SVRV Sachverständigenrat für Verbraucherfragen

Kurzgutachten „Regulierung durch Technik“

Gerald Spindler

Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen

Dezember 2016

Berlin, Dezember 2016
ISSN 2365-8436

Herausgeber:

Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin

Telefon: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525
E-Mail: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de

Diese Veröffentlichung ist im Internet abrufbar.

Mitglieder des SVRV

Prof. Dr. Lucia Reisch (Vorsitzende)
Professorin für Interkulturelle Konsumforschung und europäische Verbraucherpolitik an der Copenhagen Business School

Dr. Daniela Büchel (stellv. Vorsitzende)
Mitglied der Geschäftsleitung REWE für die Bereiche Human Resources und Nachhaltigkeit

Prof. Dr. Gerd Gigerenzer
Direktor der Abteilung „Adaptives Verhalten und Kognition“ und des Harding-Zentrums für Risikokompetenz am Max-Planck-Institut für Bildungsforschung in Berlin

Helga Zander-Hayat
Leiterin des Bereichs Markt und Recht bei der Verbraucherzentrale Nordrhein-Westfalen

Prof. Dr. Gesche Joost
Professorin für das Fachgebiet Designforschung an der Universität der Künste und Internetbotschafterin der Bundesregierung im Gremium der „Digital Champions“ der EU

Prof. Dr. Hans-Wolfgang Micklitz
Professor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz

Prof. Dr. Andreas Oehler
Professor für Finanzwirtschaft an der Universität Bamberg und Direktor der Forschungsstelle Verbraucherfinanzen und Verbraucherbildung

Prof. Dr. Kirsten Schlegel-Matthies
Professorin für Haushaltswissenschaft an der Universität Paderborn

Prof. Dr. Gert G. Wagner
Professor für Empirische Wirtschaftsforschung und Wirtschaftspolitik an der Technischen Universität Berlin, Vorstandsmitglied des Deutschen Instituts für Wirtschaftsforschung und Max Planck Fellow am MPI für Bildungsforschung

Mitarbeitende des SVRV

Leiter der Geschäftsstelle: Thomas Fischer

Wissenschaftlicher Stab der Geschäftsstelle: Mathias Bug, Dr. Irina Domurath, Dr. Christian Groß

Kurzgutachten „Regulierung durch Technik“

Prof.Dr. Gerald Spindler

I. Einleitung

Im Zuge der zunehmenden Digitalisierung der Gesellschaft und ihres Wandels zu einer „Informationsgesellschaft“ rückt das Verhältnis von digitaler Technik zu Recht zunehmend in den Fokus der rechtswissenschaftlichen, aber auch rechtspolitischen Diskussion. Algorithmen bestimmen genauso wie große Datenmengen zunehmend unser alltägliches Leben bis in die letzten Facetten hinein. Smart Homes wie auch Smart Cars sind inzwischen keine Utopie mehr, sondern stehen kurz vor ihrer massenweisen Verbreitung.

Während der übliche Fokus der Rechtswissenschaft auf der Frage liegt, wie diese Technologien reguliert werden können,[1] wie eine demokratisch legitimierte Kontrolle bewerkstelligt werden kann und Grundrechte aus der analogen Welt in der digitalen Welt realisiert werden können, wird die umgekehrte Fragestellung, ob und wie bzw. unter welchen Bedingungen Technik rechtliche Regulierung unterstützen oder gar ersetzen kann, selten gestellt. Dabei hat gerade die Diskussion im Zuge der Novellierung des europäischen Datenschutzrechts um den Ansatz „privacy by design“ gezeigt,[2] dass technologische Gestaltungen die Rahmenbedingungen für den Datenschutz verbessern können, indem sie typische Defizite in Entscheidungssituationen bewältigen, wie etwa ein von vornherein „eingebauter“ Datenschutz, der bewusst ausgeschaltet werden muss vom Datensubjekt. Gerade die typischen menschlichen Defizite, wie sie gerade in Behavioral Economics untersucht werden, z.B. bestimmten biase, Trägheit, hohen Informationskosten, Herdenverhalten etc.,[3] können mit solchen technischen Grundeinstellungen überwunden, zumindest abgemildert werden.

Ohne dass der gesamte Komplex des Ersatzes von Recht durch Technologie hier erschöpfend analysiert werden könnte, sollen im Folgenden die Rahmenbedingungen für eine Regulierung durch Technik skizziert werden. Auch wenn bei näherer Betrachtung der Gedanke der Regulierung durch Technik keineswegs neu ist, sondern etwa bei jedem Sicherheitsstandard Sicherungspflichten des potentiell Geschädigten ersetzt (z.B. Airbag etc.), erhält der Ansatz der Regulierung durch Technik durch die Digitalisierung einen neuen wirkmächtigen Impuls. Durch die Möglichkeiten der Codierung können in zuvor kaum möglicher Weise breitflächig Tätigkeiten beeinflusst, präformiert oder begrenzt werden, Kommunikationen gesteuert werden etc. Daher werden im Folgenden vor allem die Chancen, aber auch Grenzen einer Regulierung durch digitale Technik beleuchtet, indem zunächst in einem Allgemeinen Teil die generellen Bedingungen herausgearbeitet werden, um diese dann anhand einiger Anwendungsbeispiele in einem Besonderen Teil zu konkretisieren – ohne dass ein Anspruch auf Vollständigkeit erhoben werden könnte. Insbesondere können alle Probleme, die mit einem etwaigen Roboterrecht oder der künstlichen Intelligenz,[4] insbesondere selbsthandelnden Agenten im Vertragsrecht,[5] hier nicht näher behandelt werden.

---

[1] *Goerdeler/Laubach*, ZRP 2002, 115, 116 f.; *Weisser/Glas*, ZUM 2009, 914, 916 ff.; *Holznagel*, ZUM 1999, 425, 426 f.; *Ladeur*, ZUM 1997, 372, 377 ff.; LG Düsseldorf, GRUR-RS 2016, 04916 Rn. 20 ff.

[2] *Schütze,* ZD-Aktuell 2016, 05015; *Redaktion MMR-Aktuell,* MMR-Aktuell 2015, 373362; *Buttarelli*, EuABl 2016, C 67, 13-15; *Richter,* DuD 2016, 89-93; *Steinebach/Jung/Krempel/Hoffmann,* DuD 2016, 440-445; *Bunk, Goldschmidt,* DuD 2016, 463-467; *Gierschmann,* ZD 2016, 51, 52.

[3] S. dazu *Kahneman/ Tversky*, Choices, Values and Frames. Cambridge University Press, 2000; *Shleifer*, Inefficient Markets: An Introduction to Behavioral Finance. Oxford University Press, 1999; *Thaler/Sunstein*, Nudge. London: Penguin Books 2008

[4] S. dazu etwa *Calo*, Robotics and the Lessons of Cyberlaw, 103 CALIF. L. REV. 513, 514–15

II. Allgemeiner Teil

Seit den bahnbrechenden Arbeiten von Lawrence Lessig[6] ist bekannt, dass (Software-) Codes die gleiche Wirkung wie rechtliche Regelungen erzeugen können, ja effizienter als rechtliche Normen sein können, da diese des Vollzugs bedürfen, während Code von vornherein Wirkung entfaltet und unerwünschte Tätigkeiten etc. verhindert, etwa indem Nutzer aus bestimmten Ländern von einem Dienst von vornherein ausgeschlossen werden (geo-blocking).

A. Möglichkeiten einer Regulierung durch (digitale) Technik

1. Kodierungen von Rechtsnormen

In allen Fällen, in denen einer Rechtsnorm eine klare Ja-Nein-Entscheidung implementiert ist, lässt sich diese Norm entsprechend in 0-1 Befehle bzw. binäre Codes[7] umwandeln. Wie schon im Fall des Geo-Blocking angedeutet, ermöglicht ein Code etwa die Erkennung der geographischen Herkunft einer Anfrage über das Internet (Geo Location[8]) und kann so die kollisionsrechtliche Entscheidung der Anwendung einer Rechtsordnung bzw. deren Ausschluss steuern, wenn die entsprechende Norm des Internationalen Privatrechts die Berufung einer Rechtsordnung eindeutig von der geographischen Belegenheit des Nutzers abhängig macht, etwa im Urheberrecht infolge des Territorialitätsprinzips. Gleiches gilt für viele andere Anwendungsmöglichkeiten, etwa die Erkennung einer roten Ampel durch ein selbststeuerndes Kfz, die das Halten des Kfz über Softwarecodierung als Ja/Nein-Entscheidung steuert.

Allein diese wenigen Beispiele (die später noch vertieft werden) verdeutlichen bereits die essentielle Bedingung einer Substitution von Recht (oder dessen Unterstützung) durch Technologie und Code, nämlich die ein-eindeutige Entscheidung und Auflösung der Rechtsnorm in binäre Logik ohne Spielräume. Gleichzeitig resultieren daraus auch die Grenzen einer solchen Substitution:

2. „Selbst-Vollzug“

Wie bereits angedeutet, besteht ein wesentlicher Vorteil der Codierung bzw. Substitution durch Technologie in dem „Selbstvollzug“ der technisch implementierten Norm. Ohne dass es einer gesonderten Vollstreckung oder Durchsetzung durch Zwangsmaßnahmen oder Sanktionen wie Bußgelder bedürfte, liegt in der Technologie selbst schon die unmittelbare Umsetzung eines Normbefehls. Wird etwa eine Kopie eines digitalen Inhaltes verliehen und diese mit einem Mechanismus versehen, der den digitalen Inhalt nach Ablauf der Leihzeit unbrauchbar macht, bedarf es keiner gesonderten Rückgabepflicht und Durchsetzung der Rückgabe durch den Entleiher. Auch hier gilt, dass die automatisierte Durchsetzung des Normbefehls unbedingt sein muss; das System kann nur solche Faktoren berücksichtigen, die vorgegeben sind - Abwägungen oder Aufschübe, Fristen etc. können im Rahmen solcher Systeme nicht verarbeitet werden.

3. Weiterungen: selbststeuernde / adaptiv-lernende Systeme

Traditionelle technologische Lösungen zeichnen sich durch ihre Statik aus, indem sie einmal implementierte Codierungen bzw. Entscheidungsmuster nicht ändern. Demgegenüber können moderne halb-autonome Systeme ihr Verhalten und ihre Entscheidungen ändern, je nachdem welche „Erfah-

---

(2015); *Brenner*, Law in an Era of „Smart“ Technology, Oxford University Press, 2007; *Hillebrandt*, Smart Technologies and the End(s) of Law, Edward Elgar 2015; *Lipton*, Rethinking Cyberlaw, Edward Elgar 2015.

[5] Statt vieler *Choppra/White*, A Legal Theory for Autonomous Artificial Agents, Ann Arbor 2011; *Sartor*, Artif.Intell. Law (2009), 17:253-290.

[6] *Lessig*, Code Version 2.0, 2006, S. 106-111.

[7] Mit „Code“ ist jeder für Maschinen lesbare Abfolge von Befehlen gemeint, eben Software.

[8] *Gueye/Ziviani/Crovella/Fdida,* ACM Konferenzbeitrag: Constraint-Based Geolocation of Internet Hosts, S. 3-6; *Ciavarrini/Disperati/Lenzini/Luconi/Vecchio,* Geolocation of Internet hosts using smartphones and crowdsourcing, S. 2-4; *Tian/Dey/Liu/Ross,* China’s Internet: Topology Mapping and Geolocating, S. 3-5.

rungen“ die Systeme gemacht haben, indem sie die Auswirkungen ihrer Entscheidungen auf die Umwelt beobachten. Bekanntestes Beispiel für solche semi-autonomen Systeme sind elektronische Agenten, die für Vertragsschlüsse eingesetzt werden, etwa im finanziellen Bereich, Roboter oder selbststeuernde Verkehrsmittel.

Auch für die Regulierung durch Technologie ist der Einsatz solcher Systeme denkbar, bislang allerdings – nach Kenntnis des Verfassers – nicht im Einsatz. Derartige Systeme müssten die Auswirkungen von Entscheidungen bzw. Lösungen auf den Betroffenen ermitteln und danach die Algorithmen entsprechend ändern; so wäre z.B. der Einsatz von semi-autonomen Systemen im Bereich von Schutzstandards (z.B. Arbeitsschutz, Krankenversicherung, KfZ-Versicherung) denkbar, die das Verhalten der zu regulierenden Personen durch Sensoren überwachen und je nachdem bestimmte Maßnahmen ergreifen, z.B. Verringerung von Geschwindigkeiten, Ermahnungen zur Einnahme von Medikamenten oder Anpassung einer Arbeitsgeschwindigkeit.

B. Grenzen der Regulierung durch Technik

1. Code und Interessenabwägungen

Die beschriebenen Charakteristika der Codierung stellen gleichzeitig aber auch deren Grenzen dar:[9] Verwenden Rechtsnormen unbestimmte Rechtsbegriffe, können diese nur in Abhängigkeit der jeweiligen Einzelfallumstände in der konkreten Situation spezifiziert und angewandt werden. Dies gilt erst recht für entgegenstehende Rechte Dritter, insbesondere in multipolaren Verhältnissen, die erst auf der Konkretisierungsebene des unbestimmten Rechtsbegriffs Eingang in die Entscheidung finden. Auch müssten verfassungsrechtliche Einflüsse ebenso wie teleologische Reduktionen, Analogien in einer Ja/Nein-Codierung Berücksichtigung finden.

Zwar ist es theoretisch denkbar, für jeden Einzelfall eine Norm unter Einbeziehung dieser Einflüsse in Ja/Nein-Entscheidungen herunterzubrechen; auch sind durch entsprechende Big-Data Anwendungen inzwischen die Möglichkeiten, gewaltige und komplexe Datenmengen zu bewältigen, wesentlich gestiegen, so dass quasi jede jemals getroffene Entscheidung gespeichert und in einen Algorithmus einbezogen werden könnte. Doch stellen diese Anforderungen der Abwägung und Konkretisierung unbestimmter Begriffe nach wie vor mangels entsprechender Vorhersehbarkeit und aufgrund der enormen Komplexität eine praktisch nicht lösbare Aufgabe dar. Auch Big Data kann nur auf vorhandene Entscheidungen und Abwägungsprogramme rekurrieren, neue bzw. unbekannte Zusammenhänge aufdecken – allerdings immer auf der Basis bereits vorhandener Daten; neue Sachverhalte bzw. Phänomene vermögen diese Algorithmen nicht zu erfassen. Bestes Beispiel für derartige, hoch komplexe und kaum vorhersehbare Aufgabenstellungen ist etwa das allgemeine Persönlichkeitsrecht in Abwägung mit der Meinungs- bzw. Pressefreiheit: Hier ist selbst für einen ausgewiesenen Experten kaum mit genügender Sicherheit einschätzbar, welche Entscheidung vom Gesetz tatsächlich geboten ist.

2. Vollstreckungsschutzmechanismen und Code

Gleiches gilt für den Vollzug bzw. die Durchsetzung der Normbefehle: Zwar hat die Substitution durch Code den Vorteil des unbedingten „self-enforcements“; doch liegt gerade darin gleichzeitig auch der Nachteil, da der Vollzug keinerlei Abwägung im Einzelfall zulässt. Die Rechtsanwendung kennt aber oft genug den Unterschied zwischen materiell-rechtlicher Rechtslage und prozessualer Durchsetzung, ebenso auf der Ebene der Vollstreckung. Gerade das Vollstreckungsrecht wäre oft unzureichend durch Ja/Nein-Entscheidungen charakterisiert, sondern lässt auf der Ebene der Umsetzung häufig Spielraum für Abschwächungen oder Schutzmaßnahmen zugunsten des Schuldners; bekanntestes

[9] S. etwa für die Anwendung von Big Data *Yeung*, „Hypernudge“ – Big Data as a Mode of Regulation by Design, Working paper 2016, http://ssrn.com/abstract=2807574

Beispiel ist etwa die Wohnraummiete mit ihren Schutzbehelfen für den zur Räumung verurteilten Mieter. Aber selbst auf den ersten Blick hin eindeutigen Pflichten, etwa zur Zahlung einer Geldsumme, kann diese modifiziert werden, z.B. durch Teilzahlungen oder mit bestimmten Verzinsungen etc.

3. Code und Internationales Privatrecht

Ähnliche Probleme stellt für Regulierung durch Code das Internationale Recht dar: Da gerade Internetanwendungen nicht auf Territorien beschränkt sind, gewinnt die Abbildung kollisionsrechtlicher Regelungen ein besonderes Gewicht für Regulierung durch Code. Zwar können kollisionsrechtliche Prinzipien durchaus in Codierungen abgebildet werden, wie beschrieben etwa durch Geo Location und damit Geo Blocking von bestimmten Nutzern, die aus Ländern Dienste anfordern, an die der Anbieter aufgrund von Rechtsrisiken nicht liefern will – etwa im Kapitalmarktrecht, wenn aufgrund des Marktortprinzips bestimmte Nutzer keine Angebote erhalten, damit der Emittent nicht den Regeln des anderen Staates unterworfen wird. Diese vermeintlich einfachen Regeln sind jedoch oft komplexerer Natur als es auf den ersten Blick anmuten mag: Paradebeispiel ist wiederum das allgemeine Persönlichkeitsrecht, für das der Schwerpunkt der Aktivitäten des Betroffenen bzw. der Ort maßgeblich ist, was eine Vielzahl von Faktoren beinhaltet. Gleiches gilt z.B. für das Internationale Deliktsrecht, das sowohl Handlungs- als auch Erfolgsort als Anknüpfungskriterien zulässt. Erst recht liegt dies auf der Hand, wenn das allgemein konsentierte Prinzip der engsten Verbindung eines Sachverhalts zu einer Rechtsordnung herangezogen wird.[10] Oftmals finden hier unbestimmte Rechtsbegriffe und damit komplexe Abwägungsvorgänge statt.

Zwar ist es durchaus denkbar, dass für jeden einzelnen Nutzer aufgrund seines vorherigen Verhaltens festgestellt wird, zu welcher Rechtsordnung er die engsten Beziehungen unterhält; doch muss dies wiederum auf das spezielle Rechtsproblem bezogen werden, da etwa bei einem Persönlichkeitsrecht andere Kriterien zur Anwendung gelangen können als bei einem Anlegerschutzdelikt. Zudem würde wiederum eine Prognose auf der Basis von Vergangenheitsdaten erstellt; wertende, quasi „die Richtung“ ändernde Entscheidungen wären damit ausgeschlossen.

4. Die Abhängigkeit von digitalen Umgebungen

Ein weiteres Charakteristikum der Codierung als Substitut für Regulierung stellt seine Abhängigkeit von digitalen Umgebungen dar: Nur in denjenigen Fällen, in denen ein Code völlig selbstständig operiert, insbesondere als embedded Software,[11] wird der Code nicht von seiner digitalen Umgebung[12] beeinflusst. Dies impliziert allerdings auch mehrere Probleme bzw. Risiken: Zum einen kann die Funktion des Codes durch eine Änderung der digitalen Umgebung beeinflusst, ggf. sogar aufgehoben werden, so dass die eigentlich beabsichtigte automatisierte Umsetzung von Recht ebenfalls eingeschränkt oder gar unmöglich wird. Jede Änderung der digitalen Umgebung bedürfte der entsprechenden Anpassung des Codes, was durchaus durch Patches[13] etc. realisiert werden kann, häufig aber der Mitwirkung durch den Nutzer oder zumindest eines auslösenden Momentes (z.B. durch Softwarehersteller etc.) bedarf. Zum anderen ist bei einer Interaktion mit seiner digitalen Umgebung jeder Code anfällig für Angriffe Dritter (Hacking), die die Regulierung durch Technologie damit in ihr Gegenteil verkehren können; die Angriffe auf Sicherheitssysteme von selbststeuernden KfZ sind inzwischen allgemein bekannt. Bestes Beispiel ist hier der vergangene Angriff auf die ConnectedDrive BMW App des gleichnamigen Automobilherstellers. Unberechtigten war es hier möglich die ausgetauschten Informationen zwischen Auto und Server abzugreifen oder sogar zu imitieren und somit

[10] Vgl. Art. 4, 5, 6, 8 Rom-II-VO.

[11] Hier handelt es sich um fest „verbaute“ Software, mithin Software, die nicht von außen beeinflusst bzw. geändert werden kann. Insbesondere fehlt es an Schnittstellen zu anderen Netzen.

[12] Z.B. des Betriebssystems, unter dem die Software läuft, oder Virenscanner, Treibersoftware etc.

[13] Patches sind Aktualisierungen des Codes, oftmals um Sicherheitslücken, die aufgetreten sind, zu reparieren, mitunter aber auch, um neue Merkmale bzw. Funktionalitäten eines Codes einzuführen

das Auto auch ohne Schlüssel zu öffnen oder in gewissen Maße zu steuern.[14] Eine Regulierung durch Technologie muss daher Ausfallmechanismen vorsehen, die bei Versagen der technischen Systeme eingreifen können.

5. Dynamik der Regulierung und Code: Pfadabhängigkeiten

Ein anders geartetes, im Ansatz aber vergleichbares Problem stellt die Dynamik einer Regulierung dar: Während bei der klassischen Regelsetzung durch Parlamente und ihrer Umsetzung durch Gerichte etc. die Dynamik im System quasi inhärent ist und nur durch Kommunikation gegenüber Rechtsanwendern und Betroffenen effektuiert werden muss (Bekanntgabe der Gesetze etc.), tritt an deren Stelle beim Code wiederum die Erforderlichkeit von nachträglichen Anpassungen durch Patches. Zwar sind hier auch durchaus Lösungen denkbar, etwa indem entsprechende Codes automatisiert die jeweilige Rechtslage auf zentralen Plattformen abfragen und dementsprechend ihre Codierung ändern, was semi-autonomen Systemen entspräche. Doch besteht nach wie vor die Gefahr, dass Nutzer die Patches nicht oder zu spät aktivieren oder gar nicht an Systeme angeschlossen sind, mit der Folge, dass unterschiedliche Regulierungszustände in den Codes wiedergegeben wären. Entsprechende Probleme sind hinlänglich aus dem Bereich der IT-Sicherheit bekannt – die sich unter Umständen gerade als Hemmnis für die erforderliche Aktualisierung von Codes erweisen kann, da sie Schnittstellen von Systemen zur Außenwelt einschränkt oder gar untersagt.

Ferner kann der Einsatz von Codes als Regulierung gerade bei embedded Software erhebliche Pfadabhängigkeiten hervorrufen: Hat sich etwa der Gesetzgeber entschieden, eine bestimmte Regulierung zu ändern oder aufzuheben, müssen die Systeme von embedded Software ausgetauscht werden, wenn sie keine Schnittstellen zu Informationsnetzen und damit die Möglichkeit zum Firmwareupdate aufweisen. Solange noch netzunabhängige Codierungen daher verwandt werden, dürften diese sich nur in Bereichen zur Regulierung eignen, die einen hohen Beharrungsgrad bzw. allgemein gesellschaftspolitischen Konsens aufweisen.

6. Code und Privatautonomie

Die Loslösung des Code von menschlichem Einfluss impliziert ferner den Verlust von Privatautonomie durch Rechtssubjekte, da Handlungen durch den Code präformiert werden, somit potentielle Handlungsoptionen ausgeschlossen werden. Dies kann sowohl durch den unmittelbaren Ausschluss von Handlungsmöglichkeiten geschehen als auch durch die Ausnützung von psychologischen Elementen, etwa dem Ranking von Suchergebnissen im Zusammenspiel mit der Tendenz von Nutzern, nur die erste Suchseite mit ihren Ergebnissen zu nutzen.[15] Mit anderen Worten lenkt Code und Technologie den Menschen und schränkt seine Handlunsmöglichkeiten ein – was gerade für Privatrecht als rechtliche Ausgestaltung der Privatautonomie und des selbstbestimmten Handelns erhebliche Implikationen hat.[16]

7. Wer setzt den Code?

Last but not least darf nicht außer Acht gelassen werden, dass häufig nicht der Staat selbst die entsprechenden Codierungen vornimmt, sondern nur Hersteller (bzw. Importeure) zum Einkauf solcher Codebestandteile verpflichten kann. Sowohl Kapazitätsprobleme als auch die Integration solcher Regulierungscodes in bestehende Software bzw. Systeme bedingen diese Quasi-Abstinenz des Staates. Damit aber entsteht das Risiko einer Informationsasymetrie, die in entsprechender Marktmacht

---

[14] *Heuer,* Seminararbeit: Angriffssicherheit bei eingebetteten Systemen, S. 14; siehe auch das Beispiel: *Holland,* ConnectedDrive: Der BMW-Hack im Detail, abrufbar unter: http://www.heise.de/newsticker/meldung/ConnectedDrive-Der-BMW-Hack-im-Detail-2540786.html.

[15] *Mik*, The erosion of autonomy in online consumer transactions, Law, Innovation and Technology 8, S. 7 f.

[16] S. dazu aus Verbraucherschutzsicht etwa *Mik*, The erosion of autonomy in online consumer transactions, Law, Innovation and Technology 8, S. 1 ff.

und Netzwerkeffekten münden kann, indem zum einen der Staat kaum in der Lage ist, die effektive Umsetzung von Code als Regulierung zu überwachen, zum anderen nur diejenigen Unternehmen Marktzugang haben dürfen, die in der Lage sind, entsprechende Codes zu entwickeln und zu administrieren. Einher damit geht die Gefahr der Intransparenz der Regulierung, da nicht auszuschließen ist, dass „gut gemeinter" Code missbräuchlich verwendet oder abgeändert wird. Die schon jetzt bestehenden Probleme der Kontrolle über die Verwendung und Gestaltung von Codes durch marktmächtige Unternehmen würde sich bei einer Substitution von Recht durch Code noch in exponentieller Weise (und demokratisch problematischer Legitimation) verschärfen. Ein möglicher Ausweg besteht hier in der Verwendung von Open Source Code[17] – der dann allerdings wiederum frei verändert werden kann, so dass die Regulierung auch ausgehebelt werden kann und stets entsprechende Prüfungen erforderlich wären.

In Anbetracht der Wirtschaftsstrukturen im IT-Bereich besteht schließlich die Gefahr, dass derartige Algorithmen nur im außereuropäischen Ausland entwickelt werden, auf das der europäische bzw. deutsche Souverän keinen Einfluss hat.

C. Zusammenspiel von Technik und Regulierung

Die aufgezeigten Vorzüge aber auch Nachteile der Verwendung von Code als Regulierungsform legen es jedenfalls zur Zeit nahe, Codierungen nur dann einzusetzen, wenn es sich um einfach strukturierte Normbefehle mit wenig Spielraum für abweichende Fallgestaltungen handelt (Stichwort: rote Ampel), selbst dann aber mit der Möglichkeit des „Override", mithin des Ausschaltens wenn nicht vorhergesehene Situationen eintreten. Zudem muss für eine größtmögliche IT-Sicherheit gesorgt werden, um entsprechende Manipulationen der Regulierung entgegenzuwirken.

III. Besonderer Teil: Anwendungsbeispiele

Einige Anwendungsbeispiele, in denen Code Recht substitutieren kann, sollen im Folgenden kurz analysiert werden, von der Blockchain-Technologie über Scoring, selbststeuernde Fahrzeuge, Urheberrecht bzw. DRM-Systeme bis hin zu sozialen Netzwerken:

A. Blockchain Technologie[18]

1. Technologie[19]

Ein Blockchain dient allgemein gesprochen als Informationsträger, unabhängig davon, um welche Art von Informationen es sich handelt. Die im Blockchain gespeicherte und gebundene Information ist zu jeder Zeit und an jedem Ort eindeutig verifizierbar, bleibt aber sowohl auf ihrem Transportweg als auch in der Blockchain derart verschlüsselt, dass sie nur dem Absender und Adressaten zugänglich ist. Den Schlüssel besitzen nur Absender und Empfänger. In der Regel erfolgt die Übermittlung einer Information über den Blockchain mittels eines P2P-Netzwerkes, mithin über ein dezentrales System ohne zentralen Server.[20]

Neben dem Übermittlungsweg sind essentielle Bestandteile des Blockchain die sog. Hash-Abbildungen.[21] Eine Hash-Abbildung ist eine mathematische Funktion, die eine Information unbe-

[17] Bei Open Source Code kann der Quellcode, der ansonsten streng geschützt ist, von jedermann eingesehen und auch verändert werden, sofern er sich verpflichtet, die veränderte Software einschließlich Quellcode jedem frei zur Verfügung zu stellen, unter der jeweiligen Lizenz, z.B. der General Public License (GPL).
[18] Für die Mitarbeit an diesem Kapitel danke ich besonders Herrn Morick.
[19] S. hierzu *Kaulartz*, CR 2016, 474 ff. mwNachw.; *Boehm/Pesch*, MMR 2014, 75, 76.
[20] *Ziegler*, Smarte Schwärme. Die Technik hinter modernen Peer-To-Peer-Netzen, c't, Magazin 21, S. 160–164.
[21] S. dazu *Kaulartz,* CR 2016, 474, 475 f.

stimmter Länge in einen Zielwert mit festgelegter Länge umwandelt. Dabei sollte diese Funktion im besten Fall injektiv sein, also bei unterschiedlichen Informationen auch unterschiedliche Hash-Werte ergeben. Oder aber umgekehrt: Die gleiche Information liefert den gleichen Hash-Wert. Wenn zwei unterschiedliche Informationen den gleichen Hash-Wert liefern spricht man von einer Kollision, Grund dafür ist die Wahl einer schlechten Hash-Abbildung. Somit lässt sich deren Inhalt für die Betrachter identifizieren, gibt aber keinen Aufschluss über die Art des Inhalts. Da die zu übertragenden Informationen jedoch in der Regel aus großen Blöcken bestehen, bedient man sich eines weiteren effizienten Sicherheitsmerkmals, den Hash Bäumen.

Hinzu kommt die Verwendung eines Zeitservers, der die zu übertragende Information mit einem Zeitstempel versieht.[22] Da der Blockchain mit jeder neuen eingebundenen Information immer länger wird, ist der Zeitstempel zum einen ein temporärer Indikator zur Verifizierung und zum anderen ein konstantes, irreversibles Sicherheitsmerkmal. Sollte die gleiche Information im Blockchain einen anderen Zeitstempel aufweisen, wird diese von den Beteiligten nicht angenommen, sondern einfach ignoriert und somit nur die richtige Information übertragen.

Zwar sind theoretisch Angriffsszenarien denkbar, wenn der Angreifer es tatsächlich geschafft hat, eine Kollision bei einer kryptologischen Hash-Funktion herbeizuführen. Der Aufwand ist jedoch meistens so hoch, dass sich diese Art von Angriff nicht lohnt. Wenn man sich auf einen Zweites-Urbild-Angriff beschränkt, der ja einen Erstes-Urbild-Angriff enthält, so lässt sich der Aufwand sogar berechnen: bei der Hash-Abbildung SHA-1 braucht man mindestens 2^{52} Versuche. Wenn man nicht über die gehashte Information verfügt, also nur einen Erste-Urbild-Angriff vornehmen kann, dann sind es sogar 22^{104}. Das sind 2^{52} mal mehr Versuche als bei einem Zweites-Urbild-Angriff, da hier weniger Informationen zur Verfügung stehen. Bei anderen kryptologischen Hash-Abbildung potenziert sich der Aufwand abermals. Ein kleines Zahlenbeispiel soll den Aufwand einer Kollision bei SHA-1 mittels eines Second-Preimage-Angriffs zeigen: Wenn es gelingen würde pro Sekunde 1.000.000 Angriffe auf die Hash-Abbildung auszuführen, dann bräuchte man immer noch circa 6 Jahre, um eine einzige Kollision zu finden.

Sollte der Angreifer also eine Kollision in der Hash-Abbildung gefunden haben, so hat er dennoch nicht den gesamten Blockchain überwunden. Denn die zugehörigen Informationen haben ja zusätzlich noch einen Zeitstempel. Das heißt, der Angreifer müsste die gehashte Kollisionsinformation auch genau zu dem Zeitpunkt in dem Blockchain einspeisen, zu welcher die gehashte Ausgangsinformation einen Zeitstempel erhält. Dies zu bewerkstelligen ist so gut wie unmöglich. Einzig wenn der Angreifer es schaffen würde, auch den Zeitserver so zu manipulieren, dass die Ausgangsinformation und die Kollisionsinformation nach einer erfolgreichen Zweiten-Urbild-Attacke im gleichen Zeitpunkt einen Zeitstempel bekommen, wäre ein erfolgreicher Angriff möglich.

Doch auch dann ist der Angreifer noch nicht an den Blockchain vorgedrungen. Da bei dem Blockchain das P2P-Prinzip gilt, müsste der überwiegende Teil der Nutzer die gehaste Kollisionsinformation auch verifizieren. Wenn dies nicht der Fall ist, dann sind auch die vorangegangenen Bemühungen des Angreifers wertlos. Insgesamt potenziert sich der Aufwand des Angreifers nochmals.

[22] *Cadjan/Harris*, Administering NDS, S. 38 ff.

Charakteristisch ist ferner, dass eine Transaktion nicht widerrufen werden kann. Die getätigte Transaktion ist dann fest in den Blockchain integriert; diese lässt sich nur durch eine gegenteilige Transaktion wieder aufheben, die dann natürlich auch wieder in den bestehenden Blockchain integriert wird.

2. Anwendungsgebiete

Die Verschlüsselung mitsamt eindeutiger Verifizierbarkeit und extrem hoher Sicherheit bei gleichzeitiger Dezentralität macht ein Blockchain zum idealen Mittel für die rechtssichere Dokumentation und Nachverfolgung von Transaktionen. Da gleichzeitig jedwede Information gespeichert werden kann, können gleichzeitig Codierungen bzw. Algorithmen, mithin auch sog. Smart Contracts eingebettet werden.

a) Bitcoins und bargeldloses Bezahlen via NFC

Eine der bekanntesten Anwendungen stellen Bitcoins dar. Bei der Transaktion mittels Blockchain verfügt man selbst in seinem Wallet über seine gesamte virtuelle Währung, man muss keinem Dritten vertrauen. Da das Blockchain-System dezentral angelegt ist wachen alle Teilnehmer über die Transaktion. Der zweite Unterschied besteht in der Flexibilität der Transaktion mit Hilfe des Blockchains. Die Transaktion erfolgt direkt mit dem Empfänger. Man muss keine IBAN oder sonstigen privaten Daten Preis geben. Es wird nur die Information übertragen, die für die Transaktion relevant ist; denn ein Finanzintermediär ist nicht mehr erforderlich, die Leistungen werden über die Blockchain direkt ausgetauscht und eindeutig dokumentiert, quasi als „Bargeld“ in der virtuellen Welt.

Ein weiteres Beispiel wäre das bargeldlose Bezahlen mittles Near Field Communication (NFC). Viele Smartphones haben bereits heute einen NFC-Chip verbaut, der diesen Zahlungsdienst ermöglicht. Dabei hält man das entsprechende Gerät einfach an eine vorgesehende Schnittstelle und der zu zahlende Betrag wird abgebucht. Apple und Google bieten solche Dienste bereits seit einiger Zeit an. Mit der Blockchain-Technologie und einem Smart Contract könnte man diese dritten Unternehmen von der Buchung ausschließen und direkt die Zahlung tätigen. Eine NFC-Transaktion mittles Blockchain wäre dann technisch nichts anderes als eine Transaktion wie bei einer virtuellen Währung.

b) Smart Contract

Ein Smart Contract ist ein Programm, das einen intelligenten, selbst ausführenden Vertrag darstellt.[23] Ein einfaches Beispiel ist hier der Kaufvertrag, bei dem der Kaufgegenstand, z.B. ein PKW, in Raten abbezahlt werden soll. In einem Smart Contract wäre es nun möglich diesen Vertragsinhalt als ausführbares Programm zu implementieren und selbstständig und automatisiert überwachen zu lassen. Das Auto könnte dann – entsprechende Sensorik und Konnektivität vorausgesetzt – etwa bei Ausbleiben einer Rate trotz Fälligkeit durch das Programm automatisch gesperrt werden. Erst wenn die fällige Rate bezahlt wird, ließe sich das Auto wieder starten.[24] So würde der Smart Contract also letztendlich seinen eigenen „Vollzug“ überwachen.[25]

Als Smart Contract lässt sich mit *Kaulartz/Heckmann* ein Code definieren, der

> „- ein digital prüfbares Ereignis (hier: Bezahlung der Leasing-Rate: true/wahr bzw. false/falsch),
>
> - ein Programmcode, welcher das Ereignis verarbeitet (hier: Software im Boardcomputer des Autos),

[23] So z.B. die Etherum-Plattform: https://www.ethereum.org/ (zuletzt abgerufen am 06.09.2016).
[24] *Kaulartz/Heckmann,* CR 2016, 618 f. mwNachw.
[25] *Szabo*, Smart Contracts, 1994.

- eine rechtlich relevante Handlung, welche auf Grundlage des Ereignis ausgeführt wird (hier: Betriebsbereitschaft des Pkws herstellen).“[26]

betrifft.

Der Smart Contract lässt sich als Information direkt in den Blockchain implementieren oder als Gerüst für eine Reihe von vertraglichen Anordnungen heranziehen in dem der Blockchain als Informationsübermittler dient. Blockchains lösen zwar eine Reihe von Problemen; doch nützen sie nichts, wenn das der übermittelten Information bzw. dem Smart Contract zugrundeliegende Programm fehlerhaft ist. Da der Blockchain irreversibel ist, ist es auch der Smart Contract. Vertragsanpassungen, wie man sie bei regulären Verträgen machen kann, sind hier nicht möglich. Wenn sich die Bedingungen eines Vertrages ändern ist es mit beiderseitigen Parteiwillen möglich den Vertrag ex nunc zu verändern. Bei einem Smart Contract müsste man den ganzen Vertrag neu aufsetzen.

Die Interessengruppen des Smart Contract bzw. der Blockchain-Technologie kommen dabei aus ganz unterschiedlichen Lagern. So hat sich zu Beginn des Jahres der wissenschaftliche Beirat der britischen Regierung zu diesem Thema geäußert.[27] Das Papier setzt sich nicht nur mit der dahinterstehenden Technologie auseinander, sondern betrachtet auch das disruptive Potential. Des Weiteren geht man auf bestehende Anwendungsmöglichkeiten ein, wie etwa das Everledger zur automatisierten Zertifikatsvergabe von Diamanten oder SETL, eine Blockchain-basierte Infrastruktur für Kredit-, Anlagen- und Wertpapierhandel. Es gibt bereits Unternehmen, die sich auf die Programmierung von speziell zugeschnitten Smart Contracts spezialisiert haben und eine Programmierumgebung bereitstellen zur Vereinfachung der Smart Contract Erstellung.[28] Auch die BaFin hat sich bereits zu dieser Thematik geäußert und beobachtet mit großem Interessen deren Entwicklung.[29] Dabei konzentriert sich die Bafin zunächst allgemein auf den Distributed Ledger, also einem Kontoverteilungssystem und den Blockchain im Allgemeinen, um anschließend Einsatzmöglichkeiten zu untersuchen. Hier werden im Speziellen der Handel auf dem Finanzmarkt, die Speicherung von Handelsdaten, der digitale Zahlungsverkehr und der Interbankenhandel betrachtet. Des Weiteren geht die BaFin davon aus, dass die Distributed Ledger bzw. Blockchain Technologie grundsätzlich das Potenzial hat einen neuen Standard in der Finanzbranche zu setzen.

Als Einsatzgebiete[30] für Smart Contracts werden vor allem das Internet of Things im Hinblick auf die Machine-to-Machine-Kommunikation, die Abwicklung von Finanztransaktionen durch Banken sowie auf Börsen, der Ersatz von Intermediären, insbesondere von Registern jeglicher Art (Handelsregister, Grundbücher, Domains etc.) bis hin zu Versicherungen durch automatische Feststellung von Versicherungsfällen genannt.[31] Gerade in den Bereichen der Finanz- und Versicherungstechnologie (kurz: FinTech und InsurTech) eröffnen sich weitreichende Anwendungsgebiete. Es wäre möglich Geldanlagegeschäfte auf den Börsenmarkt mittels Smart Contract abzuwickeln. Gerade auf Märkten wo ein schnelles Handeln erforderlich ist, würden intelligente Verträge die Abwicklung beschleunigen und gleichzeitig sicherer gegenüber etwaigen Fehlern machen. Smart Contracts bieten sich auch für Versicherungsunternehmen an. Hier könnte automatisch festgestellt werden, ob etwa ein beschädigtes

[26] *Kaulartz/Heckmann,* CR 2016, 618.
[27] *Hancock/Vaizey*, Distributed Ledger Technology: beyond block chain - A report by the UK Government Chief Scientific Adviser.
[28] *Piotrowski*, A Next-Generation Smart Contract and Decentralized Application Platform (White Paper).
[29] Siehe *Geiling*, BaFin, Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain.
[30] Siehe dazu auch: Blockchain - Enigma. Paradox. Opportunity, abrufbar unter http://www2.deloitte.com/uk/en/pages/innovation/articles/blockchain.html (zuletzt abgerufen am 06.10.2016).
[31] *Kaulartz/Heckmann,* CR 2016, 618, 621 mwNachw.

Smartphone (die Sensorik vorausgesetzt) einem Schadensfall entspricht und die Versicherungssumme überwiesen werden soll. Der bürokratische Aufwand würde sich immens vermindern. Ein anderes Beispiel wären Darlehensverträge. Hier könnte ein Smart Contract schon im Vorfeld überprüfen, ob überhaupt die Voraussetzungen für ein zu gewährendes Darlehen bestehen und dann über die Vertragslaufzeit über das Rückzahlungsverhalten wachen. Ein intelligenter Vertrag wäre auch - die entsprechenden Informationen vorausgesetzt - in der Lage das Ausfallrisiko des Darlehensnehmers zu bestimmen und gegebenenfalls das Finanzinstitut über ein erhöhtes Risiko zu informieren oder sogar selbst entsprechende Aktionen auszuführen. Ein weiteres Beispiel für einen selbst ausführenden Vertrag wäre auch die Datenvolumenbegrenzung bei Mobilfunkverträgen, hier wird die Datengeschwindigkeit automatisch gekürzt, wenn der Nutzer eine bestimmte Datengrenze erreicht hat. Diese Begrenzung wird erst wieder aufgehoben, wenn der laufende Bezugsmonat endet.

3. Grenzen

Die aufgeführten Automatisierungen stellen auch gleichzeitig die Grenze des Einsatzes von Smart Contracts und der Blockchain Technology dar: So kann zwar – wie dargestellt – etwa der Rücktritt oder der Widerruf automatisiert und selbst vollstreckend programmiert und damit durchgesetzt werden; andere Rechte indes werfen Probleme auf, etwa das Verlangen nach Nacherfüllung bzw. Nachbesserung. Da hier keine automatisierten Prozesse ausgelöst werden, können diese Rechte nach derzeitigem Stand nicht abgebildet werden. Auch beschränkt sich der Smart Contract hinsichtlich der Transaktionen auf digitale Inhalte oder zumindest digitale Schnittstellen, etwa der Bestätigung durch einen Paketzusteller, um eine Bezahlung auszulösen.[32] Ebenso wenig können unbestimmte Rechtsbegriffe ohne weiteres codiert werden, etwa einer angemessenen Frist oder wann ein Sachmangel vorliegt.[33]

Auch bei den Smart Contracts eröffnen sich viele weitere juristische Fragen, die bislang im Wesentlichen für die Bitcoins diskutiert werden.[34] So dürfte ein Smart Contract ohne weiteres den üblichen Inhaltskontrollen nach §§ 305 ff. BGB unterfallen[35] – da er aber nicht ex ante aufgehoben werden kann, stellt sich die Frage, wie die nachträgliche Nichtigkeit einer Klausel abgebildet werden kann.

Probleme bereiten aus Verbraucherschutzsicht auch die zahlreichen Informationspflichten zugunsten des Verbrauchers: Sollte der Verbraucher seinerseits halbautonome Agenten einsetzen, können die Informationspflichten ihm gegenüber nicht erbracht werden, sondern nur dem Agenten gegenüber, so dass sie diesbezüglich ins Leere gingen. Allerdings lassen sich ähnlich wie im Urheberrecht maschinenlesbare Informationen abbilden, so dass der Agent sogar besser als der Verbraucher in der Lage wäre, die spezifischen Gefährdungen für einen Verbraucher zu erkennen, da der Agent nicht unter dem information overload Problem leidet, das Informationspflichten häufig sinnlos erscheinen lässt.

Ferner ändert die Automatisierung nichts daran, dass die Kompetenz das Vorliegen eines Tatbestandelementes festzustellen einseitig einer Vertragspartei zugeschrieben wird – und nicht immer der Verteilung der Darlegungs- und Beweislast entspricht. So impliziert die Ausübung eines Rücktritts das Vorliegen eines Mangels – bei Streit hierüber kann die Blockchain Technology bzw. der Smart contract nicht darüber „entscheiden“, ob tatsächlich ein Mangel vorliegt. Die Ausübung des Rücktritts (oder eines Widerrufs) führt per se zur Rückabwicklung bzw. Auslösung der Transaktion; diese muss komplett in der Blockchain wiederum abgebildet werden.[36] Damit werden auch faktisch Darle-

[32] *Kaulartz/Heckmann,* CR 2016, 618, 620.
[33] *Kaulartz/Heckmann,* CR 2016, 618, 623.
[34] *König/Beck*, JZ 2015, 130, 130-138; *Spindler/Bille*, WM 2014, 1369 ff.
[35] So auch *Kaulartz/Heckmann,* CR 2016, 618, 622.
[36] *Kaulartz/Heckmann,* CR 2016, 618, 624.

gungs- und Beweislasten auf die andere Vertragspartei verlagert: So müsste etwa der Kunde das Vorliegen eines Mangels nachweisen, der Verkäufer könnte solange die Rückgewähr der Leistungen verweigern – bei einem Smart Contract würde dies automatisch ausgelöst, so dass der Verkäufer das Risiko trägt, die automatisch zurückgewährten Leistungen wieder zurückzuerlangen (§§ 812 ff. BGB). Zwar würde die bei einem Verbrauchsgüterkauf umgekehrte Darlegungs- und Beweislast in den ersten 6 Monaten gerade dem Verbraucher die Durchsetzung seiner Rechte erleichtern; der Rücktritt nach Ablauf dieser 6 Monate wäre jedoch nicht möglich, der Smart Contract müsste entsprechend codiert werden. Eine völlige Verlagerung auf Smart Contracting scheidet zumindest für diese Phasen aus.

Allerdings könnte hierin auch gerade eine Chance für eine Art Verbraucherschutz by design liegen: So wäre bei geringfügigen Ansprüchen (small claims) denkbar, dass der Verbraucher nur die Rückzahlung über die Blockchain auslösen muss, ohne dass es noch einer weiteren Prüfung bedürfte, etwa wenn die Wahrscheinlichkeit eines Anspruchs bei über 90% liegt. Das Risiko, bei unberechtigten Fällen der Anspruchsgeltendmachung durch den Verbraucher die (Kaufpreis-) Zahlung für den Unternehmen dennoch durchzusetzen bzw. das zuvor durch die Blockchain abgezogene Geld wieder zu erlangen, würde beim Unternehmer liegen.

Bislang nicht diskutiert sind zudem potentielle Probleme im Hinblick auf den Datenschutz: da die Transaktionen in der Blockchain abgebildet werden und auch die dazu gehörigen Rechtssubjekte unter Umständen identifiziert werden können, liegen im Prinzip persönliche Daten im Sinne der EU-DatenschutzgrundVO vor, die grundsätzlich von jedem eingesehen werden können, da sie Teil des Block Chains sind. Selbst wenn eine Anonymisierung vorliegt, da die Transaktionen verschlüsselt erfolgen, könnte von einer Identifizierung ausgegangen werden, da die Schlüssel hierfür verfügbar sind. Allerdings dürfte selbst dann die Durchführung in einer Blockchain häufig den Tatbestand des Art. 6 EU-DSGVO erfüllen, da die Daten für die Durchführung des Vertrages erforderlich sind, damit zumindest eine Rechtfertigung für die Verarbeitung der Daten vorliegt.

Letztlich handelt es sich bei den Smart Contracts aber bei Lichte besehen nur um eine effiziente Lösung des Vollzugs des eigentlichen Rechtsgeschäfts, mithin eher um ein Geschäft auf der Verfügungsgebene.[37]

B. Scoring und automatisierte Entscheidungen

1. Technologie

Als Scoring werden gemeinhin Algorithmen bezeichnet, die aufgrund eines Datensets und Profilen von Personen (aber auch anderen Bezugsobjekten) Werte ermitteln, die zusammen mit einem Benchmark-Wert automatisierte Entscheidungen ermöglichen[38].

2. Anwendungsgebiete

Bekanntestes Beispiel des Scoring sind Urteile über die Kreditwürdigkeit, etwa durch die SCHUFA in Deutschland. Aber auch zahlreiche andere Gebiete lassen sich durch entsprechende Profile bzw. Kriterien automatisierten, etwa die Entscheidung über die Vergabe von Mietwohnungen anhand von Persönlichkeitsprofilen, die weit mehr als nur die Kreditwürdigkeit enthalten, bis hin zu – heute noch utopischen – Zugangsbeschränkungen zu Veranstaltungen etwa mit Hilfe von Gesichtserkennungen (face targetting) und den dahinter liegenden Profilen, z.B. um gewaltbereite Besucher von Großveranstaltungen (Fußballspielen etc.) auszuschließen.

---

[37] Zutr. *Kaulartz/Heckmann,* CR 2016, 618, 623.

[38] So zum Beispiel *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD),* Verbraucher-Scoring; *ULD/Kamp/Weichert,* Scoringsysteme zur Beurteilung der Kreditwürdigkeit - Chancen und Risiken für Verbraucher; *ULD/GP Forschungsgruppe,* Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen.

Besonders effizient ist der Einsatz von Scoring in Zusammenhang mit digitalisierten Geschäftsmodellen, gerade im Finanzbereich, indem in Sekundenschnelle ohne menschliches Zutun Verträge abgeschlossen und auch durchgeführt werden können. Aber auch andere auf digitale Leistungen und Inhalte ausgerichtete Leistungen können hier eingebunden werden, sei es der Zugang zu sozialen Netzwerken, Streamingdiensten (Musik, Film etc.) oder allen nur denkbaren Plattformen, bei denen die Leistungserbringung sofort erfolgt.

3. Grenzen

Ungeachtet der datenschutzrechtlichen Grenzen (§ 6a BDSG bzw. Art. 22 EU-DSGVO) wirft die Automatisierung von sonst Menschen überlassenen Entscheidungen einige rechtliche Fragen auf: So unterliegen Entscheidungen über Vertragsabschlüsse (oder sonstigen rechtsgeschäftlichen Erklärungen wie z.B. die Zulassung zu Veranstaltungen) rechtlichen Bindungen, angefangen bei unzulässigen Diskriminierungen etwa wegen Geschlechts oder Glaubenszugehörigkeit (AGG) bis hin zu Kontrahierungszwängen bei Monopolisierungen (GWB, § 826 BGB[39]). Zudem erlauben automatisierte Entscheidungen keine Abweichung vom codierten Szenario und den erfassten (Benchmark-) Profilen. Ausnahmen, Einzelfälle oder Sonderkonstellationen können daher nicht erfasst werden, Personen, die buchstäblich durch das „Raster" eines Algorithmus fallen, sind dann de facto diskriminiert. Die den menschlichen Entscheidungsträgern immer mögliche Gesamtschau und abweichende Abwägung von Kriterien in besonders gelagerten Fällen lässt sich mit einem Algorithmus nicht abbilden. Die Qualität der Entscheidung hängt dann von der Granularität des Algorithmus ab – wobei allerdings selbstlernende Systeme in der Lage wären, Entscheidungen von Menschen, die Entscheidungen des Algorithmus abändern, für die Zukunft zu berücksichtigen und so das System perfektionieren könnten. Dennoch würde es stets bei einem Residuum von nicht zu prognostizierbaren Entscheidungen bleiben.

Algorithmen müssen daher einer Überprüfung zugänglich sein – und nicht nur der Aufsicht durch Datenschutzbehörden unterliegen – und zwar sowohl generell ex ante im Hinblick auf die Geeignetheit ihrer Entscheidungskriterien als auch im Einzelfall ex post, um ihre Entscheidungen überprüfen lassen zu können

C. Selbststeuernde Verkehrsmittel

1. Technologie

Die Prinzipien selbststeuernder Verkehrsmittel sind bereits ausführlich beschrieben worden, insbesondere für selbststeuernde KfZ: Mit Hilfe von Geo Location Tools, selbstlernenden Algorithmen und Remote Steuerung sowie Verkehrsleitsystemen kann die menschliche Steuerung ersetzt werden.

2. Anwendungsgebiete

Rechtliche Verhaltenspflichten lassen sich in mannigfaltiger Hinsicht codieren und substituieren: Schon das simple Anwendungsbeispiel von Geschwindigkeitsbeschränkungen verdeutlicht dies. Durch die Codierung der Verkehrsregeln und geforderten Verhaltenspflichten sowie der Übermittlung der entsprechenden Daten der Umwelt des jeweiligen Fahrzeugs lassen sich die gewünschten Regeln unmittelbar in das Fahrverhalten implementieren, ohne dass es noch der Schnittstelle Mensch/Maschine bedürfte. Aber nicht nur Verkehrsregeln, sondern auch weitergehende Pflichten, z.B. das Bilden von Rettungsgassen, lassen sich unmittelbar codieren, indem der Informationsaustausch zwischen verschiedenen KfZ und den Rettungskräften implementiert wird, so dass optimierte Wege selbständig durch die jeweiligen Fahrzeuge gebildet werden können.

[39] Vgl. *Spindler*, in: BeckOGK BGB, § 826 Rn. 20-25, 40-41, 53-54, 61-62 und insb. 76-79.

Neben der eigentlichen Substitution von Verkehrsregeln und –pflichten durch Code sind weitere Anwendungen möglich, die nicht mehr im engeren Sinne mit Verkehrspflichten verknüpft sind, etwa die effiziente Bewirtschaftung von Parkräumen und damit Vermeidung von Suchverkehr durch vernetztes Steuern und Gewinnung von Informationen über Verkehrssituationen.

3. Grenzen

Auch wenn auf den ersten Blick das selbststeuernde Kfz und die Codierung von Verkehrsregeln das Paradebeispiel für effiziente Substitution von Recht durch Technologie darstellt, handelt es sich doch oft um Ja/Nein-Entscheidungen (Rote Ampel etc.), liegen auch hier die Probleme wieder in Abweichungen von Regelfällen. Insbesondere das Überspielen von Verkehrsregeln in Notsituationen, etwa die zeitweise Überschreitung von Geschwindigkeitsbeschränkungen, um größeren Gefahrenlagen auszuweichen, und erst recht die ethischen Konflikte bei nicht ausweichbarer Gefährdung von gleichrangigen Rechtsgütern zeigen die Beschränkungen der Codierung von Recht auf.[40] Auch wenn diese Probleme oft eher theoretischer Natur sein mögen und die Verbesserung der Sicherheit gegenüber der traditionellen Schnittstelle Mensch/Maschine erheblich ist, zudem die eingesetzten Systeme lernfähig sind und daher eine konstante Verbesserung erreicht werden kann, bleibt es beim gegenwärtigen Stand dabei, dass der Fahrer nicht vollständig von seiner Verantwortung entbunden ist, sondern einsprungbereit sein muss, wenn das System sich wegen Zielkonflikte oder (noch) nicht bekannter Situationen abschaltet.[41] Bekannte Beispiele wie der jüngste tödliche Verkehrsunfall eines Tesla-Fahrzeugs wegen mangelhafter Erkennung eines Verkehrshindernis zeigen die erforderlichen Rückkoppelungen der Systeme.[42]

D. Urheberrecht: Digital Rights Management-Systeme

1. Technologie

Digital Rights Management-Systeme (DRM) ermöglichen es den Rechteinhabern an digitalen Inhalten (Musik, Filme, eBooks, Computer, Games etc.) in der einfachsten Form das Kopieren der Inhalte, in komplexeren Varianten aber auch deren Nutzung zu verhindern oder nur unter bestimmten Bedingungen zuzulassen. Schon in den achtziger Jahren waren derartige Verfahren als sog. „dongles“ bei Computersoftware verbreitet, fanden gegen Ende der neunziger Jahre Einzug in die Musik- und später Filmindustrie, sowie der elektronischen Bücher sowie Hörbücher.[43]

2. Anwendungsgebiete

Es liegt auf der Hand, dass DRM-Systeme unmittelbar rechtliche Beschränkungen umsetzen können: Wenn der Nutzer eines digitalen Inhalts nicht oder nicht mehr berechtigt ist, den Inhalt zu nutzen, können DRM-Systeme direkt die Beschränkung „vollziehen“. Sie verhindern ebenso unberechtigte Vervielfältigungen oder Verbreitungen ohne Zustimmung des Rechteinhabers, sie können bei verliehenen digitalen Inhalten die Leihe durch Zeitablauf unmittelbar beenden. Nicht unmittelbar urheberrechtlich bedingt, da die Nutzung eines Werkes frei ist, aber schuldrechtlich möglich, erlauben sie

---

[40] *Kunnert*, CR 2016, 509, 512; *Hilgendorf*, in: Hilgendorf/Hötitzsch/Lutz (Hrsg.), Rechtliche Aspekte automatisierter Fahrzeuge, 2014, S. 15, 30 f.

[41] *Spindler*, CR 2015, 766, 766-776; *Borges*, CR 2016, 272, 272-280; *Reichwald/Pfisterer*, CR 2016, 208, 209; *Horner/Kaulartz*, CR 2016, 7, 9.

[42] *Solmecke/Jockisch*, MMR 2016, 359, 361 ff.; *Jourdan/Matschi*, NZV 2015, 26, 28; *Hartwig/Doderer,* Tödlicher Tesla Unfall - Irrtümer und Rechtsfolgen – Stellungnahme, 2016, abrufbar unter http://www.kiam-net.de/wp-content/uploads/2016/07/To%CC%88dlicher-Tesla-Unfall-%E2%80%93-Irrtu%CC%88mer-und-Rechtsfolgen.pdf.

[43] *Manegold/Czernik*, in: Wandtke/Bullinger (Hrsg), Praxiskommentar zum Urheberrecht, Vor §§ 88 ff. UrhG, Rn. 111-113; *Ratjen/Langer*, ZUM 2012, 299, 302; *Guggemos*, ZUM 2004, 183, 183 ff.; *Rohleder*, ZUM 2004, 203, 203 f.; *Arlt*, GRUR 2004, 548, 549 ff.

auch, die Nutzung des Werkes gegen Entgelt zu steuern, indem jeder Aufruf des Werkes kontrolliert wird (z.B. durch eine Freigabe über das Netz gegen eine Mikrozahlung[44]).

Sowohl urheber- als auch vertragsrechtliche Beschränkungen können daher unmittelbar codiert und „automatisch vollzogen" werden, ohne dass es noch einer zwischengeschalteten menschlichen Instanz bedürfte.

3. Grenzen

Die selbst durchsetzenden DRMs zeigen aber auch gleichzeitig deren Probleme bzw. ihrer Codierung auf, insbesondere die Durchsetzung von urheberrechtlichen Schranken, die gerade zur Einschränkung von urheberrechtlichen Verwertungsrechten für bestimmte Sachverhalte im allgemeinen Interesse dienen. Ohne DRM-Systeme kann der Nutzer eines digitalen Inhaltes ohne weiteres die ihm zugunsten kommenden Schranken in Anspruch nehmen, mit DRM-Systemen hängt es davon ab, ob die Codierung die jeweilige Schranke bzw. die beabsichtigte Nutzung erkennen kann, um den digitalen Inhalt frei zu geben. Andernfalls muss der Nutzer versuchen, vom Rechteinhaber eine entsprechende Freigabe zu erhalten, was ihn gegenüber der Lage ohne DRM-Systeme entsprechend benachteiligt und vom Verhalten des Rechteinhabers abhängig macht. Im schlimmsten Fall kann der (berechtigte) Nutzer den Rechteinhaber nicht mehr erreichen oder ausfindig machen, so dass das DRM-System den digitalen Inhalt trotz entsprechender Schranke sperrt.

Viele Schranken hängen zudem von bestimmten privilegierten Nutzungen ab, deren Tatbestandsvoraussetzungen zudem von Interessenabwägungen oder von zusätzlichen exogenen Faktoren abhängen, etwa angemessenen Verlagsangeboten, der Nutzung für Unterrichts- oder Forschungszwecke, der Verwendung als Zitat und die Weitergabe von speziellen Softwarelizenzen etc.[45] DRM-Systeme können derartige auf den Einzelfall bezogene Abwägungen kaum abbilden und tendieren daher dazu, die Last der Durchsetzung auf den Nutzer zu verlagern – entgegen dem eigentlichen System des Urheberrechts.

Neben der Verschiebung der Balance im Urheberrecht führen DRM-Systeme aber auch zu unerwünschten Wettbewerbseffekten: So können mit Hilfe von DRM-Systemen nachgelagerte Märkte (Sekundärmärkte) beherrscht werden, indem digitale Inhalte nicht interportabel sind, mit anderen Worten nicht von einem Gerät auf ein anderes (systemfremdes) Gerät übertragen werden können, so dass Nutzer gezwungen sind, bestimmte (systemeigene) Geräte zu verwenden, um den digitalen Inhalt zu nutzen. Bekanntestes Beispiel bis vor wenigen Jahren war das Musiksystem von Apple – iTunes, das mit Hilfe von DRM-Systemen die Nutzung auf eine bestimmte Zahl von Geräten sowie auf Apple-Geräte beschränkte. Ebenso wenig können Nutzer die Inhalte an Dritte weitergeben, ohne dass gleichzeitig die nötigen Systemumgebungen geschaffen werden (Portabilität), etwa bei eBooks.

Schließlich können DRM-Systeme, die rückkanalfähig sind, Daten über den Nutzer an den Rechteinhaber (oder Dritte) weitergeben, was entsprechende Datenschutzprobleme zur Folge hat. Der Nutzer

---

[44] *Klein*, Systematisierung und Beurteilung von Micropayment-Systemen aus Nachfragersicht, S. 59 ff.; *Micali/Rivest,* Micropayments Recisited, S. 1 ff.; *Pass/Shelat*, Micropayments for Decentralized Currencies, 2016, S. 4 ff.; *Kerschbaumer*, Micropayment als Option für Verlage - Wer den Cent ehrt, 2014, abrufbar unter http://www.tagesspiegel.de/medien/micropayment-als-option-fuer-verlage-wer-den-cent-ehrt/10805422.html.

[45] *Groenenboom/Helberger/Orwat/Schaub* (INDICARE Projekt), Digital Rights Management (DRM) - Irgendwelche Nebenwirkungen?, 2006, S. 8 ff.; *Hansen/Möller*, Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung, 2014; *Ermert*, Grundrechtsverträgliche DRM-Systeme gesucht, abrufbar unter http://www.heise.de/newsticker/meldung/Grundrechtsvertraegliche-DRM-Systeme-gesucht-122241.html.

kann im Wege der DRM-Systeme im schlimmsten Fall ausgespäht werden, etwa im Fall eines von Sony betriebenen DRM-Systems, das den jeweiligen PC eines Nutzers auf weitere Dateien von Sony ausspähte und die Resultate an Sony übertrug. Darüber hinaus kann aber auch jedes sonstige Verhalten protokolliert und mit dem Nutzer in Verbindung gebracht werden, so dass massive Gefährdungen der informationellen Selbstbestimmung drohen.

E. Soziale Netzwerke und Kommunikation[46]

1. Technologie

Soziale Netzwerke zeichnen sich durch eine Vielzahl eingesetzter Softwarebestandteile und Applikationen aus, angefangen bei Kommunikationsmasken und –schnittstellen bis hin zur Ablage von Dateien und digitalen Inhalten jeglicher Art, insbesondere Bilder, Videos oder Musik. Mit Hilfe von bestimmten Erkennungsalgorithmen können z.B. Gesichter auf Bildern identifiziert und anderen Netzwerkteilnehmern zugeordnet werden, aber auch bestimmte Profile durch Anwendung verschiedener Kriterien (Schule, Werdegang, Freundeskreis etc.) erstellt werden. Aber auch allgemeine Nachrichten können platziert und verteilt werden, wobei wiederum durch Algorithmen deren Gewichtigkeit und Distribution bestimmt werden können.

2. Anwendungsgebiete

Die Anwendungsgebiete entsprechender Codierungen in sozialen Netzwerken und Kommunikationsplattformen sind zahlreich: So können grundsätzlich (kinder-) pornographische Darstellungen bzw. Bilder erkannt und unterbunden werden. Denkbar sind auch Filter gegen Hate Speech oder neonazistische Propaganda. Durch entsprechende Blockaden würden von vornherein unerwünschte bzw. illegale Kommunikationsinhalte unterbunden oder könnten entsprechend gekennzeichnet werden.[47]

3. Grenzen

Gerade die angesprochene Prüfung der Kommunikationsinhalte zeigt aber auch deren Grenzen auf: Denn fast immer müssen Verletzungen von Rechtsgütern oder Verstöße gegen Strafnormen in Ausgleich mit konkurrierenden Grundrechten, insbesondere der Meinungs-, aber auch Pressefreiheit gebracht werden. Vor allem hier sind Ja/Nein-Entscheidungen äußerst schwer zu prognostizieren, umfassende Einzelfallabwägungen bestimmen die Entscheidungen. Paradebeispiel hierfür ist jüngst der Fall der Zeitung Afterposten/Norwegen, die ein berühmtes Antikriegsbild aus dem Vietnamkrieg in ihren Facebook-Auftritt einstellte, das ein schreiendes nacktes Kind nach einem Napalm-Angriff zeigte. Facebook entfernte dieses Bild aufgrund seiner Richtlinien zu Nacktbildern, ohne die historisch-politische Dimension und ohne die Relevanz für die Pressefreiheit zu erkennen. Erst nach Protesten selbst der norwegischen Regierung wurde die Sperre zurückgenommen[48]. Selbst wenn man semi-autonome, adaptive Systeme einbezieht, erscheint zweifelhaft, ob die jeweiligen Einzelfälle tatsächlich automatisiert und ohne entsprechende Nebenwirkungen für legale Kommunikationen codiert werden können.

Aus anderer Perspektive können die angesprochenen Algorithmen ebenfalls Probleme aufwerfen, insbesondere wenn die Codierung zusammen mit der Marktmacht von Plattformen dazu benutzt werden, um bestimmte Nachrichten zu priorisieren, andere geringer zu gewichten. Entsprechende

---

[46] Umfänglich zu haftungsrechtlichen Fragen und Social Media s. *Spindler,* in: Hornung/Müller-Terpitz *(Hrsg.),* Rechtshandbuch Social Media, 2015, S. 131 ff.

[47] *Wüest*, Scams and Spam to Avoid on Facebook, 2012, S. 2 ff.; *Seethakkagari*/*Ralescu*, Identifying Interesting Postings on Social Media Sites, mwNachw.

[48] *Redaktion MMR-Aktuell*, MMR-Aktuell 2016, 381226.

Vorwürfe wurden etwa gegen Facebook erhoben, dass das soziale Netzwerk im US-Vorwahlkampf bestimmte Kandidaten implizit unterstützt hätte.

Last but not least werfen derartige Codierungen die bekannten Datenschutzprobleme bei sozialen Netzwerken auf, indem gerade die Erkennung von digitalen Inhalten und deren Koppelung mit bestimmten Nutzern zu den besagten Profilen führen und so ein erhöhtes Gefährdungspotenzial für Nutzer darstellen.

IV. Schlußbetrachtung

Lässt man die verschiedenen Beispiele sowie die Möglichkeiten und grundlegenden Probleme Revue passieren kristallisiert sich ein differenziertes Bild der Regulierung durch Technik heraus:

- In Situationen, in denen eindeutige Entscheidungen getroffen werden können, ist die Regulierung durch Technik sinnvoll

- gleiches gilt für die Überwindung von Verhaltensanomalien, wie etwa durch ein „privacy by design", indem opt-in Technologien statt opt-out bevorzugt werden.

- blockchain technology kann eingesetzt werden, wenn bewußt dem Unternehmer das Risiko einer nicht gerechtfertigen Geltendmachung von Verbraucherschutzrechten überantwortet werden soll, sofern diese statistisch kaum relevant sind und die Durchsetzung von Verbraucherschutzrechten damit wesentlich effektuiert wird, etwa im Bereich von geringfügigen Ansprüchen der Verbraucher (small claims)

- umgekehrt sollten Algorithmen nur als Hilfsmittel eingesetzt werden, wenn die erforderlichen Entscheidungen komplexer Natur sind, insbesondere wenn es um Filter- und Blockadetechnologien im Bereich der Meinungsfreiheit geht. Eine menschliche Kontrolle erscheint hier unabdingbar.

- technische Schutzmittel dürfen nicht zu einem weitergehenden Schutz des Anwenders führen, als wie sie das Recht ihm zugestehen würde (DRM-Systeme)

Die Algorithmen sollten insgesamt jedoch einer Produktaufsicht unterstellt werden, wenngleich dies auch nur punktuell gelingen wird – aber allein die Risiken durch von Privaten aufgestellte Abwägungsprogramme und ggf. Fehlsteuerungen sowie Monopolisierungen drohen, rechtfertigen eine staatliche Kontrolle.[49] Dies gilt insbesondere im Hinblick auf automatisierte Entscheidungen (Scoring), bei denen dem Grundansatz des § 28b BDSG folgend der Stand der Technik dargelegt werden muss, zudem die Kriterien und ihr Zusammenspiel bei der Entscheidungsfindung. Es muss dem Staat, insbesondere Gerichten, die Kontrolle der Entscheidung möglich bleiben.

[49] S. dazu generell auch *Brown/Marsden*, Regulating Code: Good Governance and Better Regulation in the Information Age, MIT Press 2013; s. auch *Brownsword/Yeung* (eds.), Regulating Technologies, Hart Publishing 2008; *Brownsword*, Int.J.Law and Technology 20 (2012) 249;

V. Literaturverzeichnis

- *Arlt*, Digital Rights Management-Systeme - Begriff, Funktion und rechtliche Rahmenbedingungen nach den jüngsten Änderungen des UrhG - insbesondere zum Verhältnis der §§ 95a ff. UrhG zum Zugangskontrolldiensteschutzgesetz (ZKDSG), GRUR 2004, 548.
- *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung - Eine erste juristische Einordung, MMR 2014, 75.
- *Borges*, Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272.
- *Bunk/Goldschmidt*, Big Data und die Dual-Use Problematik am Beispiel öffentlicher Daten, DuD 2016, 463.
- *Buttarelli*, Zusammenfassung der Stellungnahme des Europäischen Datenschutzbeauftragten: „Bewältigung der Herausforderungen in Verbindung mit Big Data: Ein Ruf nach Transparenz, Benutzerkontrolle, eingebautem Datenschutz und Rechenschaftspflicht“, EuABl. C 67, 13.
- *Cadjan/Harris*, Administering NDS, 1999.
- *Ciavarrini/Disperati/Lenzini/Luconi/Vecchio*, Geolocation of Internet hosts using smartphones and crowdsourcing, 2015, abrufbar unter: http://portolanproject.iit.cnr.it/wp-content/uploads/2015/11/geolocation.pdf (zuletzt abgerufen am 03.10.2016).
- *Ermert*, Grundrechtsverträgliche DRM-Systeme gesucht, 2006, abrufbar unter http://www.heise.de/newsticker/meldung/Grundrechtsvertraegliche-DRM-Systeme-gesucht-122241.html (zuletzt abgerufen am 05.10.2016).
- *Geiling*, BaFin, 2016, Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain, abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2016/fa_bj_1602_blockchain.html (zuletzt abgerufen am 06.10.2016).
- *Gierschmann*, Was “bringt“ deutschen Unternehmen die DS-GVO?, ZD 2016, 51.
- *Goerdeler/Laubach*, Im Datendschungel - Zur Notwendigkeit der gesetzlichen Regelung von genetischen Untersuchungen, ZRP 2002, 115.
- *Groenenboom/Helberger/Orwat/Schaub* (INDICARE Projekt), Digital Rights Management (DRM) - Irgendwelche Nebenwirkungen?, 2006, abrufbar unter http://www.indicare.org/tiki-download_file.php?fileId=194 (zuletzt abgerufen am 05.10.2016).
- *Gsell/Krüger/Lorenz/Mayer* (Hrsg.), beck-online.Grosskommentar (BeckOGK), Kommentierung BGB, Stand 2016.
- *Gueye/Ziviani/Crovella/Fdida*, ACM Konferenzbeitrag: Constraint-Based Geo-location of Internet Hosts, 2004, abrufbar unter: http://cs-www.bu.edu/faculty/crovella/paper-archive/imc04-geolocation-full.pdf (zuletzt abgerufen am 03.10.2016).
- *Guggemos*, Digital Rights Management im praktischen Einsatz, ZUM 2004, 183.
- *Hancock/Vaizey*, Distributed Ledger Technology: beyond block chain - A report by the UK Government Chief Scientific Adviser, 2016, abrufbar unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (zuletzt abgerufen am 06.10.2016).
- *Hansen/Möller*, Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung, 2014, abrufbar unter https://www.datenschutzzentrum.de/vortraege/050510_hansen-moeller_bsi.htm (zuletzt abgerufen am 05.10.2016).
- *Hartwig/Doderer*, Tödlicher Tesla Unfall - Irrtümer und Rechtsfolgen – Stellungnahme Juli 2016, abrufbar unter http://www.kiam-net.de/wp-content/uploads/2016/07/To%CC%88dlicher-Tesla-Unfall-%E2%80%93-Irrtu%CC%88mer-und-Rechtsfolgen.pdf (zuletzt abgerufen am 04.10.2016).

- *Heuer*, Seminararbeit: Angriffssicherheit bei eingebetteten Systemen, 2015, abrufbar unter https://www.uni-koblenz-landau.de/de/koblenz/fb4/ist/AGZoebel/Lehre/Sommer2015/SeminarASidA/A2 (zuletzt abgerufen am 03.10.2016).
- *Hilgendorf,* Teilautonome Fahrzeuge: Verfassungsrechtliche Vorgaben und rechtspolitische Herausforderungen, in: Hilgendorf/Hötitzsch/Lutz (Hrsg.), Rechtliche Aspekte automatisierter Fahrzeuge: Beiträge zur 2. Würzburger Tagung zum Technikrecht im Oktober 2014, 2015, S. 15.
- *Holland*, ConnectedDrive: Der BMW-Hack im Detail, abrufbar unter http://www.heise.de/newsticker/meldung/ConnectedDrive-Der-BMW-Hack-im-Detail-2540786.html (zuletzt abgerufen am 03.10.2016).
- *Holznagel*, Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425.
- *Horner/Kaulartz*, Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7.
- *Kahneman/ Tversky*, Choices, Values and Frames. Cambridge University Press, 2000;
- *Jourdan/Matschi*, Automatisiertes Fahren - Wie weit kann die Technik den Fahrer ersetzen? Entwickler oder Gesetzgeber, wer gibt die Richtung vor?, NZV 2015, 26.
- *Kaulartz,* Die Blockchain-Technologie, CR 2016, 474.
- *Kerschbaumer*, Micropayment als Option für Verlage - Wer den Cent ehrt, 2014, abrufbar unter http://www.tagesspiegel.de/medien/micropayment-als-option-fuer-verlage-wer-den-cent-ehrt/10805422.html (zuletzt abgerufen am 05.10.2016).
- *Klein*, Systematisierung und Beurteilung von Micropayment-Systemen aus Nachfragersicht, abrufbar unter http://subs.emis.de/LNI/Proceedings/Proceedings59/GI-Proceedings.59-5.pdf (zuletzt abgerufen am 05.10.2016).
- *König/Beck*, Bitcoin: Der Versuch einer vertragstypologischen Einordnung von kryptographischem Geld, JZ 2015, 130.
- *Kunnert*, Konkrete datenschutzrechtliche Vorgaben für die Gestaltung von Kfz-IT und sonstiger Komponenten intelligenter Verkehrssysteme, CR 2016, 509.
- *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372.
- *Lessig*, Code Version 2.0, 2006, abrufbar unter: http://codev2.cc/download+remix/Lessig-Codev2.pdf (zuletzt abgerufen am 06.09.2016).
- *Micali/Rivest*, Micropayments Recisited, abrufbar unter https://people.csail.mit.edu/rivest/MicaliRivest-MicropaymentsRevisited.pdf (zuletzt abgerufen am 05.10.2016).
- *Mik*, The erosion of autonomy in online consumer transactions, Law, Innovation and Technology 8 (2016), abrufbar unter http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3688&context=sol_research (zuletzt abgerufen am 09.10.2016).
- *Pass/Shelat*, Micropayments for Decentralized Currencies, 2016, abrufbar unter https://eprint.iacr.org/2016/332.pdf (zuletzt abgerufen am 05.10.2016).
- *Piotrowski*, A Next-Generation Smart Contract and Decentralized Application Platform (White Paper), 2016, abrufbar unter https://github.com/ethereum/wiki/wiki/White-Paper (zuletzt abgerufen am 06.10.2016).
- *Ratjen/Langer*, Die räumliche Aufspaltung von Filmlizenzen am Beispiel der Vergabe der Medienrechte der Deutschen Fußball Liga, ZUM 2012, 299.
- *Redaktion MMR-Aktuell*, Privacy by Design-Forschung zur Wahrung der Privatsphäre, MMR-Aktuell 2015, 373362.
- *Reichwald/Pfisterer*, Möglichkeiten und Grenzen autonomer Handlungen, CR 2016, 208.

- *Richter*, Instrumente zwischen rechtlicher Steuerung und technischer Entwicklung, DuD 2016, 89.
- *Rohleder*, Herausforderung und Chance in der digitalen Welt, ZUM 2004, 203.
- *Schütze*, EU: ENISA veröffentlicht Bericht zu Privacy by Design in Big Data, ZD-Aktuell 2016, 05015.
- *Seethakkagari/Ralescu*, Identifying Interesting Postings on Social Media Sites, abrufbar unter http://ceur-ws.org/Vol-710/paper45.pdf (zuletzt abgerufen am 05.10.2016).
- *Shleifer*, Inefficient Markets: An Intro-duction to Behavioral Finance. Oxford University Press, 1999
- *Solmecke/Jockisch*, Das Auto bekommt ein Update! – Rechtsfragen zu Software in Pkws - Zulassungs- und Haftungsfragen zu softwarebasierten Fahrzeugsystemen, MMR 2016, 359.
- *Spindler*, Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766.
- *Ders.*, Haftungsrechtliche Probleme der Social Media, in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2015, S. 131.
- *Steinebach/Jung/Krempel/Hoffmann*, Datenschutz und Datenanalyse, DuD 2016, 440.
- *Szabo*, Smart Contracts, 1994, abrufbar unter http://szabo.best.vwh.net/smart.contracts.html (zuletzt abgerufen am 06.09.2016).
- *Tian/Dey/Liu/Ross*, China's Internet: Topology Mapping and Geolocating, 2015, abrufbar unter http://staff.ustc.edu.cn/~yetian/pub/TechRep_ChinaInternet_11.pdf (zuletzt abgerufen am 03.10.2016).
- *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)/GP Forschungsgruppe*, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, abrufbar unter https://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/studie-scoring.pdf?__blob=publicationFile (zuletzt abgerufen am 03.10.2016).
- *ULD/Kamp/Weichert*, Scoringsysteme zur Beurteilung der Kreditwürdigkeit - Chancen und Risiken für Verbraucher, 2005, abrufbar unter https://www.datenschutzzentrum.de/scoring/2005-studie-scoringsysteme-uld-bmvel.pdf (zuletzt abgerufen am 03.10.2016).
- *ULD*, Verbraucher-Scoring, 2010, abrufbar unter https://www.datenschutzzentrum.de/blauereihe/blauereihe-scoring.pdf (zuletzt abgerufen am 03.10.2016).
- *Wandtke*/*Bullinger* (Hrsg.), Praxiskommentar zum Urheberrecht, 4. Auflage 2014.
- *Weisser/Glas*, Die medienrechtliche Regulierung von Plattformen, ZUM 2009, 914.
- *Wüest*, Scams and Spam to Avoid on Facebook, 2012, abrufbar unter http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/scams_and_spam_to_avoid_on_facebook.pdf (zuletzt abgerufen am 05.10.2016).

Sachverständigenrat für Verbraucherfragen

Der Sachverständigenrat für Verbraucherfragen ist ein Beratungsgremium des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV). Er wurde im November 2014 vom Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, eingerichtet. Der Sachverständigenrat für Verbraucherfragen soll auf der Basis wissenschaftlicher Erkenntnisse und unter Berücksichtigung der Erfahrungen aus der Praxis das Bundesministerium der Justiz und für Verbraucherschutz bei der Gestaltung der Verbraucherpolitik unterstützen.

Der Sachverständigenrat ist unabhängig und hat seinen Sitz in Berlin.

Vorsitzende des Sachverständigenrats ist Prof. Dr. Lucia Reisch.

SVRV Sachverständigenrat für Verbraucherfragen