bereits Ende der 1960er Jahre steht im Mikrozensusbeschluss des deutschen Bundesverfassungsgerichts[9] zu lesen, dass es mit der Menschenwürde unvereinbar wäre, wenn der Staat Menschen zwangsweise gesamthaft registriert und katalogisiert und er sie in seiner Bestandsaufnahme wie Sachen behandelt;[10] daran würde auch eine anonym durchgeführte statistische Erhebung nichts ändern. Zugleich betonte das Bundesverfassungsgericht jedoch, dass *„[n]icht jede statistische Erhebung über Persönlichkeits- und Lebensdaten […] die menschliche Persönlichkeit in ihrer Würde [verletzt] oder […] ihr Selbstbestimmungsrecht im innersten Lebensbereich [berührt],"*[11] weshalb es die im Gesetz über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens (Mikrozensus) vom 16. 3. 1957[12] angeordnete Repräsentativbefragung zum Tatbestand „Urlaubs- und Erholungsreisen" als mit den Grundgesetz vereinbar erklärte.

4 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, Bitcoin-Miner als Prosumer: Eine Frage staatlicher Regulierung? Dargestellt am Beispiel des Glücksspielrechts, ALJ 2017 (in Endredaktion); *I. Eisenberger*, Innovation im Recht (2016) 152 ff; *Gruber/I. Eisenberger*, Wenn Fahrzeuge selbst lernen: Verkehrstechnische und rechtliche Herausforderungen durch Deep Learning? in *I. Eisenberger/Lachmayer/G. Eisenberger* (Hrsg), Autonomes Fahren und Recht (2017) 51; *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin and Cryptocurrency Technologies (2016) 282 f; *D. Tapscott/A. Tapscott*, Blockchain Revolution (2016) 271 ff.

5 Siehe *Adamovich/Funk/Holzinger/Frank*, Österreichisches Staatsrecht IV (2009) 10.

6 Siehe *I. Eisenberger*, Innovation 160.

7 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion); *Gruber/I. Eisenberger* in *I. Eisenberger/Lachmayer/G. Eisenberger* 51.

8 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 3/2017 (in Endredaktion).

9 BVerfGE 27, 1 ff.

10 *„Es widerspricht der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen (vgl BVerfGE 5, 85 [204]; 7, 198 [205])"* BVerfGE 27, 1 (4). Demgegenüber werden „Maschinen" heute zunehmend wie Menschen behandelt; siehe *Beck,* Über Sinn und Unsinn von Statusfragen – zu Vor- und Nachteilen der Einführung einer elektronischen Person, in *Günther/Hilgendorf* (Hrsg), Roboter und Gesetzgebung (2013) 239; *Calo,* Robotics and the Lessons of Cyberlaw, Californian Law Review 2015, 513; *Hubbard,* "Do Androids Dream?" Personhood and Artificial Artefacts, Temple Law Review 2010, 405; *Kersten,* Relative Rechtssubjektivität – Über autonome Automaten und emergente Schwärme, Zeitschrift für Rechtssoziologie 2017, 8; *Müller-Hengstenberg/Kirn,* Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems? MMR 2014, 307; *Schirmer,* Rechtsfähige Roboter? JZ 2016, 660; *Solum,* Legal Personhood for Artificial Intelligence, North Carolina Law Review 1992, 1231; *Teubner,* The Rights of Non-Humans: Electronic Agents and Animals as New Actors in Politics and Law, Journal of Law and Society 2006, 497.

11 BVerfGE 27, 1 (4).

12 dBGBl 1957/213.

Zählen, Registrieren und Katalogisieren beschäftigte die Gerichte immer wieder. Zentral ist dabei das Volkszählungsurteil des Bundesverfassungsgerichts. In seiner Entscheidung vom 15. 12. 1983[13] sprach das Gericht erstmals von einem Grundrecht auf informationelle Selbstbestimmung. Anlass dafür war das Volkszählungsgesetz 1983.[14] Über eine Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung sollten sämtliche EinwohnerInnen der Bundesrepublik Deutschland statistisch erfasst werden.[15] Nicht zuletzt die Furcht vor unkontrollierbarer Persönlichkeitserfassung führte zu den entscheidungsursächlichen Verfassungsbeschwerden.[16] Im Ergebnis entschied das Bundesverfassungsgericht, dass die *„[f]reie Entfaltung der Persönlichkeit […] unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus[setzt]. […] Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."*[17] Begründend führte das Bundesverfassungsgericht ua aus, dass technologische Innovationen die menschliche Persönlichkeit zunehmend gefährden, da sie es ermöglichen würden, vollständige Persönlichkeitsbilder zu erstellen und dies weitgehend unkontrollierbar durch die jeweils Betroffenen.[18]

Die Digitalisierung ermöglicht nicht nur, Personen umfassend zu zählen, zu registrieren und zu katalogisieren, sondern auch Personen und ihre Handlungen zu überwachen sowie die dabei eruierten Daten zu speichern und zu archivieren.[19] Überwachung dient dabei der Gewährleistung rechtskonformen Verhaltens einerseits und der Vorbeugung von Straftaten andererseits. Die zuvor erörterte, durch das deutsche Bundesverfassungsgericht konstatierte Gefährdung der freien Persönlichkeitsentfaltung und Selbstbestimmung trifft auf die vielfachen Überwachungsmöglichkeiten ebenfalls zu; auch diese haben die Gerichte in unterschiedlicher Weise beschäftigt.

Der österreichische VfGH prüfte beim Section-Control-Erkenntnis[20] das automatische Geschwindigkeitsmesssystem[21] auf seine Verfassungskonformität. Im Ergebnis hielt er die Datenermittlung und -verwendung zwar für zulässig, allerdings nicht flächendeckend und nur zweckgebunden, zur *„Überwachung der Einhaltung straßenpolizeilicher Vorschriften"*.[22] Diese Zweckbindung verpflichtet auch dazu, dass das Geschwindigkeitsmesssystem schon technologisch so gestaltet sein muss, dass unzulässig aufbewahrte Daten unverzüglich zu löschen sind.[23] Darüber hinaus ist die Überwachung auch vor Ort anzukündigen.[24] Ähnlich wie in den zuvor erörterten Entscheidungen des

13 BVerfGE 65, 1 ff.
14 Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung, dBGBl I 1982/369.
15 *„Mit der Volkszählung und Berufszählung werde ein vielfältiges Strukturbild der Bevölkerung in tiefer regionaler Gliederung gewonnen."* BVerfGE 65, 1 (11); siehe nur *Mendes,* Schutz vor Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung (2015) 24.
16 BVerfGE 65, 1 (3).
17 BVerfGE 65, 1 (31).
18 BVerfGE 65, 1 (30 f).
19 Für die Herausforderungen, die sich bei digitaler Überwachung im Namen von Anti-Terrormaßnahmen stellen siehe *Lachmayer/Witzleb*, The challenge to privacy from ever increasing state surveillance: a comparative perspective, UNSW Law Journal 2014, 748.
20 VfGH 15. 6. 2007, G 147/06 ua, 3.
21 § 100 Abs 5 b StVO 1960, BGBl 1960/159 idF BGBl I 2002/80 sowie des § 134 Abs 3 b Satz 1 Kraftfahrgesetz 1967, BGBl 1967/267 idF BGBl I 2002/80.
22 VfGH 15. 6. 2007, G 147/06 ua, 22.
23 VfGH 15. 6. 2007, G 147/06 ua, 22.
24 VfGH 15. 6. 2007, G 147/06 ua, 25. Mittlerweile haben die Sicherheitsbehörden gem § 54 Abs 6 Sicherheitspolizeigesetz, BGBl 1991/566 idF BGBl I 2017/130, die Möglichkeit, den öffentlichen Raum präventiv zu überwachen, dabei können sie Verkehrsdaten aus der Section Control verwenden.

Bundesverfassungsgerichts, lässt er die gegenständliche Datensammlung nur in eingeschränkter Weise zu. Auch wenn die Gefährdung der freien Persönlichkeitsentwicklung und der Selbstbestimmung vom VfGH nicht begründend herangezogen werden, ist naheliegend, dass die rechtsdogmatisch in erster Linie datenschutzrechtlich begründete Entscheidung auch dem Schutz der Selbstbestimmung gilt.[25]

Überwachen, Speichern und Archivieren spielen aber insbesondere bei der Aufklärung und Vorbeugung von Straftaten eine große Rolle und sie beschäftigten die Gerichte ebenfalls. Gegenstand höchstgerichtlicher und kontroversieller Entscheidungen waren dabei verschiedene Formen der Telekommunikationsüberwachung/Vorratsdatenspeicherung,[26] GPS-Überwachung,[27] Onlinedurchsuchung[28] oder automatisierte Kennzeichenerfassung.[29] Im Kern geht es bei all diesen Entscheidungen abermals um die grundrechtlich geschützte freie Persönlichkeitsentfaltung und Selbstbestimmung, die durch die Digitalisierung zunehmend gefährdet sind. Tenor der Entscheidungen ist, dass es einen unantastbaren Kernbereich höchstpersönlicher Lebensgestaltung gibt[30] und dass Befugnisse, die tief in das Privatleben hineinreichen und es ermöglichen, umfassende Persönlichkeitsprofile zu erstellen bzw verborgene Ermittlungsmethoden einsetzen, verfahrensrechtliche Vorkehrungen für einen effektiven Grundrechtsschutz benötigen.[31] Im Ergebnis dürfe auch die Kriminalitätsbekämpfung nicht dazu führen, dass Personen Erlebnisse höchstpersönlicher Art nicht mehr zum Ausdruck bringen können.[32]

Digitalisierung wird auch zum Sammeln von Daten genutzt, mit dem Ziel, diese miteinander zu verknüpfen und zu vergleichen. Dies geschieht beispielsweise bei der Rasterfahndung, bei der personenbezogene Daten miteinander abgeglichen werden, um jene Personen ermitteln zu können, welche für die Ermittlung relevante Merkmale aufweisen.[33] Das Bundesverfassungsgericht hält eine solche nur dann für zulässig, wenn eine konkrete Gefahr für hochrangige Rechtsgüter besteht, für eine Rasterfahndung im Vorfeld der Gefahrenabwehr bleibt jedenfalls kein Platz.[34]

Dieser Streifzug durch einschlägige Judikatur zeigt deutlich, dass der Verlust der Selbstbestimmung und der Schutz derselben seit den 1960er Jahren immer wieder Gegenstand höchstgerichtlicher Judikatur waren. Die zunehmende Digitalisierung und ihr staatlicher Einsatz lassen die Bereiche persönlicher Entfaltung und Selbstbestimmung enger werden. Neuere Entwicklungen, wie beispielsweise das Internet der Dinge, das Sensoren allgegenwärtig macht,[35] Big Data Analy-

25 Siehe idZ auch VfGH 27. 6. 2014, G 47/2012 ua.

26 BVerfGE 113, 348; BVerfGE 141, 220; VfGH 27. 6. 2014, G 47/2012 ua; EuGH 8. 4. 2014, C-293/12 ua, *Digital Rights Ireland und Seitlinger*.

27 BVerfG 12. 4. 2005, BVerfGE 112, 304 ff; U.S. Supreme Court 23. 1. 2012, 10-1259, *United States vs Jones.*

28 BVerfGE 120, 274 ff.

29 BVerfGE 120, 274 (378).

30 BVerfGE 113, 348 Rz 161; BVerfGE 112, 304 Rz 56.

31 BVerfGE 112, 304 Rz 61; BVerfGE 141, 220; EGMR 6. 12. 1978, 5029/71, *Klass vs Deutschland;* VfGH 27. 6. 2014, G 47/2012 ua.

32 BVerfGE 141, 220 Rz 121.

33 BVerfGE 115, 320 Rz 2.

34 BVerfGE 115, 320, Leitsatz 1.

35 Siehe nur *Christl*, Kommerzielle digitale Überwachung im Alltag, Studie im Auftrag der österreichischen Bundesarbeiterkammer (2014) 70; *Keller/Pütz/Siml*, Internet der Dinge, in *Mehler-Bichler/Steiger* (Hrsg), Trends in der IT 2012 (2012) 121; *Mattern/Flörkemeier*, Vom Internet der Computer zum Internet der Dinge, Informatik Spektrum 2010, 119; *Pohl,* Der bürgerliche Traum von digitaler Souveränität: Technische Bemerkungen zur völligen Unsicherheit digitaler Kommunikation, in *Friedrichsen/Bisa* (Hrsg), Digitale Souveränität, Vertrauen in der Netzwerkgesellschaft (2016) 11.

sen,[36] die die Vernetzung, Auswertung und Nutzung unterschiedlicher Daten quantitativ und qualitativ auf eine andere Ebene heben sowie algorithmische Entscheidungen in beinahe allen Lebensbereichen,[37] bringen zusätzliche Gefahren für eine Gesellschaft freier und selbstbestimmter Personen; eine Gesellschaft, die die Judikatur der letzten Jahrzehnte zumeist vergeblich versuchte zu schützen.[38] Neu an diesen Gefahren ist jedenfalls, dass sie vorerst kaum vom Staat selbst ausgehen,[39] sondern von Privaten. Private gefährden mit diesen Technologien die Privatsphäre anderer und manipulieren, diskriminieren und unterdrücken potenziell die technologienutzenden Personen.[40] Verknüpft man all diese Innovationen, lassen sich auch potentielle Verhaltensmuster einzelner Personen und Personengruppen vorhersagen.[41] Es braucht nicht allzu viel Phantasie, um zu erkennen, dass diese Entwicklungen den Raum für freie Persönlichkeitsentfaltung und Selbstbestimmung zusätzlich enger werden lassen.[42] Noch kleiner werden sie, wenn sich nicht ausschließlich Private, sondern zunehmend auch der Staat dieser Technologien bedient.

## III. Blockchain-Technologien: Neue Formen und Räume der Selbstbestimmung

Die Geschichte der Digitalisierung und Selbstbestimmung ließe sich auch anders erzählen, nicht wie zuvor als Verlustgeschichte, sondern als eine, die neue Formen und Räume der Selbstbestimmung ermöglicht. Die, der Kryptowährung Bitcoin zugrunde liegende, Blockchain-Technologie verspricht beispielsweise in ihrer Geburtsstunde ein Mehr an Selbstbestimmung.[43]

Die Blockchain-Technologie lässt sich für viele unterschiedliche Anwendungen instrumentalisieren. Verschiedene Informationen lassen sich damit speichern und verwalten, beispielsweise

36 Siehe nur *Martini,* Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, 1481; *Weichert,* Big Data, Gesundheit und der Datenschutz, DuD 2014, 831.

37 Siehe nur *Finn,* What Algorithms Want: Imagination in the Age of Computing (2017); *Hofstetter,* Wenn intelligente Maschinen die digitale Gesellschaft steuern, in *Könneker* (Hrsg), Unsere Digitale Zukunft (2017) 37; *Lessig,* Code: Version 2.0, Basic Books (2006) 200 ff; *Nyholm/Smids,* The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem?, Ethical Theory and Moral Practice 2016, 1275; *Reichwald/Pfisterer,* Autonomie und Intelligenz im Internet der Dinge: Möglichkeiten und Grenzen autonomer Handlungen, CR 2016, 209; *Skistims/ Voigtmann/David/Roßnagel,* Datenschutzgerechte Gestaltung von kontextvorhersagenden Algorithmen, DuD 2012, 31.

38 Sobald es neue Technologien gibt, werden sie auch eingesetzt und die bestehenden rechtlichen Schutzmaßnahmen erweisen sich regelmäßig als unzulängliche Schutzinstrumentarien. Kritisch dazu *Spiecker,* Zur Zukunft systemischer Digitalisierung – Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen. Warum für die systemische Haftung ein neues Modell erforderlich ist, CR 2016, 699; *Cockfield,* Towards a Law and Technology Theory, Manitoba Law Journal 2004, 383 (405); ferner *Reidenberg*, Lex Informatica: The Formulation of Information Policy Rules through Technology, Texas Law Review 1998, 554.

39 Freilich werden neue Technologien auch von Staaten eingesetzt und gefährden eine Gesellschaft freier BürgerInnen. Siehe dazu stellvertretend für Vieles die Diskussion um den Einsatz unbemannter Drohnen. *Schöberl,* „Global Battlefield?" Drohnen und der geographische Anwendungsbereich des humanitären Völkerrechts, in *Gramm/ Weingärtner* (Hrsg), Moderne Waffentechnologie (2015) 120–131; *Mützenich/Bieger,* Wege des völkerrechtlichen Umgangs mit Kampfdrohnen, S&F 2014, 25; *Löffelmann,* Der Einsatz von Kampfdrohnen zur Terrorismusbekämpfung im Schnittpunkt von humanitärem Völkerrecht und Menschenrechtsstandards, KJ 2013, 372; *Zimmermann,* Völkerrechtliche Fragen des Einsatzes bewaffneter Drohnen, MRM 2013, 96.

40 Siehe *Weichert*, Big Data und Datenschutz, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 1.

41 Siehe *Martini,* Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, 1481.

42 Siehe idZ auch *Martini,* DVBl 2014, 1481.

43 Vgl *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf (zuletzt abgefragt am 13. 11. 2017).

Transaktionen, Verträge oder Rechte.[44] Die Blockchain ist eine, unzählige Male replizierte, digitale Datenbank, in der alle Transaktionen eines bestimmten Netzwerkes gespeichert werden. Die Netzwerkteilnehmenden sind miteinander verbunden, in einem sog Peer-to-Peer-Netzwerk. Die jeweiligen Transaktionen werden dabei vereinfacht gesagt, wie einzelne Glieder in einer Kette aneinandergereiht. Die getätigten Transaktionen werden auf jedem Knoten, der Teil des Netzwerkes ist, eins zu eins abgebildet. Die Daten werden demnach nicht zentral gespeichert und verwaltet, sondern verteilt auf alle Netzwerkteilnehmenden.[45]

Weil die Blockchain auf allen teilnehmenden Knoten abgespeichert wird, gilt sie als besonders sichere Technologie, da Änderungen bei allen TeilnehmerInnen zugleich erfolgen müssen.[46] Um die Identität und die Daten der Netzwerkteilnehmenden zu schützen, sind sie pseudonymisiert.[47] Die der Blockchain zugrunde liegende Software ist Open Source, also für alle transparent und gleichermaßen zugänglich.[48]

Die meisten webbasierten Software-Applikationen arbeiten auf der Grundlage eines zentral organisierten Server/Client-Modells. Dabei wird der Informationsfluss von einer zentralen Stelle aus verwaltet und kontrolliert. Die bekanntesten NutzerInnen dieses Modells sind beispielsweise Facebook, Google und Amazon. Dezentralisierte Systeme sind hingegen Systeme, in denen der Informationsfluss nicht von einer zentralen Stelle aus verwaltet wird, sondern von einigen, wenigen Knotenpunkten. Distribuierte Systeme sind demgegenüber Systeme, bei denen der Informationsfluss von allen Teilnehmenden zugleich verwaltet und kontrolliert wird.[49]

Eine der Besonderheiten der Blockchain-Technologie ist, dass sie keine zentral verwaltete Datenbank ist, sondern als distribuierte Datenbank angedacht ist.[50] Dies trifft jedenfalls auf die Konsensbildung bei der Kryptowährung Bitcoin zu, zu der alle System-TeilnehmerInnen gleichermaßen beitragen können.[51] Das Bitcoin-Mining ist ebenfalls distribuiert konzipiert und wäre theoretisch allen NetzwerkteilnehmerInnen möglich; aufgrund der hohen Kosten, die mit dem Bitcoin-Mining verbunden sind, lassen sich in der Praxis Tendenzen hin zu einem dezentralisierten System beobachten.[52] Der Code selbst kann hingegen als ein zentralisiertes Element des Systems betrachtet werden.

44 Siehe nur *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

45 Zur Blockchain-Technologie und den verschiedenen Anwendungsmöglichkeiten siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion); *Raval*, Dezentralized Applications (2016); *D. Tapscott/A. Tapscott*, Blockchain; *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin, mit jeweils weiteren Hinweisen.

46 Kritisch zur vermeintlichen Sicherheit siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

47 *Ehrke-Rabel/Hödl,* Effizienter Steuervollzug im Lichte des Datenschutzes, in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht (2016) 231 (253 f); *Diedrich*, Ethereum 126.

48 Die Software für Etherum ist etwa direkt auf der Homepage zugänglich: https://www.ethereum.org (zuletzt abgefragt am 13. 11. 2017).

49 Siehe idZ *Raval*, Dezentralized Applications 2 ff.

50 Vgl *Nakamoto*, Bitcoin.

51 Siehe *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin 28 f.

52 Siehe *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin 272 ff. (De)Zentralisierung entsteht beispielsweise auch durch Wallets und Börsen.

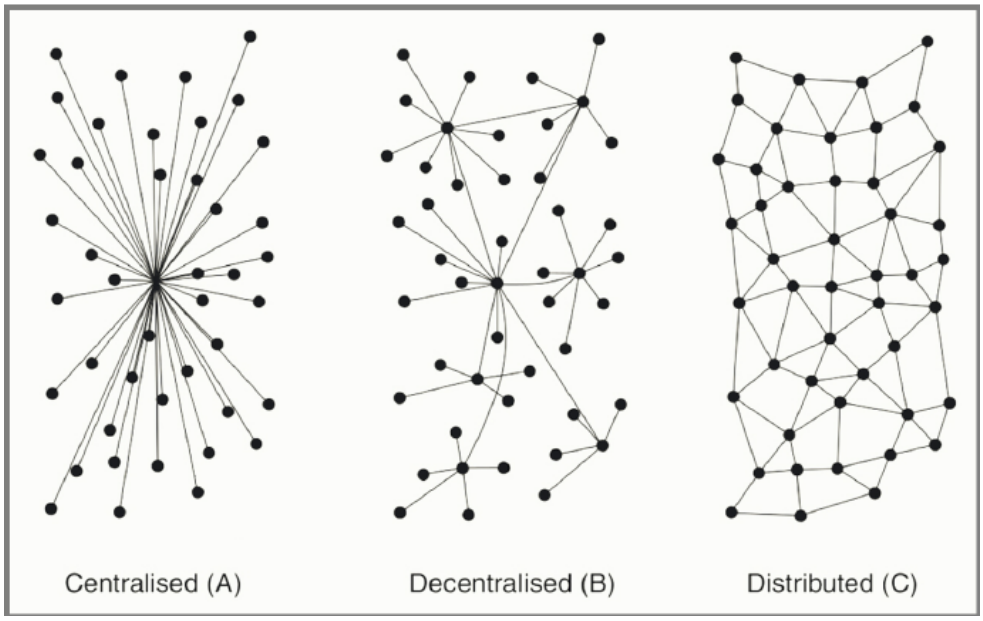


**Abb 1:** Centralised, decentralised and distributed network models[53]

Digitale Online-Datenbanken, an denen man nur verschlüsselt teilnehmen kann und die nicht zentral, sondern von allen Teilnehmenden verwaltet werden, bauen die Privatsphäre aus.[54] Aufgrund der Pseudonymisierung in der Blockchain sind die gesammelten Daten kaum rückverfolgbar,[55] ebenso schlecht lassen sich die Aktivitäten in einer privat aufgesetzten Blockchain aufgrund der mangelnden zentralisierten Verwaltung staatlich überwachen oder kontrollieren. All dies eröffnet neue Formen der Persönlichkeitsentfaltung und technologisch geschützte Räume der Selbstbestimmung. Anders als die zuvor erzählte Verlustgeschichte lässt sich die zunehmende Digitalisierung demzufolge auch als Geschichte eines Selbstbestimmungsgewinns erzählen.

Nicht übersehen werden darf in diesem Zusammenhang aber, dass Software das Verhalten seiner NutzerInnen normiert.[56] NutzerInnen können nur in den Grenzen des Codes agieren. Der Code lässt sich, im Unterschied zu rechtlichen Normen, nur mit Spezialwissen umgehen oder brechen. Der Code wirkt insofern ähnlich wie eine Bremsschwelle auf der Straße, sie zwingt die FahrerIn zu einem Bremsmanöver und verringert dadurch den persönlichen Handlungsspielraum. Der der Blockchain zugrunde liegende Code schafft in diesem Sinn nicht nur Räume der persönlichen Entfaltung und Selbstbestimmung, sondern engt diese auch ein, je nach Ziel des Systems in unterschiedlicher Intensität. Die Seratio Blockchain beispielsweise strebt die Messbarkeit immaterieller Werte an, etwa Liebe, Freundlichkeit, Freiheit oder Religion.[57] Werte wie diese, die unwiderrufbar und unlöschbar in einer Blockchain festgehalten werden, können die Freiheit und die Selbstbestimmung der NutzerInnen nachhaltig einschränken. Die Frage nach dem Verlust von oder dem Gewinn an Selbstbestimmung erscheint dann aber falsch gestellt. Die Frage

53 *Baran,* On distributed communications: I. Introduction to distributed communications network (1964) 2.
54 Siehe idZ *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin 168 ff.
55 Siehe *Ehrke-Rabel/Hödl* in *Jahnel* 231.
56 Grundlegend zur normativen Qualität technologischer Systeme siehe *Winner*, Do Artifacts Have Politics? in *Daedalus* (Hrsg), Modern Technology: Problem or Opportunity (1980), https://transitiontech.ca/pdf/Winner-Do-Artifacts-Have-Politics-1980.pdf (zuletzt abgefragt am 19. 7. 2017) 121.
57 Siehe http://www.the-blockchain.com/docs/Seratio%20Blockchain%20Whitepaper%20%2826%20October%202016%29%20%5bv1.2%5d.pdf (zuletzt abgefragt am 12. 11. 2017).

ist nicht mehr, ob wir fremd oder selbst bestimmt sind, sondern woher wir überhaupt wissen, wer bestimmt bzw wie wir diejenigen, die bestimmen, wieder sichtbar und verantwortlich machen.

## IV. Digitalisierte distribuierte Systeme: Von rechtlicher zu technologischer Steuerung

Distribuierte Systeme, wie das auf der Blockchain-Technologie beruhende Bitcoin-Netzwerk, sind Systeme, in denen die teilnehmenden Personen idR nur dann rechtlich sichtbar und greifbar werden, wenn sie von der virtuellen in die reale Welt wechseln, etwa, wenn sie Bitcoin in Euro wechseln.[58] Die mangelnde Individualisierbarkeit in digitalisierten, distribuierten Systemen erschwert die rechtliche Zuordnung und damit die rechtliche Verantwortung und Kontrolle.[59] Rechtliche Steuerung baut in rechtsstaatlichen Demokratien allerdings auf individualisierbaren Personen auf, seien es natürliche oder juristische Personen,[60] sowie auf klarer Verantwortungszuschreibung.[61] Wer TrägerIn von Rechten und Pflichten ist, muss daher eindeutig festgelegt sein, will der Staat bzw das Recht seine Steuerungskraft nicht verlieren.[62]

In den Fällen, in denen die Individualisierbarkeit der Netzwerk-TeilnehmerInnen ausnahmsweise möglich ist,[63] fehlt diesen idR jeglicher Einfluss auf das System, weshalb sie schon aus Sachlichkeitserwägungen nicht verantwortlich gemacht werden können.[64] Die globale Ausrichtung der meisten digitalisierten, distribuierten Systeme[65] behindert die Verantwortungszuweisung zusätzlich. Im Ergebnis bedeutet dies, dass im Zentrum der Steuerungsbemühungen das Netzwerk,[66] der Code und dessen ProgrammiererInnen oder das Kollektiv stehen.[67] All dies erschwert die staatliche/rechtliche Steuerung oder Fremdbestimmung,[68] denn bleibt die ProgrammiererIn unbekannt, wie beim ursprünglichen Programmcode der Kryptowährung Bitcoin,[69] und verbreitet sich dessen Code einmal im Netz, übernimmt dieser die Steuerung der Netzwerk-Teilnehmenden, selbst wenn er veränderbar ist.

## V. Digitalisierte distribuierte Systeme: Herausforderungen für demokratische Rechtssysteme

Blockchain-basierte Systeme sind idR globale Netzwerke, deren TeilnehmerInnen durch die Pseudonymisierung unbekannt bleiben, jedenfalls so lange sie sich im Netzwerk selbst bewe-

58 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, Kryptowährungen, Blockchain und Smart Contracts (Teil II), jusIT 2017, 132.
59 Vgl *Karnow*, Liability for Distributed Artificial Intelligences, Berkeley Technology Law Journal 1996, 155.
60 Siehe *Teubner,* Elektronische Agenten und große Menschenaffen: Zur Ausweitung des Akteursstatus in Recht und Politik, in *Becchi/Graber/Luminati* (Hrsg), Interdisziplinäre Wege in der juristischen Grundlagenforschung (2008) 2.
61 Siehe *Spiecker,* CR 2016, 700.
62 Siehe *Reuter*, Rechtsfähigkeit und Rechtspersönlichkeit: Rechtstheoretische und rechtspraktische Anmerkungen zu einem großen Thema, AcP 2007, (673) 681.
63 Siehe *Koops/Hildebrandt/Jaquet-Chiffelle,* Bridging the Accountability Gap: Rights for New Entities in the Information Society?, Minnesota Journal of Law, Science and Technology, 2010, 499.
64 Siehe *Spiecker,* CR 2016, 700; vgl auch *Beck,* Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR 2009, 228.
65 Vgl *Johnson/Post,* Law and Borders – The Rise of Law in Cyberspace, Stanford Law Review, 1996, 1367.
66 Siehe *Ladeur,* Die Netzwerke des Rechts, in *Bommel/Tacke* (Hrsg), Netzwerke in der funktional differenzierten Gesellschaft (2010) 143.
67 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).
68 Siehe *Koops/Hildebrandt/Jaquet-Chiffelle,* Minnesota Journal of Law, Science and Technology, 2010, 499.
69 Die Bitcoin Software wurde 2009 von einer Person(engruppe) unter dem Pseudonym „Satoshi Nakamoto" ins Leben gerufen (*Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System [2008]).

gen.[70] Unbekannt sind, wie zuvor bereits erwähnt, mitunter auch die ErfinderInnen des jeweiligen Systems; dies ist zumindest beim bislang bedeutendsten Blockchain-basierten System, der Kryptowährung Bitcoin, der Fall. In diesen softwarebasierten distribuierten Netzwerken setzen demzufolge die ProgrammiererInnen mit dem Code die normativen Standards.[71] Das für die Netzwerk-TeilnehmerInnen normativ relevante System ist kein staatlich gesetztes Recht, sondern ein von mitunter unbekannten EntwicklerInnen aufgestelltes Regelwerk.[72]

Anders als im Bereich demokratisch legitimierter Gesetzgebung geschieht dies beim Entwickeln Blockchain-basierter Systeme weitgehend ohne demokratische Legitimation und ohne demokratische Kontrolle, regelmäßig mit dem Ziel, (zentrale) staatliche Institutionen oder staatlich legitimierte Mittelspersonen zu beseitigen.[73] Besonders augenfällig ist die Verfolgung dieses libertären Ziels[74] bei den mittlerweile unzähligen Kryptowährungen, die explizit ein Finanzsystem ohne staatliche Legitimation und Kontrolle bezwecken.[75] Vom Standpunkt einer rechtsstaatlichen Demokratie aus betrachtet, sollten derartige Wünsche und Vorstellungen gesellschaftlich breit diskutiert werden und Wertentscheidung dieser Tragweite letztlich vom demokratisch legitimierten Gesetzgeber entschieden werden.[76]

Neben den demokratischen Legitimationsdefiziten setzt ein staatlich entgrenztes System, in dem die handelnden Personen unbekannt bleiben, rechtsstaatliche Demokratien vor zahlreiche Herausforderungen. Personen, an die staatliche/rechtliche Steuerung anknüpfen kann, sind regelmäßig nicht vorhanden, falls doch, sind sie aufgrund der mangelnden Einflussmöglichkeiten als rechtlicher Anknüpfungspunkt unzugänglich, staatliche Ingerenz- und Zugriffsmöglichkeiten diffundieren.[77] ProgrammiererInnen sind, selbst dann, wenn sie bekannt sein sollten, aufgrund der globalen Natur der Blockchain-basierten Systeme regelmäßig nicht greifbar. All dies verunmöglicht eine staatliche und rechtliche Steuerung dieser neuen Ordnungssysteme bislang. Zentrale rechtliche Institute, wie die Person, Zurechenbarkeit oder Verantwortlichkeit, verlieren ihre Wirkmächtigkeit.[78] Der Staat und das Recht können BürgerInnen und ihre Interessen zunehmend weniger schützen.[79]

Wenn die NetzwerkprogrammiererInnen und deren TeilnehmerInnen rechtlich kaum steuerbar sind,[80] bleibt die Frage, ob das technologische System ein rechtlicher Anknüpfungspunkt sein

70 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, jusIT 2017, 132.
71 Vgl *Spiecker*, CR 2016, 696; *Gruber/I. Eisenberger* in *I. Eisenberger/Lachmayer/G. Eisenberger* 51; *I. Eisenberger*, Das Trolley-Problem im Spannungsfeld autonomer Fahrzeuge: Lösungsstrategien grundrechtlich betrachtet, in *I. Eisenberger/Lachmayer/G. Eisenberger* (Hrsg), Autonomes Fahren und Recht (2017) 91.
72 Vgl *Lessig*, Code 120 ff; allgemein dazu *Robey*, Contract Management Magazine 2017, 18 (26) mit Verweis auf *Swan*, Blockchain: Blueprint for a New Economy (2015) 16 f.
73 Vgl *Nakamoto*, Bitcoin; *Atzori*, Blockchain Technology and Decentralized Governance: Is the State Still Necessary? SSRN 2015, 4 abrufbar unter https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713 (zuletzt abgefragt am 13. 11. 2017).
74 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, jusIT 2017, 87 (88).
75 Vgl *Huckle/White*, Future Internet (2016) 49. Siehe idZ ferner *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, Kryptowährungen, Blockchain und Smart Contracts (Teil I), jusIT 2017, 87 sowie Teil II, jusIT 2017, 129.
76 Allgemein zur Notwendigkeit demokratisch legitimierte Gesetzgebung iZm neuen Technologien siehe *I. Eisenberger*, Innovation, insb 152 ff. Für eine zurückhaltende Regulierung im Bereich der Blockchain-Technologien spricht sich hingegen *Piska*, Kryptowährungen und ihr Rechtscharakter – eine Suche im Bermuda-Dreieck, ecolex 2017, 632 aus.
77 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, jusIT 2017, 129.
78 Vgl *Spiecker*, CR 2016, 696.
79 Vgl *D. Tapscott/A. Tapscott*, Blockchain 299.
80 Siehe idZ *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

kann[81] und wenn ja, in welcher Form. Überlegungen, wie die elektronische Person[82] oder mit Rechtspersönlichkeit ausgestattete autonome Systeme,[83] stellen jedenfalls eine Herausforderung für den traditionellen Rechtsbegriff dar, wonach Recht von Menschen für Menschen gemacht ist[84] und in dem kein Platz für technologische Systeme als NormadressatInnen zu sein scheint. Mitunter ist es auch keine Frage rechtlicher Steuerung, sondern eine technologischer Normierung[85] und der Steuerung durch Design.[86] Die Zurückdrängung demokratisch-staatlicher Steuerung und damit konsensual errungener Werte liegt jedenfalls auf der Hand. Zum Schutz der Gesellschaft vor einer potentiellen Techno-Diktatur bedarf es neuer Mechanismen der Machtkontrolle und der Vorbeugung von Machtmissbrauch und eines Bewusstseinsbildungsprozesses innerhalb der neuen ProgrammiererInnen-Eliten.

## VI. Resümee

Die Frage, wie selbst- oder fremdbestimmt Menschen in der zunehmend digitalisierten Welt sind, ist, wie gezeigt wurde, die falsche Fragestellung, denn Fehlverhalten, dass in einer digitalisierten und distribuierten Welt niemandem mehr zugerechnet werden kann und keine Verantwortung mehr auslöst, führt wohl zwangsläufig zu Machtmissbrauch, sei es durch Private oder durch den Staat. Das Netzwerk-Verhalten entzieht sich darüber hinaus aufgrund der weitgehend fehlenden rechtlichen Anknüpfungspunkte staatlicher Kontrolle. Es wäre daher zu fragen, woher wir in digitalisierten Systemen überhaupt wissen, wer bestimmt und wie wir die, die bestimmen, wieder sichtbar machen. Wie können wir die, die normative Standards setzen, zur Verantwortung ziehen und damit Macht kontrollieren und Missbrauch verhindern?[87] Können wir auch in digitalisierten und distribuierten Systemen zentrale rechtliche Anliegen, wie Verantwortung, Kontrolle und Machtbeschränkung effektuieren und wenn ja, mit rechtlichen oder anderen Instrumenten? So oder so sollte sich die Gesellschaft, aber auch die Rechtswissenschaft diesen Fragen im Sinne eines *„legal foresight"*[88] eher früher als später stellen und nicht erst, wenn technologische Systeme fest in unserer Gesellschaft verankert und kaum noch steuerbar sind.[89]

81 Vgl *Dulong de Rosnay*, Peer to party: Occupy the law, 5. 12. 2016, First Monday, http://journals.uic.edu/ojs/index.php/fm/article/view/7117/5658 (zuletzt abgefragt am 20. 7. 2017).

82 *Koops/Hildebrandt/Jaquet-Chiffelle*, Minnesota Journal of Law, Science and Technology 2010, 499; *Matthias*, Automaten als Träger von Rechten (2008); *Häusermann*, Autonome Systeme im Rechtskleid der Kapitalgesellschaft (2016) siehe unter: http://www.homburger.ch/fileadmin/publications/AUTOSYKG.PDF (zuletzt abgefragt am 10. 6. 2017); *Solum*, North Carolina Law Review 1992, 1231. Siehe ferner *Wiebe,* Die elektronische Willenserklärung (2002).

83 *Häusermann,* Autonome Systeme 5 ff.

84 Anstelle aller *Kelsen*, Reine Rechtslehre[2] 9.

85 Vgl *Reidenberg*, Texas Law Review 1998, 554; *Cockfield,* Manitoba Law Journal 2004, 405.

86 Siehe idZ *Schwarz-Plaschg/Kallhoff/I. Eisenberger*, Making Nanomaterials Safer by Design? NanoEthics 2017, 1 und die darin zitierte Literatur.

87 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

88 Vgl *Gruber/I. Eisenberger* in *I. Eisenberger/Lachmayer/G. Eisenberger* 67; *Bruckmüller/Schumann*, Automatisiertes und autonomes Fahren: Strafrechtliche Rahmenbedingungen in Österreich, in *I. Eisenberger/Lachmayer/G. Eisenberger* (Hrsg), Autonomes Fahren und Recht (2017) 123 (145).

89 Zur Akzeptanzsteigerung durch Demokratisierung siehe *I. Eisenberger*, Innovation 284 ff.