Mirko Andreas Wieczorek (Hrsg.)

Digitalisierung

Rechtsfragen rund um die digitale Transformation der Gesellschaft

Tagungsband Liberale Rechtstagung 2018

Cuvillier Verlag Göttingen
Internationaler wissenschaftlicher Fachverlag

Digitalisierung – Rechtsfragen rund um die digitale Transformation der Gesellschaft

Tagungsband Liberale Rechtstagung 2018

Digitalisierung – Rechtsfragen rund um die digitale Transformation der Gesellschaft

Tagungsband Liberale Rechtstagung 2018

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.
1. Aufl. - Göttingen: Cuvillier, 2018

Nonnenstieg 8, 37075 Göttingen
Telefon: 0551-54724-0
Telefax: 0551-54724-21
www.cuvillier.de

1. Auflage, 2018
Gedruckt auf umweltfreundlichem, säurefreiem Papier aus nachhaltiger Forstwirtschaft.
ISBN 978-3-7369-9880-3
eISBN 978-3-7369-8880-4

Vorwort

„Digitalisierung – Rechtsfragen rund um die digitale Transformation der Gesellschaft“ – dieses Motto trägt die erste von VSA und FNF ausgerichtete Liberale Rechtstagung. Das Motto wurde hierbei nicht zufällig gewählt: Die hochaktuellen Themen der Digitalisierung beschäftigen die Gesellschaft insgesamt und werfen damit auch zahlreiche rechtliche Fragen auf. Die Liberale Rechtstagung 2018 soll einen Beitrag dazu leisten, Antworten zu diesen Fragen zu finden.

Dabei ist das Spektrum der Tagung weit gesteckt. Es werden unter anderem die Themenbereiche Robotik und KI, Digitalisierung von Märkten, Legal Tech, Datenschutz und Internet der Dinge abgedeckt. So konnten 16 Beiträge ausgewählt und zu diesem Tagungsband zusammengefasst werden. Sie beleuchten spannende Rechtsfragen beispielsweise im Zusammenhang mit der im Mai 2018 „scharfgestellten“ europäischen Datenschutzreform oder im Hinblick auf Zukunftsthemen wie dem autonomen Fahren, der Blockchain-Technologie oder der digitalen Marktmacht von Unternehmen.

Dank gilt an dieser Stelle in erster Linie den Referenten der diesjährigen Tagung. Mit der – vorbildlich termintreuen – Einreichung der Tagungsbeiträge sowie der Bereitschaft, zu ihrem Thema vorzutragen und sich einer anschließenden Diskussion zu stellen, haben sie maßgeblich zum Gelingen der Veranstaltung beigetragen. Dabei konnte der Fachkreis Recht, der die Liberale Rechtstagung für VSA und FNF ausrichtete, mit der Resonanz auf den im Frühjahr 2018 eröffneten Call for Papers, den Themenvorschlägen sowie der Qualität der letztendlich eingereichten Beiträge hochzufrieden sein.

Bei Vorbereitung und Durchführung der Veranstaltung ist der Fachkreis Recht dem VSA (insbesondere dem Geschäftsführer Christian Huß), der FNF und der THA (insbesondere Martin Thoma, Klaus Füßmann und dem gesamten Team der THA) zu großem Dank verpflichtet. Sie haben die Idee der Liberalen Rechtstagung euphorisch aufgegriffen und den Fachkreis Recht von Anfang an vorbehaltlos bei deren Realisierung unterstützt. Fachkreisintern geht ein besonderer Dank an Kira Schulze Lohoff, Dominik Fiedler, Julia Münzenmaier, Hannah Birkhoff, Martin Trayer und weitere unermüdliche Unterstützer, ohne die die Tagung nicht hätte zustande kommen können. Schließlich möchten wir Staatssekretär Dirk Wedel unsere Wertschätzung ausdrücken, der die Keynote Speech am 7. Dezember 2018 halten und die Liberale Rechtstagung als Schirmherr begleiten wird.

Besonderer Dank gilt den Kooperationspartnern des VSA. Sie haben es möglich gemacht, dass am 8. Dezember 2018 eine Karrieremesse stattfinden kann, die sich insbesondere an die noch nicht im Berufsleben stehenden Teilnehmer der Tagung richtet.

Zudem flossen ihre Spenden in den Druck dieses Tagungsbandes und haben uns ermöglicht, einen Best Paper Award und einen Best Speech Award mit attraktiven Preisen für die Gewinner ausloben zu können. Ausgezeichnet werden Referent*innen, die noch am Anfang ihrer wissenschaftlichen Karriere stehen und dennoch bereits herausragende Leistungen demonstriert haben. Vor diesem Hintergrund möchte sich der Fachkreis Recht im Namen der Ausrichter bei Accenture, Afringa, Bernstein Group, Kienbaum, McKinsey & Company, SOH (Schmidt, von der Osten, Huber), Boston Consulting Group sowie undconsorten für ihr beispielloses ehrenamtliches Engagement bedanken.

Der Fachkreis Recht freut sich, bereits an dieser Stelle mitteilen zu können, dass die Liberale Rechtstagung 2019 wieder in der THA stattfinden soll, wobei der November/Dezember 2019 angedacht ist, aber ein genaues Datum derzeit noch nicht feststeht. Dieses werden wir spätestens auf der diesjährigen Tagung mitteilen können. Das Thema der nächsten Tagung steht ebenfalls noch nicht fest; VSA-Mitglieder oder solche, die es werden möchten, sind herzlich dazu eingeladen, dem VSA und dem Fachkreis Recht beizutreten und an der Themenfindung und Ausrichtung mitzuwirken. Kooperationspartner, die an der Karrieremesse teilnehmen möchten, mögen sich bitte frühzeitig an den Geschäftsführer des VSA wenden und die Modalitäten klären. Fachkreis Recht, VSA, FNF und THA freuen sich auf ein Wiedersehen zur Liberalen Rechtstagung 2019!

Gummersbach, im September 2018

Dr. Mirko Andreas Wieczorek

Koordinator des Fachkreises Recht des VSA

Inhalt

Der programmierte Tod?

Autonomes Fahren und die strafrechtliche Behandlung dilemmatischer Situationen

Maximilian Lenk

Akademischer Mitarbeiter, Universität Tübingen
Maximilian.Lenk@uni-tuebingen.de

Abstract

Die Programmierung von Fahrzeugen eröffnet in erster Linie große Chancen. Gleichzeitig stellt sie Programmierer und Hersteller autonomer Fahrsysteme vor ethische Entscheidungen, die bislang der menschlichen Intuition überlassen bleiben konnten. Bei der Programmierung solcher Fahrsysteme für dilemmatische Situationen, in denen es gilt, Menschenleben um den Preis anderer Menschenleben zu retten, stellen sich Fragen um strafrechtliche Verantwortlichkeiten. Diesen will der folgende Beitrag nachgehen.

I. Einführung

Die Automobilhersteller überbieten sich derzeit mit Zukunftsvisionen für das durch den Abgasskandal gebeutelte Automobil. Integraler Bestandteil dieser Visionen ist das autonome Fahren, welches einen menschlichen Fahrer zunächst in spezifischen Anwendungsfällen (Automatisierungsgrad 4) und schließlich vom Start bis zum Ziel gänzlich obsolet (Automatisierungsgrad 5) machen soll.[1] Die „Vision Zero“, mit der die Automobilindustrie und zahlreiche ihrer Partner anstreben, die Getöteten und Schwerverletzten im Straßenverkehr auf null zu reduzieren, bleibt (vorerst) eine Utopie. Das derzeitige technische Entwicklungsniveau kann innerhalb eines heterogenen, nicht vernetzten Straßenverkehrs einen unfallfreien Straßenverkehr jedenfalls in naher Zukunft nicht gewährleisten.[2]

Folglich wirft die Programmierung autonomer Fahrsysteme strafrechtliche Fragen auf, wenn es gilt, das Fahrzeug auf Unfallsituationen „vorzubereiten“ und dabei zwischen Menschenleben abzuwägen. Zwar beteuert die Automobilindustrie, dass sich

[1] S. zu den Automatisierungsgraden *VDA*, Automatisierung, S. 15.
[2] Vgl. *BMVI*, Bericht, S. 6.

viele der konstruierten Dilemmasituationen nicht stellten, solange Sensoren wie beispielsweise Radar, Kamera oder Laserscanner noch nicht in der Lage sind, eine genaue Differenzierung von Personen vorzunehmen.[3] Doch wollen wir gerade auch solche Möglichkeiten, vor denen der technische Fortschritt jedenfalls auf lange Sicht nicht Halt machen wird, mit in die Betrachtung einbeziehen. Zum besseren strafrechtlichen Verständnis soll der Blick zunächst auf die strafrechtliche Verantwortlichkeit des menschlichen Fahrers gerichtet werden, der sich einer dilemmatischen Situation ausgesetzt sieht. Es folgt die Auseinandersetzung mit der Frage, ob und wie sich diese strafrechtlichen Ergebnisse auf bereits im Voraus programmierte Entscheidung übertragen lassen und eine entsprechende Strafbarkeit des Programmierers begründen.

II. Zur strafrechtlichen Verantwortlichkeit des menschlichen Fahrers in dilemmatischen Situationen

Die strafrechtlich relevanten Wertungsfragen auf Rechtfertigungs- und Schuldebene sollen zunächst anhand der strafrechtlichen Verantwortlichkeit des menschlichen Fahrers in dilemmatischen Situationen aufgezeigt werden.

1. Rechtfertigender Notstand, § 34 StGB

Der rechtfertigende Notstand ist ausgerichtet am Prinzip der Interessenabwägung. Hiernach rechtfertigt die Vorschrift den Eingriff in ein Rechtsgut, wenn ein anderes rechtlich geschütztes und deutlich höherwertiges Interesse auf andere Weise nicht gerettet werden kann.[4] § 34 StGB verlangt vor dem Hintergrund der begrenzten Solidaritätspflichten der Bürger untereinander ein „wesentliches“ Überwiegen des geschützten gegenüber dem beeinträchtigten Interesse. Die solidarische Aufopferung von Rechtsgütern eines unbeteiligten Dritten billigt die Strafrechtsordnung daher nur bei dieser einseitigen Interessenlage zugunsten des geschützten Rechtsguts.[5]

Weicht beispielsweise der Fahrer F zur Vermeidung eines ansonsten für ihn selbst oder einen unbekümmert über die Straße daherkommenden Passanten tödlich verlaufenden Verkehrsunfalls aus und nimmt dabei die Beschädigung des am Straßenrand parkenden Fahrzeugs eines Dritten in Kauf, fällt die Interessenabwägung zweifelsohne zugunsten des menschlichen Lebens aus, sodass die (hier vorausgesetzte) tatbestandliche Sachbeschädigung (vgl. § 303 Abs. 1 StGB) gem. § 34 StGB gerechtfertigt ist.[6]

Leben-gegen-Leben-Dilemmata überschreiten hingegen die Grenzen des rechtfertigenden Notstands, weil die Grundrechtsdogmatik eine Abwägung zwischen menschli-

[3] So *VDA*, Automatisierung, S. 23.
[4] Vgl. *Zieschang*, in: LK-StGB, § 34 Rn. 2 f.
[5] Hierzu *Hörnle/Wohlers*, GA 2018, 12 (15).
[6] Ähnliche Beispiele bei *Engländer*, ZIS 2016, 608 (609).

chen Leben verbietet.[7] Dies gilt sowohl in quantitativer (Anzahl der gefährdeten Menschenleben) als auch qualitativer (etwa die Qualifizierung nach Alter, Geschlecht oder körperlicher und geistiger Konstitution) Hinsicht. Demgemäß scheidet eine Rechtfertigung gem. § 34 StGB aus, wenn durch das Ausweichmanöver des F eine auf der Straße befindliche Kindergartengruppe gerettet, hierfür aber das Leben der auf dem Gehsteig daherkommenden 90-jährigen Rentnerin R geopfert wird. Sodann bleibt die Tat rechtswidrig, mithin das strafrechtliche Unrecht bestehen.

2. Entschuldigender Notstand, § 35 StGB

Fraglich ist, ob gegen den Fahrer im Weiteren ein Schuldvorwurf erhoben wird. In Betracht kommt zunächst der entschuldigende Notstand (§ 35 StGB), welcher einer außergewöhnlichen Motivationslage des Täters Rechnung trägt.[8] Er entschuldigt den Täter, wenn sein aus der Gefährdung fundamentalster Rechtsgüter (Leib, Leben, Freiheit) von sich oder eine ihm persönlich nahestehenden Person erwachsende Selbst- (bzw. Dritt-)erhaltungstrieb die Motivation zu rechtmäßigem Verhalten überstrahlt.[9]

Demgemäß handelt der Fahrer F in der Regel entschuldigt, wenn er einer für ihn lebensgefährlichen Verkehrssituation ausweicht und dadurch den Tod des auf dem Fußgängerweg schlendernden Passanten verursacht. Dies gilt im Einzelfall nicht, wenn er die Gefahr selbst verursacht hat (vgl. § 35 Abs. 1 S. 2 StGB), indem er etwa mit stark überhöhter Geschwindigkeit fuhr.[10] Handelt er aber zum Schutz Dritter – ihm nicht nahestehender – Personen, erkennt der entschuldigende Notstand die Motivationslage des F von vornherein nicht an. Im Beispielsfall scheidet für das Ausweichmanöver zum Schutz der Kindergartengruppe und zum Nachteil der Rentnerin R eine Entschuldigung gem. § 35 StGB aus.

3. Übergesetzlicher entschuldigender Notstand

Handelt der Täter nicht zur eigenen oder der Lebensrettung einer ihm nahestehenden Person, kommt letztlich nur ein übergesetzlicher entschuldigender Notstand (analog § 35 StGB) in Betracht, der in seinen Voraussetzungen umstritten ist.[11] Im Ausgangspunkt sind die folgenden zwei Konstellationen zu unterscheiden:

---

[7] Vgl. *Hörnle/Wohlers*, GA 2018, 12 (14).
[8] Vgl. *Zieschang*, in: LK-StGB, § 35 Rn. 3.
[9] Vgl. *Zieschang*, in: LK-StGB, § 35 Rn. 3.
[10] *Engländer*, ZIS 2016, 608 (609 f.). Allein in der Benutzung des Kraftfahrzeugs, die zivilrechtlich eine Gefährdungshaftung begründet, ist keine Gefahrverursachung im Sinne des § 35 Abs. 1 S. 2 StGB zu sehen, weil es insoweit auf eine vorwerfbare Gefahr ankommt (vgl. *Weber*, NZV 2016, 249 (251)).
[11] Relevant wurde der übergesetzliche entschuldigende Notstand in den „Euthanasie"-Fällen während der NS- Herrschaft, die nach dem 2. Weltkrieg abgeurteilt wurden (*BGH*, NJW 1953, 513). Seit dem 11.09.2001 wird im Zusammenhang mit dem Abschuss eines Passagierflugzeugs, das von Terroristen gekapert wurde und bspw. auf ein vollbesetztes Stadion zusteuert, über den übergesetzlichen entschuldigenden Notstand diskutiert (vgl. *Rönnau*, in: LK-StGB, Vor § 32 Rn. 343 ff.).

a) Gefahrengemeinschaften

Erstens die Situationen, in denen Träger von Rettungsgut und Eingriffsgut eine Gefahrgemeinschaft bilden, die bei ungehindertem Fortlauf in Gänze verloren ist, sofern nicht einzelne ihrer Mitglieder „geopfert" werden.[12] So lagen beispielsweise die „Euthanasie"-Fälle:[13] Anstaltsärzte standen während der NS-Herrschaft vor der Wahl, gem. dem „Euthanasie"-Befehl einige Patienten zu töten, um im Gegenzug anderen Patienten das Leben zu retten, oder aber nicht mitzuwirken, was ihre Ersetzung durch linientreuere Ärzte und weit mehr Tote zur Folge gehabt hätte. Hierbei wird dem Täter der übergesetzliche entschuldigende Notstand überwiegend zugestanden, weil der Täter den ansonsten unausweichlichen Tod aller auf das „kleinere Übel" beschränkt.[14] Solche Situationen sind im Straßenverkehr aber kaum vorstellbar.[15]

b) Quantitativer Lebensnotstand

Von Relevanz ist vielmehr die zweite Konstellation, nämlich die des quantitativen Lebensnotstands, für die charakteristisch ist, dass der Täter die Gefahr für eine größere Gruppe auf eine kleinere Gruppe zuvor ungefährdeter Personen umlenkt.[16] Um die Anerkennung des übergesetzlichen entschuldigenden Notstands in diesem Fall des quantitativen Notstands herrscht Streit.[17] Mithin hängt vom Ergebnis dieses Streitentscheids ab, ob sich der Fahrer F, der zur Rettung der Kindergartengruppe ausweicht und dadurch den Tod der Rentnerin R in Kauf nimmt, auf den übergesetzlichen entschuldigenden Notstand berufen kann.

Die (wohl) herrschende Ansicht hält den übergesetzlichen entschuldigenden Notstand auch in Situationen des quantitativen Lebensnotstands für einschlägig.[18] Sie beruft sich insbesondere auf den Motivationsdruck, dem sich der Täter beim quantitativen Notstand in gleichem Maße wie im Fall der Gefahrengemeinschaft ausgesetzt sieht.[19] Gewichtige Stimmen stehen ihm hingegen ablehnend gegenüber, weil andern-

[12] Vgl. hierzu *Rönnau*, in: LK-StGB, Vor § 32 Rn. 343.
[13] Vgl. *BGH*, NJW 1953, 513.
[14] So etwa *Neumann*, in: NK-StGB, § 35 Rn. 60.
[15] Vgl. aber die (konstruierte) „Fahrschlauch"-Situation bei *Hilgendorf*, ZStW 2018 (im Erscheinen).
[16] Vgl. hierzu *Rönnau*, in: LK-StGB, Vor § 32 Rn. 344.
[17] Prägend für den Streit in der strafrechtswissenschaftlichen Literatur ist der auf *Welzel*, ZStW 1951, 47 (51) zurückgehende sog. „Weichensteller"-Fall: „Auf einer steilen Gebirgsstrecke hat sich ein Güterwagen gelöst und saust mit voller Wucht ins Tal auf einen kleinen Bahnhof zu, auf dem gerade ein Personenzug steht. Würde der Güterwagen auf dem bisherigen Gleise weiterrasen, so würde er auf den Personenzug stoßen und eine große Anzahl von Menschen töten. Ein Bahnbeamter, der das Unheil kommen sieht, reißt in letzter Minute die Weiche um, die den Güterwagen auf das einzige Nebengleis lenkt, auf dem gerade einige Arbeiter einen Güterwagen entladen. Durch den Anprall werden, wie der Beamte voraussah, drei Arbeiter getötet."
[18] *Eisele*, in: Baumann/Weber/Mitsch/Eisele, AT, § 18 Rn. 49; *Lenckner/Sternberg-Lieben*, in: Sch/Sch, Vor § 32 Rn. 117a; *Rönnau*, in: LK-StGB, Vor § 32 Rn. 347; vgl. auch *Welzel*, ZStW 1951, 47 (54).
[19] Vgl. *Rönnau*, in: LK-StGB, Vor § 32 Rn. 347.

falls das verfassungsrechtliche Verbot der Verrechnung menschlichen Lebens umgangen würde.[20] Mithin befürchten sie durch die damit einhergehende Relativierung auf Schuldebene einen Dammbruch bzgl. des quantitativen und qualitativen Abwägungsverbots zwischen menschlichen Leben schlechthin.[21] Der Täter maße sich gewissermaßener an, „Schicksal zu spielen, indem er unbeteiligte Dritte mit Gefahren belastet, die von der Vorsehung gerade nicht vorgegeben sind."[22]

Es ist hier nicht der Raum dafür, den Streit zu entscheiden. Die Argumente, welche gegen die Annahme des übergesetzlichen Notstands in Fällen des quantitativen Lebensnotstands sprechen, sind jedenfalls nicht von der Hand zu weisen und damit das Strafbarkeitsrisiko für den Fahrer F im obigen Beispiel dargetan.

4. Zwischenergebnis

In dilemmatischen Situationen bevorzugt die Rechtsordnung die Wahrung des status quo.[23] Der Täter soll dem Schicksal grundsätzlich seinen Lauf lassen und nicht selbst Schicksal spielen. Schicksal zu spielen und damit bislang unbeteiligte Rechtsgüter aufzuopfern erlaubt die Rechtsordnung nur zur Wahrung eines wesentlich überwiegenden Interesses, was auf Kosten eines Menschenlebens aber nie angenommen werden kann.[24] Im Übrigen kann bei einer außergewöhnlichen Motivationslage allenfalls der Schuldvorwurf entfallen, das strafrechtliche Unrecht aber bleibt bestehen.

III. Zur strafrechtlichen Verantwortlichkeit des Programmierers bzw. Herstellers autonomer Fahrsysteme

Nachdem die strafrechtlich relevanten Gesichtspunkte auf den Ebenen der Rechtswidrigkeit und Schuld herausgearbeitet wurden, stellt sich im Weiteren die Frage, ob – und wenn ja, welche – Folgerungen hieraus für den Programmierer erwachsen. Wenngleich das Unfallszenario den Anlass für eine mögliche Strafbarkeit gibt, ist Anknüpfungspunkt einer strafrechtlichen Verantwortlichkeit des Programmierers bzw. Herstellers autonomer Fahrsysteme die Programmierungsentscheidung, weil bereits sie die „Reaktion" des Fahrzeugs im Unfallszenario veranlasst.[25] Angesichts dessen er-

[20] So *Schlehofer*, in: MüKo-StGB, Vor § 32 Rn. 298 ff.; *Neumann*, in: NK-StGB, § 35 Rn. 61.
[21] Vgl. die Aufzählung von Fällen bei *Jäger*, ZStW 2003, 765 (779), bei denen dann ebenfalls eine Entschuldigung anzunehmen wäre; auch *Roxin*, AT I, § 22 Rn. 163, der bei Gefahrengemeinschaften einen „Verantwortungsausschluss" annimmt, einen solchen für den quantitativen Lebensnotstand aber nicht befürwortet, weil die Überwälzung von Gefahren auf andere „jederzeit vielfältig möglich" sei.
[22] *Jäger*, ZStW 2003, 765 (779); vgl. auch *Stübinger*, ZStW 2011, 403 (446): „[…] Anmaßung von Willkür […] entscheiden zu wollen, wer leben darf und wer sterben muss"; vgl. auch *Hilgendorf*, in: ders., Systeme, 143 (157 f.), unter Hinweis auf ungleich verteilte Lebenschancen vor dem Eingreifen.
[23] Hierzu *Weigend*, ZIS 2017, 599 (602).
[24] *Weigend*, ZIS 2017, 599 (602).
[25] Vgl. *Hörnle/Wohlers*, GA 2018, 12 (22 ff.), die ihre Präferenzentscheidungen deshalb für die Programmierung treffen; s. hierzu auch *Sander/Hollering*, NStZ 2017, 193 (202).

scheint zunächst sachlich geboten, die Unterschiede zwischen der Situation des menschlichen Fahrers einerseits und derjenigen des Programmierers anderseits aufzuzeigen.

1. Unterschiede in der Entscheidersituation

Stellt man die Situationen von menschlichem Fahrer und Programmierer gegenüber, ergeben sich beträchtliche Unterschiede,[26] welche einer (gänzlichen) strafrechtlichen Gleichbehandlung möglicherweise entgegenstehen.

Zu nennen sind zum einen die äußeren Umstände der Entscheiderposition. Bei den zuvor dargestellten Fällen sind wir stets davon ausgegangen, dass der Fahrer überhaupt noch die Zeit hatte, entsprechende Entschlüsse zu fassen und willentlich umzusetzen. Nur unter diesen Voraussetzungen kann dem Täter der Vorwurf vorsätzlichen Handelns, also einer willentlichen Tatbestandsverwirklichung in Kenntnis aller objektiven Tatumstände, gemacht werden.[27] Geht man – in derlei Situationen (wohl) realitätsnäher – von einem nur intuitiven Verhalten aus, kommt allenfalls ein Fahrlässigkeitsvorwurf in Betracht, wobei ein objektiver Sorgfaltspflichtverstoß kaum anzunehmen ist, wenn der Fahrer selbst keine Verkehrsregeln verletzt hat, die mitursächlich für das Unfallgeschehen waren.[28] Der Programmierer hingegen trifft seine Entscheidung darüber, wie sich das Fahrzeug in einer dilemmatischen Situation verhalten soll, stets berechnend im Voraus einer Gefahrensituation und damit wissentlich und willentlich.

Zum anderen sind die inneren Umstände der beiden Entscheiderpositionen zu unterscheiden. Während sich der Fahrer einer Zwangslage – mitunter für das eigene Leben – ausgesetzt sieht, trifft der Programmierer seine Entscheidung lange Zeit vor der konkreten Unfallsituation, ohne selbst auch nur im Entferntesten gefährdet und ohne selbst dem Gewissenskonflikt der konkreten Situation ausgesetzt zu sein.

2. Strafbarkeitsrisiken des Programmierers

Unter Beachtung dieser Unterschiede stellt sich die Frage nach der strafrechtlichen Verantwortlichkeit der Programmierer bzw. Hersteller autonomer Fahrsysteme. Wie bereits erwähnt, ist dabei auf die Programmierungsentscheidung als Anknüpfungspunkt einer strafrechtlichen Würdigung abzustellen. Wird das Fahrzeug, welches sich vor die Situation gestellt sieht, entweder Kurs auf der Straße zu halten und dadurch die

[26] Eingehend hierzu *Hevelke/Nida-Rümelin*, JWE 2015, 5 (8 ff.).

[27] Vgl. hierzu auch der jüngst entschiedene „Berliner Raser-Fall“, wobei der BGH nochmals klarstellt, dass „sich wegen eines vorsätzlichen Delikts nur strafbar macht, wer ab Entstehen des Tatentschlusses noch eine Handlung vornimmt, die in der vorgestellten und für möglich gehaltenen Weise den tatbestandlichen Erfolg […] herbeiführt“ und dies verneint, wenn zum Zeitpunkt, in dem der Täter den Tatentschluss fasst, bereits keine Möglichkeit zur Vermeidung des Unfallgeschehens mehr bestand (*BGH*, NJW 2018, 1621 (1622)).

[28] Vgl. *Sander/Hollering*, NStZ 2017, 193 (201); auch *Weber*, NZV 2016, 249 (251).

Kindergartengruppe tödlich zu erfassen oder aber auf den Gehsteig auszuweichen, wodurch das Leben der 90-jährigen Rentnerin R beendet würde, für letztere Option zu Lasten der R programmiert, steht eine Strafbarkeit der an der Programmierung Beteiligten wegen einer täterschaftlich begangenen Tötung gem. §§ 212, 211 StGB zur Diskussion.[29]

a) Tatbestandsmäßige Tötung durch Programmierungsentscheidung

Setzt man dabei voraus, dass das Fahrzeug in der konkreten Verkehrssituation (autonom) durch das Fahrassistenzsystem gesteuert wird, dem Fahrer indes keinerlei Tatherrschaft über das Fahrzeug zukommt, ist eine täterschaftliche Begehungsweise in Betracht zu ziehen.[30] Im Ausgangspunkt kann kein Zweifel daran bestehen, dass die Programmierungsentscheidung kausal für die Reaktion des Fahrzeugs ist. Mit Blick auf die im Zeitpunkt der Kollision arg- und wehrlose R ist sogar das Mordmerkmal der Heimtücke diskutabel,[31] unter Beachtung der diesbezüglich restriktiven BGH-Rechtsprechung im Ergebnis aber abzulehnen[32].[33]

(1) Objektiv zurechenbare Handlung

Nach den Grundsätzen der objektiven Zurechnung muss der Täter durch sein Verhalten ein rechtlich unerlaubtes Risiko geschaffen haben, das sich im tatbestandlichen Erfolg realisiert, sodass der Erfolg ein „Werk" des Täters darstellt.[34] Da die Programmierung gerade zu dem Zweck erfolgte, in einer entsprechenden dilemmatischen Verkehrssituation das tödlich verlaufende Fahrmanöver durchzuführen, kann im Ausgangspunkt kein Zweifel an der objektiven Zurechnung bestehen.[35]

Beachtenswert ist zwar, dass ein unerlaubtes Risiko letztverantwortlich erst durch das In-Gang-Setzen des Fahrzeugs durch den Fahrer ausgelöst wird, der insoweit auch in Kenntnis der Programmierung handelt. Ob das tödlich endende Ausweichmanöver damit einzig dem Fahrer aufgrund seines eigenverantwortlichen Dazwischentreten in Form des Fahrzeugstarts zuzurechnen ist, darf jedoch bezweifelt werden, da die Aus-

[29] So jedenfalls im Ergebnis *Sander/Hollering*, NStZ 2017, 193 (202 f.).
[30] So *Sander/Hollering*, NStZ 2017, 193 (202). Zu einer Beihilfestrafbarkeit tendierend *Engländer*, ZIS 2016, 608 (615); auch *Weber*, NZW 2016, 249 (253 m. Fn. 39).
[31] Bejahend (wohl) *Sander/Hollering*, NStZ 2017, 193 (202).
[32] Der *BGH* verlangt für die Annahme der Heimtücke, dass der Täter *in feindseliger Willensrichtung* die Arg- und Wehrlosigkeit *bewusst ausnutzt* (zuletzt *BGH*, NStZ-RR 2017, 278 (279)), was in der Person des Programmierers fernliegend erscheint.
[33] Diskutabel erscheint auch eine Tötung mit „gemeingefährlichen Mitteln". Das gesteigerte Unrecht des Mordmerkmals liegt in der sozialpsychologisch vermittelten Verunsicherung der Allgemeinheit begründet, weil ein Tötungsmittel mit Breitenwirkung verwendet wird und dadurch Unbeteiligte miteinbezogen werden (*Schneider*, in: MüKo-StGB, § 211 Rn. 126). Fraglich ist, ob die den Mitteln typischerweise innewohnende Unberechenbarkeit auch dem autonomen Fahrsystemen zugeschrieben werden kann.
[34] Eingehend *Roxin*, AT I, § 11 Rn. 1 ff., 44 ff.
[35] *Sander/Hollering*, NStZ 2017, 193 (202).

gangsgefahr bereits in der Programmierung selbst angelegt ist und sich durch das In-Gang-Setzen des Fahrzeugs nur fortsetzt, mithin der Fahrer auf sie ohne jeglichen Einfluss bleibt.[36]

Weiterhin wäre – auch in Anbetracht einer staatlichen Zulassung – überlegenswert, in selbstfahrenden Kraftfahrzeugen schon gar kein unerlaubtes Risiko zu erblicken. Begründen ließe sich dieser Ansatz damit, dass autonome Systeme mit entsprechender Programmierung Schäden so gering wie möglich halten, das Unfallrisiko insgesamt erheblich senken und damit einen großen gesellschaftlichen Nutzen bringen; das Risiko von Dilemma-Situationen ist zwar vorhanden, aber demgegenüber sehr gering, sodass unter dem Strich der gesellschaftliche Mehrwert überwiegt.[37] Diskutiert wird ein solcher Zurechnungsausschluss bisher aber nur, wenn zuvor ein gesellschaftlicher Konsens über Präferenzentscheidungen getroffen worden ist, also darüber, nach welchen Kriterien das autonome Fahrzeug auf dilemmatische Situationen reagieren soll.[38] Hierfür spricht zunächst, dass ein autonomes Fahrsystem nicht ohne vorherige staatliche Prüfung und Genehmigung (voraussichtlich durch das Kraftfahrtbundesamt) die Werkbank verlässt, was die Einstufung als „erlaubtes Risiko" auf den ersten Blick unterstreicht. Freilich steht die zulassende Behörde insoweit vor demselben Dilemma. Vor dem Hintergrund, dass das *Bundesverfassungsgericht* eine Entscheidung gegen das Leben tatunbeteiligter Menschen in der Entscheidung zur Abschussermächtigung nach dem Luftsicherheitsgesetz als mit dem Recht auf Leben für unvereinbar erklärt hat, dürfte eine solche Zulassungsentscheidung nur schwer zu begründen sein.[39]

Doch selbst wenn ein solcher gesellschaftlicher Konsens erzielt würde, sprechen entscheidende Gründe gegen die Annahme eines erlaubten Risikos. Denn es erscheint bedenklich, bereits das Handlungsunrecht des zum Tod führenden, programmierten Ausweichmanövers zu negieren, obwohl der hierdurch verursachte konkrete Tod mit einer anderen Programmierung vermeidbar gewesen wäre. Gerade in der fehlenden Vermeidungsmacht liegt indes der tragende Gedanke des Zurechnungsausschlusses über das erlaubte Risiko.[40] Die Aufopferung von Menschenleben ist kein geeignetes Mittel zur Erreichung eines gesellschaftlichen Zwecks, namentlich der Nützlichkeit autonomer Systeme. Andernfalls stellte man abstrahierende Opferstatistiken über kon-

[36] So zutreffend *Engländer*, ZIS 2016, 608 (615 m. Fn. 47).
[37] Vgl. *Hilgendorf*, in: ders., Systeme, 143 (164 ff.); *Schuster*, in: Hilgendorf, Systeme, 99 (113 f.), hält dies für einen „denkbaren Ansatz".
[38] S. *Hilgendorf*, in: ders., Systeme, 143 (169); dies verkennt wohl *Engländer*, ZIS 2016, 608 (611 f.).
[39] Vgl. BVerfGE 115, 118.
[40] Zutreffend unter Hinweis auf das für das erlaubte Risiko entscheidende Merkmal der fehlenden „Vermeidemacht", *Engländer*, ZIS 2016, 608 (612); ebenso *Erb*, Neumann-FS, S. 785 (792 ff.). Schulbeispiel für eine solche „objektive Zufälligkeit", bei der der Täter weder die Möglichkeit der Erfolgsherbeiführung noch der Erfolgsverhinderung hat, ist der sog. „Gewitterfall": Jemand schickt einen anderen in den Wald, in der Hoffnung, der andere werde vom Blitz erschlagen (hierzu *Roxin*, AT I, § 11 Rn. 44).

krete Menschenleben.[41] Eine solch rein utilitaristische Betrachtungsweise vermag nicht zu überzeugen.

(2) Subjektiver Tatbestand

Im Weiteren müsste der Programmierer vorsätzlich gehandelt haben. Vorsatz meint den Willen zur Tatbestandsverwirklichung in Kenntnis aller Tatumstände. Gem. § 16 Abs. 1 S. 1 StGB muss der Tatvorsatz im Zeitpunkt der zum Taterfolg führenden Handlung vorliegen.[42] *Sander* und *Hollering* führen diesbezüglich konsequent aus:

> *„Denn die bewusste Programmierungsentscheidung […] lässt kaum Raum für die Annahme von Fahrlässigkeit. […] Denn es wird lediglich die programmierte Prioritätensetzung realisiert, indem die Kollision […] vermieden und stattdessen das für Dritte tödliche Manöver ausgeführt wird. Dass hier genau jenes geschieht, was die Verantwortlichen im Rahmen der Fahrzeugentwicklung gewollt haben, macht den maßgeblichen Unterschied aus zu den Fällen, in denen sich Fehler des automatisierten Fahrsystems in Schädigungen niederschlagen. Die Programmierung bzw. das Inverkehrbringen des so programmierten Fahrzeugs in Kenntnis dieser Umstände wirken im Übrigen in der konkreten Fahrsituation in einer Weise fort, die für eine täterschaftliche Tatbestandsverwirklichung spricht, zumal der Fahrer beim konkreten automatisierten Fahrmanöver weder über Tatherrschaft noch über einen diesbezüglichen Willen verfügen dürfte. Dass Programmierung und Markteinführung zeitlich ggf. lange vor der konkreten Tatsituation vorgenommen wurden, steht einer Strafbarkeit nicht entgegen.“*[43]

Zunächst trifft zu, dass der Programmierer im Zeitpunkt seiner Programmierungsentscheidung, die sich (gegebenenfalls) realisiert, wissentlich und willentlich handelt. In dem Umstand, dass jegliche zeitliche und räumliche Nähe zum Erfolgseintritt fehlt, liegt (wohl) die Ursache einiger hieraus entstehender skurriler Folgen begründet: Beim autonomen Fahren kann der Erfolg gar noch Jahre und sogar Jahrzehnte nach der Programmierungsentscheidung eintreten.[44] In der Konsequenz heißt das, dass der Programmierer im Laufe seines Berufslebens zigtausende (latente) Tötungsvorsätze auf sich lädt, die bei einer Erfolgsrealisierung – dem tödlich verlaufenden Ausweichmanöver in der dilemmatischen Situation – gewissermaßen auf ihn zurückfallen und seine (mögliche) Strafbarkeit gem. § 212 Abs. 1 StGB begründen. Denkt man unter dieser

[41] Vgl. *Erb*, Neumann-FS, S. 785 (790).
[42] *BGH*, NStZ 2018, 27.
[43] *Sander/Hollering*, NStZ 2017, 193 (202); ähnlich *Schuster*, in: Hilgendorf, Systeme, 99 (114). Anders *Beck*, in: Hilgendorf, Systeme, 117 (120), die eine Fahrlässigkeitsstrafbarkeit annimmt, dabei aber unzutreffend darauf abstellt, dass die Dilemma-Situation nicht vorsätzlich herbeigeführt wurde.
[44] Abgesehen von im Laufe der Jahre möglichen Updates bzw. Umprogrammierungen, die den Zurechnungszusammenhang unterbrechen können.

Prämisse weiter an eine Versuchsstrafbarkeit des Programmierers, ergeben sich weitere Fragezeichen: Bedient man sich hierfür des Modells der mittelbaren Täterschaft, da der Fahrer sein Auto wie ein Tatmittler führt, weil er aufgrund des autonomen Fahrsystems keine Tatherrschaft innehat (vgl. o.), ist fraglich, wann der Versuch zum Totschlag durch unmittelbares Ansetzen (vgl. § 22 StGB) beginnt. Wer an dieser Stelle der sog. Freisetzungstheorie folgt, nach der es auf den Zeitpunkt ankommt, in dem der Täter das Tatmittel aus seinem Herrschaftsbereich entlässt,[45] müsste konsequenterweise bereits einen Versuch in dem Zeitpunkt annehmen, in dem das Fahrzeug von der Werkshalle auf den Käufer übergeht. Freilich hat der Programmierer im Zeitpunkt seiner Programmierung aber überhaupt keine Ahnung davon, wann, wo, wie und ob überhaupt eine dilemmatische Situation und ein damit einhergehendes Ausweichmanöver eintritt.

Ob der Vorsatz des Programmierers in Anbetracht dieser zahlreichen Unwägbarkeiten hinreichend konkretisiert ist, darf immerhin in Frage gestellt werden. Lösungsansätze, sofern sie überhaupt für notwendig befunden werden – auch das soll hier zur Diskussion gestellt werden –, sind für derartige Distanz-Probleme der Literatur bislang nicht zu entnehmen. Ob mit der zunehmenden Möglichkeit von Programmierungen und dem damit einhergehenden Zwang, alle Einzelentscheidungen zuvor abstrahierend und ohne Kenntnis konkreter Situationen zu treffen,[46] neue Vorsatzprobleme entstehen, muss hier dahinstehen. Nach herkömmlicher Dogmatik ändern die Unwägbarkeiten am Vorsatz jedenfalls nichts.[47]

b) Rechtfertigungsgründe

Die gesetzlichen Rechtfertigungsgründe (§§ 32, 34 StGB) kommen bei dilemmatischen Situationen, möchte man sie nicht der Unkenntlichkeit preisgeben, nicht in Betracht (vgl. o.).

Vergegenwärtigt man sich die unterschiedlichen Entscheidersituationen von menschlichem Fahrer und Programmierer und insbesondere die auseinanderfallenden Entscheidungszeitpunkte, könnte für die Programmierungsentscheidung eine rechtfertigende Pflichtenkollision anzunehmen sein.[48] *Weigend* nimmt insoweit an, dass der Programmierer vor zwei – in ferner Zukunft liegenden – Unterlassungspflichten steht: das allgemeine Tötungsverbot verbiete dem Programmierer in der (hypothetischen) Dilemmasituation die Tötung eines jeden Lebens; in unserem Beispielfall also sowohl eine Entscheidung zulasten der Kindergartengruppe, als auch zulasten der R. Entschei-

[45] So etwa *Roxin*, AT II, § 29 Rn. 244; *Schünemann*, in: LK-StGB, § 25 Rn. 154.
[46] *Hilgendorf*, ZStW 2018 (im Erscheinen), spricht bzgl. der maschinengerechten Aufarbeitung aller relevanten Entscheidungsschritte von einem „Explikationszwang".
[47] Vgl. *Erb*, Neumann-FS, S. 785 (795); *Sander/Hollering*, NStZ 2017, 193 (202).
[48] So *Weigend*, ZIS 2017, 599 (603 f.).

det sich der Programmierer in dieser unausweichlichen Kollision gezwungenermaßen für eine der nur alternativ bestehenden Handlungsmöglichkeiten, verwirkliche der Täter kein Unrecht, sofern er damit die höher- oder immerhin gleichrangige Unterlassungspflicht erfüllt.[49]

Dem ist entgegenzuhalten, dass die gedankliche Konstruktion einer Unterlassungspflicht nur die Handlungspflicht tarnt, die besagt, die tödliche Handlung zu vermeiden. Dann aber steht der jeweiligen Handlungspflicht eine Unterlassungspflicht gegenüber, die gemeinhin am Maßstab des § 34 StGB und dem damit einhergehenden Abwägungsverbots von menschlichen Leben (s.o.) zu messen ist.[50] Insoweit entpuppt sich diese Lösung nur als eine gedankliche, nicht aber rechtlich tragfähige Konstruktion. Folglich bleibt es dabei, dass wegen des Abwägungsverbots menschlichen Lebens Rechtfertigungsgründe nicht in Betracht kommen.

c) Entschuldigungsgründe

Die Rückschau auf die strafrechtliche Verantwortlichkeit des menschlichen Fahrers zeichnet folgendes Bild: der menschliche Fahrer darf sich im Falle einer Gefährdung für das eigene Leben aufgrund des im Vordergrund stehenden Selbsterhaltungstriebs regelmäßig auf den entschuldigenden Notstand gem. § 35 Abs. 1 StGB berufen (s.o.). Hinsichtlich der Gefährdung Dritter dürfte es regelmäßig an einem Näheverhältnis zwischen menschlichem Fahrer und dem gefährdeten Dritten fehlen, sodass ein Ausweichmanöver mit tödlichem Verlauf für einen Unbeteiligten allenfalls auf der Grundlage eines außergesetzlichen Notstands entschuldigt werden kann (s.o.). In der Person des Programmierers fehlt es von vornherein an einer für den entschuldigenden Notstand notwendigen Motivationslage. Weder ist das eigene Leben des Programmierers, noch – in aller Regel – dasjenige eines ihm nahestehenden Dritten gefährdet, mit der Folge, dass ein entschuldigender Notstand gem. § 35 StGB (auch zugunsten des Fahrers!) ausscheidet.

Sodann kommt beim Programmierer allenfalls ein übergesetzlicher Notstand in Gestalt des quantitativen Lebensnotstands in Betracht. Seine Anerkennung vorausgesetzt, stünde der Programmierer vor dreierlei Interessenpositionen, die es untereinander abzuwägen gilt: zum einen das Leben der/des Fahrers/Fahrzeuginsassen, zum anderen das Leben der/des Gefährdeten und unbeteiligter Dritter, die infolge eines möglichen Ausweichmanövers aufgeopfert würden. Hier wird offenbar, dass menschliche Leben zwangsläufig quantitativ oder qualitativ gegeneinander abgewogen werden müssten. Mag die herrschende Ansicht dem menschlichen Fahrer den übergesetzlichen entschuldigenden Notstand auch deshalb zugestehen, weil er sich in einem aku-

[49] *Weigend*, ZIS 2017, 599 (603).
[50] So auch *Erb*, Neumann-FS, S. 785 (796).

ten Gewissenskonflikt befindet (s.o.), spricht gegen die Anerkennung im Fall des Programmierers, dass er aus der Distanz heraus berechnend agiert, damit einem akuten Gewissenskonflikt nicht unterliegt und somit Lebenschancen generalisierend verteilt.[51]

3. Rechtliches Ergebnis

Die Untersuchung zur strafrechtlichen Verantwortlichkeit von Programmierern bzw. Herstellern autonomer Fahrsysteme hat gezeigt, dass die strafrechtlichen Grundsätze für dilemmatische Situationen trotz unterschiedlicher Entscheidersituationen auf Programmierungsentscheidungen in gleicher Weise wie auf Entscheidungen des menschlichen Fahrers Anwendung finden. Die Strafrechtsordnung verbietet den aktiven Eingriff in einen Geschehensablauf, wenn ihm Menschenleben zum Opfer fallen. Weder kann die Zurechnung des Erfolgs noch eine Rechtfertigung auf der Grundlage einer Pflichtenkollision dogmatisch überzeugen. Konzeptionelle Einschränkungen im Bereich des subjektiven Tatbestands sind bislang nicht ersichtlich, wenngleich die zeitliche und räumliche Distanz zwischen Programmierungsentscheidung und (möglichem) Erfolgseintritt Fragen aufwirft.

Ein maßgeblicher Unterschied zum menschlichen Fahrer stellt sich allein durch die Tatsache, dass die Fahrzeuginsassen und insbesondere der „Fahrer“ das Heft des Handelns nicht mehr selbst in Händen hält und insoweit als Passagier den Programmierungsentscheidungen mehr oder minder ausgeliefert ist. Damit geht folgerichtig einher, dass sich ein (programmierter) aktiver Eingriff auch dann verbietet, wenn hierdurch das Leben der Fahrzeuginsassen gerettet werden könnte, weil ein Näheverhältnis, wie es der entschuldigende Notstand in § 35 StGB voraussetzt, nicht besteht.

IV. Schlussbetrachtung

Damit ist das Strafbarkeitsrisiko von Programmierern bzw. Herstellern autonomer Fahrsysteme dargetan. Das diagnostizierte Strafbarkeitsrisiko könnte zu der Annahme verleiten, die strafrechtliche Behandlung dilemmatischer Situationen stelle auch die Automobilindustrie vor ein Dilemma: Möchten sich Hersteller bzw. Programmierer autonomer Fahrsysteme nicht auf ein Rendezvous mit dem – rechtlich unverlässlichen – übergesetzlichen entschuldigenden Notstand einlassen,[52] weist sie das eben diagnostizierte Strafbarkeitsrisiko an, in dilemmatischen Situation eine aktiv eingreifende Programmierung, in deren Folge lebensgefährdende Richtungsänderungen eintreten, zu

[51] Einen übergesetzlichen entschuldigenden Notstand deshalb wohl zu Recht verneinend *Hilgendorf*, in: ders., Systeme, 143 (157); *Joerden*, in: ebda., 73 (86 f.); insoweit zust. *Schuster*, in: ebda., Systeme, 99 (106). Bejahend hingegen: *Engländer*, ZIS 2016, 608 (614); *Weigend*, ZIS 2017, 599 (605), der gleichwohl ein gravierendes Problem in der „digitalen Operationalisierung der ‚weichen‘ Regeln des übergesetzlichen entschuldigenden Notstands“ erkennt.

[52] Hierauf zu Recht hinweisend *Schuster*, in: Hilgendorf, Systeme, 99 (106).

unterlassen.[53] Das gilt selbst dann, wenn hierdurch das Leben der Fahrzeuginsassen gerettet werden könnte. Infolgedessen büßt der Schutz der Fahrzeuginsassen, der im Bereich der passiven Verkehrssicherheit im Automobilbau stets an erster Stelle stand, seine prioritäre Stellung ein. Man darf auf die Werbeslogans gespannt sein, welche ein Automobil anpreisen, das trotz bestehender Abwendungsmöglichkeiten dem Schicksal seinen Lauf lässt und auf diese Weise das Leben seiner Fahrzeuginsassen „opfert".[54] Die Verkaufsargumente dürften im Wert auch dadurch nicht steigen, dass die Automobilindustrie die zu treffenden Präferenzentscheidungen darüber, wie ein Automobil in dilemmatischen Situationen reagieren soll, auf den Fahrer überantwortet und sich somit ihres Strafbarkeitsrisikos zu Lasten des Autokäufers entledigt.[55]

Entgegenzuhalten ist diesem wirtschaftlich bedeutsamen Interesse der Automobilindustrie, dass bei objektiver Betrachtung kein Grund dafür ersichtlich ist, die Fahrzeuginsassen beim autonomen Fahren in den Genuss eines gegenüber Unbeteiligten höherwertigen Schutzes kommen zu lassen.[56] Der Fahrzeuginsasse und insbesondere der Fahrzeugführer muss sich bei autonomen Fahrsystemen lediglich seiner neuen Rolle als Passagier bewusst sein und mit ihr abfinden können. Möchte er das nicht, muss er von autonomen Fahrsystemen die Finger lassen. Damit aber haben die strafrechtlichen Folgen ihr Bewenden. Die Besorgnis, wonach die Unlösbarkeit entsprechender Dilemmata das Ende der Entwicklung autonomer Fahrsysteme begründen soll, ist unbegründet.[57] Vielmehr ist dem (vielgepriesenen) verständigen Verbraucher zuzutrauen, dass er den gesellschaftlichen Nutzen und Mehrwert entsprechender Systeme (an)erkennt und diese Einsicht auch finanziell umsetzt.

Gleichwohl wollen einige in dem neuen Gewand, in dem sich das alte Problem der Behandlung dilemmatischer Situationen bei autonomen Fahrsystemen präsentiert, ein Bedürfnis dafür erkennen, über die strafrechtliche Behandlung dilemmatischer Situationen von Grund auf neu zu diskutieren, indem über das Abwägungsverbot bezüglich menschlicher Leben gesellschaftlich neu verhandelt wird.[58] Dementsprechende für Leben-gegen-Leben-Dilemmata ausgearbeitete Entwürfe von Präferenzentscheidungen[59] erscheinen jedoch wenig erfolgversprechend, da der gesellschaftliche Konsens über die Aufopferung von Menschenleben in der Vergangenheit nicht erzielt wurde

[53] So auch *Erb*, Neumann-FS, S. 785 (797); *Joerden*, in: Hilgendorf, Systeme, 73 (82 ff.).
[54] Vgl. *Gless/Janal*, JR 2016, 561 (575); überspitzt *Weigend*, ZIS 2017, 599 (604), der einen Selbstzerstörungsmechanismus zur Diskussion stellt.
[55] Vgl. hierzu *Weber*, NZV 2016, 249 (251 m. Fn. 25).
[56] Vgl. *Gless/Janal*, JR 2016, 561 (575).
[57] Vgl. aber *Hörnle/Wohlers*, GA 2018, 12 (34).
[58] Hierfür werbend *Hörnle/Wohlers*, GA 2018, 12; *Joerden*, in: Hilgendorf, Systeme, 73 (97).
[59] Vgl. der bemerkenswerte Entwurf von *Hörnle/Wohlers*, GA 2018, 12 (24 ff.)

und auch in Zukunft nicht zu erwarten ist.[60] Möchte man ihn gar noch vor der Einführung autonomer Fahrsysteme herbeiführen, hieße das, die Entwicklung autonomer Fahrsysteme auf den „Sankt-Nimmerleins-Tag“ zu verschieben. Vor diesem Hintergrund ist davon abzuraten, wegen der – selten genug – auftretenden Dilemmata die Grundsätze der deutschen Strafrechtsdogmatik über Bord zu werfen.[61] Denn sie sind es, die der Entwicklung als rechtssichere Orientierung dienen.

Literaturverzeichnis

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI; Hrsg.), Bericht der Ethik-Kommission: Automatisiertes und vernetztes Fahren, Juni 2017 (URL: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile).
Verband der Automobilindustrie e.V. (VDA; Hrsg.), Automatisierung – Von Fahrassistenzsystemen zum automatisierten Fahren, 2015 (URL: https://www.vda.de/dam/vda/publications/2015/automatisierung.pdf).

Engländer, Armin, Das selbstfahrende Kraftfahrzeug und die Bewältigung dilemmatischer Situationen, ZIS 2016, 608-618.

Erb, *Volker,* Automatisierte Notstandshandlungen, in: Saliger, Frank (Hrsg.), Rechtsstaatliches Strafrecht – Festschrift für Ulfrid Neumann zum 70. Geburtstag, Heidelberg 2017, S. 785-797.

Gless, Sabine/Janal, Ruth, Hochautomatisiertes Fahren und autonomes Autofahren – Risiko und rechtliche Verantwortung, JR 2016, 561-575.

Hevelka,Alexander/Nida-Rümelin, Julian, Selbstfahrende Autos und Trolley-Probleme: Zum Aufrechnen von Menschenleben im Fall unausweichlicher Unfälle, JWE 2015, 5-23.

Hilgendorf, Eric (Hrsg.), Autonome Systeme und neue Mobilität, Baden-Baden 2017.

Ders., Dilemma-Probleme beim automatisierten Fahren. Ein Beitrag zum Problem des Verrechnungsverbots im Zeitalter der Digitalisierung, ZStW 2018 (im Erscheinen).

[60] Vgl. *BMVI*, Bericht, S. 11: „Derartige in der Rückschau angestellte und besondere Umstände würdigende Urteile des Rechts lassen sich nicht ohne weiteres in abstrakt-generelle Ex-ante-Beurteilungen und damit auch nicht in entsprechende Programmierungen umwandeln“.
[61] Vgl. auch *Erb*, Neumann-FS, S. 785 (796); *Joerden*, in: Hilgendorf, Systeme, 73 (92 ff.); anders wohl *Hörnle/Wohlers*, GA 2018, 12 (34), die der h.M. unterstellen, etablierte Dogmen als „Tabus“ zu behandeln.

Hörnle, Tatjana/Wohlers, Wolfgang, The Trolley Problem Reloaded – Wie sind autonome Fahrzeuge für Leben-gegen-Leben-Dilemmata zu programmieren?, GA 2018, 12-34.

Jäger, Christian, Die Abwägbarkeit menschlichen Lebens im Spannungsfeld von Strafrechtsdogmatik und Rechtsphilosophie, ZStW 2003, 765-790.

Leipziger Kommentar zum Strafgesetzbuch, Erster Band, 12. Aufl., Berlin 2007.

Leipziger Kommentar zum Strafgesetzbuch, Zweiter Band, 12. Aufl., Berlin 2006.

Roxin, Claus, Strafrecht Allgemeiner Teil, Band I, 4. Aufl., München 2006.

Ders., Strafrecht Allgemeiner Teil, Band II, München 2003.

Sander, Günther M./Hollering, Jörg, Strafrechtliche Verantwortlichkeit im Zusammenhang mit automatisiertem Fahren, NStZ 2017, 193-206.

Stübinger, Stephan, „Not macht erfinderisch" – Zur Unterscheidungsvielfalt in der Notstandsdogmatik – am Beispiel der Diskussion über den Abschuss einer sog. „Terrormaschine", ZStW 2011, 403-446.

Weber, Philipp, Dilemmasituationen beim autonomen Fahren, NZV 2016, 249-254.

Weigend, Thomas, Notstandsrecht für selbstfahrende Autos?, ZIS 2017, 599-605.

Welzel, Hans, Zum Notstandsproblem, ZStW 1951, 47-56.

Mensch-Maschine-Analogien bei der Fehlerbeurteilung intelligenter Agenten im Recht der Produkt- und Produzentenhaftung

Robert Welker

Wiss. Mitarbeiter, Humboldt-Universität zu Berlin
robert.welker@rewi.hu-berlin.de

Abstract

Der Beitrag untersucht, ob Vergleiche zwischen der Leistungsfähigkeit von intelligenten Agenten und Menschen, die mit derselben Aufgabe betraut wären, zur Konkretisierung des Fehlerbegriffs im Recht der Produzenten- und Produkthaftung geeignet sind. Hierfür werden, nach einer knappen Einführung in die Herstellerhaftung (II.), die für intelligente Agenten fruchtbar zu machenden Fehlerkategorien erörtert (III.). Sodann werden die möglichen Spielarten von Mensch-Maschine-Analogien herausgearbeitet (IV.), deren Eignung zur Fehlerbeurteilung an den Zielen des Rechts der Produzenten- und Produkthaftung (hierzu V.) gemessen wird. Anhand einer (ökonomischen) Analyse wird gezeigt, dass Mensch-Maschine-Analogien nur unter sehr eng umgrenzten Voraussetzungen ein signifikanter Erkenntnisgewinn zu entnehmen ist (VI.).

I. Entscheidungsautomatisierung durch intelligente Agenten: Autonomierisiko und Zurechnungslücken

Die Automatisierung komplexer Tätigkeiten erfordert Algorithmen, die ihr Vorgehen in hohem Maße autonom und adaptiv an veränderten Anforderungen ausrichten können. Bei derartigen intelligenten Agenten – komplexe Algorithmen, die zu einem gewissen Grad autonomiefähig bzw. zu eigenständigem und eigendynamischem Handeln fähig sind[1] – ist unvorhergesehenes Verhalten Teil des Funktionsprinzips. Diese Entkopplung zwischen dem Verhalten des Agenten und den Steuerungsmöglichkeiten seines Prinzipals stellt die Funktionsfähigkeit zivilrechtlicher Zurechnungsnormen auf die Probe: Die deliktsrechtlich zutreffende Zuweisung des „Autonomierisikos“[2] derartiger Systeme ist notorisch umstritten.[3] Werden beim Betrieb intelligenter Agenten

[1] Vgl. hierzu *Russel/Norvig,* Artificial Intelligence, S. 39 f.
[2] *Zech,* Zivilrechtliche Haftung für den Einsatz von Robotern, S. 175.
[3] Einen Überblick über mögliche Anknüpfungspunkte für eine Haftung de lege lata und de lege ferenda gibt *Hanisch,* Zivilrechtliche Haftungskonzepte für Robotik.

deliktsrechtlich geschützte Rechtsgüter verletzt, kommt eine Haftung des „Quasi-Handelnden“ intelligenten Agenten mangels Rechtspersonalität nicht in Betracht.[4] Eine Haftung des Nutzers nach § 823 Abs. 1 BGB greift indessen nur, sofern bereits die Inbetriebnahme des Systems einen Sorgfaltspflichtverstoß darstellt, was wohl nur bei der Delegation von Entscheidungen an einen intelligenten Agenten in besonders risikogeneigten Bereichen oder an einen technisch seiner Aufgabe nicht mächtigen Agenten angenommen werden könnte, oder sofern der Nutzer seine Verkehrspflicht zur Überwachung des Agenten verletzt.[5] De lege lata ist das Verhalten intelligenter Agenten im Rahmen von § 823 Abs. 1 BGB somit in der Regel nur als menschliches Unterlassen erfassbar, dessen haftungsbegründende Wirkung ihre Grenzen in der Zumutbarkeit von Überwachungs- und Kontrollmaßnahmen findet.[6] Schäden aus dem Betrieb intelligenter Agenten können jedoch auch aus deren Fehlerhaftigkeit resultieren; die daran anknüpfende Produzenten- und Produkthaftung des Herstellers ist Gegenstand dieses Beitrags.

II. Die Haftung des Herstellers nach der Produzenten- und Produkthaftung

Die in ständiger Rechtsprechung[7] zu § 823 Abs. 1 BGB entwickelte Produzentenhaftung beschreibt einerseits die Verkehrspflicht eines Herstellers, in zumutbarem Umfang zu verhindern, dass durch das Inverkehrbringen fehlerhafter Produkte Schäden an den von § 823 Abs. 1 BGB geschützten Rechtsgütern eintreten.[8] Andererseits ist mit der Produzentenhaftung eine weitgreifende Beweislastumkehr zugunsten des Geschädigten verbunden.[9] Der Geschädigte muss lediglich die Fehlerhaftigkeit des Produkts und den Kausalzusammenhang zwischen Produktfehler und Rechtsgutsverletzung nachweisen. Er muss jedoch nicht die Quelle des Fehlers innerhalb der betrieblichen Organisation des Herstellers darlegen und damit die „verhaltensbezogene Seite“ des Sorgfaltspflichtverstoßes nachweisen.[10] Bei der Produzentenhaftung handelt es sich – ihrer Verankerung in § 823 Abs. 1 BGB entsprechend – um eine verschuldensabhängige Haftung.

[4] Vgl. zur umfangreichen Diskussion über den rechtlichen Status intelligenter Agenten nur *Teubner*, Digital Personhood?, SSRN.
[5] Zu letzteren *Spindler,* CR 2015, 766 (768).
[6] *BGH*, NJW 2013, 48 m.w.N.: Die rechtlich gebotene Verkehrssicherung umfasst (nur) „diejenigen Maßnahmen, die ein umsichtiger und verständiger, in vernünftigen Grenzen vorsichtiger Mensch für notwendig und ausreichend hält, um andere vor Schäden zu bewahren“.
[7] Beginnend mit dem „Hühnerpest“-Urteil, BGHZ 51, 91.
[8] Vgl. *BGH*, NJW 2009, 1080 (1082, Rn. 19 m.w.N.).
[9] *Kötz/Wagner,* Rn. 615.
[10] *Kötz/Wagner,* Rn. 610, 615.

Neben sie tritt die Produkthaftung aus § 1 Abs. 1 ProdHaftG, die regelmäßig als Gefährdungs- bzw. verschuldensunabhängige Haftung charakterisiert wird.[11] Ein solcher Befund führte jedoch in die Irre: Auch der Produkthaftung liegt, da der Hersteller nicht für die Schäden aus dem Betrieb aller seiner Produkte, sondern nur seiner *fehlerhaften* Produkte haftet, ein objektiver Sorgfaltspflichtverstoß zugrunde.[12] Die Verschuldensprüfung wird lediglich in den Fehlerbegriff verlagert.[13] Für die Einordnung als Verschuldenshaftung- oder Gefährdungshaftung spielt es keine Rolle, ob der haftungsbegründende Tatbestand auf die pflichtwidrige Fehlerhaftigkeit eines in den Verkehr gebrachten Produktes (so § 1 Abs. 1 ProdHaftG) oder auf das pflichtwidrige Inverkehrbringen eines fehlerhaften Produktes (so § 823 Abs. 1 BGB) abstellt.[14]

Den Ausgangspunkt einer Herstellerhaftung aus § 823 Abs. 1 BGB oder § 1 Abs. 1 ProdHaftG bildet jeweils die – nahezu vollständig aneinander angeglichene, s. sogleich – Feststellung eines Produktfehlers. Unterschiede zwischen beiden Regelungen bestehen primär im deutlich kleineren Anwendungsbereich des ProdHaftG.[15] Da eine Anwendung von § 823 Abs. 1 BGB außerhalb des Anwendungsbereichs des ProdHaftG nicht ausgeschlossen ist (§ 15 Abs. 2 ProdHaftG), sind die praktischen Auswirkungen dieser Begrenzung ohnehin fraglich.

Das betrifft auch die für die Haftung bei intelligenten Agenten virulente Frage, ob Software, die nicht auf einem körperlichen Datenträger ausgeliefert wird, mangels Sacheigenschaft überhaupt ein Produkt i.S.v. § 2 ProdHaftG darstellt. Keine Probleme wirft der Fall auf, in dem Software zur Steuerung einer beweglichen Sache eingesetzt und gemeinsam mit dieser vertrieben wird: Die vorinstallierte Softwaresteuerung eines Staubsaug-, Pflegeroboters oder autonomen Fahrzeugs ist – genau wie jede fest verbaute Hardwaresteuerung – Teil dieses Produkts.[16] An der Produkteigenschaft von Software lässt sich jedoch zweifeln, sofern diese separat erworben und auf ein System aufgespielt werden kann: Man denke an ein Gerät, dass lediglich über ein rudimentäres Betriebssystem verfügt, auf dem die intelligenten Agenten anderer Hersteller per Download installiert werden können. Eine Einordnung dieser Software als „Produkt“ wäre allenfalls als Resultat eines Analogieschlusses zu § 2 ProdHaftG denkbar.[17] Das scheint überzeugend, kann für die Zwecke dieser Arbeit jedoch offenbleiben, weil den

[11] Vgl. die erschöpfende Darstellung des Meinungsstandes bei *Seibl,* in: BeckOGK, § 1 ProdHaftG Rn. 18 ff.
[12] Das gilt jedenfalls in Bezug auf – für die Beurteilung intelligenter Agenten ganz primär relevanten, s.u. – Konstruktionsfehler. Zur dahingehenden (zutr.) Unterscheidung zw. Fabrikations- und anderen Fehlern *Wagner,* in: MüKo-BGB, Einl. ProdHaftG Rn. 17 ff. m.w.N.
[13] *Kötz/Wagner,* Rn. 614 m.w.N.
[14] *Kötz/Wagner,* Rn. 614 m.w.N.
[15] Vgl. nur § 1 Abs. 1 ProdHaftG: Beschränkung der geschützten Rechtsgüter auf Leben, Körper und andere, privat genutzte Sachen.
[16] *Wagner,* in: MüKo-BGB, § 2 ProdHaftG Rn. 19.
[17] *Wagner,* AcP 217 (2017), 708 (718).

Anbieter von Downloadsoftware ohnehin zumindest die Verkehrspflichten aus § 823 Abs. 1 BGB treffen.[18]

III. Die Fehlerhaftigkeit intelligenter Agenten: Grundsätze

Die Feststellung eines Produktfehlers bildet somit die zentrale Voraussetzung für ein Eingreifen der Herstellerhaftung. Das Inverkehrbringen fehlerhafter Produkte bildet eine Verkehrspflichtverletzung i.R.v. § 823 Abs. 1 BGB. Diese verpflichten jeden, der eine Gefahrenquelle eröffnet oder unterhält, sein Verhalten in zumutbarer Weise so zu gestalten, dass es nicht zu vermeidbaren Verletzungen der in § 823 Abs. 1 BGB geschützten Rechtsgüter kommt.[19] Sie stehen unter dem Vorbehalt der Zumutbarkeit, enthalten also insbesondere kein Gebot, größtmögliche Sicherheit zu gewährleisten.[20] Zu ihrer Konkretisierung muss vielmehr auf die berechtigten Sicherheitserwartungen des Verkehrs[21] unter Berücksichtigung des zumutbaren Aufwands für Schadensvermeidungsmaßnahmen abgestellt werden.[22] Übereinstimmend hiermit definiert § 3 ProdHaftG den Produktfehler über ein Unterschreiten der berechtigten Sicherheitserwartungen, die zum Zeitpunkt des Inverkehrbringens des Produkts bestanden. Die Deckungsgleichheit der Fehlerkonzepte von Produzenten- und Produkthaftung wurden durch den BGH grundsätzlich bestätigt.[23]

Wie der Rekurs auf die „berechtigten" Sicherheitserwartungen des Verkehrs dokumentiert, liegt der Fehlerfeststellung kein empirisches Konzept zugrunde: Es kommt also nicht auf die *tatsächlich* vorhandenen Sicherheitsvorstellungen der relevanten Nutzergruppen an; der Fehlerbeurteilung liegt vielmehr ein normatives, Aufwand und Nutzen von Fehlervermeidungsmaßnahmen des Herstellers abwägendes Prüfprogramm zugrunde.[24]

Konkretisiert wird das Pflichtenprogramm des Herstellers durch die in Rechtsprechung und Literatur herausgebildeten Fehlerkategorien: Ein Produkt gelangt fehlerfrei in den Verkehr, wenn es zu diesem Zeitpunkt frei von Fabrikations-, Konstruktions- und Instruktionsfehlern ist.[25] Fabrikationsfehler liegen vor, wenn einzelne Exemplare einer Produktserie wegen Mängeln in der Fertigung negativ vom Sollzustand der Produktserie abweichen. Konstruktionsfehler liegen vor, wenn das Produkt wegen eines unzureichenden Produktdesigns Sicherheitsmängel aufweist. Instruktionsfehler

[18] Dazu *Wagner,* in: MüKo-BGB, § 2 ProdHaftG Rn. 1.
[19] So der BGH, mit verschiedenen Formulierungen, in st. Rspr., vgl. *BGH*, NJW 2008, 3775 (3776 m.w.N.).
[20] *BGH*, NJW 2009, 1669 (1670, Rn. 12).
[21] *BGH*, NJW 2009, 1669 (1670, Rn. 6).
[22] *BGH*, NJW 2009, 2952 (2953 f., Rn. 18 m.w.N.).
[23] *BGH*, NJW 2009, 2952 (2952 f., Rn. 12 m.w.N.).
[24] Ebenso *Wagner,* in: MüKo-BGB, § 3 ProdHaftG Rn. 6; in diesem Sinne auch *BGH*, NJW 2009, 2952 (2953 f., Rn. 18).
[25] Hier und im Folgenden: vgl. *Kötz/Wagner,* Rn. 616 ff.

liegen schließlich dann vor, wenn der Hersteller über die Restrisiken bei der Verwendung seines konstruktions- und fabrikationsfehlerfreien Produkts den Nutzer nicht in zumutbarem Ausmaß aufklärt. Von einer Haftung für Entwicklungsfehler, also der Nichtberücksichtigung solcher Risiken, die zum Zeitpunkt des Inverkehrbringens nach dem Stand von Wissenschaft und Technik nicht erkannt werden konnten (vgl. § 1 Abs. 2 Nr. 5 ProdHaftG), ist der Hersteller freigestellt.

Im Kontext von intelligenten Agenten dürften primär Konstruktions- und Instruktionsfehler eine Rolle spielen. Fabrikationsfehler dürften nur dann auftreten, wenn der elektronische Kopiervorgang der Software fehlerhaft abläuft[26] – diese Fälle stellen das Produkthaftungsrecht aber vor keine besonderen Schwierigkeiten. Das Fehlverhalten eines intelligenten Agenten kann – von diesen Fällen abgesehen – nur in einer Fehlkonzeption oder unzureichenden Implementierung des Software-Algorithmus liegen, die alle Exemplare der Produktserie gleichermaßen betrifft.[27] Das Auftreten unvorhersehbarer Entscheidungen ist dabei Teil des Funktionsprinzips eines intelligenten Agenten und für dessen optimale Aufgabenerfüllung ebenso notwendig wie erwünscht. Die Fähigkeit zu unvorhergesehenem Verhalten stellt daher per se noch keinen Konstruktionsfehler dar.[28] Es handelt sich zugleich aber auch nicht um einen unbeachtlichen Entwicklungsfehler, da zumindest die Gefahr von unvorhergesehenen Fehlentscheidungen – wenn auch nicht unbedingt Art, Umfang und Ausmaß dieser Fehlentscheidungen – nach dem derzeitigen Stand von Wissenschaft und Technik wohlbekannt sind.[29]

Ob ein intelligenter Agent fehlerhaft konstruiert ist, hängt vielmehr davon ab, auf welche Art und mit welcher Häufigkeit der intelligente Agent Schäden welchen Ausmaßes herbeiführt. Das gilt unabhängig davon, ob der intelligente Agent sein erratisches Verhalten erst durch Prozesse des maschinellen Lernens im Betrieb entwickelt hat. Insbesondere begründet dieser Umstand nicht den Einwand des § 1 Abs. 2 Nr. 2 ProdHaftG. Denn die unzureichend eingegrenzte Fähigkeit zur autonomen Fortentwicklung der Steuerungslogiken war dem intelligenten Agenten bereits zum Zeitpunkt des Inverkehrbringens immanent.

IV. Mensch-Maschine-Analogien als maßgeblicher Performance-Test?

Welche Sicherheitsanforderungen die Schwelle zum Konstruktionsfehler bei intelligenten Agenten definieren, ist darüber hinaus noch weitgehend unklar. Die Herausbildung allgemeingültiger Sorgfaltsstandards gestaltet sich aus (mindestens) zwei Gründen als

[26] Ebenso *Gomille,* JZ 2016, 76 (78); *Wagner,* AcP 217 (2017), 708 (725 f.).
[27] Ebenso *Wagner,* AcP 217 (2017), 708 (726).
[28] A.A. *Zech,* Zivilrechtliche Haftung für den Einsatz von Robotern, S. 192 f.
[29] Ebenso *Zech,* Zivilrechtliche Haftung für den Einsatz von Robotern, S. 184; differenzierend *Sosnitza,* CR 2016, 764 (769).

herausfordernd: Zum einen gerät der – ansonsten gängige[30] – Rückgriff auf den etablierten Stand von Wissenschaft und Technik bei neuartigen Technologien schnell an seine Grenzen. Zum anderen vereint der Topos des intelligenten Agenten eine Vielzahl sehr unterschiedlicher Produkte, die in nahezu beliebigen Einsatzbereichen – von der Verwaltung von Terminen über das Rasenmähen bis zur Überwachung der Sicherheit eines Atomkraftwerks – eingesetzt werden können. Ein Umstand ist intelligenten Agenten jedoch regelmäßig gemein: Durch ihren Einsatz soll die Steuerung einer Aktivität durch einen Menschen (teil-)ersetzt werden. Könnten die berechtigten Sicherheitserwartungen der Nutzer also dahingehend konkretisiert werden, dass diese zumindest eine Leistung des intelligenten Agenten auf dem Niveau eines Menschen erwarten können, der mit derselben Aufgabe betraut wäre?

Ein derartiger Performance-Test wird im Schrifttum in unterschiedlicher Deutlichkeit vorgeschlagen, wenngleich – soweit ersichtlich – bislang ausschließlich im Kontext autonomer Fahrzeuge.[31] Soweit sich diese Äußerungen auf den US-amerikanischen *consumer expectations test* beziehen,[32] sind sie auf die deutsche Rechtslage jedoch nicht übertragbar, da diesem Fehlermaßstab abweichend vom deutschen Produkthaftungsrecht ein empirisches Konzept zugrunde liegt. Ob Nutzer intelligenter Agenten ein Performance-Niveau äquivalent zu einem menschlichen Operator *tatsächlich* erwarten, muss hier daher auch nicht näher erörtert werden.

Eine Mensch-Maschine-Analogie kommt im Wesentlichen in drei Spielarten in Betracht: Es könnte (1.) im Rahmen eines **situationsspezifischen Einzelvergleichs** zu fordern sein, dass der intelligente Agent bei der Bewältigung der konkreten zum Schaden führenden Situation einem sorgfältigen menschlichen Operator mindestens ebenbürtig gewesen wäre.[33] Der Mensch-Maschine-Analogie könnte auch (2.) ein **systembezogener Gesamtvergleich** zwischen den insgesamt verursachten Schäden beim Betrieb des intelligenten Agenten und jenen eines durchschnittlichen menschlichen Operators zugrunde liegen.[34] Schließlich könnte eine Mensch-Maschine-Analogie (3.) auch ausschließlich herangezogen werden, um das Sicherheitsniveau eines intelligenten Agenten zu bezeichnen, ab dem ein Produktfehler **mit Sicherheit ausgeschlossen** werden kann.[35]

[30] Vgl. statt vieler *Förster,* in: BeckOK-BGB, § 823 BGB Rn. 683 ff.
[31] *Borges,* CR 2016, 272 (275 f.); *Gomille,* JZ 2016, 76 (77); *Gurney,* U. Ill. J. L. T. 2013, 247 (261); *Geistfeld,* Cal. L. Rev. 105 (2017), 1611 (1638 f. u. 1651 ff.); teilweise kritisch *Wagner,* AcP 217 (2017), 708 (733 ff.); ablehnend *Vladeck,* Wash. L. Rev. 89 (2014), 117 (130 ff.).
[32] *Gurney,* U. Ill. J. L. T. 2013, 247 (261); *Geistfeld,* Cal. L. Rev. 105 (2017), 1611 (1638 f.).
[33] *Borges,* CR 2016, 272 (275 f.); *Gomille,* JZ 2016, 76 (77); kritisch *Wagner,* AcP 217 (2017), 708 (733 ff.).
[34] *Wagner,* AcP 217 (2017), 708 (734).
[35] *Geistfeld,* Cal. L. Rev. 105 (2017), 1611 (1638 f.); *Wagner,* AcP 217 (2017), 708 (735).

Alle diese Ansätze werden für die Übergangszeit diskutiert, in der erste autonome Produkte mit von Menschen gesteuerten Produkten konkurrieren. Je stärker der Einsatz von intelligenten Agenten zur Norm wird und je eher diese Produkte eine Sicherheit gewährleisten, die diejenige eines menschlichen Operators übersteigt, desto stärker verlieren Mensch-Maschine-Analogien an Aussagekraft.

V. Auslegung des Fehlerbegriffs anhand der Ziele des Schadensersatzrechts

Die Eignung von Mensch-Maschine-Analogien zur Konkretisierung des Fehlerbegriffs muss anhand einer funktionalen Analyse, die deren Vereinbarkeit mit den Zielen des Haftungs- und Schadensrechts untersucht, beurteilt werden.

Durch die Haftungsbestimmungen des Deliktsrechts soll eine (Re-)Allokation von Schäden erreicht werden, die optimale Anreize zur Schadensprävention generiert.[36] Optimale Anreizeffekte resultieren dabei nicht aus einer Rechtsnorm, die das größtmögliche Ausmaß an Schadensprävention erzwingt. In der ökonomischen Analyse des Rechts wurden vielmehr – vor allem durch *Calabresi*[37] – Bedingungen für effizienzbasierte Haftungsregime aufgestellt, die die soziale Nützlichkeit schadensgeneigter Tätigkeit maximieren. Dazu gehört die Reduktion primärer Schadenskosten, die sich aus der Summe der Schadensvermeidungskosten und der eingetretenen Schäden zusammensetzen.[38] Diese Kosten erreichen nach der sog. marginalisierten Learned Hand-Formel ihren Tiefstwert, sobald die Grenzkosten zusätzlicher Schadensvermeidungsmaßnahmen höher ausfallen als der hierdurch erzielte Grenznutzen in Form eines verminderten Schadenserwartungswerts (das Ausmaß der Schäden multipliziert mit der Eintrittswahrscheinlichkeit).[39] Darüber hinausgehende, überoptimale Schadensvermeidungsmaßnahmen wären teurer als der durch sie abgewandte Schaden – sie zu unterlassen ist ökonomisch vorzugswürdig (genauer: Kaldor-Hicks-effizient).[40]

Ein verschuldensabhängiges Haftungsregime – wozu, wie gezeigt, auch die Haftung des Herstellers für fehlerhaft konstruierte Produkte gehört – setzt Anreize zur Erreichung eines optimalen Vorsorgeniveaus, sofern der Sorgfaltspflichtmaßstab gerade nur die nach der Learned Hand-Formel optimale Vorsorge beinhaltet.

---

[36] Grundlegend *Wagner,* AcP (206) 2006, 352 (451 ff.). Zur Leerformelhaftigkeit der noch immer häufig angeführten „Ausgleichsfunktion“: *Schäfer/Ott,* Ökonomische Analyse, S. 150 f.; *Wagner,* in: MüKo-BGB, Vor § 823 Rn. 43.

[37] *Calabresi*, The Cost of Accidents.

[38] *Calabresi,* The Cost of Accidents, S. 26 u. 68 ff.

[39] Zurückgehend auf Judge Learned Hand in der Entscheidung United States v. Carroll Towing Co., 159 F. 2d 169 (2d Cir. 1947). Vgl. für eine zutreffende formalisierte Definition der Marginalbedingungen nach der Learned Hand-Formel *Schäfer/Ott,* Ökonomische Analyse, S. 183, Fn. 8.

[40] *Schäfer/Ott,* Ökonomische Analyse, S. 154.

Das deutsche Produkthaftungsrecht folgt diesen ökonomischen Prinzipien: Wie gezeigt, erwartet das Produkthaftungsrecht keine optimale Sicherheit, sondern nur die Vornahme zumutbarer Sicherheitsverbesserungen. Der für Konstruktionsfehler vom BGH anerkannte *risk utility*-Test fragt danach, ob eine Alternativkonstruktion des Produkts Kosten verursachen würde, die über die damit einhergehende Schadensverminderung hinausgehen.[41] Ist das der Fall, überschreitet eine solche Alternativkonstruktion das Maß an Sorgfalt, das dem Hersteller zumutbar ist – und kann daher nicht berechtigterweise erwartet werden. Dieses Kriterium entspricht der Learned Hand-Formel.[42]

Die ökonomische Analyse des Schadensersatzrechts ist in Fällen bilateral verursachter Schäden, also solcher Schäden, die (wie zumeist) sowohl durch Vorsorgemaßnahme des Schädigers als auch des Geschädigten verhütet werden können, zu modifizieren. Ein effizientes Sorgfaltsniveau wird hier erreicht, wenn Schädiger und Geschädigter das für sie jeweils optimale Niveau an Schadensvermeidungskosten aufwenden.[43] Kann der Erwartungswert von Schäden durch eine Partei unabhängig vom Sorgfaltsniveau der anderen kostengünstiger verringert werden, liegt es nahe, die Haftungsrisiken bei diesem sog. *cheapest cost avoider* zu allozieren.[44] Das deutsche Produkthaftungsrecht trägt diesem Umstand Rechnung, indem ein Unterschreiten des optimalen Sorgfaltsniveaus durch den Geschädigten ein Mitverschulden begründet (§ 6 Abs. 1 ProdHaftG, § 254 BGB), die zu einer Anspruchskürzung bis zu einem vollständigen Anspruchsausschluss führen kann.[45]

VI. Analyse der Geeignetheit von Mensch-Maschine-Analogien zur Konkretisierung des Fehlerbegriffs

Von den Fällen, in denen der Betrieb eines intelligenten Agenten zu Schäden führt, sind somit zunächst diejenigen abzuschichten, in denen der Geschädigte als *cheapest cost avoider* einzuordnen ist. Denn dann kommt es auf die Bestimmung des Sorgfaltsmaßstabs des Herstellers ohnehin nicht an, da Schadensersatzansprüche spätestens am ganz erheblich überwiegenden Mitverschulden des Geschädigten (§ 6 Abs. 1 ProdHaftG, § 254 Abs. 1 BGB) scheitern.

Beispiel: Ein durch einen intelligenten Agenten gesteuerter, autonomer Mähroboter scheitert wegen Unvollkommenheiten an der Steuerungssoftware daran, be-

[41] *BGH*, NJW 2009, 2952 (2953 f., Rn. 18); *Wagner*, in: MüKo-BGB, § 823 Rn. 820; *ders.,* in: MüKo-BGB, § 3 ProdHaftG Rn. 39.
[42] *Schäfer/Ott,* Ökonomische Analyse, S. 375.
[43] Vgl. *Schäfer/Ott,* Ökonomische Analyse, S. 262 ff.
[44] *Calabresi,* The Cost of Accidents, S. 135 ff.
[45] Zur Anwendung der „Cheapest Cost Avoider"-Figur i.R.v. § 254 BGB: *Schäfer/Ott,* Ökonomische Analyse, S. 254.

sonders flache Objekte zu erkennen und zu umfahren. Auf der Rasenfläche liegende Handtücher und Kleidungsstücke werden von ihm daher regelmäßig beschädigt. Eine Verbesserung des Algorithmus, durch die derartige Schäden vermieden würden, stellt sich als außerordentlich kostspielig heraus. Dem Nutzer des Mähroboters ist eine Schadensvermeidung hingegen unschwer möglich, indem er wahlweise seine Rasenfläche ordentlich hält oder anderenfalls den Betrieb des Roboters zeitweilig unterbricht. Unterlässt er diese Schadensvermeidungsmaßnahmen, kommen Schadensersatzansprüche gegen den Hersteller – unabhängig davon, ob die Softwareunvollkommenheit einen Konstruktionsfehler darstellt – wegen des deutlich überwiegenden Mitverschuldens des Geschädigten nicht in Betracht. Der Hersteller ist allerdings im Rahmen seiner Instruktionspflichten gehalten, auf die Schwäche des Mähroboters bei der Erkennung flacher Objekte in zumutbarer Art hinzuweisen.

In allen übrigen Fällen setzt die Feststellung eines Konstruktionsfehlers nach dem *risk utility-Test* den Nachweis voraus, dass der Hersteller mit seinem Produktdesign das optimale Sorgfaltsniveau unterschritten hat. Lassen Mensch-Maschine-Analogien einen hinreichend plausiblen Rückschluss auf dieses optimale Sorgfaltsniveau zu, um als Prinzip „mittlerer Reichweite“ eine genauere Feststellung des Sorgfaltsniveaus entbehrlich zu machen?

Der o.g. **situationsbezogene Einzelvergleich** dürfte hierfür unergiebig sein und zugleich erhebliche Fehlanreize hinsichtlich einer optimalen Schadensprävention generieren. Denn die Situationen, deren Bewältigung einem intelligenten Agenten besonders schwer- oder leichtfallen, dürften selten mit den Situationen korrespondieren, die einem menschlichen Operator große oder geringe Mühen bereiten. Ein autonomes Fahrzeug mag etwa eine helle Lkw-Plane nur mit Mühe von einem hochhängenden Straßenschild unterscheiden können,[46] dafür aber Fußgänger selbst bei Dunkelheit und im „peripheren“ Sichtfeld erheblich besser wahrnehmen als ein menschlicher Fahrer. Ein situationsbezogener Einzelvergleich würde nun Verhaltensanreize setzen, die Leistung des intelligenten Agenten *nur* in jenen Bereichen zu verbessern, in denen er einem menschlichen Operator unterlegen ist. In Bereichen, in denen der intelligente Agent einem menschlichen Operator bereits mindestens ebenbürtig ist, würde eine weitere Produktverbesserung ausschließlich die Schadensvermeidungskosten des Herstellers erhöhen, ohne dass hierdurch sein Haftungsrisiko gesenkt würde. Hinzu kommt, dass die Verbesserung der „Schwächen“ des intelligenten Agenten im Einzelfall ein erheblich schlechteres Kosten-Nutzen-Verhältnis aufweisen könnte als eine weitere Verbesserung seiner „Stärken“. Im schlechtesten Fall führt ein situationsbezogener Einzelvergleich somit zu überoptimaler Sorgfalt hinsichtlich der „Schwächen“

[46] Vgl. Zeit Online v. 3.7.2016, Tesla-Autopilot hielt Lkw für Verkehrsschild, abrufbar unter https://goo.gl/p4oFyB.

des intelligenten Agenten und zu unteroptimaler Sorgfalt hinsichtlich seiner „Stärken“; derartig fehlgesteuerte Präventionsanreize könnten zu einer Reduktion an Produktsicherheit bei einer gleichzeitigen Erhöhung der Herstellungskosten führen.

Diese Schwächen vermeidet ein **systembezogener Gesamtvergleich,** in dessen Rahmen die durchschnittlichen Gesamtschäden aus dem Betrieb des intelligenten Agenten den durchschnittlichen Gesamtschäden eines menschlichen Operators gegenübergestellt werden.

Beispiel: Ein autonomer Staubsaugerroboter verursacht Schäden am Mobiliar, die durch eine imperfekte Objekterkennung und Routenplanung herbeigeführt werden. Der Hersteller des Staubsaugerroboters kann die zu erwartenden Schäden durch eine Verbesserung des Algorithmus reduzieren; diese Verbesserungsmaßnahmen weisen einen abnehmenden Grenznutzen auf. Der Geschädigte kann die Schäden nur effektiv eindämmen, indem er an Möbelkanten Lichtschranken installiert; deren Preis ist so exorbitant, dass sein optimales Vorsorgeniveau erreicht ist, wenn er keine einzige Lichtschranke installiert. Die Funktion des Schadenserwartungswerts in Abhängigkeit von den Schadensvermeidungskosten des Herstellers lautet:[47]

Vermeidungskosten des Herstellers	Schäden (Erwartungswert)	Σ
0	200	200
5	100	105
10	50	60
15	25	40
20	15	35
25	12	37
30	10	40

Das optimale Vorsorgeniveau liegt damit bei Vermeidungskosten von 20 und einem Schadenserwartungswert von 15 pro verkaufter Einheit.

Im Rahmen einer Mensch-Maschine-Analogie würde nun die Schadensgeneigtheit eines Produkts mit intelligentem Agenten mit der Schadensgeneigtheit eines vom Menschen gesteuerten Produkts verglichen. In der Logik des *risk utility*-Tests stellt die manuelle Steuerung also eine alternative Produktgestaltungsoption für den Hersteller dar.

[47] Von Auswirkungen des Aktivitätsniveaus auf den Erwartungswert wird vorliegend abstrahiert. Zu einer Steuerung des Aktivitätsniveaus ist die verschuldensabhängige Haftung für Konstruktionsfehler ohnehin ungeeignet: vgl. allgemein zu diesem Defizit der Verschuldenshaftung *Schäfer/Ott,* Ökonomische Analyse, S. 234 ff.

Nehmen wir an, ein Mensch, der seine Wohnung selbst staubsaugt, verursacht durch Kollisionen mit Möbelstücken im Durchschnitt Schäden von 11. Die Feststellung des optimalen Vorsorgeaufwands verändert sich hierdurch wie folgt:

Gestaltungsoption	Vermeidungskosten des Herstellers	Schäden (Erwartungswert)	Σ
	0	200	200
Verbess. des Algorithmus	15	25	40
	20	15	35
	30	10	40
Verzicht auf Algorithmus-Steuerung	0	11	11

Der Verzicht auf eine algorithmische Steuerung verursacht dem Hersteller keine Kosten, sodass die Gesamtkosten dieser Gestaltungsoption denjenigen Schäden entsprechen, die durch menschliches Versagen im Durchschnitt entstehen. Da die Optimierung eines intelligenten Agenten stets Kosten > 0 verursacht, könnte dieser nur dann konstruktionsfehlerfrei sein, *wenn die verursachten Schäden die Gesamtschäden eines menschlichen Operators unterschreiten*. Der Nachweis eines Konstruktionsfehlers könnte sich dann in der Tat darauf beschränken, den im Vergleich zu einem menschlichen Operator erhöhten Schadenserwartungswert beim Betrieb eines intelligenten Agenten darzulegen.

Ein so verstandener *risk utility*-Test greift allerdings zu kurz. Denn der Fokus der soeben durchgeführten Betrachtung liegt ausschließlich auf den Risiken der neuen Technologie, trägt ihren Vorzügen aber keinerlei Rechnung. Das Ziel des Schadensersatzrechts ist es aber, Handlungsanreize zu setzen, durch die der soziale Nutzen einer schadensgeneigten Tätigkeit maximiert wird.[48] Der soziale Nutzen setzt sich zusammen aus dem kumulierten Nutzen, den Schädiger und Geschädigter aus der Aktivität ziehen, abzüglich der Summe an Schäden und kombinierten Schadensvermeidungskosten von Schädiger und Geschädigtem. Der Umstand, dass bei autonomen Fahrzeugen eine systembezogene Mensch-Maschine-Analogie denkbar erscheint, dürfte darauf zurückführbar sein, dass eine Schadensquote unterhalb von menschlichen Fahrern vergleichsweise leicht erreichbar erscheint und Kraftfahrzeuge ohnehin bereits eine ausgesprochen gefährliche Technologie darstellen. Bei zahlreichen anderen autonomen Geräten dürfte eine höhere Schadensgeneigtheit gegenüber einem menschlichen Ope-

[48] *Schäfer/Ott,* Ökonomische Analyse, S. 157 ff.

rator durch den automatisierungsbedingten Komfortgewinn mehr als aufgewogen werden. Der entgangene Komfortgewinn, wenn statt eines intelligenten Agenten ein Mensch die Steuerung eines Geräts übernimmt, lässt sich in Form von Opportunitätskosten ausdrücken. In der Logik des oben entwickelten *risk utility*-Tests, in dem eine Gerätevariante mit manueller Steuerung als Gestaltungsoption berücksichtigt wurde, stellen diese Opportunitätskosten einen Schadensvermeidungsaufwand durch den Geschädigten dar. Mit anderen Worten: Der Nutzer verzichtet auf den Komfort aus dem Einsatz eines intelligenten Agenten, um die erwarteten Schäden zu reduzieren.

Nehmen wir also an, der Zugewinn an Zeit durch das autonome Tätigwerden des Staubsaugroboters verfügt über einen durchschnittlichen Wert von 80. Wird der Verzicht auf diesen Zugewinn in Opportunitätskosten zur Schadensvermeidung umgedeutet, verändert sich die vorherige Darstellung folgendermaßen:

Gestaltungs-option	Verm.-Kosten Hersteller	Verm.-Kosten Nutzer	Schäden (Erwartungswert)	Σ
Verbess. des Algorithmus	0	0	200	200
	15	0	25	40
	20	0	15	35
	30	0	10	40
Verzicht auf Algorithmus-Steuerung	0	80	11	91

In dieser Betrachtung verliert die Mensch-Maschine-Analogie jegliche Relevanz. Das optimale Vorsorgeniveau von Hersteller und Nutzer tritt vielmehr (wieder) ein, wenn der Hersteller einen intelligenten Agenten einbaut und diesen mit Kosten von 20 pro verkaufter Einheit optimiert. Eine darüber hinausgehende Verbesserung des Algorithmus ist ineffizient.

Eine Einbeziehung des Automatisierungsgewinns soll nicht bedeuten, dass im Rahmen des Produkthaftungsrechts stets die Konsumentenrente des Nutzers berücksichtigt werden sollte. Das würde einerseits Produkthaftungsprozesse überfordern und andererseits unterschiedliche Sorgfaltsstandards gegenüber jedem individuellen Nutzer provozieren. Das Produkthaftungsrecht ist aus verschiedenen Gründen ohnehin nicht geeignet, die soziale Nützlichkeit von Aktivitäten zu gewährleisten.[49] In der hier vorgeschlagenen Betrachtungsweise geht es vielmehr ausschließlich darum, die Kosten

[49] Vgl. zur Verschuldenshaftung allgemein *Schäfer/Ott*, Ökonomische Analyse, S. 202 ff. und zu bilateralen Schäden ebd., S. 267 f.

der einen Gerätesteuerung (dem Algorithmus) in verschiedenen Optimierungsgraden den Kosten einer alternativen Gerätesteuerung (der Steuerung und Überwachung durch einen Menschen) gegenüberzustellen. Die Schadensvermeidungskosten werden bei einem Verzicht auf den intelligenten Agenten regelmäßig nicht gemindert, sondern lediglich auf den Nutzer in Form eines erhöhten Steuerungs- und Kontrollaufwands übergewälzt.

Mangelt es Mensch-Maschine-Analogien also generell an Aussagekraft zur Feststellung eines fehlerhaft konstruierten intelligenten Agenten? Eine von *Geistfeld*[50] zum US-amerikanischen Produkthaftungsrecht entwickelte Mensch-Maschine-Analogie erscheint unter drei Bedingungen plausibel: Das Produkt stellt (1.) die Ersteinführung eines autonomen Produkts dar. Die Verbesserung des Schadenserwartungswerts verursacht (2.) nicht nur Kosten, sondern verzögert auch die Produkteinführung. Gerade bei Algorithmen, die auf maschinellem Lernen beruhen, kostet die für eine Verbesserung erforderliche Erhöhung der Trainingszyklen Zeit. Und (3.) soll die Mensch-Maschine-Analogie nicht zur Ermittlung des optimalen Vorsorgeniveaus herangezogen werden, sondern dient dem Hersteller als Verteidigungsmittel, um seinen hinreichenden Vorsorgeaufwand plausibel zu machen.

Unter diesen Voraussetzungen überzeugt es prima facie, einen Konstruktionsfehler ab einer Schadensverminderung von 50 % gegenüber einem menschlichen Operator mit einiger Sicherheit zu verneinen. Während einer Verzögerung der Produkteinführung, um den intelligenten Agenten weiter zu optimieren, wären Nutzer auf die Verwendung der nicht-autonomen, mindestens doppelt so schadensgeneigten Technologie angewiesen. Unterstellt, der Betrieb eines intelligenten Agenten führt im Schnitt zu Schäden i.H.v. 0,5; ein durchschnittlicher menschlicher Operator verursacht im gleichen Zeitraum Schäden i.H.v. 1,0. Die Entscheidung des Herstellers, die Produkteinführung zugunsten weiterer Optimierungen zu verzögern, führt also kausal dazu, dass derjenige Nutzer, der auf den manuellen Betrieb angewiesen bleibt, während der Verzögerungszeit zusätzliche Schäden i.H.v. 0,5 verursacht. Das durch die Verzögerung herbeigeführte „Mehr“ an Schaden ist damit mindestens so groß wie der Schaden, der durch die weitere Produktverbesserung verhindert werden soll.

Einem Hersteller, der sich im Einklang mit diesen Überlegungen für eine frühere Produkteinführung entscheidet, kann daher kaum der Vorwurf gemacht werden, er habe mit seiner Entscheidung ein sorgfaltspflichtwidrig unausgereiftes Produkt in den Verkehr gebracht. Dieser Einwand befreit den Hersteller selbstverständlich nicht davon, seinen intelligenten Agenten in der Folgezeit so lange zu optimieren, bis das op-

[50] *Geistfeld,* Cal. L. Rev. 105 (2017), 1611 (1651 ff.); zust. *Wagner,* AcP (207) 2017, 708 (734 f.).

timale Schadensvorsorgeniveau nach dem *risk utility*-Test bzw. der marginalisierten Learned Hand-Formel erreicht wird.

VII. Ausblick

Mensch-Maschine-Analogien verfügen in den meisten Konstellationen über keinen relevanten Aussagegehalt, der ihre Eignung als Prinzip mittlerer Reichweite zur Bestimmung eines Konstruktionsfehlers bei intelligenten Agenten rechtfertigen würde. Eine eng umgrenzte Ausnahme stellt das mindestens 50%ige Unterschreiten der Schadensquote eines menschlichen Operators dar, deren weitere Verbesserung die Ersteinführung eines autonomen Produkts verzögern würde.

Geschädigten bleibt damit vorerst nichts anderes übrig, als unmittelbar die Voraussetzungen des *risk utility*-Tests nachzuweisen. Für einen solchen Fehlernachweis braucht der Geschädigte nicht das genaue Sorgfaltsoptimum zu ermitteln; es genügt vielmehr der Nachweis, dass durch eine (beliebige) Alternativkonstruktion eine Schadensverringerung herbeigeführt würde, die die Zusatzkosten dieser Alternative übersteigt.[51] Ein solcher Nachweis kann sich seriös auf das erkennbar überlegene Verhalten konkurrierender intelligenter Agenten in bestimmten Situationen stützen.[52] Dass der Hersteller selbst zu einem späteren Zeitpunkt eine Produktverbesserung (bspw. durch ein Update) vorgenommen hat, durch die der Schaden vermieden worden wäre,[53] kann hingegen weder im Rahmen von § 823 Abs. 1 BGB[54] noch im Rahmen der Produkthaftung (§ 3 Abs. 2 ProdHaftG) verwertet werden.

Die mit dem Nachweis eines Konstruktionsfehlers verbundenen Schwierigkeiten dürften angesichts der Komplexität moderner KI-Algorithmen dennoch signifikant sein – wenn auch nicht notwendig höher als jene Schwierigkeiten, denen Geschädigte anderer Hightech-Produkte ausgesetzt sind. Eine Vereinfachung des Fehlernachweises würde allerdings einem Under-Enforcement der produkthaftungsrechtlichen Regelungen begegnen und dadurch deren Präventionswirkung stärken. In Betracht käme – neben der Herausbildung operabler „Faustformeln“ zur Fehlerhaftigkeit intelligenter Agenten durch Rechtsprechung und -wissenschaft – eine Durchsetzung von Produkthaftungsansprüchen in kollektiven Rechtsschutzverfahren.

Die Einführung einer strikten Gefährdungshaftung für die Hersteller intelligenter Agenten würde schließlich Kläger und Gerichte von der Notwendigkeit befreien, das

[51] Zu dieser Lesart der Learned Hand-Regel *Schäfer/Ott,* Ökonomische Analyse, S. 210 ff.
[52] *Wagner,* AcP (217) 2017, 708 (736) spricht in diesem Zusammenhang anschaulich von „blinden Fleck[en]“.
[53] *Gurney,* U. Ill. J. L. T. 2013, 247 (266).
[54] Das zumutbare Maß an Verkehrssicherung ist stets aus der ex ante-Perspektive, also der Perspektive zum Zeitpunkt der zur Rechtsgutsverletzung führenden Handlung, zu bestimmen: *Wagner,* in: MüKo-BGB, Vor § 823 BGB Rn. 70.

optimale Sorgfaltsniveau bei der Konstruktion eines intelligenten Agenten zu ermitteln. Sofern eine solche Regelung eine Mitverschuldenseinrede umfasst, wäre dieser Vorteil indes wieder hinfällig, da in Konstellationen bilateraler Schadensverursachung das optimale Sorgfaltsniveau des Geschädigten nur mit Rücksicht auf das optimale Sorgfaltsniveau des Schädigers bestimmt werden kann.[55] Eine Mitverschuldensregelung ist wiederum dringend zu empfehlen, um die Allokation von Haftungsrisiken beim *cheapest cost avoider* zu gewährleisten und unteroptimale Schadensvermeidungsbemühungen des Geschädigten zu unterbinden. Bei der Ausgestaltung eines optimalen Haftungsregimes für die Herstellung intelligenter Agenten bewegt sich der Gesetzgeber somit in einer komplexen, von Zielkonflikten geprägten Gemengelage widerstreitender Anreizeffekte.

Literaturverzeichnis

Borges, Georg, Haftung für selbstfahrende Autos. Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272.

Calabresi, Guido, The Costs of Accidents: A Legal and Economic Analysis, New Haven/London 1970.

Geistfeld, Mark A., A roadmap for autonomous vehicles: State tort liability, automobile insurance, and federal safety regulations, Cal. L. Rev. 105 (2017), 1611.

Gomille, Christian, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76.

Gurney, Jeffrey K., Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles, U. Ill. Journal of Law, Technology and Policy 2013, 247.

Gsell, Beate et al. (Hrsg.), beck-online.Großkommentar BGB, München, Stand: 1.3.2018.

Hanisch, Jochen, Zivilrechtliche Haftungskonzepte für Robotik, in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, S. 27-61, Baden-Baden 2013.

Kötz, Hein / Wagner, Gerhard, Deliktsrecht, 13. Aufl., München 2016.

Russell, Stuart J. / Norvig, Peter, Artificial Intelligence: a modern approach (International Edition), 3. Aufl., New Jersey 2010.

Säcker, Franz Jürgen et al. (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 7. Auflage, München 2017.

[55] *Schäfer/Ott,* Ökonomische Analyse, S. 266.

Schäfer, Hans-Bernd / Ott, Claus, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5. Aufl., Berlin/Heidelberg 2012.

Sosnitza, Olaf, Das Internet der Dinge - Herausforderung oder gewohntes Terrain für das Zivilrecht?, CR 2016, 764.

Spindler, Gerald, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien?, CR 2015, 766.

Teubner, Gunther, Digital Personhood? The Status of Autonomous Software Agents in Private Law, 2018, abrufbar auf SSRN: https://ssrn.com/abstract=3177096.

Vladeck, David C., Machines without Principals: Liability Rules and Artificial Intelligence, Wash. L. Rev. 89 (2014), 117.

Wagner, Gerhard, Produkthaftung für autonome Systeme, AcP 217 (2017), 708.

ders., Prävention und Verhaltenssteuerung durch Privatrecht – Anmaßung oder legitime Aufgabe?, AcP 206 (2006), 352.

Zech, Herbert, Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, S. 163–204, Baden-Baden 2016.

Einsatz autonomer unbemannter Flugsysteme im bewaffneten Konflikt und seine Konformität mit dem Völkerrecht

Dr. iur. Nato Natalie Tsomaia, LLM.Eur.

Hochschule für Wirtschaft und Recht Berlin
natuli_ts@yahoo.de

Abstract

Im Beitrag wird der Unterschied zwischen teil- und vollautonomen unbemannten Luftfahrtsystemen vorgestellt und deren Einsatz aus der Perspektive des humanitären Völkerrechts bewertet. Es wird festgehalten, dass die technische Weiterentwicklung neuer vollautonomer Luftfahrtsysteme anhand des Verhältnismäßigkeits- und Unterscheidungsgrundsatzes des Völkerrechts beschränkt ist, da die menschliche Beteiligung an dem hochkomplexen Abwägungsprozess unentbehrlich ist. Die Programmierung und Ausstattung von Drohnen mit diesem Beurteilungsspielraum wird für unmöglich erklärt, da dieser Prozess ohne Gewissensentscheidung nicht zu verwirklichen ist. Ziel des Beitrags ist es, einen angemessenen Ausgleich zu finden, um somit dem Verharmlosen von Töten entgegenzuwirken. Ferner werden die Rechte der Zivilbevölkerung, welche an Feindseligkeiten nicht teilnehmen, definiert und in diesem Zusammenhang die Pflicht zum Gewaltverbot der an dem bewaffneten Konflikt beteiligten Parteien zu Gunsten und zum Schutz von Zivilisten herausgearbeitet. Es wird zwischen legalen und illegalen Maßnahmen abgegrenzt und folglich die letale Gewaltanwendung gegen die Zivilbevölkerung nur in besonders gelagerten Ausnahmefällen zum Zweck eines konkreten militärischen Vorteils unter Voraussetzung der Einzelfallprüfung bei genauer Kenntnis aller relevanten Aspekte gerechtfertigt.

I. Ziel der Untersuchung

Ziel des Beitrags ist, die praktischen Auswirkungen der Digitalisierung auf Grund- und Menschenrechte beim Einsatz autonomer Luftfahrtsysteme darzustellen. Prozesse der Digitalisierung in der Luftfahrt führen zu Schwierigkeiten des Schutzes von Leib und Leben, werfen Fragen hinsichtlich der technischen Umsetzung von Befehlen auf und ziehen die Notwendigkeit einer gezielten rechtlichen Regulierung nach sich. Eines der Problemfelder der Digitalisierung mit Bezug auf die körperliche Unversehrtheit sowie

sicherheitsrelevante Aspekte ist der Einsatz von unbemannten Luftfahrtsystemen. Die Problematik kann vor dem Hintergrund der Terrorabwehr anhand von Art. 2 EMRK betrachtet werden. Art. 2 EMRK umfasst kein absolutes Recht auf Leben, sondern lediglich den Schutz gegen die willkürliche Beraubung des Lebens.[1] Nach dieser Ansicht wird nach Art. 2 Abs. 2 EMRK eine Tötung dann nicht als Verletzung des Rechts auf Leben angesehen, wenn sie durch eine Gewaltanwendung verursacht wird, die unbedingt erforderlich erscheint, um einen oder mehrere Menschen gegen rechtswidrige Gewalt zu verteidigen. Dabei geht es hauptsächlich um Tötungen durch bewaffnete Drohnen in einem bewaffneten Konflikt außerhalb des eigentlichen Kampfgeschehens.[2] Schwerpunktmäßig soll die Anwendung von Gewalt mittels unbemannter Flugsysteme untersucht werden, um eine rechtliche Bewertung der verwendeten Waffen, Sensoren und die Rolle des Bodenpersonals vorzunehmen. Es soll eine Abgrenzung zwischen voll- und teilautonomen bemannten Systeme erfolgen und die Klärung der Frage, ob das System in der Lage ist zwischen Kombattanten[3] und Zivilpersonen zu unterscheiden und zuletzt wie die Prüfung des Verhältnismäßigkeitsgrundsatzes stattfindet und ob die Vorgaben des humanitären Völkerrechts gewahrt sind. Für die Beantwortung der aufgeworfenen Fragen bedarf es zunächst der Konkretisierung des Untersuchungsgegenstandes sowie der rechtlichen Rahmenbedingungen.

II. Untersuchungsgegenstad

Die Begriffe unbemanntes Luftfahrzeug (Unmanned Aerial Vehicle (UAV)) und Drohne können synonym verwendet werden.[4] Von diesen Begriffen umfasst ist das Luftfahrzeug selbst, ohne dazugehörige Komponenten, die nicht unmittelbar zur Fortbewegung nötig sind, nicht mitumfasst sind demnach Waffen oder Sensoren zur Bodenaufklärung.[5] Der Begriff der autonomen unbemannten Flugsysteme (Unmanned Aerial System (AUS)) ist hingegen weiter[6] und umfasst über das eigentliche Flugobjekt hinaus alle zu einander in Verbindung stehenden Komponenten wie Flugkörper, darauf mon-

[1] *Schmahl*, in: Leutheusser-Schnarrenberger, S. 185; *Oeter*, AVR 2002, 422 (435); *Tomuschat*, VN 2004, 136 (136).
[2] *Von Arnauld*, § 14 Rn. 1189.
[3] Zur Begriffsdefinition hat sich die an den Aktivitäten orientierte Strukturierung von Private Military Companies (PMC) durchgesetzt, hierbei ist die Nähe des Unternehmens zur Kampfhandlung charakterlich (darunter umfasst sind 3 Typen: Military Provider Firms, Military Consultant Firms und Military Support Firms. Demnach werden militärische Operationen, Sicherheitsdienstleistungen, Ausbildung und Beratung sowie Versorgung und Logistik differenziert. Dazu ausführlich: *Giesen*, S. 81 f. m.w.N.). Neben PMCs fallen unter Kombattanten auch Befreiungsbewegungen, Guerilleros und Terroristen, wobei der Klärung der Frage nach dem Kombattantenstatus entscheidende Bedeutung zukommt (Dazu ausführlich: *Giesen*, S. 93 f.). Der Kombattantenstatus bestimmt sich nach Art. 1 und 2 HLKO, Art. 4 ZP-III GK und Art. 43 ZP-I GK.
[4] *Städele*, S. 26.
[5] *Seiring*, S. 27.
[6] *Städele*, S. 25.

tierte Waffen[7], Sensoren[8], Bodenkontrollstation[9] und Bodenpersonal.[10] Somit besteht das UAS aus dem ferngesteuerten Fluggerät, welches ohne menschlichen Piloten[11] fliegt (UAV), einer Bodensteuerungseinheit, Sensoren und optional einem Wirkmittel zu Anwendung von Gewalt.[12] Ist die Rede von einer bewaffneten Drohne also Unmanned Combat Aerial Vehicles (UACV) ist sie Träger einer oder mehrerer Waffen und dient dem Zweck des Kampfeinsatzes.[13]

Das System der Autonomie umfasst mehrere Abstufungen.[14] Gesteuert werden die Drohnen entweder fern, hier handelt es sich um die niedrigste Autonomiestufe oder sie fliegen teil- oder vollautonom, währenddessen das System in unterschiedlichem Maße eine oder mehrere Aufgaben selbständig ausführt.

Fernsteuerung liegt vor, solange Sichtkontakt, also die Steuerung über Funkverbindung gegeben ist, oder kein Sichtkontakt vorhanden ist und die Steuerung über eine

[7] Nach der teleologischen Auslegung des Art. 36 ZP-I GK werden Waffen den Mitteln der Kriegsführung untergeordnet. Somit ist davon auszugehen, dass der Begriff Waffe enger zu verstehen ist als ein Mittel der Kriegsführung, wenngleich die Waffe sicherlich als Mittel der Kriegsführung zu qualifizieren ist, hingegen nicht jedes Mittel der Kriegsführung eine Waffe darstellt. Der Waffe ist eine funktional-kausale Nähe zur schädigenden Wirkung immanent, denn durch sie oder ihre Munition tritt die schädigende Wirkung ein. Im Gegensatz dazu werden vom Mittel der Kriegsführung solche Gegenstände umfasst, die den Angriff lediglich ermöglichen, ohne dabei an der Schädigungshandlung mitzuwirken (*Borrmann*, S. 32).

[8] Die Drohnen können je nach Model und Einsatzprofil mit unterschiedlichen Sensoren ausgestattet werden, welche nicht für die Selbstlokalisation, Navigation oder Selbsterhaltung sondern für die Missionserfüllung bestimmt sind. Anhand dieser Nutzsensoren wird die Bildgebung gewährleistet, man unterscheidet zwischen passiver und aktiver Bildgebung, passive Sensoren nehmen nur Informationen wie Licht auf, aktive Sensoren hingegen senden Signale wie Laser, Radar, Infrarot aus und messen somit die Reflektion (*Städele*, S. 36). Ferner erfolgt die signalerfassende Aufklärung, darunter ist die Aufklärung und Überwachung von Aktivitäten im elektromagnetischen Spektrum, also das Erfassen des gegnerischen Frequenzspektrums sowie seines Funkverkehrs zu verstehen (*Städele*, S. 38). Zuletzt soll die Laserzielmarkierung hervorgehoben werden, wonach anhand des Laserstrahls die Distanz zum anvisierten Objekt bestimmt wird. Dabei erfolgt das Anvisieren des Objekts, welches den Laserstrahl reflektiert und wiederempfängt. Das markierte Objekt kann vom Suchkopf der Waffe gefunden werden und ungeachtet seiner Sichtbarkeit für den Piloten vom markierenden UCAV abgefeuert werden (*Städele*, S. 28).

[9] Das operative Zentrum eines UAV-Einsatzes, wo alle Daten gesammelt und von dem Piloten und Nutzlastbediener ausgewertet, verarbeitet und gesteuert werden, was wiederum nicht zwangsläufig mit der Start- und Landestelle sowie Instandsetzung übereinstimmen muss (*Städele*, S. 27).

[10] *Seiring*, S. 27.

[11] Unter dem Begriff des Piloten ist die Person zu verstehen, die für die Drohne die Verantwortung übernommen hat, sie entweder steuert, überwacht und Mittel ergreift, um in den Einsatzablauf einzugreifen. In der Regel werden Drohnen von verschiedenen Personen gestartet bzw. gelandet und geflogen. Der Begriff des Piloten ist auf die Person anzuwenden, welche für die Fortbewegung die Verantwortung übernimmt. Somit handelt es sich um mindestens zwei Personen, eine von ihnen ist für die Fortbewegung und die andere für die Bedienung der Nutzlast - der sogenannte Nutzlastbediener – verantwortlich. Der Nutzlastbediener ist für die Steuerung und Ausrichtung der Sensoren sowie die Auswertung der gewonnenen Daten in Echtzeit verantwortlich. Handelt es sich um eine bewaffnete Drohne, so ist die Bedienung der Bewaffnung auch unter der Bedienung der Nutzlast umfasst (*Städele*, S. 26 f.).

[12] *Seiring*, S. 32.

[13] *Arendt*, in: Frau, S. 20 m.w.N.

[14] Dazu und zum Folgenden: *Arendt*, in: Frau, S. 21.

Satellitenverbindung mit Hilfe der Signalübertragung erfolgt.[15] Demnach erfolgt der Einsatz mit einem ferngesteuerten UAV gemäß den Eingaben eines Bedieners, welcher allein die Entscheidungsbefugnis über die zu fliegende Route, die Verifizierung eines identifizierten Ziels und das Vorgehen gegen dieses Ziel innehat.[16] Das UAV führt lediglich die Eingaben des Bedieners aus.

Was die teil- und vollautonome Steuerung betrifft, so ist sie entweder mit Hilfe von GPS (US-amerikanisches Global Position System) oder dem europäischem Pendant Galileo zwar möglich,[17] allerdings herrscht über Wesen und Ausmaß von Autonomie wenig Klarheit. Fest steht, dass der Einsatz der autonomen Systeme das Erfassen unbekannter Situationen, ihre Bewertung und daraus resultierende eigenständige Aktionen voraussetzt. Demnach handelt es sich nicht um die Ausführung vorprogrammierter Aufträge, sondern um die Ermittlung von Zielen, Informationsbeschaffung, Entscheidungsfindung über die Übermittlung von Daten sowie die selbständige Ausführung von Angriffshandlungen. Folglich bedeutet Autonomie die Fähigkeit eines Systems, nach Inbetriebnahme ohne jede Form externer Kontrolle zu operieren und mithin die Wahrnehmung, Verarbeitung, Kommunikation, Planung, Entscheidungsfindung und Ausführung des definierten Zieles zu steuern.[18]

Die technische Umsetzung eines solchen Auftrages knüpft an die künstliche Intelligenz, mithin an die Übernahme der Entscheidung über Leben und Tod, an. Folglich führt das vollständig autonome System tödliche Gewalt ohne Rückkopplung zu einer menschlichen Entscheidung aus, indem es entweder das Ziel oder den Zeitpunkt des Einsatzes letaler Gewalt oder aber beides gleichzeitig selbständig bestimmt.[19] Automatisierung wird anhand DIN 19233 definiert, danach wird erklärt, dass Automatisierung anhand der Ausrüstung einer Einrichtung gewährleistet werden kann, wonach die Ausrüstung ohne teilweise oder vollständige Mitwirkung des Menschen einsetzbar ist.[20] Das mit der Automatisierung herbeigeführte Ziel ist die Minimierung des menschlichen Handlungseinflusses auf die Durchführung einer Aufgabe. Damit wird versucht, die Qualität des Ergebnisses und dessen Reproduzierbarkeit sicherzustellen sowie aufgabenspezifische Gefährdungen für den menschlichen Ausführenden zu reduzieren. Abgestellt wird in diesem Kontext auf die Erfüllung der defensiven Aufgaben, wo kurze,

[15] *Städele*, S. 32.
[16] *Mahn-Gauseweg*, in: *Frau*, S. 8.
[17] Dazu und zum Folgenden: *Städele*, S. 33 m.w.N.
[18] *Mahn-Gauseweg*, in: Frau, S. 11 m.w.N.
[19] *Arendt*, in: Frau, S. 21.
[20] Dazu und zum Folgenden: *Mahn-Gauseweg*, in: Frau, S. 8 f. m.w.N.

durch Menschen nicht realisierbare Reaktionszeiten, erforderlich sind.[21] Die Herstellung solcher vollautonomen Systeme ist gegenwärtig noch nicht möglich.[22]

Zu der Begriffsbestimmung von UACVs kann ferner ausgeführt werden, dass sie als Waffen vermittelnde Vehikel zu betrachten sind.[23] Folglich werden sie unter dem Begriff Mittel der Kriegsführung, bzw. Mittel zur Schädigung des Feindes, des Kampf- und Angriffsmittels, des Waffensystems und der Plattform definiert.[24] Somit sind die UACVs zwar Mittel der Kriegsführung, aber da ihre Zuständigkeit lediglich auf die Lieferung von Zielinformationen oder Aufklärungsdaten beschränkt ist, liegt eine unmittelbare Teilhabe an der Schädigungshandlung nicht vor und folglich scheidet die Qualifizierung als Waffensystem aus, auch wenn grundsätzlich der Begriff des Waffensystems Bestandteil der Begriffsdefinition eines Mittels der Kriegsführung darstellt.[25] Somit sind UACVs als Mittel der Kriegsführung, Mittel zur Schädigung des Feindes, Kampfmittels und Angriffsmittels[26] zu qualifizieren, abzulehnen wäre die Definition als Waffe.[27]

III. Kontext der Fragestellung des Drohneneinsatzes

Nach Art. 22 HLKO wird den Kriegsführenden kein Recht eingeräumt, die Wahl der Mittel zur Schädigung des Feindes frei zu bestimmen. Auch in dem einschlägigem Zusatzprotokoll zum Genfer Abkommen vom 12.08.1949 über den Schutz der Opfer internationaler bewaffneter Konflikte ist diese Frage geregelt. Art. 35 Abs. 1 ZP-I GK versagt ein unbeschränktes Recht in der Wahl der Methoden und Mittel der Kriegsführung. Dies dient dem Zweck, überflüssige Verletzungen oder unnötige Leiden zu vermeiden. Nach der Definition des Art. 35 Abs. 2 ZP-I ist ein Angriff überflüssig oder unnötig, wenn er militärisch keinen Vorteil bringt und sich folglich mit dem Grundsatz der Notwendigkeit oder Erforderlichkeit nicht vereinbaren lässt.[28] Des Weiteren sind die Staaten an die Vorgaben des Art. 36 ZP-I der GK gebunden, danach ist bei der Prüfung, Entwicklung, Beschaffung oder Einführung neuer Waffen oder neuer Methoden und Mittel der Kriegsführung zu klären, ob ihre Verwendung stets oder unter bestimmten Umständen verboten wäre. Die Prüfungspflicht erstreckt sich sowohl auf die Waffen und deren Munition als auch auf die Trägersysteme.

[21] *Mahn-Gauseweg*, in: Frau, S. 11.
[22] *Mahn-Gauseweg*, in: Frau, S. 15 f.
[23] *Borrmann*, S. 33.
[24] *Borrmann*, S. 41.
[25] *Borrmann*, S. 36.
[26] Anwendung der bewaffneten Gewalt gegen den Gegner sowohl offensiver als auch defensiver Art unter Vorbehalt der Bestimmung des Art. 57 Abs. 2 lit. a) ii) I-ZP GK, wonach als Angriffsmittel solche Gegenstände in Frage kommen, welche zivile Kollateralschäden verursachen. Hier ist auf den Eintritt des Schädigungserfolges abzustellen, was nicht direkt sondern mittelbar anhand der Beschaffung von Zieldaten verursacht werden kann (*Borrmann*, S. 40).
[27] *Borrmann*, S. 47.
[28] *Müller*, in: Baade/Ehricht, S. 72 m.w.N.

Gegenwärtig ist weder der Einsatz der bereits existierenden Drohnen noch für zukünftige autonomen Waffensysteme reguliert oder von einer Konvention explizit mitumfasst.[29] Es ist kein spezielles Drohnenrecht in Kraft.[30] Auf die Drohnen finden lediglich die Kardinalprinzipien des Internationalen Gerichtshofes (IGH) Anwendung, wodurch die Wahlfreiheit der Staaten bei bewaffneten Konflikten eingeschränkt wird.[31] Diese Prinzipien haben Niederschlag in dem Ersten Zusatzprotokoll zur Genfer Konvention gefunden. Zum einen handelt es sich dabei um den Unterscheidungsgrundsatz gem. Art. 48 ZP-I der GK. Die Norm legt die Pflicht zur Unterscheidung zwischen Kombattanten und Personen, die direkt an den Feindseligkeiten teilnehmen, auf sowie des Weiteren die Unterscheidung zwischen militärischen Objekten und Zivilisten sowie zivilen Objekten. Zum anderen wird gem. Art. 35 Abs. 2 ZP-I GK das Verbot der Verursachung überflüssiger Verletzungen oder unnötiger Leiden festgelegt.

IV. Rahmenbedingungen für den Einsatz der unbemannten Flugsysteme

Die rechtliche Bewertung eines Drohneneinsatzes findet auf den jeweiligen Einzelfall bezogen statt. Für die Bewertung des Einsatzes ist das eingesetzte System irrelevant, vielmehr kommt es auf die Umstände des Einsatzes an. Die Umstände wiederum werden von dem Einsatz steuernden Drohnenpiloten und seinem Kommandanten beeinflusst.[32] Ferner ist für die Prüfung der rechtlichen Bewertung nicht die Drohne selbst, sondern das eingesetzte Kampfmittel entscheidend. Ein Angriff ist zulässig, solange die mögliche Schädigung der Zivilbevölkerung nicht unverhältnismäßig zum militärischen Vorteil ist.

Für den Einsatz und mithin die erfolgreiche Durchsetzung der militärischen Ziele ist eine detaillierte Planung und die nötige Sorgfalt in Bezug auf Organisation und Kontrolle der Operation erforderlich. Für einen bewaffneten Einsatz sind die Verantwortung tragende Befehlshaber verpflichtet, die Balance zwischen der Gefahr für eigene Kräfte und Minimierung von Kollateralschäden zu halten, hierbei handelt es sich um einen Abwägungsprozess, welcher kontinuierlich stattfindet. Die Abwägung wird meist vom Drohnenpiloten oder seinem Kommandanten vorgenommen. Hier ist geboten zu klären, wie sich dieser Prozess mit den Grundsätzen der Unterscheidung gem. Art. 48 ZP-I

[29] *Wuschka*, in: Baade/Ehricht, S. 49.
[30] *Becker*, DVBI 2018, 619 (620). Der Autor befürwortet die Entwicklung eines speziellen Vertragsvölkerrechts wie im Fall der Chemiewaffenkonvention (Übereinkommen über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen vom 13.01.1993) oder des Landminenabkommens (Übereinkommen über das Verbot des Einsatzes, der Lagerung, der Herstellung und der Minensysteme oder Landminen vom 03.12.1997 (Ottawa-Konvention), der zwar alle EU-Mitgliedstaaten angehören aber nicht die USA).
[31] *IGH*, Nuclear Weapons, S. 257; dazu und zum Folgenden: *Wuschka*, in: Baade/Ehricht, S. 50 m.w.N.
[32] Dazu und zum Folgenden: *Wuschka*, in: Baade/Ehricht, S. 51 f. m.w.N.

GK sowie mit Art. 51 Abs. 4 ZP-I GK, dem Verbot der unterschiedslosen Angriffe, und der Verhältnismäßigkeit des humanitären Völkerrechts vereinbaren lässt. Denn sowohl die Unterscheidung als auch der Verhältnismäßigkeitsgrundsatz erfordern komplexe Wertungsentscheidungen, um festzustellen, ob das erwogene Ziel ein rechtlich legitimes Ziel darstellt. Würde man das Flugsystem vollautonom konzipieren und auf den Piloten verzichten, müsste der Fokus vor dem Hintergrund der Abwägung und Entscheidungsfindung gem. Art. 36 ZP-I der GK von dem Piloten auf das eingesetzte System selbst und dessen Fähigkeiten verlagert werden. Da dieser Prozess aber sehr komplex ist, der technische Fortschritt der Entwicklung von Drohnensystemen aber noch nicht so weit fortgeschritten ist, sind die rechtlichen Grenzen entsprechend eng gehalten. Die Rechtmäßigkeit des Einsatzes ist über die technischen Gegebenheiten hinaus von der Abwägung determiniert. Da die Abwägung bekanntlich ein menschlicher Prozess ist und technische Systeme noch keine qualitativen Faktoren, wie beispielsweise eventuelle Risiken berücksichtigen können, ist für die taktische und operative Verwendung der autonomen unbemannten Luftsysteme eine menschliche Beteiligung absolut notwendig.[33] Autonomes Handeln kann in Teilfunktionen im Zusammenspiel mit menschlichem Eingriff stattfinden.[34] Die Befassung mit der Materie der vollautonomen bewaffneten unbemannten Systeme ist daher dringend geboten, bevor die technische Entwicklung vollendete Tatsachen schafft.

In diesem Kontext sollen Art. 2 EMRK und Art. 6 IPbpR[35] hervorgehoben werden. Auch wenn die technische Entwicklung und ihre zukünftige Anwendung nach dieser Rechtsgrundlage nicht explizit verboten werden, stellt sie hohe Anforderungen an Staaten zum Schutz des Rechts auf Leben und die Verhinderung und Verfolgung von Verletzungen dieses Rechts. Daher führt unabhängig von der Art der eingesetzten Mittel die Folgeverpflichtung zur Hoheitsgewalt des agierenden Staates und mithin wieder zum menschlichen Prozess der Verpflichtung zur Planung und Vorbereitung von Angriffen sowie der Aufklärung ihrer Todesfälle.[36] Hier ist an die prozessrechtliche Verpflichtung aus Art. 2 EMRK zu erinnern, wonach dem verursachenden Vertragsstaat bei ungeklärten Todesfällen eine effektive behördliche Untersuchung über die Rechtmäßigkeit und Aufklärung der Tötungsumstände obliegt.[37] Zumal die Wirkung des Art. 6 IPbpR nicht auf das Staatsgebiet einer Vertragspartei beschränkt ist. Sie erstreckt sich auf alle Gebiete, wo die Hoheitsgewalt des jeweiligen agierenden Staates durch seinen

[33] *Städele*, S. 25 m.w.N.
[34] Ähnlich: *Mahn-Gauseweg*, in: Frau, S. 15.
[35] Art. 6 Abs. 1 IPbpR: „Jeder Mensch hat ein angeborenes Recht auf Leben. Dieses Recht ist gesetzlich zu schützen. Niemand darf willkürlich seines Lebens beraubt werden".
[36] Ähnlich *Stroh*, in: Frau, S. 162.
[37] *EGMR*, Urt. v. 27.09.1955, Nr. 18984/91, McCann u.a./Vereinigtes Königreich, Rn. 161.

Hoheitsträger in Form einer effektiven Kontrolle ausgeübt wird.[38] Gleiches gilt auch für die EMRK. Der EGMR legte fest, dass die EMRK extraterritorial wirkt, wenn eine effektive Kontrolle über ein fremdes Gebiet bzw. Autorität und Aufsicht über Personen in einem ausländischen Gebiet vorliegt oder effektive physische Macht und Kontrolle über eine Person ausgeübt wird.[39]

V. Verhältnismäßigkeitsgrundsatz des humanitären Völkerrechts

Ausgangspunkt des humanitären Völkerrechts sind die Art. 51 und 57 ZP-I der Genfer Konvention. Während zwischen Kombattanten und Zivilisten unterschieden wird, können Kombattanten stets mit tödlicher Gewalt angegriffen werden, hingegen dürfen Zivilisten gem. Art. 51 Abs. 2 ZP-I niemals ein Ziel einer Attacke sein. Ferner garantieren Art. 51 Abs. 5 lit. b) ZP-I sowie Art. 57 Abs. 2 ZP-I der Genfer Konvention den Schutz der Zivilbevölkerung vor unterschiedslosen Angriffen. Nach Art. 51 Abs. 5 lit. b) ZP-I wird auch ein unverhältnismäßiger Angriff als unterschiedslos eingestuft, wenn Verluste, Verwundung von Zivilpersonen, die Beschädigung ziviler Objekte oder mehrere derartige Folgen zusammen verursacht werden, welche in keinem Verhältnis zu einem erwarteten und unmittelbaren militärischen Vorteil stehen. Gem. Art. 57 Abs. 2 lit. a) iii) ZP-I ist von dem Angriff abzusehen, wenn Verluste und Verwundung unter der Zivilbevölkerung, Beschädigung ziviler Objekte oder mehrerer derartigen Folgen zusammen verursacht werden, welche in keinem Verhältnis zum erwarteten konkreten und unmittelbaren militärischen Verteil stehen. Nach Art. 57 Abs. 2 lit. b) ZP-I wird ferner der Abbruch des Angriffs vorgesehen, demnach ist der Verhältnismäßigkeitsgrundsatz sowohl im internationalen als auch im nicht-internationalen Konflikt im Völkerrecht und im Völkergewohnheitsrecht verankert.[40]

Von dem humanitären Völkerrecht nicht mitumfasst ist die Tötung oder Schädigung von Kombattanten, in der Abwägung werden lediglich zivile Opfer und Schäden berücksichtigt.[41] An und für sich ist im Rahmen des militärischen Verhältnismäßigkeitsprinzips die Abwägung von Menschenleben durchaus zulässig.[42] Allerdings darf eine Abwägung zu Lasten von Menschenleben nur als zulässig erachtet werden, wenn auf der anderen Seite ebenfalls Menschenleben oder andere höchst gewichtige Interessen stehen. Somit sind die Angriffe zu identifizieren und die davon erhofften Vorteile gegen den zu erwartenden Verlust an Menschenleben abzuwägen. Wenn der Angriff auf ein militärisches Ziel ausgeübt wird, bei dem der Verlust unter der Zivilbevölkerung als

[38] *Deutscher Bundestag*, BT-Drs. 18/6730 – Antwort: Mögliche Teilnahme eines Verbindungsoffiziers der Bundeswehr bei Auswahlprozessen für sogenannte gezielte Tötungen – Drucksache 18/6322 vom 17.11.2015, S. 1684.
[39] *EGMR*, Urt. v. 23.03.1995, Nr. 15318/89, Loizidou/Türkei, Rn. 62.
[40] *Wuschka*, in: Baade/Ehricht, S. 55.
[41] *Müller*, in: Baade/Ehricht, S. 72.
[42] Dazu und zum Folgenden: *Müller*, in: Baade/Ehricht, S. 76 ff.

Nebeneffekt eintritt, ist darauf abzustellen, ob solche Verluste vorherzusehen gewesen sind.[43] Somit ist die Abwägung der schwierigste Schritt, die einerseits die Festlegung eines konkreten unmittelbaren militärischen Zieles voraussetzt, welches gegen die Verletzung von Zivilisten und die Beschädigung ziviler Objekte abgewogen wird. Da keine allgemein gültigen Kriterien für die Abwägung vorgesehen sind, ist im konkreten Fall eine subjektive Entscheidung vorzunehmen. Dabei ist zu berücksichtigen, dass der Angriff auf einen hochrangigen gegnerischen Kombattanten relativ höher eingeschätzt wird als die Tötung eines niederrangigen Kombattanten. Folglich ist in diesem Zusammenhang auch der Verlust unter der zivilen Bevölkerung zu bewerten, ob er aufgrund des konkreten militärischen Vorteils rechtlich hinnehmbar wäre.[44] Was den Schaden von zivilen Objekten betrifft, so wird der zu erreichende militärische Vorteil nicht zwingend durch die Zerstörung eines spezifischen Objekts erreicht, sondern das Gesamtbild der durchgeführten Operation ist in die Betrachtung einzubeziehen.[45] Beurteilt wird die Vorbereitung, Planung und Kontrolle einer militärischen Operation, unter Hinzuziehung aller weiteren Normierungen aus dem Art. 57 ZP-I Genfer Konvention.[46] Insbesondere sollen gem. Art. 57 Abs. 2 lit. b) ZP-I GK die vorzunehmenden Maßnahmen je nach Lage und Informationsstand angepasst oder abgebrochen werden.[47] Nach Art. 57 Abs. 3 ZP-I GK ist für die Erreichung des militärischen Vorteils das mildeste Mittel bzw. das Ziel zu wählen, dessen Bekämpfung Zivilpersonen am wenigsten gefährdet.

Bei dieser Beurteilung ist der Gefährlichkeitsfaktor der anzugreifenden Person, gegen die sich die staatliche Gewalt richtet, entscheidend, da der Faktor der Gefährlichkeit die Anwendung der letalen Gewalt rechtfertigt.[48] Somit ist nicht nur der auf einen Kombattanten ausgeübte Angriff, sondern auch der auf einen Zivilisten legal, solange er an den Feindseligkeiten beteiligt ist und sich sehenden Auges in die Risikosituation begibt und somit mit dem Einsatz tödlicher Gewalt rechnen muss.[49] Geht von einer zivilen Person keine Gefahr aus, so darf sie kein Angriffsobjekt werden, allerdings wäre es rechtmäßig, wenn eine zivile Person sich in physischer Nähe zu einer Gefahrenquelle befindet und sie im Zuge dessen unbeabsichtigt Opfer der staatlichen Gewaltanwendung wird.[50] Entwickelt sich die Lage wider Erwarten anders, oder sind trotz Anwendung der entsprechenden Sorgfalt gewisse Umstände nicht erkennbar, sind gravie-

[43] Dazu und zum Folgenden: *Wuschka*, in: Baade/Ehricht, S. 56 m.w.N.
[44] *Wuschka*, in: Baade/Ehricht, S. 59 m.w.N.; *Müller*, in: Baade/Ehricht, S. 73 f.
[45] *Wuschka*, in: Baade/Ehricht, S. 59 m.w.N.
[46] *Müller*, in: Baade/Ehricht, S. 73 m.w.N.
[47] Dazu und zum Folgenden: *Müller*, in: Baade/Ehricht, S. 73.
[48] *Müller*, in: Baade/Ehricht, S. 81.
[49] *Müller*, in: Baade/Ehricht, S. 81.
[50] *Müller*, in: Baade/Ehricht, S. 81.

rende Negativfolgen der Tötungsakte nicht völkerrechtswidrig.[51] Allerdings müssen in der Abwägung der letalen staatlichen Gewalt alle zu Gunsten der Tötungshandlung vorliegenden Faktoren besonders deutlich ausgeprägt und die Anforderungen der strikten Verhältnismäßigkeitsprüfung gewahrt sein.[52]

In der Verhältnismäßigkeitsprüfung ist der quantitative Faktor[53] zu berücksichtigen. Sowohl im Rahmen der Prüfung nach Art. 2 EMRK als auch gem. Art. 51 ZP-I GK wird bei dem Aspekt des Verlustes an Menschenleben in der Zivilbevölkerung auf den konkreten unmittelbaren militärischen Vorteil abgestellt und mithin kommt der quantitative Faktor zum Tragen, hier wird die Zahl der zivilen Opfer im Vergleich 100 zu 10 andere Auswirkung haben.[54] Allerdings fehlen Kriterien, wonach die Menschenleben zu einander in Verhältnis zu setzen sind, ob es dabei über die Zahl hinaus auf andere Parameter wie Lebenserwartung, Geschlecht, Verwundbarkeit und Anfälligkeit, wie im Falle von Frauen und Kindern, abzustellen ist, wird nicht vorgegeben.[55]

Da die gegeneinander abzuwägenden Güter oft ungleich sind und die Verhältnismäßigkeitsfrage ihrer Natur nach keinen subjektiven, sondern einen objektiven Standard erfordert, wird subjektive Entscheidung des Kommandanten als objektiv einzuschätzen sein,[56] vorausgesetzt sie wurde unter Beachtung der objektiven Sorgfaltsanforderungen und in Kenntnis des Lagebildes getroffen.[57] Trotz des Entscheidungsspielraumes bleibt die Entscheidung des Kommandanten objektiv, denn sie wird über die Bewertung und Einschätzung der Sachlage hinaus von Rules of Engagement (ROE)[58] und Law of Armed Conflict (LOAC)[59] eingeschränkt und fällt somit nicht willkürlich aus.[60]

Relativ unumstritten ist die Einordnung der Tötung von gefährlichen Personen sowohl völkerrechtlich als auch völkergewohnheitsrechtlich. Es wird von der Rechtmä-

[51] *Müller*, in: Baade/Ehricht, S. 83.
[52] Der EGMR fordert im Fall McCann et al. V. UK (GC), ECtHR Appl. No. 18984/91, Judgment, 27.9.1995, § 150 die Unterziehung der Beurteilung einer äußerst sorgfältigen Überprüfung.
[53] McCann et al. V. UK (GC), ECtHR Appl. No. 18984/91, Judgment, 27.9.1995, Joint Dissenting Oinion of Judges Ryssdal et al., § 9.
[54] *Müller*, in: Baade/Ehricht, S. 83.
[55] *Müller*, in: Baade/Ehricht, S. 83.
[56] *Wuschka*, in: Baade/Ehricht, S. 57.
[57] *Wuschka*, in: Baade/Ehricht, S. 58.
[58] ROE sind für alle unterstellten Einheiten bindend, da diese zusätzlich die nationalen Einschränkungen definieren und einen Waffeneinsatz deutlich limitieren oder ausschließen können (*Werres*, in: Gillner/Stümke, S. 47).
[59] Nach LOAC müssen angemessene Vorsichtsmaßnahmen getroffen werden, damit die Offensive lediglich auf militärische Ziele gestartet wird; Zivilbevölkerung darf nicht absichtlich bekämpft werden; der absehbare Tod von Zivilisten sowie an zivilen Objekten darf nicht überproportional zu dem zu erwartenden konkreten unmittelbaren militärischen Vorteil stehen (*Werres*, in: Gillner/Stümke, S. 47).
[60] Ähnlich *Wuschka*, in: Baade/Ehricht, S. 58. Ein Verbot der willkürlichen Tötung ist rechtlich gem. Nuklearwaffen-Gutachten des IGH vorgegeben (*IGH*, Legality oft he Threat or Use of Nuclear Weapons, Judgement, ICJ Reports 1996, Rn. 25; *Wuschka*, in: Baade/Ehricht, S. 60).

ßigkeit des finalen Rettungsschusses[61] und der gezielten Tötung im humanitären Völkerrecht ausgegangen. Wie bereits in der Einführung unter I. dargestellt, erklärt Art. 2 Abs. 2 EMRK eine Tötung nicht als Verletzung des Rechts auf Leben, wenn sie durch eine Gewaltanwendung verursacht wird, die unbedingt erforderlich erscheint, um einen oder mehrere Menschen gegen rechtswidrige Gewalt zu verteidigen. Völkerrechtlich ist lediglich der Einsatz von verbotenen Waffen oder Kampfmethoden unzulässig und gem. Art. 85 Abs. 3 lit. a) i.V.m. Abs. 5 I. ZP-GK; Art. 8 Abs. 2 lit. b) sublit. i), lit. e) sublit. i) IStGH-Statut ist die Tötung von Zivilisten und sonstigen geschützten Personen völkerrechtswidrig, was wiederum ein Kriegsverbrechen darstellt. Völkerrechtlich zulässig ist die Tötung gefährlicher Personen auch dann, wenn von ihnen keine tödliche Gefahr ausgeht, da sie beispielsweise unbewaffnet sind[62] aber weitere Faktoren in die Abwägung miteinfließen, welche den Angriff rechtfertigen. Gemeint ist die Erwartung von Gewaltanwendung und der Mangel an Alternativen zur eigenen letalen Gewaltanwendung aufgrund mangelnder Zugriffsmöglichkeiten,[63] sowie bereits gescheiterte Verhandlungen oder ihre Sinnlosigkeit. Diese Alternativlosigkeit rechtfertigt den Einsatz der tödlichen Gewalt, welche in Anbetracht der Umstände unbedingt erforderlich erscheint.

Ferner wird das Recht auf Leben gem. Art. 15 Abs. 2 EMRK unter strengen Voraussetzungen der Rechtmäßigkeit von Kriegshandlungen ebenfalls eingeschränkt, denn rechtmäßige Gewaltakte gelten nicht als willkürlich. Die Rechtmäßigkeit eines Einsatzes der bewaffneten Drohne liegt vor, wenn die nationale Gesetzgebung des agierenden Staates hierfür eine ausreichende Rechtsgrundlage bietet.[64]

Nicht einheitlich ist die Bewertung der sog. gezielten Tötungen (targeted killings[65]) von Personen, die nicht unmittelbar Unversehrtheit oder Leben anderer Personen bedrohen, sich aber an der Planung oder Durchführung von Gewalt bei terroristischen Akten beteiligen.[66] Unter gezieltem Töten wird die vorsätzliche Anwendung tödlicher

[61] *Grabenwarter*, 146 (149).
[62] McCann v UK (GC), ECtHR Appl, No. 18984/91, Judgment, 27.09.1995, § 149.
[63] Dazu und zum Folgenden: *Müller*, in: Baade/Ehricht, S. 68.
[64] *Deutscher Bundestag*, BT-Drs. 18/6730 – Antwort: Mögliche Teilnahme eines Verbindungsoffiziers der Bundeswehr bei Auswahlprozessen für sogenannte gezielte Tötungen – Drucksache 18/6322 vom 17.11.2015, S. 1684.
[65] „gezieltes Töten" dieser Begriff wird in der englischsprachigen Literatur häufig mit Synonymbegriffen wie „extrajudicial executions", „strategic elimination" sowie „statesponsored assassination" bezeichnet, wobei die Verwendung des jeweiligen Begriffs von der dahinterstehenden Bewertung der konkreten Maßnahme und mithin von der Anerkennung der Legalität oder Unzulässigkeit des Angriffs beeinflusst wird. Das Etablieren des Begriffs targeted killing ist auf die Eliminierung mutmaßlicher Terroristen und Rebellen zurückzuführen (*Löffler*, S. 64 f. m.w.N.).
[66] *Müller*, in: Baade/Ehricht, S. 69; Zur Definiton vgl. Study on Targeted Killings, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, A/HRC/14/24/Add.6.28.5.2010, Rn. 7-9.

Gewalt durch einen Staat oder seine Bediensteten verstanden.[67] Dieser Prozess umfasst die Auswahl, Identifizierung, Festlegung der Vorrangigkeit der Zielperson, Anvisieren, die Wahl der anzuwenden Mittel und nicht zuletzt die Vorgehensweise unter Vorbehalt der Abwägung vom konkreten unmittelbaren militärischen Ziel.[68] Die US-Administration betrachtet solche Personen als Kombattanten und mithin als legale Angriffsziele,[69] hingegen stuft der israelische Supreme Court sie als „unlawful combatants" und mithin als Zivilisten ein.[70] Völkerrechtlich sind sie gem. Art. 51 Abs. 3 ZP-I der GK nicht mehr als Zivilisten geschützt, da sie an den Feindseligkeiten beteiligt sind. Sie gewinnen ihre Immunität gegen Angriffe, wenn sie an Feindseligkeiten nur einmalig oder sporadisch beteiligt sind und davon Abstand nehmen, dies gilt nicht für Personen mit Entscheidungsbefugnis, welche einer bewaffneten Gruppierung oder terroristischen Organisation angehören. Sie bleiben ein legales Angriffsziel auch zwischen den eigentlichen Kampfhandlungen.[71]

VI. Vor- und Nachteile des Drohneneinsatzes

Als besonderes Merkmal einer Drohne ist die Präzision ihres Einsatzes anzusehen. Anzumerken ist, dass die niedrige Fluggeschwindigkeit der Drohne Sicherheit im Hinblick auf die genaue Aufklärung der Ziele und fragwürdiger Objekte gewährleistet. Drohnen sind in der Lage, stundenlag über die Ziele zu fliegen und genaue Informationen ohne unmittelbaren Sichtkontakt des Piloten zu sammeln. Erst nach Beschaffung der notwendigen Informationen werden die entsprechenden Angriffe ausgelöst.[72]

Die Minimierung der Zeitspanne zwischen Aufklärung und Angriff - „Sensor-to-shooter-sycle" - ermöglichen es, Aufklärungs- und Angriffsaufträge gleichzeitig auszuführen, oder aber es können parallel sowohl Aufklärungs- als auch Angriffsdrohnen eingesetzt werden, um mit Hilfe ihrer langen und unbemerkten Verweildauer vor Ort im Moment der Entdeckung das erkannte Ziel unverzüglich anzugreifen.[73] Der technische Fortschritt erlaubt es, mit hochauflösender Sensorik mehrere potenzielle Ziele gleichzeitig zu überwachen. Durch das Zusammenlegen von Aufklärungs- und Kampf-

[67] Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, Rn. 13 aufrufbar auch unter:
http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf.
[68] *Rudolf/Schaller*, S. 8, abrufbar unter:
http://www.swp-berlin.org/fileadmin/contents/products/studien/2012_S01_rdf_slr.pdf
[69] H.H. Koh, Legal Adviser, U.S. Department of State, ASIL Annual Meeting, 25.03.2010, III.B. „Use of Force", US Supreme Court, Ex parte Quirin et al., 317 U.S. I (1942), zitiert nach *Müller*, in: Baade/Ehricht, S. 69.
[70] *Supreme Court of Israel*, Public Committee against Torture in Israel et al., HCJ 769/02, 11.12.2005, §§ 25 f., 28, zitiert nach *Müller*, in: Baade/Ehricht, S. 69.
[71] *Müller*, in: Baade/Ehricht, S. 70.
[72] *Wuschka*, in: Baade/Ehricht, S. 51 m.w.N.
[73] Dazu und zum Folgenden: *Löffler*, S. 68 f. m.w.N.

funktion wird zugleich die eigene defensive Kapazität erhöht und somit ist es möglich, unerwartete Angriffe ohne Zeitverzug und mit maximaler Präzision auszuführen.

Des Weiteren stellt das unbemannte Luftfahrzeug deutlich mehr räumliche Kapazität zur Verfügung, was zu Gunsten der Aufrüstung genutzt werden kann, um somit eine differenzierte und präzise Bekämpfung der Ziele zu gewährleisten. Denn infolge des Verzichts von menschlichem Piloten am Bord entfallen diverse Systeme für die Lebenserhaltung sowie Aufnahme- und Bewegungsraum der Besatzung.

Ferner ist hervorzuheben, dass die Effektivität der Zielbekämpfung ungeachtet der langen Einsatzdauer konstant bleibt, da das Bodenpersonal jederzeit abgelöst werden kann und somit keine Aufmerksamkeitslücken oder Ausdauerbeeinträchtigungen entstehen können. Mithin werden die Entscheidungen in Anbetracht der physischen Entfernung unter geringerem psychischen Druck und dadurch reflektierter getroffen.[74]

Durch Wegfall der physischen Belastung für den fliegenden Piloten können Routen absolviertet werden, die in der Form mit einem menschlichen Piloten unmöglich ausgeführt werden könnten.[75] Der Verzicht der menschlichen Komponente führt zum Wegfall der Lebensgefahr für den Piloten, somit besteht die Möglichkeit, Ziele in einem sehr geringen Abstand zu überfliegen. Die langsame Fluggeschwindigkeit der Drohnen führt zur Gewährleistung eines präziseren Angriffs, als dies im Falle eines traditionellen Kampfjets gegeben wäre.[76] Folglich verringert sich auch das Risiko eines unterscheidungslosen Angriffs.[77]

Die Kostenfrage sowohl in der Produktion als auch im Betrieb sowie in der Wartung (keine Notwendigkeit für Lebenserhaltungssysteme für die Besatzung, kein kostenverursachendes Personal) ist als weiteres Argument für die Befürwortung eines unbemannten Systems in Erwägung zu ziehen.[78]

Der Einsatz von unbemannten Systemen weist im Fall von gezielten Tötungen – targeted-killing Vorteile hinsichtlich der Sicherheit der eigenen Streitkräfte auf, denn durch ihren Einsatz wird die Präsenz von Soldaten entbehrlich.[79]

Insgesamt bergen einzelne aufgezählte Beispiele auch Nachteile, beispielsweise können Drohnen aufgrund langsamer Fluggeschwindigkeit ein leichtes Abschussziel von Abwehrmaßnahmen werden.[80]

[74] *Löffler*, S. 69 m.w.N.
[75] *Löffler*, S. 69 m.w.N.
[76] *Wuschka*, in: Baade/Ehricht, S. 51.
[77] *Wuschka*, in: Baade/Ehricht, S. 51.
[78] *Löffler*, S. 70 m.w.N.
[79] *Löffler*, S. 72.
[80] *Löffler*, S. 71 m.w.N.

Dem Aspekt der Präzision der Angriffsmaßnahme durch autonome unbemannte Luftsysteme ist entgegenzubringen, dass technische Verfahrensabläufe Angriffsfläche für informationelle Störungen bieten und sogar zu einer insgesamt schlechteren Informationslage führen können, was dem Übermaß der von ihnen generierten Daten geschuldet ist.[81]

Problematisch ist im Falle gezielter Tötungen die Hemmschwelle, die durch die räumliche Distanz schwindet, viele Kritiker weisen in diesem Zusammenhang auf die Gefahr der Play Station Mentalität hin. Denn durch Distanz nehmen Empathie und Mitleid ab, hingegen steigt die Angriffsbereitschaft. Durch eine signifikante Opferzahlreduzierung unter eigenen Streitkräften geht die abschreckende Wirkung der Gewaltanwendung verloren.[82] Bereits nachgewiesen ist die Gemeinsamkeit der Mechanismen zwischen realen Drohnen und Hard- und Software von Videospielen, welche von der amerikanischen Armee sowohl für Werbezwecke als auch für Ausbildungszwecke zur Einsatzvorbereitung der Piloten verwendet werden.[83] Die Gefahr, die die erwähnte Gemeinsamkeit birgt, ist der Verlust der Grenzziehung bzw. der Unterscheidung zwischen Realität und Spiel, sowie die Gefahr von automatischen Gewohnheitshandlungen in der Vorgehensweise, was der Tatsache der häufigen Angriffsausführung geschuldet ist. Gemeint ist die Simulation eines Kampfes bzw. Angriffs im Videospiel, dessen Spielerfolg von der zeitlich begrenzten quantitativen Vernichtung des Feindes abhängt ist. [84] Je höher die Vernichtungsrate ausfällt, desto höher ist der unmittelbare Erfolg. Diese Meinung kann zwar mit empirischen und wissenschaftlichen Studien nicht nachgewiesen werden, dennoch darf sie nicht unterschätzt werden. Insbesondere, wenn die Staaten zur Überprüfung neuer Mittel der Kriegführung im Sinne von Art. 36 ZP-I GK verpflichtet werden und das Leben mittelbar oder unmittelbar unter ihrer Hoheitsgewalt stehender Streitkräfte sowie Zivilpersonen gleichermaßen zu verantworten haben.[85]

Über die Hemmschwelle hinaus zieht die Maßnahme gezielter Tötungen den Nachteil von Kollateralschäden mit sich, unter den Opfern befinden sich nicht selten unbeteiligte Zivilisten. Schätzungen zufolge sind in den Jahren zwischen 2004 und 2016 durch US-Drohnen während der Maßnahmen von targeted killig in Pakistan zwischen 2282 und 3619 Menschen getötet worden, davon mindestens 255 bis 1769 Unbeteilig-

[81] *Stroh*, in: Frau, S. 162.
[82] Den veröffentlichten Angaben zufolge sind in Pakistan und zuvor in Kosovo durch die USA von 2004-2016 400 Luftangriffe durchgeführt worden, in den Jahren zuvor von 2008-2011 waren es 284 und in den Jahren 2004-2007 lediglich 10 Luftangriffe. Die Angaben deuten auf eine mehr als 25fache Steigerung der Drohneneinsätze. *Löffler*, S. 73 m.w.N.
[83] *Löffler*, S. 77 m.w.N.
[84] *Löffler*, S. 77 m.w.N.
[85] *Stroh*, in: Frau, S. 162.

te oder Zivilisten.[86] Die Präzision der Angriffe ist in Frage zu stellen, da die Zahl der durch unbemannte Flugsysteme getöteten Zivilisten eindeutig höher ist, als die durch den Einsatz von Jetpiloten bzw. durch herkömmlichen Waffeneinsatz getöteten Zivilisten.[87] Die Gründe für Kollateralschäden sind zwar grundsätzlich auf den physikalischen Effekten einer Waffe, wie ihre Druckwelle, Splitterwirkung, Feuer, Kraterbildung zurückzuführen, aber darüber hinaus traten in der Vergangenheit nicht selten auch unbeabsichtigte Fehler wie eine falsche Anwendung von Verfahren oder eine falsche Zielidentifizierung, auf. Nachgewiesen wurde, dass die meisten unbeabsichtigten Kollateralschäden durch die fehlerhafte Identifizierung des Ziels eingetreten sind,[88] was wiederum gegen die beschworene Präzisionseigenschaft der unbemannten Flugsysteme spricht und von einem Übermaß der Kollateralschäden zeugt.

In diesem Kontext ist auch auf die sogenannten „signature strikes“ einzugehen, denn bei Angriffen mittels unbemannten Flugsystemen werden Personen gezielt getötet, deren Identität nicht bekannt ist, sie fallen aufgrund ihrer Verhaltensmuster auf und werden somit mit einem bestimmten Profil assoziiert. Folglich werden wertgebundene Entscheidungen über Leben und Tod mit Algorithmen erzeugte Trefferwahrscheinlichkeiten ersetzt.[89]

Ferner kann aus dem heutigen Standpunkt keine Prognose für die zukünftige Preisstabilität gemacht werden und mithin kann nicht mit Sicherheit davon ausgegangen werden, dass die Kosten für unbemannte Systeme unterhalb der für herkömmliche Fluggeräte liegen werden. Zusammenfassend ist festzuhalten, dass der Einsatz von Drohnen zwar Nachteile aufweist, unter menschlicher Beteiligung wäre dieser Einsatz aber nicht als rechtswidrig zu betrachten. Geboten ist hier die Akzentsetzung auf die Art und Weise ihrer Verwendung und folglich die Beschränkung der vollautonomen Einsätze und somit keine Schaffung neuer Regelungen, sondern die sachgerechte Interpretation des bestehenden humanitären Völkerrechts.[90]

VII. Fazit

Wie die voranstehende Prüfung zeigt, kann eine mit dem humanitären Völkerrecht einhergehende Programmierung von vollautonomen unbemannten Systemen gegenwärtig technisch nicht umgesetzt werden. Das Scheitern der Programmierung des Verhältnismäßigkeitsgrundsatzes ist darauf zurückzuführen, dass Wertungen und somit

[86] *Löffler*, S. 79 m.w.N.
[87] *Löffler*, S. 79 m.w.N.
[88] *Werres*, in: Gillner/Stümke, S. 48.
[89] *Deutscher Bundestag*, BT-Drs. 18/6730 – Antwort: Mögliche Teilnahme eines Verbindungsoffiziers der Bundeswehr bei Auswahlprozessen für sogenannte gezielte Tötungen – Drucksache 18/6322 vom 17.11.2015, S. 1683.
[90] *Platek*, in: Frau, S. 56.

die Abwägungskriterien sich nicht abstrahieren lassen. Beim Einsatz von unbemannten Systemen soll den Staaten insbesondere in Anbetracht der Fehlerquoten bei signature strikes ein definierter und einschränkbarer Gestaltungsspielraum zur Wahrnehmung ihrer grundrechtlichen Schutzpflicht für Leib und Leben der Zivilbevölkerung zukommen. Mit großer Sorgfalt ist für jeden militärischen Einsatz die Aufklärung und Kontrolle, Vorbereitung und Durchführung vorzunehmen, damit es nicht zu Einbußen von grundlegenden Menschenrechten kommt. Es sei davor gewarnt, Zivilisten als Mittel zur Rettung anderer zu benutzen, zu verdinglichen und zugleich ihres Rechts zu berauben.[91] Notwendig ist die Berücksichtigung von moralisch ethischen und analytischen Fragen vor Ausübung letaler Gewalt wie targeted killing ohne dabei die Legitimität des Unterscheidungsgebots zwischen Kombattanten und Zivilisten zu leugnen. Denn nach der hier vertretenen Auffassung wird die militärische Legalität eines Einsatzes egal wie sie begründet wird[92] nicht bestritten, sondern davor gewarnt Drohnenangriffen pauschal die Völkerrechtskonformität zu unterstellen und somit Kollateralschäden in Kauf zu nehmen. Zum Ziel soll folglich die Prüfung der Frage erklärt werden, wann eine Ausnahme vom Tötungsverbot bei unbeteiligten Zivilpersonen gerechtfertigt werden kann, um folglich die signifikante Zunahme ziviler Opfer zu reduzieren. Dieses Ziel kann nur erreicht werden, wenn das Verhältnismäßigkeitsprinzip in Form des Verbots von überflüssigen Verletzungen oder unnötigen Leiden gewahrt wird. Die Rechtfertigung eines Einsatzes kann ausschließlich dann erfolgen, wenn der Angriff einen militärischen Vorteil im Verhältnis zu zivilen Verlusten ermitteln lässt, was wiederum mit enormen Schwierigkeiten verbunden ist. Die Frage, ob der Drohneneinsatz dem Völkerrecht entspricht, lässt sich nur in der Einzelfallprüfung beantworten. Auf diesem Wirkungsfeld gilt es, die Erkenntnisse aller Akteure zu sammeln und auszuwerten, insofern sich Individuen, Unternehmen und Staat im Zuge des Prozesses der Digitalisierung wechselseitig beeinflussen. Der technologische Fortschritt der Digitalisierung in der Luftfahrt ist zu nutzen, ohne dabei substantielle Eingriffe in die Privatheit vollziehen zu müssen. Aus den durch die Digitalisierung angetriebenen Veränderungen ergibt sich die Herausforderung, den Wandel durch Wissenszuwachs auch rechtlich und rechtschützend mitzugestalten.

[91] BVerfGE 115, 118 – 166, Rn. 124.

[92] Die militärischen Maßnahmen haben eine unterschiedliche Ausgangslage, entweder werden sie zum Schutz der Menschenrechte der Bevölkerung im Hoheitsgebiet eines anderen Staates vorgenommen oder aber als Unterstützung einer legitimen Regierung zur Stabilisierung des Friedens in einem geostrategisch wichtigen Raum oder als Abwehrmaßnahme vor Agieren nichtstaatlicher Akteure, was der Territorialstaat selbst nicht unterbinden kann oder will.

Literaturverzeichnis

Arnauld von, Andreas, Völkerrecht, Heidelberg u.a. 2012.

Baade, Horst/Ehricht, Sebastian (Hrsg.), Verhältnismäßigkeit im Völkerrecht, Tübingen 2016, S. 45-63; S. 65-83.

Becker, Peter, Neue Erkenntnisse zur Drohnenkriegführung. DVBI 2018, 619-628.

Borrmann, Robin, Autonome unbemannte bewaffnete Luftsysteme im Lichte des Rechts des internationalen bewaffneten Konflikts, Anforderungen an das Konstruktionsdesign und Einsatzbeschränkungen, Berlin 2014, zugl.: Frankfurt (Oder), Univ., Diss., 2013.

Frau, Robert (Hrsg.), Drohnen und das Recht. Völker- und verfassungsrechtliche Fragen automatisierter und autonomer Kriegsführung, Tübingen 2014, S. 1-17; S. 19-34; S. 35-57; S. 137-162.

Giesen, Stefan, Private Military Companies im Völkerrecht, Baden-Baden 2013, zugl.: Düsseldorf, Univ., Diss., 2012.

Gillner, Matthias/Stümke, Volker (Hrsg.), Kollateralopfer, Die Tötung von Unschuldigen als rechtliches und moralisches Problem, 1. Aufl., Münster 2014, S. 47-50.

Grabenwarter, Christoph, Europäische Menschenrechtskonvention, 5. Aufl., München 2012.

Leutheusser-Schnarrenberger, Sabine, Vom Recht auf Menschenwürde, 60 Jahre europäische Menschenrechtskonvention, Tübingen 2013, S. 183-194.

Löffler, Severin, Militärische und zivile Flugroboter, Ausgewählte strafrechtliche Problemfelder beim Einsatz von Kampf- und Überwachungsdrohnen, Baden-Baden 2018, zugl.: Würzburg, Univ., Diss., 2017.

Oeter, Stefan, Terrorismus und Menschenrechte, AVR 2002, 422-453.

Seiring, Olaf, Der Einsatz unbemannter Flugsysteme in nicht internationalen bewaffneten Konflikten, Berlin 2017, zugl.: Potsdam, Univ., Diss., 2015.

Städele, Julius Philipp, Völkerrechtliche Implikationen des Einsatzes bewaffneter Drohnen, Berlin 2014, zugl.: Bielefeld, Univ., Diss., 2014.

Tomuschat, Christian, Gezielte Tötungen (Targeted Killings), VN 2004, 136-140.

Märkte ohne Geld?

Der kartellrechtliche Marktbegriff im Licht der Digitalisierung

Maximilian Volmar

Max-Planck-Institut für ausländisches und internationales Privatrecht, Hamburg
volmar@mpipriv.de

Abstract

Jahrzentelang bestand ein Markt im Kartellrecht aus dem Tausch einer Leistung gegen eine Geldzahlung. Mit dem Aufkommen der Internetplattformen hat sich diese Ansicht geändert. Viele Internetplattformen sind für den Nutzer kostenlos und finanzieren sich durch Werbung. Diese Geschäftsmodelle sollten dem Kartellrecht nicht entzogen werden. Zuletzt ist mit der Einführung des § 18 Abs. 2a GWB deutlich geworden, dass ein Markt auch vorliegen kann, wenn kein Geld gezahlt wird. Das raubt dem Marktbegriff jedoch seine simple Definition und wirft die Frage auf, wann ein Markt vorliegt, in dem kein Geld gezahlt wird. Dieser Frage geht der vorliegende Beitrag nach.

I. Einleitung

„Price and competition are so intimately entwined that any discussion of theory must treat them as one."[1] Mit diesem Satz brachte Supreme Court Justice *Reed* die Besessenheit des Kartellrechts mit dem Preis auf den Punkt. Insbesondere die ökonomische Forschung konzentrierte sich auf die Effekte des Wettbewerbs auf den Preis, da diese Effekte leicht zu zählen waren. Mit der Machtergreifung der Internetplattformen ist in dieser Hinsicht ein Paradigmenwechsel eingetreten. Dienste im Internet sind häufig kostenlos – Google, Facebook, Wikipedia. Sollte deswegen dort kein Markt vorliegen? Nein, sagen mittlerweile die Mehrheit in Literatur, Rechtsprechung und auch der Gesetzgeber. Doch das wirft eine viel schwierigere Frage auf: Wie sieht ein Markt ohne Geld aus? Dieser Frage widmet sich der vorliegende Beitrag. Zu Beginn führt er in das Kartellrecht ein und zeigt auf, wo der Markt als Rechtsbegriff relevant wird (II.). Auf dieser Basis werden alte Ansichten nachgezeichnet und der jüngere Paradigmenwechsel beschrieben, der schließlich zu unserer zentralen Problemstellung führt (III.). Das

[1] *U.S. v. E. I. du Pont de Nemours & Co.,* 351 U.S. 377, 392 (1956).

Problem wurde auf unterschiedliche Weise zu lösen versucht. Die Ansichten dazu werden in IV. dargestellt und schlussendlich einer meiner Auffassung nach vorzugswürdigen Ansicht gegenübergestellt.

II. Wo kommt der Markt im Kartellrecht vor?

Der Marktbegriff taucht im Kartellrecht an drei Stellen auf, die den drei Säulen entsprechen, aus denen das Kartellrecht aufgebaut ist.

1. Missbrauchsaufsicht

Die erste Säule ist die Missbrauchsaufsicht. Gemäß § 19 GWB und Art. 102 AEUV ist es Unternehmen verboten, sich in einer bestimmten Weise zu verhalten, sofern sie eine marktbeherrschende Stellung einnehmen. Beispielsweise ist es diesen Unternehmen verboten, ungerechtfertigt anderen Unternehmen die Belieferung zu verweigern. In dem vielzitieren Urteil *United Brands* verbot z.B. der Europäische Gerichtshof („EuGH“) dem Unternehmen UBC, einem anderen Unternehmen die Belieferung mit UBCs bekannten Chiquita-Bananen zu verweigern.[2]

Wann liegt eine solche marktbeherrschende Stellung vor? Diese Frage beantwortet der Europäische Gerichtshof mit der knappen Definition, damit sei „die wirtschaftliche Machtstellung eines Unternehmens gemeint, die dieses in die Lage versetzt, die Aufrechterhaltung des wirksamen Wettbewerbs auf dem relevanten Markt zu verhindern, indem sie ihm die Möglichkeit verschafft, sich seinen Wettbewerbern, seinen Abnehmern und schließlich den Verbrauchern gegenüber […] unabhängig zu verhalten“.[3] § 18 Abs. 1 GWB zufolge ist ein Unternehmen marktbeherrschend, soweit es als Anbieter oder Nachfrager einer bestimmten Art von Waren oder gewerblichen Leistungen auf dem sachlichen und räumlich relevanten Markt (1.) ohne Wettbewerber ist, (2.) keinem wesentlichen Wettbewerb ausgesetzt ist oder (3.) eine im Verhältnis zu seinen Wettbewerbern überragende Marktstellung hat.

In der Praxis wird in zwei Schritten vorgegangen, um das Vorliegen einer marktbeherrschenden Stellung festzustellen: Zuerst wird der relevante Markt abgegrenzt. Nach dem sogenannten Bedarfsmarktkonzept gehören jene Produkte in denselben Markt, die aus Verbrauchersicht funktional austauschbar sind.[4] So entschied der EuGH in *United Brands*, dass es einen Markt für Bananen gebe, der ausschließlich Bananen umfasse, nicht jedoch anderes Frischobst wie Pfirsiche oder Trauben.[5] Die Banane unterscheide sich durch „ihr Ansehen, ihren Geschmack, ihre weiche Beschaffenheit, das Fehlen von Kernen, eine einfache Handhabung und ein gleichbleibendes Produktions-

[2] *EuGH*, Entscheidung vom 14.02.1978, Rs. 27/76, Slg. 1978, 207, Rn. 163 ff. – *United Brands.*
[3] *EuGH*, Entscheidung vom 14.02.1978, Rs. 27/76, Slg. 1978, 207, Rn. 63 – *United Brands.*
[4] *Rittner/Dreher/Kulka,* Wettbewerbs- und Kartellrecht, 427 f.
[5] *EuGH*, Entscheidung vom 14.02.1978, Rs. 27/76, Slg. 1978, 207, Rn. 34 – *United Brands.*

niveau“ von anderen Obstsorten.[6] Sobald ein solcher Markt abgegrenzt ist, wird er im zweiten Schritt näher untersucht. Es werden Marktanteile bestimmt und potentielle Wettbewerber identifiziert, die noch nicht im Markt tätig sind, es aber bald sein könnten. Hohe Marktanteile und geringer potentieller Wettbewerb sprechen dafür, dass ein Unternehmen seinen Markt beherrscht.[7] Hier stellt der Markt demnach einen zentralen Begriff des Tatbestands dar.

2. Fusionskontrolle

Auch in der Fusionskontrolle, der zweiten Säule des Kartellrechts, ist die marktbeherrschende Stellung wichtig. Gemäß § 36 Abs. 1 GWB bzw. Art. 2 Abs. 3 FKVO wird ein Zusammenschluss untersagt, wenn durch den Zusammenschluss eine marktbeherrschende Stellung entsteht oder verstärkt wird. Hier wird grundsätzlich die gleiche Definition und Methodik wie in der Missbrauchsaufsicht verwendet – mit bestimmten Besonderheiten. Eine Fusion kann auch untersagt werden, wenn allgemein nachgewiesen wird, dass der Wettbewerb durch sie beeinträchtigt wird.[8] Das Entstehen oder Verstärken einer marktbeherrschenden Stellung ist aber ein häufig genutztes Regelbeispiel für das Vorliegen einer Wettbewerbsbeeinträchtigung. Auch hier ist demnach der Marktbegriff von zentraler Bedeutung.

3. Kartellverbot

§ 1 GWB bzw. Art. 101 Abs. 1 AEUV verbieten es Unternehmen, Absprachen zu treffen, die den Wettbewerb beeinträchtigen. Ein Beispiel: Die von Produkten im Einzelhandel bekannte Formulierung „unverbindliche Preisempfehlung“ ist unverbindlich, weil sich die Einzelhändler daran nicht halten müssen. Würde der Hersteller seinen Händlern vorschreiben, welchen Preis sie von den Kunden zu verlangen haben, würde es den Händlern unmöglich gemacht, ihre Konkurrenten mit günstigeren Preisen zu unterbieten. Der Preiswettbewerb würde ausgeschaltet. Eine solche Preisbindung der zweiten Hand verstieße u.a. gegen das Kartellverbot in § 1 GWB bzw. Art. 101 Abs. 1 AEUV.[9] Wo ist hier der Markt relevant? Ausnahmsweise können solche Vereinbarungen pauschal freigestellt sein, weil der Gesetzgeber meint, dass sie ohnehin den Wettbewerb nicht beeinträchtigen. Das ist jedoch nur der Fall, wenn der Marktanteil des anbietenden Unternehmens 30% nicht überschreitet.[10] Damit dieser Marktanteil ermittelt werden kann, ist eine Marktabgrenzung nötig. Eine Vereinbarung kann demnach nur freigestellt werden, wenn auch ein Markt vorliegt.

---

[6] *EuGH*, Entscheidung vom 14.02.1978, Rs. 27/76, Slg. 1978, 207, Rn. 23 – *United Brands.*
[7] Vgl. *EuGH*, Entscheidung vom 14.02.1978, Rs. 27/76, Slg. 1978, 207, Rn. 97 ff. – *United Brands.*
[8] *Rittner/Dreher/Kulka,* Wettbewerbs- und Kartellrecht, 559.
[9] *Zimmer,* in: Immenga/Mestmäcker, Wettbewerbsrecht, Art. 101 Abs. 1 AEUV Rn. 275.
[10] Art. 3 Abs. 1 VO 330/2010 vom 20.4.2010, ABl. (EU) 2010 L 102/1 („Vertikal-GVO“).

Der Marktbegriff besetzt demnach in allen drei Säulen des Kartellrechts zentrale Positionen.

III. Das Problem: Unentgeltliche Märkte im Internet

Wie ist es zur Diskussion um den Marktbegriff gekommen? Die Problematik des Marktbegriffs ist durch das Aufkommen von Internetplattformen relevant geworden. Für viele Dienste im Internet zahlen die Nutzer kein Geld. Google ist kostenlos, Facebook ist kostenlos, Wikipedia ist kostenlos. Es soll eine „Kostenlos-Kultur" im Internet geben, da sich viele Angebote durch Werbung finanzieren.[11]

Jahrzehntelang war es in der deutschen Rspr. aber üblich, dass ein Markt nur dort vorliegt, wo auch Geld für ein Produkt oder eine Dienstleistung bezahlt wird. Im Fernsehen gab es lediglich einen Markt für Fernsehwerbung und für Pay-TV, nicht jedoch für Zuschauer des Free-TV.[12] Das gleiche galt für den Lesermarkt bei kostenlosen Anzeige-Zeitungen.[13] Noch im Jahr 2015 entschied das OLG Düsseldorf in einem in dieser Hinsicht skandalösen Urteil, dass bei der Hotelbuchungsplattform HRS ein Markt nur zwischen HRS und den Hotels vorliege, weil die Hotels eine Gebühr bezahlten, nicht jedoch zwischen HRS und den vielen Plattformnutzern, die kostenlos die Hotels verglichen.[14]

Diese Ansicht war bereits zum Zeitpunkt der Entscheidung etwas veraltet. Die Europäische Kommission hatte bereits Jahre zuvor Internetmärkte geprüft, ohne an der Unentgeltlichkeit dieser Märkte Anstoß zu finden.[15]

Endgültig bereitete aber der deutsche Gesetzgeber dem Spuk ein Ende. 2017 wurde § 18 Abs. 2a in das GWB eingefügt, der besagt, dass es dem Vorliegen eines Marktes nicht entgegensteht, dass die Leistung unentgeltlich erbracht wird. Damit war diese Diskussion beendet.

Ist sie das? Tatsächlich führt uns die Feststellung, dass es unentgeltliche Märkte gibt, zu der viel schwierigeren Frage, *wann* ein solcher Markt vorliegen soll: Wenn ein Markt nicht im Austausch von Geld gegen Waren besteht, worin besteht er dann? Gibt es einseitige Märkte, in denen der Internetnutzer schlicht die Leistung erhält und damit der Markt in seiner Gänze bereits vorliegt? Was muss gegeben sein, damit ein Markt vorliegt?

[11] *Körber,* NZKart 2016, 303 (305).
[12] *BKartA*, Entscheidung vom 19.01.2006, B6-103/05, 23 – *Springer/ProSiebenSat.1.*
[13] *BKartA*, Entscheidung vom 12.4.2000, B6-20/00, 5 – *akzent.*
[14] *OLG Düsseldorf*, Entscheidung vom 09.01.2015, VI Kart 1/14 (V), NZKart 2015, 148, Rn. 35 – *HRS.*
[15] *Kommission*, Entscheidung vom 03.10.2014, M.7217 – *Facebook/WhatsApp.*

IV. Was ist ein Markt?

Mit dieser fundamentalen Frage haben sich erstaunlich wenige Juristen befasst. In jüngerer Zeit haben lediglich *Podszun/Franz* einige grundlegende Überlegungen veröffentlicht.[16] Darüber hinaus lassen sich aus der Rspr. zu Internetplattformen einige potentielle Voraussetzungen ableiten. Sechs verschiedene Ansichten werden im Folgenden dargestellt. Gleichzeitig wird gezeigt, weshalb sie meiner Auffassung nach nicht überzeugen. Daher wird schlussendlich ein eigener Begriff vorgestellt.

1. Zwei Willenserklärungen

In der Entscheidung *VG Media/Google* deutete das Bundeskartellamt („BKartA") an, dass ein Markt nur vorliegen könne, wenn zwei übereinstimmende Willenserklärungen vorliegen, d.h. wenn die Voraussetzungen für einen Vertrag gemäß § 145 BGB gegeben sind. In dem Fall hatte die VG Media, eine Organisation, die verschiedene Verlage vertritt, Google auf Vergütung nach dem kürzlich neu geschaffenen Leistungsschutzrecht (§§ 87f ff. UrhG) in Anspruch genommen. Diese auch als „Lex Google" bekannten Normen sollten Online-Zeitungen die Möglichkeit geben, eine Vergütung dafür zu verlangen, dass Google ihre Zeitungsartikel in Kurzform als sogenannten Snippet in seiner Google-News-Sparte anzeigt. Leider reagierte Google auf dieses Begehren damit, den Verlagen zu drohen, ihre Snippets nicht mehr anzuzeigen. Dadurch würden die Verlage einen Großteil ihrer Besucher verlieren, die häufig Nachrichtenartikel über Google News finden. Daher sahen die Verlage sich dazu gezwungen, auf die Vergütung zu verzichten. In der Drohung Googles sahen sie aber den Missbrauch der marktbeherrschenden Stellung Googles gemäß § 19 GWB, Art. 102 AEUV.[17] Wo ist hier der Marktbegriff problematisch?

Das BKartA konnte die Marktabgrenzung im Ergebnis offen lassen. Es deutete jedoch an, dass eine Art Markt für die Vermittlung von Internetinhalten vorliegen könnte. In diesem Markt stehen sich die Inhalteanbieter – wie z.B. die Verlage – und die Suchmaschinen gegenüber. Suchmaschinen verschaffen den Inhalteanbietern die Möglichkeit, ihre Inhalte zu verbreiten. Problematisch fand das BKartA die Handlungen, welche die beiden Parteien vornahmen. Inhalteanbieter müssen nämlich nicht aktiv tätig werden, um bei einer Suchmaschine als Suchergebnis aufgeführt zu werden. Die Suchmaschine findet vielmehr selbständig die Ergebnisse durch das sogenannte Crawling. Dadurch werden grundsätzlich alle Inhalte im Internet angezeigt, *es sei denn*, der Inhalteanbieter hinterlegt in dem Code seiner Website die Datei „robots.txt", in der Anweisungen an den Crawler gespeichert sind – das sogenannte Robots Exclusion Protocol. In dieser Datei kann die Anweisung gespeichert werden, dass die Website bei

[16] *Podszun/Franz,* NZKart 2015, 121.
[17] *BKartA*, Entscheidung vom 08.09.2015, B6-126/14, WuW 2016, 38, Rn. 44 ff. – *VG Media/Google.*

Suchmaschinen nicht angezeigt werden darf. Die Website muss demnach nicht aktiv *handeln*, um mit der Suchmaschine zu interagieren. Bereits das Unterlassen führt zur „Interaktion". Ein solches Schweigen stellt aber nach der deutschen Rechtsgeschäftslehre im BGB gerade keine Willenserklärung dar. Daher bezweifelte das BKartA das Vorliegen eines Marktes.[18]

2. Kein Markt bei Allgemeingütern

In der gleichen Entscheidung deutete das BKartA an, dass auch aus einem weiteren Grund kein Markt vorliege. Das Crawling und das Auflisten der Webinhalte könnte nämlich lediglich die Nutzung von im Internet frei verfügbaren und nicht gehandelten Vorprodukten darstellen.[19] Google greife lediglich auf ein Allgemeingut zu, so wie jeder Logistikkonzern Luft als Allgemeingut nutzt, um die Motoren seiner Lastkraftwagen zu kühlen. Deswegen liegt noch kein „Markt für Luft" vor. Bei diesem einseitigen „Abgrasen" von Rohstoffen soll kein Markt vorliegen.

Tatsächlich haben Informationen im Internet Ähnlichkeiten mit Allgemeingütern. Ein Gericht in den USA entschied beispielsweise, dass das Unternehmen LinkedIn anderen Unternehmen den Zugang zu seiner Seite nicht blockieren dürfe, da es sich bei solchen Internetseiten um öffentliche Foren handele.[20] Andererseits ist es den Internetanbietern üblicherweise möglich, andere Private von der Nutzung auszuschließen. Durch das Robot Exclusion Protocol beispielsweise kann der Inhalteanbieter verhindern, dass seine Inhalte von Google genutzt werden. Allgemeingüter zeichnen sich aber gerade dadurch aus, dass niemand von der Nutzung ausgeschlossen werden kann.[21] Hinsichtlich des Internets scheint daher das Vorliegen eines Allgemeinguts wenig hilfreich zu sein, um den Marktbegriff abzugrenzen.

3. Andersartige Gegenleistungen

Eine weitere Ansicht vertritt, dass in einem Markt, wenn schon nicht mit Geld gezahlt wird, eine andere Form der Gegenleistung erbracht werden muss. Schließlich müssten auch Tauschbörsen Märkte darstellen. Im Internet werde außerdem hauptsächlich mit

[18] *BKartA*, Entscheidung vom 08.09.2015, B6-126/14, WuW 2016, 38, Rn. 135 ff. – *VG Media/Google; Brox*/*Walker,* Allgemeiner Teil des BGB, 46; *Petersen*/*Medicus,* Bürgerliches Recht, 25. Ähnlich *Graef,* EU Competition Law, Data Protection and Online Platforms, 86 f.

[19] *BKartA*, Entscheidung vom 08.09.2015, B6-126/14, WuW 2016, 38, Rn. 139 – *VG Media/Google.*

[20] *HiQ Labs v LinkedIn,* Case No. 17-cv-03301-EMC (N.D. Cal. Aug. 14, 2017).

[21] Vgl. zur Frage der Gemeingüter im Internet insg. *Lessig,* The Future of Ideas, 19 ff. *Lessig* vertritt die Ansicht, bei Internetinhalten handle es sich gerade um Allgemeingüter ("commons"), da viele Internetquellen wie der HTML-Code frei verfügbar sind. Dabei bezieht er sich aber nicht ausdrücklich auf das Crawling.

Daten oder mit Werbeaufmerksamkeit bezahlt. So finanzieren sich schließlich die Plattformen.[22]

Dieser Ansicht könnte man den Wortlaut des § 18 Abs. 2a GWB entgegenhalten. Hiernach gibt es auch *unentgeltliche* Märkte. Unentgeltlich heißt nämlich im deutschen Zivilrecht, z.B. bei der Schenkung in § 516 BGB, dass eine Pflicht zur Gegenleistung nicht besteht.[23] Unentgeltlich bedeutet demnach nicht nur, dass keine Geldzahlung entrichtet werden muss, sondern dass keine Gegenleistung irgendeiner Form geschuldet ist. Ein Entgelt ist kein „Entgeld", sondern jede Form der Gegenleistung. Nach dieser Lesart stellt § 18 Abs. 2a GWB klar, dass es auch Märkte geben soll, in denen eine Gegenleistung nicht erbracht wird. Der Monopolkommission zufolge erübrigt sich daher die Frage, ob eine andere Form der Gegenleistung, wie zum Beispiel Daten, vorliegen muss, um eine Marktbeziehung feststellen zu können.[24]

Tatsächlich meinte der Gesetzgeber damit etwas anderes. Ein Markt erfordert eine Austauschbeziehung, so die Regierungsbegründung zur 9. GWB-Novelle. „Demzufolge" liege ein Markt auch vor, wenn „kein Entgelt" – wohl im Sinne eines Entgelds – gezahlt werde. Es seien auch Angebote „ohne direkte monetäre Gegenleistung" erfasst.[25] Der Begriff der Unentgeltlichkeit in § 18 Abs. 2a GWB unterscheidet sich daher von dem des BGB. Unentgeltlich bedeutet lediglich, dass die Gegenleistung nicht in einer Geldzahlung bestehen muss – irgendeine Gegenleistung muss aber erbracht werden.

4. Wirtschaftliche Tätigkeit

Das BKartA, die Bundesregierung, die Europäische Kommission und die Literatur fordern für das Vorliegen eines Marktes, dass das Angebot Teil einer wirtschaftlichen Tätigkeit ist. Die Regierungsbegründung stellt fest, dass unentgeltliche Leistungen, die aus nicht-wirtschaftlichen Motiven angeboten werden, ohne Teil einer zumindest mittelbar oder längerfristig auf Erwerbszwecke angelegten Strategie zu sein, nicht Teil eines Marktes sind.[26] Das BKartA meint, eine unentgeltliche – gemeint ist: kostenlose – Leistung sei dann ein Marktgeschehen, wenn sie mit einer zahlungspflichtigen Nutzerseite verknüpft ist. Maßgeblich hierfür sei, dass zwischen den Plattformseiten ein enger Zusammenhang bestehe und dann ein einheitlicher Erwerbszweck anzunehmen sei.[27] Damit weist das BKartA auf die Mehrseitigkeit von Internetplattformen hin: Plattformen verbinden verschiedene Nutzergruppen, zum Beispiel verbinden Dating-

[22] Vgl. *BKartA*, Arbeitspapier: Marktmacht von Plattformen und Netzwerken, 2016, Az. B6-113/15, 41 f; *Louven,* NZKart 2018, 217 (219); *Podszun*/*Franz,* NZKart 2015, 121 (122).
[23] *Weidenkaff,* in: Palandt BGB, § 516 Rn. 8.
[24] *Monopolkommission*, Wettbewerb 2018 (XXII. Hauptgutachten) (3.7.2018), Rn. 617.
[25] Entwurf der Bundesregierung eines 9. Gesetzes zur Änderung des GWB, 28.09.2016, 51.
[26] Entwurf der Bundesregierung eines 9. Gesetzes zur Änderung des GWB, 28.09.2016, 51 f.
[27] *BKartA*, Entscheidung vom 22.10.2015, B6-57/15, Rn. 83 – *Online-Dating-Plattformen;* Arbeitspapier: Marktmacht von Plattformen und Netzwerken, 2016, Az. B6-113/15, 41.

Plattformen – der Gegenstand der BKartA-Entscheidung – Frauen und Männer. Einige Dating-Plattformen sind für Frauen kostenlos, für Männer aber kostenpflichtig. Da aber trotzdem insgesamt ein kommerzielles Geschäftsmodell vorliege, sei auch hinsichtlich der Frauen von einem Markt auszugehen. Viele andere Plattformen finanzieren sich auch durch Werbung und sind auf diesem Wege insgesamt wirtschaftlich tätig.

Die deutsche Literatur folgt dieser Ansicht größtenteils.[28] Auch die Europäische Kommission wies in *Google Shopping* darauf hin, dass die Unentgeltlichkeit der Suchmaschine kein Problem für die Marktabgrenzung sei, da trotzdem eine wirtschaftliche Tätigkeit vorliegen könne.[29]

Festzuhalten ist, dass eine stark vertretene Ansicht in Literatur und Praxis die wirtschaftliche Tätigkeit als Voraussetzung für das Vorliegen eines Marktes betrachtet. Der Gesetzgeber und das BKartA fordern möglicherweise mehrere Bedingungen kumulativ, damit ein Markt vorliegt. So ist es z.B. denkbar, dass nach Ansicht des BKartA eine nicht-monetäre Gegenleistung *und* eine wirtschaftliche Tätigkeit vorliegen müssen.

Diese Ansicht vermischt jedoch meiner Auffassung nach zwei Rechtsbegriffe. Jeder kartellrechtliche Tatbestand richtet sich nur an *Unternehmen* als Normadressaten. Ein Unternehmen ist der Rspr. des BGH und des EuGH zufolge jede Einheit, die eine Tätigkeit im geschäftlichen Verkehr ausübt.[30] Damit ist die wirtschaftliche Tätigkeit bereits ein Erfordernis des Unternehmensbegriffs. Gedanklich muss das Vorliegen eines Unternehmens vor dem Vorliegen eines Marktes geprüft werden, da zuerst ein Normadressat gegeben sein muss. Liegt ein Unternehmen vor, steht mithin bereits fest, dass eine wirtschaftliche Tätigkeit ausgeübt wird. Prüft man dies nochmals im Marktbegriff, kann daraus kein Erkenntnisgewinn erwachsen, da ohnehin alle Unternehmen in Märkten tätig sind. Anders gewendet gibt es keine Unternehmen, die nicht in Märkten tätig sind. Der Marktbegriff dieser Ansicht vermag es damit nicht, Fälle auszusortieren, die nicht schon vorher im Unternehmensbegriff aussortiert wurden. Das Merkmal der wirtschaftlichen Tätigkeit ist daher nicht in der Lage, den Marktbegriff einzugrenzen und mithin eine redundante Voraussetzung. Erforderlich ist ein anderes Abgrenzungsmerkmal.

[28] *Esser/Höft,* NZKart 2017, 259 (262); *Pohlmann/Wismann,* WuW 2017, 257; *Pohlmann/Wismann,* NZKart 2016, 555 (557). A.A. *Podszun/Franz,* NZKart 2015, 121.
[29] *Kommission*, Entscheidung vom 27.06.2017, AT.39740, Rn. 152, 321 – *Google Shopping.*
[30] *BGH*, Entscheidung vom 19.9.1974, KZR 14/73, NJW 1974, 2236; Entscheidung vom 6.11.1972, KRB 1/72, NJW 1973, 94, 95; Entscheidung vom 26.10.1961, KZR 1/61, NJW 1962, 196, 200; EuGH, Entscheidung vom 19.2.2002, C-309/99, NJW 2002, 877, Rn. 46 – *Wouters;* Entscheidung vom 23.4.1991, C-41/90, NJW 1991, 2891 – *Höfner und Elser/Macrotron.*

5. Offener Marktbegriff

Podszun/Franz vertreten einen „offenen Marktbegriff". Der Marktbegriff sei als „Organisationsform des Gütertauschs" zu interpretieren. Ein Markt entstehe durch Transaktionen und sei ein soziales Netzwerk von Akteuren, die innerhalb einer bestimmten Ordnung knappe Ressourcen neu verteilen. Zu dieser Ordnung zählen zum Beispiel rechtliche Regeln oder Transaktionskosten. Eine solche Definition gestalte den Marktbegriff „autonom, offen und dynamisch".[31] Das stimmt allerdings. Der Begriff ist derart offen, autonom und dynamisch, dass jede soziale Interaktion ohne jeglichen Bezug zum Kartellrecht darunter fällt. Was macht den Bezug zum Kartellrecht aus? Das GWB dient dem Schutz des Wettbewerbs.[32] Dieser Wettbewerbsbezug fehlt jedoch bei dem offenen Marktbegriff. Angenommen, ich lobe einen Gewinn aus, bei dem jeder teilnehmen kann. Den Gewinner wählt das Los. Hier findet zwischen den Teilnehmern kein Wettbewerb statt. Die Teilnehmer müssen sich in keiner Weise hervorheben oder bestimmte Eigenschaften oder Voraussetzungen erfüllen, um zu gewinnen. Der Ausgang ist schlicht vom Zufall abhängig. Trotzdem verteilen hier Akteure in einem sozialen Netzwerk eine knappe Ressource. Dem Kartellrecht ist jedoch nicht gedient, wenn diese Organisationsform des Gütertauschs einen Markt darstellt. Der Marktbegriff muss daher weiter präzisiert werden. Festzuhalten ist, dass nicht jede soziale Interaktion einen Markt darstellen kann. Es muss einen Wettbewerbsbezug geben, da sonst die Schutzfunktion des GWB nicht aktiviert ist.

Dagegen ließe sich einwenden, dass es auch Märkte gibt, die monopolisiert sind und auf denen ergo kein Wettbewerb herrscht. Fordert man einen Wettbewerbsbezug, würden gerade diese Märkte, in denen das Schutzbedürfnis besonders hoch ist und das GWB eingreifen müsste, vom Marktbegriff ausgenommen.

Bei dieser Kritik wird jedoch ein enger Begriff von Wettbewerb zugrunde gelegt. So gibt es auch potentiellen Wettbewerb. Auch wenn ein Anbieter bezüglich seines Produktes ein Monopol besitzt, steht er stets in der Gefahr, dass ein neuer Anbieter den Markt betritt, oder, falls auch das beispielsweise durch rechtliche Schranken unmöglich ist, durch ein innovatives neues Produkt den Markt verbreitert. Zum Beispiel steht ein staatliches Monopol auf Telefonnetzwerke seit der Zeit des Internets mit Internettelefonie in Konkurrenz. Der Wettbewerbsbezug kann damit auch auf Märkten bestehen, auf denen *prima facie* kein Wettbewerb herrscht. Monopolisierte Märkte werden also nicht vom Marktbegriff ausgeschlossen, wenn ein Wettbewerbsbezug erforderlich ist. Damit kommen wir der vorzugswürdigen Ansicht bereits näher.

[31] *Podszun/Franz,* NZKart 2015, 121 (126).
[32] *Immenga/Mestmäcker,* in: Immenga/Mestmäcker, Wettbewerbsrecht, Einl. Rn. 30; *Jung,* in: Grabitz/Hilf/Nettesheim, Recht der EU, Art. 102 AEUV Rn. 6.

6. Autonome Auswahlentscheidung im Wettbewerb

Einen weiteren Schritt in Richtung der nötigen Präzisierung geht der BGH. Er hat sich in einer Entscheidung zu unentgeltlichen Märkten geäußert. Es ging um die Fusion zweier Krankenhäuser und den Markt für stationäre Krankenhausbehandlung. Der BGH erwog, ob ein der Fusionskontrolle zugänglicher Markt deshalb fehle, weil gesetzlich versicherte Patienten gegenüber den Krankenhäusern nicht selbst zahlungspflichtig werden. Schuldner seien vielmehr die Krankenkassen. Zwischen den Patienten und den Krankenhäuser liege demnach ein unentgeltlicher Markt vor. Die Rechtsbeschwerde zog sogar die Parallele zu kostenlosen Fernsehzuschauer- und Lesermärkten (vgl. oben III.). Der BGH verwarf diese Argumentation jedoch. Ein Markt setze nicht voraus, dass es die Leistungsempfänger sind, die das Entgelt bezahlen. Es reiche aus, dass die Leistungsempfänger eine *autonome Auswahlentscheidung* unter mehreren konkurrierenden Leistungserbringern treffen, die wettbewerbliche Handlungsspielräume haben. Der Zweck der Fusionskontrolle, Verschlechterungen der Marktstruktur durch die Entstehung oder Verstärkung marktbeherrschender Stellungen zu verhindern, gebiete es, die §§ 35 ff. GWB auch auf derartige Märkte anzuwenden. Wettbewerbsstrukturen seien dort nicht weniger schutzwürdig als im Regelfall, in dem der Nachfrager, der eine Ware oder Dienstleistung auswählt, sie auch bezahlen muss.[33]

Hier tritt der Wettbewerbsbezug deutlich zutage. Einleitend bemerkte der BGH, dass der Fusionskontrolle Zusammenschlüsse nur insoweit unterliegen, als sie sich auf einen Markt beziehen, der Wettbewerbskräften unterworfen ist.[34] Mit diesem Gebot wäre der offene Marktbegriff bereits nicht vereinbar. Der BGH fordert mithin einen Wettbewerbsbezug.

Nicht nachvollziehbar ist jedoch das Erfordernis der autonomen Auswahlentscheidung. Weshalb sollten nicht-autonome Entscheidungen nicht dem Marktbegriff unterfallen? Eine nicht autonom gefällte, d.h. eine fremdbestimmte Entscheidung liegt beispielsweise bei Zwang vor. Doch gerade wenn ein Anbieter seinen Markt beherrscht und der Abnehmer auf ein Produkt angewiesen ist, kann die Entscheidung für das Produkt unter Zwang zustande gekommen und damit nicht-autonom sein. Gerade ein Marktbeherrscher ist in der Lage, seinen Abnehmern Konditionen abzuzwingen, denen sie bei effektivem Wettbewerb nicht zustimmen würden. Soll gerade die Situation des größten Schutzbedürfnisses aus dem Marktbegriff herausfallen?

Außerdem setzt die Möglichkeit einer *Auswahl*entscheidung implizit voraus, dass der Verbraucher tatsächlich die Wahl zwischen mehreren Anbietern hat. Wenn es je-

[33] *BGH*, Entscheidung vom 16.1.2008, KVR 26/07, NJW-RR 2008, 1426, Rn. 22–33 – *Kreiskrankenhaus Bad Neustadt.*
[34] *BGH*, Entscheidung vom 16.1.2008, KVR 26/07, NJW-RR 2008, 1426, Rn. 22 – *Kreiskrankenhaus Bad Neustadt.*

doch nur einen Anbieter – einen Monopolisten – gibt, ist eine solche Auswahlentscheidung nicht möglich. Demnach würde in der Monopolsituation kein Markt vorliegen. Erneut besteht in dieser Lage das größte Schutzbedürfnis und trotzdem soll ein Markt nicht gegeben sein. Das Erfordernis der autonomen Auswahlentscheidung ist aus diesen Gründen abzulehnen. Dem BGH ist daher in dieser Hinsicht nicht zu folgen.

7. Teleologischer Marktbegriff

a) Gründe für einen teleologischen Marktbegriff

Vorzugswürdig ist stattdessen ein rein teleologischer Marktbegriff, wie ihn der BGH ohne die Einschränkung der autonomen Auswahlentscheidung vertreten würde. Der teleologische Bezug besteht dabei in dem Sinn und Zweck des GWB, dem Schutz des Wettbewerbs als freien Prozess.[35] Dort, wo Wettbewerb stattfindet, muss ein Markt vorliegen.

Wie eingangs gezeigt, wird ohne Markt das Kartellrecht seiner Anwendbarkeit beraubt. Der Markt stellt in allen drei Säulen des Kartellrechts einen derart zentralen Begriff dar, dass er darüber entscheidet, ob die kartellrechtlichen Normen anwendbar sind. Ohne Markt kann keine marktbeherrschende Stellung vorliegen und somit auch kein Normadressat vorliegen, der von einem Verbot betroffen sein könnte. Ohne Markt sind die Abnehmer und Lieferanten vor dem Missbrauch der Marktmacht dominanter Unternehmen nicht geschützt. Genauso kann eine Fusion nur daraufhin geprüft werden, ob durch sie eine marktbeherrschende Stellung entsteht, wenn ein Markt vorliegt. Liegt kein Markt vor, ist es für Unternehmen einfacher, sich „unter dem Radar" der Fusionskontrolle zusammenzuschließen. Das Vorliegen eines Marktes und die Schutzmöglichkeiten des Kartellrechts gehen damit Hand in Hand. Daher muss ein Markt dort vorliegen, wo die Schutzfunktion des Kartellrechts – der Wettbewerbsschutz – aktiviert ist.

Klarzustellen ist, dass es um den Schutz des Wettbewerbs geht. Es muss auf den Zweck des Gesetzes ankommen, in dem der Marktbegriff vorkommt. *Podszun/Franz* hingegen stellen darauf ab, der Markt sei ein normativer Zweckbegriff, weil die Marktabgrenzung der Feststellung von Marktmacht diene.[36] Dies ist jedoch der Zweck der Marktabgrenzung *als Instrument* und nicht der Zweck des Gesetzes, der im Rahmen der teleologischen Auslegung von Rechtsbegriffen maßgeblich ist. Die teleologische Auslegung muss sich daher auf den Wettbewerbsschutz beziehen, nicht auf den methodischen Zweck der Marktabgrenzung.

---

[35] *Immenga/Mestmäcker,* in: Immenga/Mestmäcker, Wettbewerbsrecht, Einl. Rn. 30; *Jung,* in: Grabitz/Hilf/Nettesheim, Recht der EU, Art. 102 AEUV Rn. 6.

[36] *Podszun/Franz,* NZKart 2015, 121 (125). Sie verweisen auf *Möschel,* Recht der Wettbewerbsbeschränkungen, 65.

b) Anwendungsbeispiel

Die Wettbewerbsrelevanz wird regelmäßig bei Behinderungsmissbräuchen vorliegen, da dort die Wettbewerbsbeeinträchtigung eine Voraussetzung ist.[37] Auch bei Ausbeutungsmissbräuchen kann jedoch ein Wettbewerbsbezug vorliegen. Ein Beispiel liefert das aktuelle Facebook-Verfahren des BKartA. Das Amt stört sich an der Praxis von Facebook, Daten nicht nur von registrierten Nutzern auf seiner eigenen Website zu sammeln, sondern auch von nicht registrierten Internetnutzern auf Websites Dritter. Sofern eine Drittwebsite einen Facebook-Login oder –Share-Button besitzt, sammelt Facebook Daten. Das betrifft in erster Linie die Nutzer. Eventuell verstößt diese Praxis gegen das Datenschutzrecht und die Datensubjekte werden ausgebeutet.[38] Wettbewerbsrelevanz entfaltet der Fall aber in zweierlei Hinsicht:

Erstens sind die Nutzer eventuell dazu gezwungen, ihre Daten abzugeben, da Facebook keine Konkurrenten hat. Für die Teilhabe am sozialen Leben im Internet könnte eine Anmeldung bei Facebook unabdingbar sein. Nur aufgrund dieser Zwangslage würden die Nutzer der Datenausbeutung zustimmen. Zweitens verschafft sich Facebook durch sein Verhalten einen Wettbewerbsvorteil. Daten sind das „Öl der Internetwirtschaft“ und sind wertvoll, um Werbung auf einen Nutzer hin zu individualisieren. Indem Facebook mehr Daten erhebt, baut es seine starke Marktposition aus. Der Wettbewerbsschutz ist damit gleich in zweierlei Hinsicht tangiert. Somit sollte zwischen den Nutzern und Facebook ein Markt vorliegen, obwohl hier kein Geld gezahlt wird.

c) Vergleich mit dem Meinungsspektrum

Vergleichen wir diese Ansicht einmal mit den bisher genannten:

(1) Zwei Willenserklärungen

Durch das Erfordernis der zwei Willenserklärungen wird der eigentlich ökonomische Marktbegriff verrechtlicht. Es werden wettbewerblich relevante Zusammenhänge aus dem Anwendungsbereich des Kartellrechts ausgeschlossen. Das beste Beispiel dafür ist das VG-Media-Verfahren des BKartA, in dem es diese Ansicht andeutete. Google konnte mit dem erzwungenen Verzicht auf die den Verlagen gesetzlich zustehende Vergütung seine Marktmacht demonstrieren. Weshalb sollte den Betroffenen der Schutz des Kartellrechts in dieser Lage entzogen werden? Die Vermittlung von Internetinhalten ist ein wettbewerblich höchst relevantes Geschäft, in dem Google eine Gatekeeper-Funktion innehat. Derart viele Personen nutzen Google, dass Inhalteanbieter darauf angewiesen sind, bei Google angezeigt zu werden. Die Inhalteanbieter konkurrieren

[37] Behinderungsmissbräuche sind horizontale Verhaltensweisen, die sich gegen Wettbewerber richten. Ausbeutungsmissbräuche richten sich hingegen in vertikaler Hinsicht gegen Lieferanten oder Abnehmer.
[38] *BKartA*, Hintergrundpapier zum Facebook-Verfahren (19.12.2017).

unter sich scharf um die Verbreitung ihrer Inhalte. Daher sollte in dieser Hinsicht auch ein Markt vorliegen, der es ermöglicht, dass die Normen des Kartellrechts für fairen Wettbewerb sorgen.

(2) Andersartige Gegenleistungen

Ebenso ist nicht ersichtlich, weshalb der Marktbegriff dadurch limitiert werden sollte, dass eine bestimmte Art der Gegenleistung erfolgt. Zwei Beispiele sprechen dagegen:

Die Gesetzesbegründung zur 9. GWB-Novelle liefert das beste Beispiel. Auch um die Vergabe privater Stipendien können die Bewerber in Wettbewerb stehen.[39] Auch hier würde eine wettbewerbsbeschränkende Absprache zwischen Bewerber und Stipendiengeber dem Sinn und Zweck des GWB zuwiderlaufen. Auch hier ist nicht ersichtlich, weshalb ein Bewerber nicht des Schutzes vor marktmächtigen Anbietern bedarf. Daher sollten auch Beziehungen, in denen lediglich eine Leistung ohne Gegenleistung erbracht wird, ein Marktgeschehen darstellen können.

Zweitens kann Wettbewerb auch vorliegen, bevor ein marktreifes Produkt zur Verfügung steht. In forschungsintensiven Branchen läuft häufig der Wettbewerb fast zur Gänze vor der Marktreife ab. Mehrere Pharmaunternehmen konkurrieren beispielsweise um das erstmalige Produzieren eines bestimmten Medikaments. Sobald ein Unternehmen ein Patent dafür besitzt, endet der Wettbewerb.[40] Erst dann jedoch wird das Produkt verkauft und eine Gegenleistung dafür erbracht. Davor passiert aber der schutzbedürftige Wettbewerbsprozess. Daher sind in Deutschland, der EU und den USA vorgelagerte Innovations- oder Entwicklungsmärkte kartellrechtlich anerkannt.[41]

Eine Gegenleistung sollte mithin nicht erforderlich sein, damit ein Markt vorliegt.

(3) Wirtschaftliche Tätigkeit

Eine teleologische Auslegung bedeutet dabei nicht, dass nun auch nicht-wirtschaftliche und rein soziale Beziehungen dem Kartellrecht unterfielen. Weiterhin sind Normadressaten der GWB-Normen allein Unternehmen, die nur vorliegen, wenn die Einheit im geschäftlichen Verkehr tätig ist. Dass das GWB nur wirtschaftliche Zusammenhänge erfasst, ist bereits durch den Unternehmensbegriff sichergestellt. Dadurch beschränkt sich das Kartellrecht weiter auf wirtschaftlichen Wettbewerb. Andere Arten des Wettbewerbs – wie beispielsweise sportlicher Wettkampf – bleiben außen vor, soweit sie nicht auch eine wirtschaftliche Komponente haben.

---

[39] Entwurf der Bundesregierung eines 9. Gesetzes zur Änderung des GWB, 28.09.2016, 51 f.
[40] Zumindest endet der Wettbewerb bis zur möglichen Produktion von Generika.
[41] *BKartA*, Innovationen - Herausforderungen für die Kartellrechtspraxis. Nr. 2 der Schriftenreihe "Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft" (November 2017), 31 ff; *DOJ, FTC*, Antitrust Guidelines for the Licensing of Intellectual Property (12.1.2017), 11 ff; *Kommission*, Entscheidung vom 27.3.2017, M.7932, Rn. 342 ff. – *Dow/DuPont.*

V. Fazit

Der Marktbegriff ist die Stellschraube vieler kartellrechtlicher Tatbestände und hat gleichwohl nur geringe Aufmerksamkeit im Schrifttum erfahren. Die Frage nach dem Vorliegen des Marktes stellt sich praktisch nur, wenn kein Entgelt auf dem Markt gezahlt wird, was besonders häufig im Internet der Fall ist. Doch wie sieht ein Markt ohne Geld aus? Der vorliegende Beitrag hat das Meinungsbild zusammengefasst und bewertet.

Eine Ansicht vertritt, dass der Marktbegriff zwei Willenserklärungen erfordert. Die zweite Ansicht fordert eine Gegenleistung in nicht-monetärer Form. Gleichzeitig soll ein Markt jedenfalls dann nicht vorliegen, wenn die „Leistung“ in einem Allgemeingut besteht. Viertens wurde gefordert, ein Markt liege vor, sobald eine wirtschaftliche Tätigkeit vorliegt. Ein fünfter – offener – Marktbegriff will weitreichend alle sozialen Beziehungen mit dem Ziel der Neuverteilung einer knappen Ressource erfassen. Der BGH schließlich sieht einen Markt dort, wo Wettbewerb vorliegt und der Abnehmer eine autonome Auswahlentscheidung trifft.

Vorzugswürdig ist ein rein teleologischer Marktbegriff. Ein Markt liegt vor, wo Wettbewerb stattfindet. Diese Rückbesinnung auf den Sinn und Zweck des GWB – den Schutz des freien Wettbewerbs – ist offen genug, alle schutzbedürftigen Beziehungen zu erfassen und ufert dabei nicht aus.

Literaturverzeichnis

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der EU, München 2016.

Brox, Hans/Walker, Wolf-Dietrich, Allgemeiner Teil des BGB, 39. Aufl., München 2015.

Immenga, Ulrich/Mestmäcker, Ernst-Joachim (Hrsg.), Wettbewerbsrecht (Bd. 2 GWB), 5. Aufl., München 2014.

Esser, Michael/Höft, Jan Christoph, Fusions- und Missbrauchskontrolle 4.0, Die 9. GWB-Novelle als Antwort auf die Herausforderungen der Digitalisierung?, NZKart 2017, 259-263.

Graef, Inge, EU Competition Law, Data Protection and Online Platforms, Data as Essential Facility, Alphen Aan Den Rijn 2016.

Körber, Torsten, "Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, "Datenmacht" und Kartellrecht - Teil 1, NZKart 2016, 303-309.

Lessig, Lawrence, The Future of Ideas, The Fate of the Commons in a Connected World, New York 2001.

Louven, Sebastian, Datenmacht und Zugang zu Daten, NZKart 2018, 217-222.

Möschel, Wernhard, Recht der Wettbewerbsbeschränkungen, Köln 1983.

Petersen, Jens/Medicus, Dieter, Bürgerliches Recht, 26. Aufl., München 2017.

Podszun, Rupprecht/Franz, Benjamin, Was ist ein Markt? - Unentgeltliche Leistungsbeziehungen im Kartellrecht, NZKart 2015, 121-127.

Pohlmann, Petra/Wismann, Thomas, Digitalisierung und Kartellrecht, Der Regierungsentwurf zur 9. GWB-Novelle, NZKart 2016, 555-563.

Pohlmann, Petra/Wismann, Thomas, Markt, Marktmacht und Transaktionswertschwelle in der 9. GWB-Novelle, WuW 2017, 257-261.

Rittner, Fritz/Dreher, Meinrad/Kulka, Michael, Wettbewerbs- und Kartellrecht, Eine systematische Darstellung des deutschen und europäischen Rechts, JURATHEK Studium, 8., neu bearbeitete Auflage 2009, Heidelberg, Neckar 2014.

Palandt, Otto, Bürgerliches Gesetzbuch. 76. Aufl., München 2017.

Immenga, Ulrich; Mestmäcker, Ernst-Joachim, Wettbewerbsrecht (Bd. 1 EU), Kommentar zum Europäischen Kartellrecht. 5. Aufl., München 2012.

5AMLD, cryptocurrency regulation, member states' adoption and practicability

Sven Werner

Goethe-Universität Frankfurt am Main
svenhwerner@gmail.com

Abstract

5AMLD sets out to establish a coherent approach to regulate cryptocurrencies and its entities on a European level. The EU recognizes the future threats this new technology poses for Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) policy. This paper analyzes the background of this Directive as well as the goals of 5AMLD. The second step is to look at member states who have already come forward with 5AMLD compliant laws in the recent months. The third step is to analyze the practicability of the 5AMLD measures. 5AMLD falls short of providing coherent and well-thought-out amendments.

I. Introduction

Virtual Currencies (VCs) are rising in popularity and the pseudo-anonymity for both the sender and the recipient is one of the reasons why. The public ledger, Blockchain, records every VC transaction, keeps the users pseudo-anonymous though.[1] Because of that, some see it already as "the new frontier in terrorism fundraising".[2]

"If you care about cryptocurrency gaining adoption, you can't close your eyes to illicit actors trying to use it. If they're going to use it, we need to look at this as a society and a government to understand what it means.[3]", said Yaya Fanusie, U.S. national security advisor of the Foundation for *Defense of Democracies* think-tank and former Central Intelligence Agency analyst.[4]

[1] *Zenko,* „Bitcoin for Bombs".
[2] *Fanusie,* „The new frontier in terror fundraising: Bitcoin".
[3] *del Castillo,* „Think tanks links rising Bitcoin price to terrorist use".
[4] *Fanusie*, "Our team" (2018).

In his published report he observed that Islamic extremist groups show an increased willingness to raise funds with Bitcoin although the crowdfunding efforts through cryptocurrencies have not necessarily been very successful in the recent past.[5]

The European Union introduced 5AMLD as a reaction to the terror attacks in Europe since 2015 and the Panama Papers revelations. The revision of the EU anti-money laundering law is part of the commission's "Action Plan for strengthening the fight against terrorist financing".[6] This paper shall observe the background of the 5AMLD directive, member states' adoption and the practicability of the rules of 5AMLD that concern cryptocurrencies and its entities.

II. Background

1. Current Situation

"In the EU, virtual currency is not currently regulated and cannot be regarded as being subject to the (current) PSD or the EMD. As the phenomenon is still relatively new and also moving into different areas, it would be too early to try making new, tailor-made legislation." was stated by the European Central Bank in its 2015 report.[7]

In the 4AMLD directive cryptocurrencies were not addressed specifically, some regulations might have affected VCs but this is part of a scholarly debate.[8]

The 4AMLD framework and its list of obliged entities did not include VCP, which is an insurmountable hurdle to attach the framework to the crypto scheme.[9]

An achievable hurdle for VC in the scope of AMLD4 is the connecting factor of "property" and "funds", both are defined as assets of any kind and legal documents or instruments in any form including digital and electronic, hinting an interest of 4AMLD into the cryptocurrency market. In the scope of 4AMLD, VC can be seen as incorporeal immovable assets.[10]

The Commission recognized these shortcomings and initiated legislative action to bring Virtual Currency Exchange Providers (VCEP) and Custodian Wallet Providers (CWP) under the scope of the future AMLD.[11] The directive recognizes that under the current law, obligations for traditional financial institutions don't apply to VCP and CWP. The obligations that have not applied to these entities is the duty to identify sus-

[5] *del Castillo*, "Think tanks links rising Bitcoin price to terrorist use".
[6] *Hartmann*, "The European Parliament adopts the 5th Anti-Money Laundering Directive".
[7] *European Central Bank*, "Virtual currency schemes – A Further Analysis 24", p. 24.
[8] *Houben/Snyers/Tax3 committee*, "Cryptocurrencies and blockchain", p.62.
[9] *Houben/Snyers/Tax3 committee*, "Cryptocurrencies and blockchain", p.62.
[10] *Houben/Snyers/Tax3 committee*, "Cryptocurrencies and blockchain", p.62; *Vandezande*, "Virtual currencies: a legal framework", p. 295.
[11] *Vandezande*, "Virtual currencies: a legal framework", p. 286-209.

picious activities, which are aimed at combating money laundering and terrorism financing.[12]

Another goal of the directive is to tackle the anonymity of VC, which it sees as enabling criminal behaviour. 5AMLD aims to extend the AML/CTF laws to VC and the intermediaries dealing with them.

5AMLD is a revision of 4AMLD from 2015 in order to include the risks and challenges of VCs. February 2nd, 2016 the commission published their announcement. May 26th, 2016 the European Parliament passed their resolution regarding VC, the first draft of the bill was published by the Commission on July 5 2016. The first reading in the European Parliament took place on April 19, 2018 (574 votes to 13 votes, with 60 abstentions). The Council adopted the directive on May 14, 2018 and was finally published on June 19 in the *Official Journal of the European Union*.[13] The directive will enter into force on July 9, EU member states will have until January 10, 2020 to implement the directive into national law.[14]

2. Levels of Regulation so far

There are different levels of how to approach the regulation of VC. Level 0 would be ignoring it, Level 1 would be monitoring it, this is the case when a state authority has issued a statement that the institution, which is responsible for supervising financial institutions, is aware of the existence of VC and will deal with them in the future. This approach is currently the strategy of Croatia and Ireland. Level 2 would be a recommendation from a state authority for an approach to VC, but which warns against the risks, for example the report of the European Banking Authority in 2014. At Level 2 the authorities warn the public about the volatility of VCs and the misuse for criminal activities, in the European Union Denmark, France, Greece, Hungary and Portugal followed this approach.

The Level 3 approach means that a state authority has issued guidance to govern the method of using VC, the approach can only affect certain aspects of the use of VC. The Czech Republic is a European country that sees VC transactions as subjects to restrictions similar to those applicable to financial transactions in terms of AML laws. The 5AMLD directive can be seen as a Level 3 measure. Enforcing Level 3 effectively poses challenges or even impossible hurdles, because of the nature of VC. The higher levels

[12] Directive (EU) 2018/843, 30 May 2018, Recital 1-9.
[13] Official Journal of the European Union, Volume 61, 19 June 2018.
[14] *Read/Gräslund*, "EU-Regulierung von Bitcoin und anderen virtuellen Währungen: erste Schritte", Volume 7 2018, p. 506-507; *EU*, „Briefing-Revision of 4AMLD".

of regulation in Lansky's model are not enforced or considered by a European country.[15]

III. Definitions and Goals of 5AMLD

1. Definitions

An important step of the 5AMLD is to define what a cryptocurrency and cryptocurrency exchanges are.

a) Cryptocurrencies

Cryptocurrencies are named as VCs and it is pointed out that these should not be confused with electronic money:[16]

"Virtual currencies" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically".

This definition is broad enough to cover as many tokens and potential uses as possible. This definition is very surprising, as usually the legislator falls short of providing a thorough definition of money itself. By providing this definition of VC, It is clear what the legislator understands as VC in terms of Anti-Money Laundering (AML) law. The ECB was not content with the first proposed definition of VC as it might have been too open and positive towards a money innovation, from a central bank point of view.

b) Wallet Providers and Exchanges

In order to regulate cryptocurrency wallets and its entities, what falls under these expression has to be defined first: "Custodian wallet provider" means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies." „Cryptocurrency exchanges, referred to in 5AMLD as virtual currency exchange providers (VCP), are providers engaged in exchange services between virtual currencies and fiat currencies".[17] Remarkably this definition, maybe intentionally, does not include exchange services between virtual currencies itself.

2. Goals regarding AML and CTF

It recognizes that the VCEPs as well as the CWPs are under no EU obligation to identify suspicious activity, it concludes that terrorist groups are able to transfer money into

[15] *Lanksy*, „Possible state approaches to cryptocurrencies", p. 22-24.
[16] Directive (EU) 2018/843, 30 May 2018, Recital 10.
[17] Directive (EU) 2018/843, 30 May 2018, Amendment 1c `g.

the Union financial system or within virtual currency networks, by benefitting from the anonymous or pseudo-anonymous technical nature of the Blockchain technology.

The goal as 5AMLD clearly states, is not only AML it also tries to counter the financing of terrorism (CFT). The solution is to monitor the use of VC: „competent authorities should be able, through obliged entities, to monitor the use of virtual currencies"[18].

The EU does not cherish the illusion that it could somehow solve the anonymity problem of VC as transactions are possible without CWP or VCP. National Financial Intelligence Units (FIU) should be able to obtain information allowing them to associate VC addresses to the identity of the owner. Self-declaration to designated authorities on a voluntary basis should be further assessed, according to 5AMLD.[19]

The new regulation forces the cryptocurrency entities to be registered with authorities and they have to abide to common banking due diligence rules such as customer verification and the EU's Anti-Money Laundering Directive. The transactions will have to be monitored by these entities to identify suspicious activities. Such activities will have to be reported to the FIU and these entities will have to be registered with the AML authority of their jurisdiction. New customers of VCEPs and CWPs will have to undergo KYC procedures (Know Your Customer).[20]

As of June 2018, 68 percent of the exchanges allow its users to trade crypto and fiat without conducting formal identification procedures, meaning that only 32 percent of exchanges are ready for 5AMLD.[21]

Appropriate proposals regarding user registration will be included in the Commission's next supranational risk assessment, which is due by 26 June 2019, for example maintaining a central database registering users' identities and wallet addresses accessible to FIUs and self-declaration forms for the use of VC users.[22]

The (pseudo) anonymity of users of fiat currency to VC exchanges and of CWPs may have come to an end as 5AMLD forces theses users with the above explained regulations out of the anonymity.[23]

[18] Directive (EU) 2018/843, 30 May 2018, Recital 8.
[19] Directive (EU) 2018/843, 30 May 2018, Recital 9.
[20] *Hartmann*, 5AMLD; *Conheady*, „INSIGHT: EU Regulation of Cryptocurrency Exchanges: 5AMLD Ups the Ante".
[21] *Covesting*, „P.A.ID Strategies Reports Crypto Exchanges Face KYC Problems".
[22] *Houben/Snyers/Tax3 committee*, "Cryptocurrencies and blockchain", p. 64.
[23] *Houben/Snyers/Tax3 committee*, "Cryptocurrencies and blockchain", p. 64.

IV. Member States' Adoption

1. Estonia

In November 2016 the Estonian Supreme Court decided that extra regulation should be applied to Bitcoin trading, including the requirement to meet the customers in person. Additionally the traders are required to keep the Ids of all customers and report those who would trade more than 1,000 Euros per month. This ruling applied to all Blockchain tokens and assets.[24] This ruling already implements some AML regulations, Estonia is the first country which transposed the directive's provisions. It now requires VCP and CWP to get authorized provide transparent services.[25]

Estonia requires these entities to either obtain a wallet license[26] or an exchange license[27], the first licensed CWP and VCP licenses were obtained by Coin Metro in May 2018. The licenses provide a framework for establishing robust checks for AML, CTF and KYC.[28] Estonia was the first country to have implemented the directive into national law, this might give Estonia a competitive advantage in the European crypto-industry.[29]

2. United Kingdom

The view of UK regulators has been to treat cryptocurrencies as a commodity, rather than a currency or a security. The UK Financial Conduct Authority (FCA) recently confirmed that virtual commodities like Bitcoin are not currently regulated by the national financial regulatory authorities and that it will be up to the Parliament to decide on any changes to these will be up to the Parliament to decide on any changes to these rules.[30]

In April 2018 FCA announced that companies offering cryptocurrency derivatives would require authorization from the FCA. Such companies would need to comply with applicable FCA rules and EU regulations. The FCA might consider cryptocurrency derivatives as financial instruments under the EU's Markets Especially cryptocurrency options, futures and contracts for differences will require FCA authorization.[31] Ex-

[24] *Hansen*, „Digital currencies: international actions and regulations – Estonia", *Riigikohus*, Lahendid.
[25] *Veberaitė, Aistė*, „What impact will the 5th Anti Money Laundering Directive have on the crypto world?".
[26] *MTR*, „Wallet Licence".
[27] *MTR*, „Exchange Licence".
[28] *BitcoinNews*, „Estonia Grants Licenses for Wallet and Exchange Services to Coin Metro".
[29] *BitcoinNews*, „Estonia Grants Licenses for Wallet and Exchange Services to Coin Metro".
[30] *Holman/Stettner*, „Anti-Money laundering regulation of cryptocurrency: US and global approaches", p. 30; *Binham*, „UK finance watchdog head says no plans to push bitcoin regulation".
[31] *FCA*, „Cryptocurrency derivatives - FCA statement on the requirement for firms offering cryptocurrency derivatives to be authorised".

changes do not have to register under AML regulations so far.[32] Concrete announcements or implementations regarding CWP or VCP have not been made and, depending on the form of Brexit, might not be necessary in accordance with 5AMLD.

3. Italy

With the implementation of 4AMLD Italy already incorporated definitions for cryptocurrency consistent with the FATF-definition. Cryptocurrency-to-fiat conversion services, exchanges in that sense, were classified as „non-financial intermediaries, which are regulated under the AML Decree.[33] The Italian AML obligations already include KYC, record keeping and communications to the authorities as well as suspicious transaction reporting.[34] Cryptocurrency service providers have to register in a special section of the Italian registry of currency exchange professionals, furthermore they have to communicate with the Ministry of Economy and Finance about exchange activities carried out within the Italian territory.[35]

4. Germany

Cryptocurrencies that have the characteristics of a cash instrument are considered as a financial instrument under the German Banking Act (KWG) by the German Federal Financial Supervisory Authority (BaFin). The use of VC as payment for goods and services does not trigger the AML regulation, and these users do not have to seek authorisation under applicable German banking laws.[36] Commercial dealings with cryptocurrencies can trigger an authorisation requirement, if the platform involves buying and selling cryptocurrencies in order to carry out principal broking services, or when operating as a multilateral trading facility.[37]

VCPs are generally subject to authorisation. These companies have to obtain a licence as a credit institution or financial services institution under applicable German banking laws they are treated as an „obliged entity"[38] under the German Money Laundering Act (GWG), which transposes the AML requirements of 4AMLD.[39]

The BaFin decides if a VC is a security or not on a case-by-case basis, the rights associated with the respective VC. This is in so far important as a characterization as a se-

[32] *Hansen*, „Digital currencies: international actions and regulations – United Kingdom".
[33] *Holman/Stettner*, p. 29.
[34] *Holman/Stettner*, p. 29.
[35] *Holman/Stettner*, p. 29.
[36] *Holman/Stettner*, p. 30; *Bafin*, „Virtual Currency (VC)".
[37] *Holman/Stettner*, p. 30.
[38] *Holman/Stettner*, p. 30.
[39] *Holman/Stettner*, p. 30.

curity might trigger conduct and prospectus requirements, which go beyond licencing requirements and a resulting AML regulation.[40]

V. Practicability

1. Definition of Money and the Legal Framework

VCs do not fit into the legal framework for fiat currencies and payment transactions of most national states. As it is neither characterized as money nor a foreign currency nor a commodity in the respective legal frameworks, it poses a challenge for the legislator and the fiscal authorities.[41]

The decision of the US Securities and Exchange Commission in March 2018 to characterize VC as "digital assets" received great attention. By recognizing VC as "digital assets", the SEC sees its definition of securities fulfilled and therefore VC fall in its jurisdiction.[42]

The 5AMLD provides contradicting or at least confusing definitions of money. Fiat currency is defined as: "Coins and banknotes that are designated as legal tender and electronic money of a country, accepted as a medium of exchange in the issuing country".[43]

The definition tries to draw the line between VC and fiat currencies, Euro can be seen as virtual though and is a fiat money too. Virtual refers to the appearance, whereas fiat is referring to the process of creation. Commodity money instead of VC might be a more understandable and correct expression for the counterpart of fiat money.[44] PSD2 refers to fiat money as "legally established currency"[45] as a counterpart to VC, this might have been a solution for 5AMLD, too.[46]

The initiator of the *Prepaid Verband Deutschland (PVD)* sees the definition as mainly containing negative statements what does not constitute a VC. The positive statements that remain apply to 90 percent of our money (except cash) and therefore the definition cannot be seen as a success. The definition is not inviting, as it makes the abyss between central bank currencies and VC more apparent: no secured link, no guarantee and no legal status.

[40] *Holman/Stettner*, p. 30; *BaFin*, „Initial Coin Offerings: BaFin veröffentlicht Hinweisschreiben zur Einordnung als Finanzinstrumente".
[41] *Holman/Stettner*, p. 30; *BaFin*, „Initial Coin Offerings: BaFin veröffentlicht Hinweisschreiben zur Einordnung als Finanzinstrumente".
[42] *SEC*, „SEC Statement on Potentially Unlawful Online Platforms for Trading Digital Assets".
[43] Directive (EU) 2018/843, Recital 8.
[44] *Godschalk*, „Virtual currencies deciphered (1) – the new legal definition and AMLD5".
[45] *Godschalk*, „Virtual currencies deciphered (1) – the new legal definition and AMLD5"..
[46] *Godschalk*, „Virtual currencies deciphered (1) – the new legal definition and AMLD5"..

As the definition is very broad it will apply to any instrument with a monetary function without a material structure that has not fallen under the regulatory provisions of the AMLD so far.

The ECON committee recently defined money as: "Money is primarily the generally accepted means of exchange and constitutes an economic category sui generis".[47] 5AMLD contradicts this statements as it states that "*the objective of this Directive is to cover all the potential uses of virtual currencies." A VC like any other currency or money should be accepted as a means of exchange according to the ECON definition. The 5AMLD approach therfore is confusing, as there seems to be a consensus among economists and lawyers that if a value is not a means of exchange and payment, it does not constitute money.*[48]

The 5AMLD does not give any specifics to what a "means of exchanges" constitutes. A good basis for the definition of medium of exchange regarding VC is the following: "cryptocurrencies should be able to be used to facilitate the sale, purchase of trade of goods between parties and represent a standard of value that is accepted between the parties"[49]

Iota, which instead of Blockchain technology uses the tangle system, and is not designed as means of exchange[50] as well as *Neo* to name the more prominent examples, clearly do not fall under the 5AMLD definition. This might cause some problems, as coins, one might refer to as a cryptocurrency, do not fall under the definition of VC and are therefore not regulated.[51] These cryptocurrencies will fall under the definition once they are exchanged in order to commit a money laundering or terrorist financing offence though.[52] This inaccuracy intentional or not shows the uncertainty of 5AMLD.

Another problem arises when considering that some cryptocurrencies are not used as means of exchange but instead as investment instruments. One can argue that these cryptocurrencies are not the scope of 5AMLD any more then, another point of view might be that 5AMLD does not specify if means of exchange should be the predominant function of a VC. A fiat currency can simultaneously be used as an investment instrument and a means of exchange.[53]

[47] *ECON-Committee*, „Virtual Currencies-Monetary Dialogue July 2018".
[48] *Godschalk*, „Virtual currencies deciphered (1) – the new legal definition and AMLD5".
[49] *Investopedia*, „Medium of exchange"; Houben*/Snyders /Tax3 committee*, p. 74.
[50] *Hertig*, „IOTA: The $3.7 Billion Crypto Developers Love to Hate".
[51] *Houben/Snyders/Tax3 committee*, p. 74.
[52] *Houben/Snyders/Tax3 committee*, p. 74.
[53] *Houben/Snyders/Tax3 committee*, p. 74.

As with *Iota* and *Neo*, this case shows the inaccuracy of the definition and thoughtlessness to abstain from providing more detailed regulation, which would prevent different interpretations and possible legal disputes.

2. Challenges of VC

VC pose various challenges for regulation and AML and CFT measures, a short overview of the challenges from a legal perspective follows:

a) Pseudonyms of VC Users

Electronic payment transactions offer not many loopholes for anonymity in comparison to a VC. Although the public keys of the sender and recipient of a VC transaction are, as the name already suggests, public but discovering the real identity behind the participants of the transaction requires effort. These efforts can be counteracted by using measures such as Mixers/Tumblers and the *TOR Browser*, just to name a few examples, which complicate the identity stripping.[54]

b) Decentralized

As there are no central servers with decentralized VCs, no central entity exists that can be subject of prosecution or sequestrations.[55]

c) Global Reach of Cryptocurrencies

Independent from any governmental entity and accessible from anywhere with the internet, transactions cross national borders and therefore user data and transaction data is spread throughout various jurisdictions. National authorities can therefore not or not completely access this data.[56]

Anonymity or pseudo-anonymity for VC users will be a thing of the past, if they hold their VC via a CWP or submit and receive transactions via a VCP. The due diligence requirements, that CWP and VCEP entities have to abide to, prohibits anonymity.[57]

But, although the 5AMLD introduces profound rules and regulations, loopholes or workarounds still exist. Any other wallet but a CWP like a hardware or software wallet is not addressed by 5AMLD as is trading via P2P network or any alternative to a VCP. The user can still operate anonymously.[58]

[54] *Read/Gräslund*, p. 507; *Khatwani*, „6 ways to guarantee anonymity when making a bitcoin transaction".
[55] *Read/Gräslund*, p. 507.
[56] *Read/Gräslund*, p. 507.
[57] *Houben/Snyers/Tax3 committee*, p. 79.
[58] *Keatinge/Carlisle/Keen/Terr committee*, „Virtual currencies and terrorist financing: assessing the risks and evaluating responses", p. 38-42; *Houben/Snyers/Tax3 committee*, p. 80.

3. Blind Spots

a) CBDC

Central Bank Digital Currencies (CBDC) are not covered by the 5AMLD definition, restrictively interprets as it states "Cryptocurrencies are a special case of digital/virtual currencies". The inconsistency of 5AMLD regarding CBDC becomes apparent with the fact that it only regulates payments with state cash in excess of 10.000 Euros, but excludes payments with state CBDC, hence this creates a loophole for platforms on which legally anonymous money can be traded without any legal AML obligations, Venezuelan *Petro* or the idea of the Swedish *E-Krona* comes to mind.[59]

b) Decentralized VCEPs

Atomic swap or decentralized cryptocurrency exchanges do not fall under the 5AMLD definition of VCEP. Additionally cryptocurrency exchanges that only accept payments in other cryptocurrencies will not fall under the scope of 5AMLD either, leaving another loophole open.[60] Criminals will prefer to operate via such exchanges and can easily avoid the exchanges that fall under the scope of 5AMLD, the inaccuracy of 5AMLD in other areas is for a change not the case here, one might say the definition is too narrow.[61]

c) Hardware and software CWPs

Hardware wallet providers and software wallet providers do not fall under the scope of the 5AMLD's definition of CWP, leaving yet another loophole. The providers do not safeguard their customers' funds, instead they just supply them with the necessary tools and software to store their cryptocurrency themselves and to trade between themselves without an intermediary.[62]

d) Conclusion

The blind spots 5AMLD leaves for money laundering and terrorist financing are vast and point to a lack of attention for details and the resulting risks. There is no incentive for potential terrorists to stick to the entities that fall under the scope of 5AMLD.[63]

A trend to self-regulation is not completely far-fetched, as many entities want to build up a reputation in order to attract non-fringe groups, but there will always be a market for customers who will use the blind spots. These customers must not be necessarily terrorists, as the cryptocurrency world has its roots and an underlying libertar-

[59] *Keatinge/Carlisle/Keen/Terr committee*, „Virtual currencies and terrorist financing: assessing the risks and evaluating responses", p. 38-42; *Houben/Snyers/Tax3 committee*, p. 80; *Riksbank*, „e-Krona".
[60] *Houben/Snyers/Tax3 committee*, p. 77.
[61] *Houben/Snyers/Tax3 committee*, p. 77.
[62] *Houben/Snyers/Tax3 committee*, p. 78.
[63] *Houben/Snyers/Tax3 committee*, p. 79.

ian philosophy, the majority of these customers might just be concerned with their privacy and the utopian idea of stateless money.

4. Criticism

Proposing legal rules that are obviously ineffective, the European Commission and the institutions that took part in drafting 5AMLD are falling short of regulating and surveilling the most relevant players, the miners, and the system itself, the Blockchain. Miners can be seen as the bankers in the crypto-world and the Blockchain as the tool that makes all this possible. It seems naïve to regulate only users or the intermediaries such as VCP or CWP, whose role is secondary in the crypto-world.[64]

Paying voluntarily taxes or voluntarily registering him- or herself is unrealistic, even for a normal user. If the users don't use a CWP or VCEP, it is nearly impossible to enforce the law. The authorities would have to see every individual who owns a computer on which a Blockchain node exists or can be downloaded as a suspect for violating the rule of self-declaring.[65]

VI. Outlook

The EU is not unaware of shortcomings in terms of surveilling and regulating VC of 5AMLD.

National financial intelligence units should be able to associate VC public keys with the identity of the user, as is proposed today for the future. Furthermore the possibility of self-declaring of users to the designated authorities on a voluntary basis will be further assessed.

Nothing concrete can be expected from Brussels anytime soon. The Commission is required to include solutions to these shortcomings in its next supranational risk assessment, due by June 26, 2019.

These proposals should include self-declaration forms for the VC users and empowerments to set-up and maintain a central database registering users' identities and wallet addresses, which can be accessed by financial intelligence units.[66]

This is the opposite direction one might expect from the EU as these proposals seem to point towards a voluntary registration and not a mandatory one.

These proposals don't seem thought through as the users that are targeted by the AML and CFT measures won't be the ones who submit their data and identity voluntar-

[64] *Gikay*, „Regulating decentralized cryptocurrencies under payment services law: lessons from the European Union law", p. 28.
[65] *Gikay*, „Regulating decentralized cryptocurrencies under payment services law: lessons from the European Union law", p. 28.
[66] *Houben/Snyers/Tax3 committee*, p. 80.

ily. Counteracting money laundering, terrorist financing and tax evasion will not be very efficient if the EU wants to go down this road.

A more intrusive approach including mandatory registration and a pre-set date when it applies might be the more successful solution.[67]

5AMLD also falls short of taking the variety of VC into account. Pseudo-anonymous VC and their users such as Bitcoin can, with great effort, be unveiled by the authorities, whereas anonymous VC such as *Dash* and *Monero* are almost impossible to surveil, these VC might be the solutions for the user group that is targeted by 5AMLD.

User's compliance is key to the mandatory registration, adequate sanctioning might be an adequate tool the authorities should consider. VC entities could decide not to accept fully anonymous VC such as *Dash* and *Monero* and therefore possibly build up a reputation of being 100 percent compliant with the state's vision and subsequently building a trustworthy image from the eyes of the normal user. A ban of the use of VC will certainly be the wrong way, and it does not look like this is a viable option for the EU and the respective authorities.

VII. Conclusion

No meaningful step has been taken by or in the European Union. VCs will challenge the traditional legal approaches and rules, due to the decentralized and pseudo-anonymous nature of the Blockchain technology and VC as their products. A tighter regulatory framework will be inevitably put in place if it will and can discourage the use of VCs that threaten the state and the fulfillment of its duties. A payment system whose strength is undoubtedly the lack of regulation and surveillance will struggle with the first meaningful and serious regulations, when enforced, but these regulations seem not to become reality anytime soon in the European Union.

The IMF pointed out: "the changing nature of the technology requires that regulation be flexible and can be adapted to evolving circumstances" This might be a pragmatic and the right approach to the topic of cryptocurrencies, yet 5AMLD falls short of providing a framework that would cover all the difficulties and loopholes of the cryptocurrency world.

[67] *Houben/Snyers/Tax3 committee*, p. 80.

Bibliography

Houben, Robby/ Snyers, Alexander/Tax3-committee, "Cryptocurrencies and blockchain" (2018), p.64, http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf, accessed 14.08.2018.

BaFin, „Virtual Currency (VC)" (2016) <https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html, accessed 14.08.2018.

BaFin, „Initial Coin Offerings: BaFin veröffentlicht Hinweisschreiben zur Einordnung als Finanzinstrumente", https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1803_ICOs.html, accessed 14.08.2018.

Binham, Caroline, „UK finance watchdog head says no plans to push bitcoin regulation" (2017), https://www.ft.com/content/33c8f65b-2448-33fd-a627-46235ef91111, accessed 14.08.2018.

Bitcoin News, „Estonia Grants Licenses for Wallet and Exchange Services to Coin Metro" (2018), https://cryptonewsmonitor.com/2018/06/07/estonia-grants-licenses-for-wallet-and-exchange-services-to-coin-metro/, accessed 14.08.2018.

Conheady, Gina, INSIGHT: EU Regulation of Cryptocurrency Exchanges: 5AMLD Ups the Ante" (2018), https://www.bna.com/insight-eu-regulation-n73014476945/, accessed 14.08.2018.

Covesting, „P.A.ID Strategies Reports Crypto Exchanges Face KYC Problems" (2018), https://ci.covesting.io/news/cryptocurrency-news/pid-strategies-reports-crypto-exchanges-face-kyc-p, accessed 14.08.2018.

del Castillo, Michael, „Think tanks links rising Bitcoin price to terrorist use" (2017), https://www.coindesk.com/u-s-think-tank-finds-rising-bitcoin-price-linked-terrorist-interest/, accessed 14.08.2018.

ECON-Committee, „Virtual Currencies-Monetary Dialogue July 2018" (2018), http://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf, accessed 14.08.2018.

European Central Bank, Virtual currency schemes – A Further Analysis 24 "(2015), https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, accessed 14.08.2018.

Fanusie,Yaya,„The new frontier in terror fundraising: Bitcoin“ (2018), https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin, accessed 14.08.2018.

Fanusie, Yaya, “Our team” (2018), http://www.defenddemocracy.org/about-fdd/team-overview/yaya-j-fanusie/, accessed 14.08.2018.

FCA, Cryptocurrency derivatives - FCA statement on the requirement for firms offering cryptocurrency derivatives to be authorised“ (2018), https://www.fca.org.uk/news/statements/cryptocurrency-derivatives, accessed 14.08.2018.

Gikay, Asress, „Regulating decentralized cryptocurrencies under payment services law: lessons from the European Union law“ (2018), https://scholarlycommons.law.case.edu/jolti/vol9/iss1/1/, accessed 14.08.2018.

Godschalk, Hugo, „Virtual currencies deciphered (1) – the new legal definition and AMLD5“ (2018) <https://paytechlaw.com/en/new-legal-definition-amld5/, accessed 14.08.2018.

Hansen, Dax, „Digital currencies: international actions and regulations – Estonia“ (2018), https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#Estonia, accessed 14.08.2018.

Hansen, Dax, „Digital currencies: international actions and regulations – United Kingdom“ (2018), https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#United%20Kingdom, accessed 14.08.2018.

Hartmann, Ulrich, “The European Parliament adopts the 5th Anti-Money Laundering Directive” (2018), https://blogs.pwc.de/compliance-fs/aktuelles/the-european-parliament-adopts-the-5th-anti-money-laundering-directive/712/, accessed 14.08.2018.

Hertig, Alyssa, „IOTA: The $3.7 Billion Crypto Developers Love to Hate“, https://www.coindesk.com/iota-2-7-billion-cryptocurrency-developers-love-hate/, accessed 14.08.2018.

Holman, Daniel/ Stettner, Barbara, „Anti-Money laundering regulation of cryptocurrency: US and global approaches“ (2018), p. 30, http://www.allenovery.com/publications/en-gb/Documents/AML18_AllenOvery.pdf, accessed 14.08.2018.

Investopedia, „Medium of exchange“ (2018), https://www.investopedia.com/terms/m/mediumofexchange.asp, accessed 14.08.2018.

Keatinge, Tom/ Carlisle, David/ Keen, Florence/ Terr committee,„Virtual currencies and terrorist financing: assessing the risks and evaluating responses“ (2018), http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf, accessed 14.08.2018.

Lansky, Jan, „Possible state approaches to cryptocurrencies“ (2018), http://www.si-journal.org/index.php/JSI/article/viewFile/335/325, accessed 14.08.2018.

Lexology, „Virtual currencies & the 4th Anti-money Laundering Directive: ECB Opinion on the Commission’s proposals“ (2018), https://www.lexology.com/ library/detail.aspx?g=96ecd2c9-3e81-4613-ba08-c036a4e7768d, accessed 14.08.2018.

MTR, „Wallet Licence“ (2018), https://mtr.mkm.ee/taotluse_tulemus/483668?backurl=%40juriidiline_isik_show%3Fid%3D227953, accessed 14.08.2018.

MTR, „Exchange Licence“ (2018), https://mtr.mkm.ee/taotluse_tulemus/483684?backurl=%40juriidiline_isik_show%3Fid%3D227953, accessed 14.08.2018.

Riigikohus Lahendid (2018), https://www.riigikohus.ee/lahendid?asjaNr=3-3-1-75-15, accessed 14.08.2018.

Riksbank „e-Krona“ (2018.), https://www.riksbank.se/en-gb/financialstability-/payments/e-krona/, accessed 14.08.2018.

SEC, „SEC Statement on Potentially Unlawful Online Platforms for Trading Digital Assets“ (2018), https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading, accessed 14.08.2018.

Vandezande, Niels, “Virtual currencies: a legal framework”.

Veberaitė, Aistė A, „What impact will the 5th Anti Money Laundering Directive have on the crypto world?“ (2018), https://hackernoon.com/what-impact-will-the-5th-anti-money-laundering-directive-have-on-the-crypto-world-f903f6d08900, accessed 14.08.2018.

Zenko,Micah,„Bitcoin for Bombs“ (2017), https://www.cfr.org/blog/bitcoin-bombs, accessed 14.08.2018.

„Fair-Use“ im Zeitalter digitaler Kulturtechniken

Die Wandlung des Urheberrechts in Bezug auf referenzielle Kunst

Stefan Papastefanou, LL.B

Center for Transnational IP, Media and Technology Law and Policy, Bucerius Law School, Hamburg
Stefan.papastefanou@law-school.de

Abstract

Im Zeitalter digitaler Kunst, insbesondere moderner Medienplattformen und die dadurch hervorgerufene Bedeutung und neuartige Ausformung von referenzieller Kunst, stellt sich die Frage, wie sich das deutsche Urheberrecht im Spannungsverhältnis von Eigentumsrechten und Kunstfreiheit positioniert. Vermehrt werden im Rahmen der Diskussion politische und medienwissenschaftliche Argumente bezüglich einzelner Kunstformen eingebracht. Gerade die Bedeutung und rechtliche Bewertung von „Fanfiction“ mit Bezug auf populäre Werke ist Gegenstand von aktueller Diskussion.[1]

Der Aufsatz bietet zunächst eine Übersicht über die Bedeutung und die Auswirkung des BVerfG-Urteil „Sampling“[2] und inwiefern sich die vermeintliche „digitale Leitlinie“ zur Anerkennung digitaler Kulturtechniken in jüngster Zeit entwickelt hat. Auf dieser Grundlage wird erörtert, wie sich das grundlegende Verfassungsprinzip der praktischen Konkordanz im Rahmen der Digitalisierung der Leistungsschutzrechte verändert und welche Form es schließlich angenommen hat. Außerdem wird dargestellt, welche rechtsdogmatischen Schwierigkeiten sich bei einer medienwissenschaftlichen Betrachtungsweise bieten, indem eine Übersicht über die Vielfalt der Formen von referenzieller Kunst gegeben wird. Schließlich beschreibt der Beitrag in einer mikrofunktionellen rechtsvergleichenden Analyse die Vor- und Nachteile einer Übertragung der „Fair-Use Doctrine“ aus dem US-amerikanischen Recht des geistigen Eigentums. Abschließend stellt der Beitrag dar, welche Auslegung von Grenzen und Schranken zugunsten der Nutzer im digitalen Zeitalter angemessen ist.

[1] In den 2012 vom US-Kongress gesammelten Kommentaren der Electronic Frontier Foundation wurde festgestellt, dass täglich 2000 bis 6000 Videos auf YouTube hochgeladen werden, die urheberrechtliche geschützte Werke anderer enthalten, S. 39.
[2] *BVerfG*, ZUM 2016, 626 – Sampling.

I. „Digitale Leitlinie“ des BVerfG

Fast jeder populäre Musiktitel der letzten Jahre wirft Erinnerungen an andere Musik der vergangenen Jahrzehnte auf. Dass dies kein Zufall ist, lässt sich durch die beeindruckende Anzahl an Samplings beobachten.[3]

Das Bundesverfassungsgericht legte in seiner Sampling-Entscheidung Wert auf die Formulierung der praktischen Konkordanz zwischen Eigentumsschutz des Urhebers und der Kunstfreiheit des Nutzers. Der Eingriff in das Vervielfältigungsrecht könnte jedoch durch eine verfassungsrechtliche Schranke auch ohne eine entsprechende Lizenz möglich sein, so wie es auch der BGH im vorhergehenden Verfahren eingeschätzt hatte.[4]

Wo der BGH noch eine analoge Anwendung des Rechts auf freie Benutzung nach § 24 UrhG für möglich gehalten hatte, lehnte das BVerfG diese Einschätzung ab. Das vom BGH entwickelte Kriterium der „gleichwertigen Nachspielbarkeit“ als Grenze für die analoge Anwendung war bereits zuvor heftig kritisiert worden[5] und auch in Karlsruhe als nicht vereinbar mit der Kunstfreiheit aus Art. 5 Abs. 3 GG erachtet worden.[6] Darüber hinaus war bereits im damaligen Verfahren die europarechtliche Komponente des Rechtsstreits bekannt, welche eventuell zu einer Vorlagefrage bezüglich der Einheitlichkeit des Werksbegriffs führen könnte.

1. Praktische Kondordanz

Zur Abwägung zwischen künstlerischer Gestaltungsfreiheit und den Leistungsschutzinteressen des Rechteinhabers verwies das BVerfG auf das bekannte Prinzip der praktischen Konkordanz.

Zunächst ist bedeutsam, dass das BVerfG bei der Bestimmung der künstlerischen Gestaltungs- und Entfaltungsfreiheit einen kunstspezifischen Begriff zugrunde legte, bei dem auch genretypische Aspekte anerkannt werden müssen.[7]

Daneben wurden die wirtschaftlichen Interessen der Rechteinhaber als flexibel eingestuft und die teleologische Auslegung des Urheberrechts in Bezug auf Leistungsschutzinteressen betont.[8] Bereits diese Auslegung zeigt in ihrem Ansatz wie sich eine vermeintliche Nähe zu der Methodik der „Fair-Use-Doctrine“ im US-Recht erkennen lässt. Die besondere Verknüpfung des deutschen Urheberrechts mit dem Persönlich-

[3] Eine interessante und interaktive Übersicht bietet whosampled.com.
[4] *BGH*, MMR 2009, 253.
[5] *Dreier/Leistner*, GRUR-Beilage 2014, 13 (16 m. w. N.).
[6] *BVerfG*, MMR 2016, 463 (465 ff.).
[7] *BVerfG*, MMR 2016, 463 (466 f.).
[8] *BVerfG*, MMR 2016, 463 (470).

keitsrecht des Schöpfers spielte in diesem Fall keine Rolle, was jedoch gerade bei bestimmten Ausformungen von referenzieller Kunst nicht der Fall sein muss.

Als besondere Kriterien wurden anschließend der inhaltliche und zeitliche Abstand zum Originalwerk festgehalten, was gerade die Abwägung zugunsten der Kunstfreiheit entscheiden kann. Während sich der zeitliche Abstand zum Originalwerk noch leicht feststellen und quantifizieren lässt, ist eine inhaltliche Bewertung doch mit erheblichen Schwierigkeiten verbunden, sodass sich auch hier wieder die Frage stellt, wie sich dieses Kriterium rechtssicher gestalten lässt.

Insgesamt liegt der Entscheidung ein „offener Abwägungsprozess“ zugrunde, der auch an die Fair-Use-Doctrine erinnert und nicht mehr die klassische verfassungsrechtliche Struktur von Rechten und Schranken verfolgt.[9]

2. Genretypische Aspekte referenzieller Kunst?

Das BVerfG hat durch die Anerkennung der künstlerischen Leistung im Sampling angedeutet, dass eine bestimmte Richtlinie für Instanzgerichte gegeben ist, gerade im Bereich von referenzieller Kunst. Stellenweise wird im ursprünglichen BGH-Urteil und der Bedeutung des „Nachspielbarkeits-Kriterium“ eine überkommene Vorstellung des urheberrechtlichen Schöpfungsprozesses gesehen,[10] von welchem sich jedoch das BVerfG durch diese Anerkennung abgewendet hat.

Es ist jedoch bemerkenswert schwierig, die beschriebenen Maßstäbe auch auf andere referenzielle Kunstformen des digitalen Zeitalters zu beziehen. Dies hängt primär mit der großen Varianz an Kunstformen zusammen.

a) Übersicht über bedeutsame referenzielle Kunstformen

Die Funktionsweise des Sampling wurde in den bereits besprochenen Urteilen hinreichend dargestellt. Die von dem BVerfG angewandten Kriterien lassen sich gut auf das Verständnis des Samplings anpassen, insbesondere der zeitliche und inhaltliche Abstand. Dies liegt insbesondere an der Natur des Samplings. Hierbei wird im Regelfall nur ein Teil des geschützten Werkes verwendet, welches keinen eigenständigen Teil des referenziellen Werkes darstellt, sondern durch (üblicherweise) wesentliche kreative Eigenleistungen des Referenz-Künstlers ergänzt und erweitert wird.

Ein weiterer erheblicher Unterschied, welcher das Sampling in seiner Grundform von anderen Formen der referenziellen Kunst unterscheidet, ist die Irrelevanz der Erkennbarkeit des ursprünglichen Werkes. Bei anderen Arten der referenziellen Kunst ist dieser Aspekt erheblich weiter ausgeprägt, wie es etwa aus der klassischen Kunstform

[9] So auch *Podszun*, ZUM 2016, 606 (607); *Grünberger*, ZUM 2018, 271 (274 f.).
[10] *Leistner*, GRUR 2016, 772 (773 ff.); *Podszun*, ZUM 2016, 606 (607); *Schonhofen*, GRUR-Prax 2016, 277 (278 f.).

der parodierenden Werke schon sehr lange bekannt ist. Hierbei kommt es dem Referenzkünstler gerade darauf an, dass ein Betrachter oder Wahrnehmender des Referenzwerkes das Ursprungswerk wiedererkennt und so die eigentliche Aussage des Referenzwerkes erkennen kann.

Besonders YouTube-Kanäle oder Twitch-Channel, die mittels Compilations, Bewertungen und Reviews, Let's Plays, Walk-Throughs, Riff-Trax[11] oder Live-Streaming Unterhaltungsprogramme[12] darbieten, erfreuen sich seit einiger Zeit großer Beliebtheit und nehmen in jüngster Vergangenheit noch an Bedeutung zu. Im Regelfall liegt die Besonderheit dieser Referenzwerke[13] darin, dass es zwar von maßgeblicher Bedeutung ist, dass der Betrachter das Ursprungswerk als solches wieder erkennt und wahrnimmt, aber es fehlt ein parodierender Charakter, da die eingebetteten Szenen oder Tonspuren ohne Veränderung dargestellt werden und erst durch die Kommentierung (im weitesten Sinne)[14] des Referenzkünstlers das Referenzwerk als solches Gestalt annimmt.[15]

Als besondere Gruppe ist noch die sehr spezielle aber durchaus populäre Referenzform des sog. „YouTube Poop" zu erwähnen, welche sich durch ihre spezielle Art nicht nur die Leistungsschutzrechte des Urheberrechts betrifft, sondern zusätzlich mit Regelmäßigkeit die Persönlichkeitskomponente des Urheberrechts und Persönlichkeitsrechte im Allgemeinen berührt. Diese Form der „remix culture" ist eine sonderbare und bisweilen auch bizarre Ausformung.[16] Auch hierbei ist es in der Regel gewollt, dass der Betrachter das Ursprungswerk erkennt, aber dessen Popularität spielt eine untergeordnete Rolle bzw. bietet vielmehr die Grundlage für die weitergehende Verarbeitung des Projekts. Gegenstand von „YouTube Poop" sind häufig Zusammenschnitte und Verzerrungen von TV-Aufnahmen oder anderen Video-Elementen, welche in teilweise sehr aufwendiger und präziser Arbeit so verarbeitet werden, dass es auf den tatsächlichen Inhalt des Ursprungswerk gar nicht mehr ankommt. Der Unterhaltungswert soll vielmehr dadurch erreicht werden, dass das Ursprungswerk noch als solches

[11] Eine in der Regel humorvolle Kommentierung von Filmwerken, die den gesamten Film andauert.
[12] Mit einer ähnlichen Übersicht: *Klass*, ZUM 2016, 801 (801 f.).
[13] Der Begriff „Werk" an dieser Stelle ist nicht gleichzusetzen mit dem Werkbegriff des Urheberrechts, da es durchaus denkbar ist und auch vorkommt, dass die genannten Unterhaltungsformen nicht die Schöpfungshöhe eine urheberechtlichen Werks erreichen.
[14] In vielen Fällen erfolgt keine direkte Kommentierung, sondern lediglich eine implizite Kommentierung durch den Kontext oder die Verbindung mit anderen Video- oder Tonelementen.
[15] Da es bei professionellen YouTube-Kanälen häufig um die Quantität des veröffentlichen Materials geht, ist diese Entwicklung wenig verwunderlich. Die Produktion einer „Review" ist deutlich kostengünstiger und weniger zeitintensiv als die Produktion von komplett originärem Content.
[16] „absurde Remixe, welche die niedrigsten technischen und ästhetischen Standards der Remix-Kultur nachäffen und verspotten, die Remix-Kultur als solche zu kommentieren." - 2012 vom US-Kongress gesammelten Kommentaren der Electronic Frontier Foundation, S. 39.

erkannt wird, was den „Parodie-Charakter“ oder sonst gewünschten „bizarren“ Charakter der Film- und Tonwerke erreicht.

Aufgrund dieser erheblichen Unterschiede im Inhalt auch innerhalb einzelner Kunstrichtungen ist es ausgeschlossen, dass einzelne Kunstrichtungen einen „Freischein“ erhalten, wie dies etwa bei Fanfiction zur Förderung der Kreativität bei Heranwachsenden vereinzelt in Erwägung gezogen wurde. Hierin liegt eine kurzsichtige Betrachtung der Referenzkunst und ihrer Vielfalt, sodass eine generalisierende, medienpolitische Begünstigung keine interessengerechte Lösung sein kann – vielmehr ist sich auf rechtssichere und inhaltsbezogene Maßstäbe zu verlassen.

Ganz erhebliche Probleme bietet in diesem Zusammenhang die Abgrenzung von Kunst- und Meinungsfreiheit, wobei letztere durch das Urheberrecht deutlich einfacher eingeschränkt werden kann. Viele Formen referenzieller Kunst stellen sich bei näherer Betrachtung jedoch eher als Facette der Meinungsfreiheit dar. In der Regel steht jedoch die Wichtigkeit dieser Abgrenzung in keinem Verhältnis zu der tatsächlichen Auseinandersetzung, die Gerichte in diesem Fall vornehmen.

3. Bedeutung der Originalität im Urheberrecht

In der ursprünglichen Bedeutung des deutschen Urheberrechts, hängt die „persönliche geistige Schöpfung“ nach § 2 Abs. 2 UrhG erheblich mit der Persönlichkeit des Urhebers zusammen, was auch durch den Ausschluss der Übertragbarkeit und Mechanismus der Lizenzvergabe verstärkt wird. Dieser Bezug zum Urheber als Person zeigt, dass zentrales Element der Schöpfung die Originalität sein soll.[17] In der Kunsttheorie und Kunstgeschichte lässt sich doch der Trend entdecken, dass eine solche Fixierung auf das Original in den letzten Jahrzenten bereits stark an Bedeutung verloren hat. Die „Gegenbewegung“ der bereits erwähnten Remix-Kultur arbeitet hingegen mit Übernahme, Abwandlung, Erweiterung und Ergänzung von bereits bestehendem.[18] Aufgrund dieser Wandlung im Rahmen des künstlerischen Selbstverständnisses wird plädiert, dass auch die rechtliche Einordnung im Rahmen des Urheberrechts und der Kunstfreiheit die „Verschiebung von persönlich-originellem Schöpfungsakt zu transformierender Übernahme fremder Originale“ nachzuvollziehen hat.[19]

Dieser Formulierung fehlt es allerdings an tatsächlich relevanten Einordnungsmerkmalen. Der Vorgang, sich von anderen Künstlern inspirieren zu lassen, dürfte in etwa so alt sein wie Kunst selbst, was auch durch das Urheberrecht berücksichtigt wird, indem es gerade keinen Ideenschutz gibt. Die Gleichstellung des BVerfG zwischen

[17] *Peifer*, Individualität im Zivilrecht, 2001, S. 54 ff.; *Podszun*, Wandlungen des Schutzgegenstandes, in: Vom Magnettonband zu Social Media, Festschrift 50 Jahre Urheberrechtsgesetz, 2015, S. 361 (371).
[18] *Podszun*, ZUM 2016, 606 (608); *Perloff*, Unoriginal Genius – Poetry by other means in the new century, 2010.
[19] *Leistner*, GRUR 2016, 772 (775 ff.); *Podszun*, ZUM 2016, 606 (608); *Wagner*, MMR 2016, 513 (515).

Sampling zu „tongestalterischen Zwecken“ und zu „Zwecken der kritischen Auseinandersetzung“[20] als Anerkennung im Rahmen der Kunstfreiheit stellt insofern keine Besonderheit dar, da der Kunstbegriff und das Urheberrecht nicht deckungsgleich sind. Die Einordnung unter den Kunstbegriff im Rahmen des Art. 5 Abs. 3 GG bedeutet nicht, dass eine entsprechende Schutzfähigkeit oder Schutzwürdigkeit im Rahmen des Urheberrechts geboten ist. Darüber hinaus verkörpert das Urheberrecht eine Anerkennung der persönlichen Leistung und auch der wirtschaftlichen Verwertung, während die Kunstfreiheit in erster Linie eine Negativfreiheit darstellt, sodass Kunst vor Eingriffen, gerade im Wirkbereich geschützt werden muss.

Dennoch wird das BVerfG-Urteil vielfach so ausgelegt, dass durch diese Entscheidung auch andere Arten der referenziellen Kunst positiv betroffen sind und auch hierdurch eine Vereinfachung in der Ausübung dieser Kunstformen möglich ist. Die aufgezählten Kriterien des BVerfG: „stilprägende Elemente“, „erforderliche kunstspezifische Betrachtung“ und „genrespezifischer Aspekte“ im jeweiligen Schaffensprozess erlauben keine beliebige Übertragung auf jegliche existenten Kunstformen. Zwar hat hierdurch der Begriff der Abwägung das zentrale Element übernommen, aber ein eindeutiges Bevorzugen von referenzieller Kunst lässt sich nicht unabhängig feststellen. Es ist vielmehr von einer Klarstellung auszugehen, indem dem Sampling-Prozess nicht grundsätzlich die künstlerische Komponente aberkannt wurde, wie es vielleicht noch der BGH vorantreiben wollte. Insbesondere bleibt fraglich, ob die typischen Beleidigungen in Rap-Songs als „stilprägende Elemente“ oder Schmähkritik wie das satirische Gedicht von Jan Böhmermann auf den türkischen Politiker Recep Tayyip Erdogan[21] anerkannt werden und damit als zentraler Teil der Kunstform im Abwägungsvorgang besondere Berücksichtigung finden kann.[22] Eine Übertragbarkeit an dieser Stelle dürfte insbesondere daran scheitern, dass in der Sampling Entscheidung in erster Linie die wirtschaftlichen Verwertungsrecht des Urheberrechts in Frage gekommen sind, während die persönliche Seite keine Rolle gespielt hat.[23]

4. Dichotomie des Urheberrechts?

Die Leistungsschutzrechte des Urheberrechts wurden durch einige Ausführungen im BVerfG-Urteil erheblich in ihrer Wirkungsweise eingeschränkt, indem gerade die Absolutheit des Schutzcharakters abgesprochen wurde und vielmehr eine Lösung über die

[20] *BVerfG*, MMR 2016, 463 (467).
[21] *Podszun*, ZUM 2016, 606 (609) - spricht hier von „stilprägenden Elementen“ der „Meta-Ironisierung“, wobei allerdings offen bleibt, welche Maßstäbe hier gelten, um eine Beliebigkeit der Kunstformen und des Kunstbegriffs zu vermeiden.
[22] *AG Tiergarten*, ZUM 2015, 904 und *LG Berlin*, ZUM 2015, 903; vgl. *Oglakcioglu/Rückert*, ZUM 2015, 876 (876).
[23] Die typischen Beleidigungen in einem Rap-Song dürften zwar in der Regel nicht zusätzlich eine Urheberrechtsverletzung darstellen, aber gerade im Rahmen der „YouTube Poop“-Werke ist das durchaus üblich.

Zahlung eines angemessenen Entgelts als Kernbestandteil als vorrangig angesehen wurde.[24]

Besonders spezifiziert hat das BVerfG jedoch das zeitliche Element im Rahmen der Abwägung zwischen Kunstfreiheit und Urheberrecht. So wandelt sich der Charakter des Ausschließlichkeits- und Verwertungsrechts dahingehend, dass sukzessive Rechte zugunsten des gesellschaftlichen Raums aufgegeben werden müssen. Das Individualrecht wird Allgemeingut.[25] Interessant ist diese Differenzierung insofern, als dass ein gesetzlicher Wechsel von Individual zum Allgemeingut bereits vorgesehen ist.[26] Dass eine sukzessive Verringerung der Rechte bereits während dieses Zeitraums eintritt, dürfte kaum mit der gesetzgeberischen Bestimmung vereinbar sein bzw. auch der Realität der Durchsetzung nicht entsprechen. Die Gemeinfreiheit ist keine Unbekanntheit im Urheberrecht, sodass eine solche institutionelle Erosion des Urheberrechts bedenklich erscheint.

Das BVerfG hingegen möchte in der Abwägung die Sozialbindung des Eigentums gem. Art. 14 Abs. 2 GG betonen, welche den Abwägungsausgang für vertretbar erklärt, solange der Rechteinhaber ein angemessenes Entgelt für seine Leistung erhält.[27] Augenscheinlich fehlen in diesem Aspekt der Sozialbindung die besondere Verknüpfung von Individualität und Persönlichkeitsbezug des Urheberrechts.

5. Rein ökonomische Perspektive

Das BVerfG geht in seiner Entscheidung noch etwas weiter als in der vorangegangenen Germania 3 Entscheidung[28] und betont innerhalb der Abwägung zulasten des Referenzkünstlers die „Gefahr merklicher wirtschaftlicher Nachteile (z.B. Absatzrückgäng)“,[29] die nur dann gegeben ist, wenn ein horizontales Wettbewerbsverhältnis gegeben ist, was gerade bei einem Zweitverwertungsmarkt nicht vorliegt. Eine andere Position hatte noch der BGH vertreten, indem er alle Verwertungsrechte grundsätzlich dem Rechteinhaber zugesprochen hat. Das Erfordernis einer solchen wettbewerbstechnischen Betrachtung mag auf den ersten Blick sinnvoll und schützenswert erscheinen, birgt aber Abgrenzungsschwierigkeiten.

a) Besonderheiten bei digitaler Referenzkunst bzgl. des Werk- und Wirkbereichs

So bedarf es gerade bei digitalen Kunstformen einer digitalen Vorlage zur Bearbeitung und Veränderung. Insofern lässt sich der Bereich der Schaffensphase in drei Phasen

[24] *BVerfG*, MMR 2016, 463 (466).
[25] *BVerfG*, MMR 2016, 463 (466); *Duhanic*, GRUR Int. 2016, 1007 (1014); *Ohly*, GRUR 2017, 964 (966 ff.).
[26] Vgl. nur § 85 Abs. 3 S. 1 UrhG.
[27] *Grünberger*, ZUM 2018, 321 (338); *Duhanic*, GRUR Int. 2016, 1007 (1014); *BVerfG*, MMR 2016, 463 (465).
[28] *BVerfG*, NJW 2001, 598 (599).
[29] *BVerfG*, NJW 2001, 598 (599).

einteilen. In der ersten Phase ist es für den Künstler notwendig, eine digitale Version des Originalwerks zu erlangen, sodass es hier auf eine Frage der Verfügbarkeit hinausläuft. Die zweite Phase beschäftigt sich mit der digitalen Bearbeitung, welche in der Regel nicht öffentlichkeits-wirksam ausgeführt wird und auch eine etwaige Urheberrechtsverletzung praktisch nicht nachweisbar ist. Für die Analyse der Problematik ist diese Phase daher vernachlässigbar. Die dritte Phase betrifft die Veröffentlichung, welche dann die allgemeine Frage der Zulässigkeit der entsprechenden Bearbeitung im Rahmen des Wirkbereichs der Kunstform aufwirft und bereits angesprochen wurden.

Von besonderer Bedeutung ist an dieser Stelle bereits die erste Phase, die in der Regel eher von geringerer Relevanz für die rechtliche Bewertung ist, da die Verfügbarkeit bei analogen Originalwerken in der Regel keine rechtliche Besonderheit darstellt.[30] Häufig können hier von Künstlern Aufzeichnungen von Sendungen o.Ä. angefertigt werden bzw. die Musikstücke über physische Speichermedien oder Online-Vertriebe erworben werden. Bei vielen der genannten digitalen Referenzkunstformen ist jedoch eine Version von aktuellen Kinofilmen oder anderen Werken erforderlich, deren Erwerb sich auf legale Weise erst bei einem eventuellen DVD bzw. Blue-Ray Release[31] verwirklichen lässt.

Da jedoch gerade bei den erfolgreichen Review-Kunstformen für den größten Wirkungsbereich eine zeitnahe aber auch qualitativ hochwertige Veröffentlichung wünschenswert ist, ist eine digitale Version möglichst zeitnah nach der Erst-Veröffentlichung des Originalwerks erforderlich. In der Praxis ist daher folgender Ablauf zu beobachten: Nach der Erst-Veröffentlichung eines Kino-Film etwa, kommt es zunächst zu einer Online-Verbreitung von sog. Cam-Rips[32], die jedoch aufgrund ihrer unzureichenden Qualität für eine hochwertige Weiterverarbeitung ungeeignet sind. Sobald ein erster DVD- oder Blu-ray-Release zugänglich wird, wird eine entsprechende Kopie auf zahlreichen File-Sharing-Websites hochgeladen, sodass zur selben Zeit auch die entsprechenden Review-Projekte mit dieser – nun illegal erworbenen digitalen Kopie – in Bearbeitung gehen (2. Phase). Kurze Zeit später werden die fertigen Referenzwerke auf den jeweiligen Mediaplattformen wie YouTube veröffentlicht (3. Phase).

Hier stellt sich daher die Frage, wie diese Besonderheit innerhalb der ersten rechtlich zu beurteilen ist. Im Rahmen der Kunstfreiheit nach Art. 5 Abs. 3 S. 1 GG wird regelmäßig der gesamte Werk- und Wirkbereich der Kunst anerkannt.[33] Während sich die 3. Phase regelmäßig dem Wirkbereich – Verbreitung, Darbietung bzw. kommunika-

[30] Von der Problematik des unrechtmäßigen Erwerbs, das sich hier auch unmittelbar stellt, ist insofern abzusehen, da dies nicht den Regelfall darstellt.
[31] Vom Problem der Umgehung des Kopierschutzes als Urheberrechtsverletzung oder sonstige unrechtmäßige Handlung einmal abgesehen.
[32] Mitschnitte aus dem Kino durch eine mitgebrachte Kamera oder ähnliches.
[33] *Epping/Hillgruber*, in: BeckOK GG, Art. 5 Rn. 168; *Scholz*, in: Maunz/Dürig GG, Art. 5 Rn. 18.

tive Vermittlung[34] – zuordnen lässt und die 2. Phase klassischerweise dem Prozess der künstlerischen Schöpfung zuzuordnen ist, bleibt fraglich, ob hiervon auch die 1. Phase der Zugänglichmachung der Materialien erfasst ist.

Der BGH hat erst wieder kürzlich festgestellt, dass das Filmurheberrecht aus § 94 Abs. 1 S. 1 UrhG bereits durch das Herunterladen bzw. Anbieten selbst kleinster Partikel einen Eingriff darstellt.[35] Auch wurde hierbei auf zwei für den vorliegenden Fall relevante Punkte hingewiesen:

1. Zunächst sind „aufgrund des unionsrechtlichen Hintergrunds des dem Filmhersteller zustehenden Leistungsschutzrechts der öffentlichen Zugänglichmachung in Art. 3 II Buchst. c der RL 2001/29/EG ausschließlich Unionsgrundrechte zu prüfen (…), soweit die Richtlinie den Mitgliedstaaten keinen Umsetzungsspielraum überlässt, sondern zwingende Vorgaben macht.[36]
2. Daraus folgert der BGH mithin, dass sich ein Nutzer eines Filesharing-Netzwerks „zur Rechtfertigung seiner Teilnahme an einer Internet-Tauschbörse nicht auf das Grundrecht der Kunstfreiheit (…) berufen“ kann.[37]

Das stellt insofern eine interessante rechtliche Herausforderung dar, als dass die Unionsgrundrechte zwar in Art. 13 S. 1 GRCh die Kunstfreiheit anerkennen, allerdings gibt es bisher keine relevante oder wegweisende Rechtsprechung des EuGHs oder des EGMR, sodass die Auslegung vor erheblicher Unsicherheit steht. Es besteht nur insoweit Einigkeit, dass eine weite Auslegung erforderlich ist und der Werk- und Wirkbereich von der Kunstfreiheit umfasst ist.[38] Mithin ist zwar ein Gleichlauf zum deutschen Grundrecht der Kunstfreiheit erreicht, aber der BGH hat einer direkten Anwendung eine entsprechende Absage erteilt.

Die Ausweitung des Schutzbereichs der Kunstfreiheit auf vorbereitende Handlungen zur künstlerischen Tätigkeit und Schaffensphase bringt folgendes Dilemma. Einerseits scheint sie verfassungsrechtlich geboten, da der Werkbereich der Kunst eine weite Auslegung erfährt und ein Schutzentzug der Beschaffung der digitalen Version des Originalwerks in der Theorie dazu führen könnte, dass die Schöpfungsphase insgesamt

[34] *Epping/Hillgruber*, in: BeckOK GG, Art. 5 Rn. 168; *Scholz*, in: Maunz/Dürig GG, Art. 5 Rn. 18.
[35] *BGH*, NJW 2018, 784 (785 Rn. 19) – in diesem Fall ging es in erster Linie um die Frage, ob durch die „Zerstückelung“ der Ursprungsdatei in einem Peer-2-Peer Netzwerk in kleinere Datenpakete überhaupt eine wesentliche Verletzung der Urheberrechte vorliegt, was der BGH insgesamt bejaht hat.
[36] *BGH*, NJW 2018, 784 (785 Rn. 23).
[37] *BGH*, NJW 2018, 784 (785 Rn. 23).
[38] *Bergmann*, in: Bergmann/Dienelt, Ausländerrecht, EU-Grundrechte-Charta, Art. 13 Rn. 1; *Jarass*, GrCh, Art. 13 Rn. 5.

sehr eingeschränkt wird.[39] Da die Review-Ersteller in vielen Fällen auf diese Beschaffung angewiesen sind, um ihre konkreten Projekte zu verwirklichen, könnte eine solche Einschränkung durch Versagen der Kunstfreiheit dazu führen, dass im Wege einer Umgehung der gesamte Bereich der digitalen Referenzkunst eine Einschränkung erfährt.

Andererseits würde eine entsprechend weite Auslegung des Werkbereichs weitreichende Konsequenzen haben, was die Verfolgung von unrechtmäßigem Filesharing angeht. Zunächst ist anerkannt, dass der Werkbereich auch solche Schaffensprozesse der Kunst schützt, die einen Fehlschlag darstellen oder aufgrund anderer Gründe nicht über den Werkbereich hinausgehen.[40] In diesem Fall könnte der ursprünglich unrechtmäßige Erwerb zu einer dauerhaften Rechtmäßigkeit führen – eine Löschungspflicht oder ähnliches wäre praktisch unmöglich durchzusetzen. Außerdem ließe dies eine entsprechende Rechtfertigungsmöglichkeit für unrechtmäßiges Filesharing zu, die erhebliches Missbrauchspotential bietet. Eine Überprüfung auf künstlerische Tätigkeit ist kaum realisierbar, da es für den Urheberrechtsinhaber oder Rechtverwerter keine Einsichtsmöglichkeit darstellt. Auch eine Plausibilitätsprüfung der künstlerischen Tätigkeit wird sich nur vor Gericht klären lassen, was einen erheblichen Prozess zur Entwicklung von praktikablen Kriterien bedeutet und eine immense Kasuistik befürchten lässt.

Eine Lösung dieses Problems könnte jedoch darin zu finden sein, dass der BGH in seiner Entscheidung den Fokus auf eine Verletzung des Rechts aus § 94 Abs. 1 S. 1 UrhG gelegt hat, welcher jedoch nur bei dem Angebot zum Download relevant ist, nicht bei dem Download selbst. Eine Nutzung der Filesharing-Netzwerke ist ohne Angebot zwar nicht möglich, aber es existieren auch Sharehoster-Plattformen, die gerade kein Angebot verlangen.[41] Bevor man hier jedoch über eine Erfassung notwendiger Nebenrechtsverletzungen nachdenkt, reicht es aus, sich auf das Vervielfältigungsrecht aus § 16 UhrG zu beschränken, welches auch bei einem entsprechenden Download verletzt wird.[42] Insofern bleiben die Bedenken auch bei anderweitiger Betrachtung des Sachverhalts bestehen.

II. „Fair-Use Doctrine“ als Leitbild?

Die Fair-Use Doctrine in den Vereinigten Staaten stellt sich in diesem Zusammenhang als deutlich expliziter und eindeutiger dar. So ist im Copyright Act unter Sect. 107 di-

[39] Praktisch ist dies jedoch nicht zu erwarten, da einerseits die Verfolgung von unrechtmäßigen Downloads technisch erheblich erschwert werden kann und andererseits das Bewusstsein der Referenzkünstler für eine Abgrenzung in rechtmäßige und unrechtmäßige Beschaffung nicht gegeben sein wird.
[40] *Scholz*, in: Maunz/Dürig GG, Art. 5 Rn. 18 m. w. N.
[41] Rapidshare.com als prominentestes Beispiel.
[42] Zumindest nach herrschende Meinung, Kommentar – Eine Privilegierung nach § 53 Abs. 1 UrhG scheitert daran, dass es sich bei den einschlägigen Sharehoster- und Filesharing-Websites augenscheinlich um nicht rechtmäßig erworbene Originale handelt.

rekt festgehalten, dass die Verwendung von urheberrechtlich geschützten Werken keine Verletzungshandlung darstellt, wenn diese zum Zweck der Kommentierung, Kritik, etc. „fair“ eingesetzt werden.[43]

Problematisch ist allerdings, dass eine explizite Nennung der Parodie oder referenzieller Kunst fehlt, sodass es in der Rechtsprechung der US-Gerichte zu einer interessanten Entwicklung kam, gerade im Bereich des Samplings. Noch 2005 entschied das United States Court for the Sixth Circuit, dass Sampling selbst bei kleinsten Ausschnitten eine Verletzung des Copyrights darstellt, indem es unmissverständlich festhielt: „Get a licence or do not sample“.[44]

2016 stellte sich das United States Court for the Ninth Circuit gegen die vorherige Entscheidung und stellte gegensätzlich fest, dass gerade die de minimis Analyse ein zentraler Bestandteil sein kann, um eine Verletzung von Copyright-geschützten Materialien auszuschließen.[45]

1. Einzelne Kriterien der Fair-Use-Doctrine und die Erfassung von Parodien

Sect. 107 des Copyright Act gibt einen Katalog an Kriterien vor, welche wesentlich den ursprünglichen Kriterien aus der Entstehung der Fair-Use-Doctrine der Judikative von 1841[46] entsprechen. Auch gibt es eine Vorgabe des Supreme Court of the United States, wonach die Kriterien nicht isoliert betrachtet und geprüft werden sollen, sondern eine gesamtheitliche Betrachtung unter Einbeziehung der Wirkung des Urheberrechts erfolgen muss.[47] Mithin ist eine Ähnlichkeit zum Abwägungskonzept des deutschen BVerfG gegeben.

Die Kriterien der US-amerikanischen Fair-Use-Doctrine sind entsprechend: (1) Sinn und Zweck der Verwendung, insbesondere die kommerzielle Nutzung, (2) die Art des geschützten Ursprungswerks, (3) die Quantität und Eigenständigkeit des Teils des verwendeten Ursprungswerks im Verhältnis zum gesamten Ursprungswerk und (4) die Auswirkung der Verwendung des Ursprungswerks auf den potentiellen Markt oder den Wert des Ursprungswerks.

[43] Bevor die Fair-Use-Doctrine per Gesetz festgehalten wurde, war sie erheblich im Wege der judikativen Rechtsfortbildung entwickelt worden. Bereits 1841 (9 F. Cas. 342 (C.C.D. Mass 1841) (No. 4, 901) wurde die Notwendigkeit für die referenzielle Nutzung von Originalwerken erkannt, zunächst als Abwehrmechanismus, die eine Urheberrechtsverletzung rechtfertigen konnten und später als darüber hinausgehende Verneinung der Verletzung Insgesamt, so wie es auch das Gesetz nun übernommen hat.
[44] 410 F.3d 792 (6th Cir. 2005), S. 801.
[45] 824 F.3d 871 (9th Cir. 2016), S. 886.
[46] 9 F. Cas. 342 (C.C.D. Mass 1841.
[47] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 578 (1994).

a) Sinn und Zweck der Verwendung

Zunächst ist zu analysieren, ob durch das Referenzwerk[48] dem Originalwerk ein neues Element hinzugefügt wird, welches eine neue Aussage, Bedeutung oder Botschaft ermöglicht.[49] Wenn dieser Aspekt bejaht wird und damit eine sogenannte transformative Benutzung des Originalwerks vorliegt, spielen andere Aspekte, wie etwa eine kommerzielle Nutzung (die in der Regel gegen einen Fair-Use des Originalwerks spricht), eine weniger bedeutsame Rolle.[50] Insbesondere ist ein neues Element dann gegeben, wenn mit dem Referenzwerk eine neue Meinung oder Kritik über das Originalwerk ausgedrückt wird.[51] Ein Indiz gegen die Anwendung der Fair-Use-Doctrine soll aber in jedem Fall dann gegeben sein, wenn das Referenzwerk sich nur den originalen Bestandteilen bedient, um etwa „Aufmerksamkeit zu erlangen, oder schlicht die kreative Mühe umgehen möchte, ein eigenes originelles Werk zu schaffen."[52]

Gerade im Vergleich zur Sampling-Entscheidung des deutschen BVerfG zeigen sich hier erhebliche Unterschiede auf, da gerade das Sampling in seiner Grundfunktion nicht dazu dient, das Originalwerk, dem es entstammt, in einer besonderen Form zu kritisieren oder zu kommentieren. Im US-Kontext wird insofern von einer „re-contextualization"[53] gesprochen, die aber auch einen transformativen Charakter haben kann, wenn die Verarbeitung ein neues Werk hervorbringt.[54] Dies wird in der Regel damit begründet, dass dem Grundgedanken der Originalität des Urheberrechts dadurch am ehesten Rechnung getragen wird, dass ein neues Werk einen größeren Schaffungsprozess bedeutet als eine Parodie, welche an ein spezifisches vorheriges Originalwerk gebunden ist.[55] Die erste Variante der Nutzung bedeutet in diesem Fall eine größere Verwirklichung von Originalität.

In der jüngsten Entwicklung haben sich auch Instanz-Gerichte in den USA dazu entschieden, die Definition der transformativen Nutzung zu erweitern und verzichten na-

[48] Die Terminologie weicht im Rahmen der US-Gerichte etwas ab, hier ist von einem „secondary use" die Rede.
[49] Campbell, 510 U.S. S. 579 (mit Bezug auf Folsom v. Marsh, 9 F. Cas. 342, 348 (C.D.D. Mass 1841) (No. 4,901)).
[50] *Samuelson*, Washington Law Review 2015, 815 (853 ff.); *Peyton*, North Carolina Law Review 2018, 1085 (1115).
[51] In der Campbell-Entscheidung ging es um eine Parodie des bekannten Liedes „Oh, Pretty Woman" von Roy Orbisons durch die Band 2 Live Crew, welche die vermeintliche Banalität und Einfallslosigkeit des Originalwerks kommentieren sollte.
[52] Campbell, 510 U.S. S. 580 (""to get attention or to avoid the drudgery in working up something fresh").
[53] *Ashtar*, Theft, Transformation, and the Need of the Immaterial: A Proposal for a Fair Use Digital Sampling Regime, 19 ALB. L.J. SCi. & TECH, 263 (295).
[54] Campbell, 510 U.S. S. 580; *Peyton*, North Carolina Law Review 2018, 1085 (1116).
[55] *Peyton*, North Carolina Law Review 2018, 1085 (1116); *Samuelson*, Washington Law Review 2015, 815 (853 ff.).

hezu gänzlich auf die Funktion der Referenzwerke als Kritik oder Kommentar.[56] Es ist vielmehr ausreichend, dass eine neue Bedeutung oder ein neuer Zweck durch das Referenzwerk ausgedrückt werden soll.[57] In einer prägnant formulierten Entscheidung des Second Circuit Courts, wurde festgehalten, dass „wenn das Rohmaterial [des Originalwerks] gewandelt wird, um neue Informationen, neue Ästhetik, neue Erkenntnisse oder Einblicke zu erschaffen – ist genau die Art von Aktivität erreicht, welche durch die Fair-Use-Doctrine gefördert werden soll, um die Bereicherung der Gesellschaft zu sichern.“[58] Auf dieser Basis ist die eigentliche Bedeutung des Samplings vielmehr so klären, ob „das Sample die Grundlage eines neuen musikalischen Ausdrucks ist, oder lediglich ein Effekt.“[59] Bei vielen Formen der Referenzkunst lässt sich dies noch mit überdurchschnittlicher Rechtssicherheit analysieren, sodass hier ein wirksames und sinnvolles Kriterium gewonnen ist.

Bezüglich der Kommerzialisierung bzw. wirtschaftlichen Verwertung ist die Auslegung des Kriteriums innerhalb der Fair-Use-Doctrine auch eindeutiger. Ein einfacher Blick auf die Aufzählung der klassischen kommerziellen Branchen wie Berichterstattung, Kritik, etc. zeigt, dass auch die wirtschaftliche Verwertung erfasst ist, da sonst diese Aspekte nicht in Sect. 107 Copyright Act aufgenommen worden wären. Gerade im Rahmen der digitalen referenziellen Kunst, wie es bei den hier relevanten Beispielen der Fall ist, ist in der Regel eine gewinnbringende Veröffentlichung durch Werbeeinnahmen beabsichtigt. Allerdings kommt an dieser Stelle auch wieder der Abwägungscharakter der Fair-Use-Doctrine in Betracht, welcher speziell – und damit deutlich praktikabler und präziser als die deutsche Abwägung zwischen Kunstfreiheit und Eigentumsfreiheit – zwischen dem Grad der Transformation des Originalwerks und der kommerziellen Bedeutung des Referenzwerks abwägt.

b) Die Art des geschützten Ursprungswerks

Im zweiten Kriterium dreht sich die Abgrenzung insbesondere darum, ob das Originalwerk durch Kreativität oder Wiedergabe von Fakten gekennzeichnet ist.[60] Hier ist für die Zwecke des Rechtsvergleichs zu sagen, dass dies kaum eine relevante Rolle spielt, da die Originalwerke im Bereich der digitalen Referenzkunst weit überwiegend klassisch kreative Werke sind. Auch in der US-amerikanischen Diskussion wurde erkannt

[56] 448 F.3d 605 (2d Cir. 2006).
[57] *Peyton*, North Carolina Law Review 2018, 1085 (1117); *Brauneis*, Syracuse Law Review 2018, 7 (31 ff.).
[58] Cariou, 714 F.3d at 706.
[59] A. Dean Johnson, Music Copyrights: The Need for an Appropriate Fair Use Analysis in Digital Sampling Infringement Suits, 21 FLA. ST. U. L. REv. 135, 149 (1993).
[60] "separating the fair use sheep from the infringing goats" - Campbell, 510 U.S. at 586.

und aufgezeigt, dass die Anwendung dieses Kriteriums immer dazu führen müsste, die Abwägung zulasten des Referenzkünstlers zu beeinflussen.[61]

c) Quantität und Eigenständigkeit des Teils des verwendeten Ursprungswerks

Der dritte Faktor ist dem Maßstab des BVerfG am ähnlichsten, wenn es um die Frage nach der Quantität und Selbstständigkeit des entlehnten Elements aus dem Originalwerk geht. Der Begriff der Selbstständigkeit im Rahmen der Fair-Use-Doctrine geht hierbei jedoch insbesondere darauf ein, ob es sich um das „Kern-Element" des Originalwerks handelt.[62] Hier zeigt sich auch die erhebliche Ähnlichkeit zum BVerfG, die kunstspezifischen Aspekte zu berücksichtigen, wobei die Aussagen zur „Parody"[63] deutlich überzeugender sind als die Anmerkungen des BVerfG zur Kunstform des Samplings.

Diese relative, aber im Vergleich zur deutschen Herangehensweise deutlich präzisere und rechtssichere Variante ist unter anderem darauf zurückzuführen, dass das amerikanische Verfassungssystem das deutsche Konzept der „Kunstfreiheit" nicht kennt, sondern vielmehr das allgemeine Grundrecht der „Freedom of Speech and Expression" nutzt. Dieses erfährt jedoch auch in der Jurisprudenz oder juristischen Diskussion keine erhebliche oder relevante Ausformung als eigenständiges Recht der Kunstfreiheit.

Insofern ist die Etablierung und Anwendung der „Fair-Use-Doctrine" auch keine verfassungsrechtliche Problematik, sondern eine freie Abwägung zwischen verschiedenen Interessen, was die Gesetzgebung erheblich vereinfacht und keine verschiedenen Konstellationen der Abwägung auftreten, wie dies im Rahmen der deutschen verfassungsrechtlichen Unterbringung geschieht, insbesondere die Abgrenzung von Meinungs- gegenüber Kunstfreiheit.

Als erheblicher „Nachteil" bzw. Besonderheit für den europäischen und deutschen Rechtsraum ist jedoch zu sagen, dass auch Beleidigungen ohne tatsächlichen Meinungscharakter von dem US-amerikanischen Grundrecht erfasst werden, sodass eine erheblich weitere Rechtfertigung möglich ist.

d) Der Effekt der Verwendung auf den potentiellen Markt oder den Wert des Ursprungswerks

Das vierte Kriterium der Fair-Use-Doctrine ähnelt zunächst dem neu durch die Verfassungsrechtsprechung identifizierten Schwerpunkt der wirtschaftlichen Betrachtung des

[61] *Peyton*, North Carolina Law Review 2018, 1085 (1119).
[62] „[go] to the heart" of the orignal. - Campbell, 510 U.S. at 586; *Brauneis*, Syracuse Law Review 2018, 7 (31 ff.).
[63] Eine schlichte und zutreffende Beschreibung der Besonderheit bei Parodien durch Campbell, 510 U.S. at 580, 581: "Parody needs to mimic an original to make its point, and so has some claim to use the creation of its victim's (or collective victims') imagination.

deutschen Urheberrechts. Auch hier wird die Frage aufgeworfen, ob durch die transformative Änderung ein ausreichend großer Abstand geschaffen wird, sodass das Referenzwerk nicht als Markt-Substitut für das Originalwerk fungiert und damit dem Originalkünstler wirtschaftlichen Schaden zufügen kann.[64] Allerdings kennt auch das hier das amerikanische System eine relevante Abgrenzung zwischen des „sich Anmaßens“ von wirtschaftlicher Nachfrage durch eine Copyright-Verletzung und der einfachen „Unterdrückung“ von wirtschaftlicher Nachfrage etwa durch eine kritische Kommentierung des Werks.[65] Während auch in der deutschen Rechtsprechung keine wirtschaftliche Gefahr durch Sampling gesehen wird, geht man in der US-amerikanischen Diskussion etwas weiter und geht sogar von einer wirtschaftlichen Begünstigung aus.[66]

III. Fazit: Abkehr von Originalität?

Sowohl die Fair-Use-Doctrine als auch die deutsche Verfassungsrechtsprechung halten weiterhin mit Blick auf die Intention des Urheberrechts eindeutig an dem Kriterium der Originalität fest, zumal sich auch keine passende oder praktikable Alternative bietet. Allerdings ergibt sich gerade im Zeitalter der modernen und digitalen Referenzkunst eine Neufindung der Zulässigkeit der Referenznutzung.

Die deutsche Abwägungslösung über Grundrechte ist an dieser Stelle besonders rechtsunsicher und ungeeignet, sodass sich an dem besser ausdefinierten Kriterienkatalog der Fair-Use-Doctrine orientiert werden sollte. Hierbei muss jedoch auch der Persönlichkeitsrechts-Charakter des Urheberrechts gewahrt werden, um der Ausgestaltung des deutschen zwei-teiligen Urheberrechts gerecht zu werden.

In Anbetracht dieser analytischen Ergebnisse scheint es zielführend, einen neuen „Fair-Use“-Paragraphen in das Urheberrecht einzuführen, welcher diese Ergebnisse berücksichtigt und folgende Form annehmen könnte:

[64] *Goetsch*, New England Law Review 1980, 39 (50 ff.); *Peyton*, North Carolina Law Review 2018, 1085 (1122).
[65] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 588 (1994) mit Bezug auf Fisher v. Dees, 794 F.2d 432, 438 (9th Cir. 1986).
[66] *Peyton*, North Carolina Law Review 2018, 1085 (1122); *Goetsch*, New England Law Review 1980, 39 (51 ff.).

§ 24 UrhG – Zulässige Referenz-Benutzung und Verwertung

(1) Ungeachtet anderer Vorschriften dieses Gesetzes ist die Benutzung und Verwertung von anderen Werken (Originalwerk) zulässig, wenn dies in einem referenziellen Rahmen (Referenzwerk), wie einer Parodie, Kritik, Kommentierung, Berichterstattung, Lehre und Forschung erfolgt und eine interessengerechte Benutzung erfolgt.

(2) Eine interessengerechte Benutzung ergibt sich aus der Abwägung der jeweiligen Interessen und der Art und Weise der Benutzung. Sie ist insbesondere unter der Berücksichtigung der folgenden Kriterien vorzunehmen:

   a. Sinn und Zweck der Benutzung, insbesondere das Maß an Transformation und die Absicht zur Kommerzialisierung.

   b. Gestalt und Kreativität des Originalwerks, wobei bei referenzieller Benutzung auch eine notwendige Nähe Gegenstand der Natur der referenziellen Kunst und somit unschädlich sein kann.

   c. Die Quantität und Bedeutung des Referenzteils im Verhältnis zum Gesamt-Originalwerk sowie die Bedeutung des Referenzteils für das Referenzwerk.

   d. Die Gefahr eines wirtschaftlichen Schadens für die Verwertung des Originalwerks durch Verdrängung von Marktanteilen durch das Referenzwerk.

   e. Die Gefahr einer unangemessenen Schädigung des ideellen Wertes des Originalwerks oder des Schöpfers.

Literaturverzeichnis

Ashtar, Reuven, Theft, Transformation, and the Need of the Immaterial: A Proposal for a Fair Use Digital Sampling Regime, Albany Law Journal of Science & Technology 2009, 263-283.

Bergmann/Dienelt (Hrsg.), Ausländerrecht – Kommentar, 12. Aufl. 2018, München.

Brauneis, Robert, Parodies, Photocopies, Recusals, and Alternate Copyright Histories: The Two Deadlocked Supreme Court Fair Use Cases, Syracuse Law Review 2018, 7-50.

Dreier, Thomas/Leistner, Matthias – Urheberrecht im Internet: die Forschungsherausforderungen, GRUR-Beilage 2014, 13-28.

Duhanic, Ines, Copy this Sound! The Cultural Importance of Sampling for Hip Hop Music in Copyright Law – A Copyright Law Analysis of the Sampling Decision of the German Federal Constitutional Court, GRUR Int. 2016, 1007-1017.

Epping /Hillgruber (Hrsg.), Grundgesetz – Beck’scher Online-Kommentar, 37. Edition, 2018, München.

Goetsch, Charles C., Parody as Free Speech – The Replacement of the Fair Use Doctrine by First Amendment Protection, New England Law Review 1980, 39-66.

Grünberger, Michael, Die Entwicklung des Urheberrechts im Jahr 2017 – Teil I, ZUM 2018, 271-285.

Grünberger, Michael, Die Entwicklung des Urheberrechts im Jahr 2017 – Teil I, ZUM 2018, 321-340.

Herzog/Scholz/Herdegen/Klein (Hrsg.), Grundgesetz – Kommentar, Bd. I Art. 1-5, 58. Ergänzungslieferung 2010, München (zitiert als Maunz/Dürig).

Jarass (Hrsg.), Charta der Grundrechte der Europäischen Union – Kommentar, 3. Aufl. 2016, München.

Johnson, A. Dean, Music Copyrights: The Need for an Appropriate Fair Use Analysis in Digital Sampling Infringement Suits, Florida State University Law Review 1993, 149-165.

Klass, Nadine, RE-USE: Kompilation, Parodie, Doku-Fiction – Rechtliche Rahmenbedingungen abhängigen Werkschaffens im Film, ZUM 2016, 801-804.

Leistner, Matthias, Die „Metall auf Metall“-Entscheidung des BVerfG – Oder: Warum das Urheberrecht in Karlsruhe in guten Händen ist, GRUR 2016, 772-777.

Miller, Peyton E., Good Artists Borrow; Great Artists Steal: How the Fair Use Doctrine Can Bring Harmony to the Federal Circuits on Digital Music Sampling, North Carolina Law Review 2018, 1085-1124.

Oglakczioglu, Mustafa Temmuz/Rückert, Christian, Anklage ohne Grund – Ehrschutz contra Kunstfreiheit am Beispiel des sogenannten Gangsta-Rap, ZUM 2015, 876-883.

Ohly, Ansgar, Hip Hop und die Zukunft der „freien Benutzung“ im EU-Urheberrecht – Anmerkungen zum Vorlagebeschluss des BGH „Metall auf Metall III“, GRUR 2017, 964-969.

Peifer, Karl N., Individualität im Zivilrecht, 2001.

Perloff, Marjorie, Unoriginal Genius – Poetry by other means in the new century, 2010.

Podszun, Rupprecht, Postmoderne Kreativität im Konflikt mit dem Urheberrechtsgesetz und die Annäherung an »fair use«, ZUM 2016, 606–612.

Podszun, Rupprecht, Wandlungen des Schutzgegenstandes in: Vom Magnettonband zu Social Media, Festschrift 50 Jahre Urheberrechtsgesetz, 2015, 361-371.

Samuelson, Pamela, Possible Futures of Fair Use, Washington Law Review 2015, 815-860.

Schonhofen, Sven, Sechs Urteile über zwei Sekunden, und kein Ende in Sicht: Die „Sampling"-Entscheidung des BVerfG, GRUR-Prax 2016, 277-279.

Wagner, Kristina, Sampling als Kunstform und die Interessen der Tonträgerhersteller – Auswirkungen der BVerfG-Rechtsprechung auf die Kunstfreiheit, MMR 2016, 513-518.

Subsumtionsautomaten der Zukunft?

Algorithmen und automatisierte Entscheidungen in der Justiz

Marc Bauer

Universität zu Köln
marc.bauer1@t-online.de

Abstract

Ist die menschliche Willkür der scheinbaren Objektivität eines Computerprogramms vorzuziehen? Nachdem das Verfassungsrecht nur einen groben Rahmen vorgibt und lediglich eine Privatisierung der Entscheidungsfindung sowie ein Letztentscheidungsrecht für Algorithmen verbietet, ist dies eine Frage der Rechtspolitik. Algorithmen sind nützliche Hilfsmittel, die die richterliche Tätigkeit unterstützen können und sollen. Eine menschliche, wertende Entscheidungsfindung im Einzelfall sollten sie aber nicht einschränken. Auf Beweisebene können sie wie herkömmliche Beweismittel eingeführt werden. Auf Ebene der Strafzumessung ist ihre Einführung als besonderes, standardisiertes Hilfsmittel für Prognoseentscheidungen empfehlenswert, dessen Einsatz aber den revisionsrechtlichen Maßstab nicht verändert. Bei Wertungsfragen hat ein Einsatz dagegen zu unterbleiben. In jedem Falle müssen die Algorithmen transparent und diskriminierungsfrei eingesetzt werden.

I. Einführung

Den Straftäter schon vor der Tat fassen: Was Steven Spielberg 2002 im Film Minority Report noch als scheinbare Utopie in ferner Zukunft (im Washington D.C. des Jahres 2054) darstellte, ist inzwischen mit Methoden des Predictive Policing, also der computergestützten, automatisierten Auswertung unterschiedlicher Daten zwecks Gewinnung von Wahrscheinlichkeitsaussagen über das Auftreten bestimmter Kriminalitätsformen in der Zukunft,[1] Realität. Gegenstand dieses Beitrags soll allerdings nicht der Einsatz modernster Technik in der Prävention, sondern der Repression sein. Auch hier sind Algorithmen, die anstatt von Menschen entscheiden, keine Science-Fiction mehr. In den USA gibt es bereits zahlreiche Anbieter solcher Prognoseprogramme, die den

[1] *Singelnstein*, NStZ 2018, 1 (1).

Gerichten die Rechtsfindung erleichtern sollen. Welche Bedeutung Algorithmen im deutschen Strafprozessrecht erlangen dürfen und sollten, wird im Folgenden aufgezeigt werden.

II. Tatrichterlicher Entscheidungsspielraum de lege lata

Coram iudice et in alto mari sumus in manu Dei.[2] Diese Juristenweisheit bezieht sich nicht nur auf die faktischen Unwägbarkeiten, die mit einem Prozess stets verbunden sind, sondern findet auch eine normative Grundlage.

1. Richterliches Ermessen bei der Beweiswürdigung

Über das Ergebnis der Beweisaufnahme entscheidet das Gericht nach seiner freien, aus dem Inbegriff der Verhandlung geschöpften Überzeugung, heißt es seit 1877 in der StPO, § 261.[3] In der lakonischen Sprache der Reichsjustizgesetze erteilt das Gesetz knapp eine Absage an gesetzliche Beweisregeln.[4] Wahrheit im strafprozessualen Sinne ist kein objektives, etwa aus Perspektive eines verständigen Dritten zu beurteilendes Faktum, sondern Ergebnis der inneren, subjektiven Überzeugung des Gerichts.[5] Das heißt zum einen, dass die richterliche Überzeugung auch hinreicht, wenn die Schlussfolgerungen unwahrscheinlich sind,[6] zum anderen, dass eine hohe Wahrscheinlichkeit die richterliche Überzeugung nicht zu ersetzen vermag.[7]

Der Tatrichter muss also keine absolute, das Gegenteil denknotwendig ausschließende Gewissheit haben. Vielmehr genügt ein nach der Lebenserfahrung ausreichendes Maß an Sicherheit, das vernünftige Zweifel nicht aufkommen lässt. Dabei haben solche Zweifel außer Betracht zu bleiben, die realer Anknüpfungspunkte entbehren und sich lediglich auf die Annahme einer theoretischen Möglichkeit gründen.[8] Die Revision ist auf die Nachprüfung beschränkt, ob der Tatrichter die von ihm festgestellten Tatsachen nicht unter allen für die Entscheidung wesentlichen Gesichtspunkten gewürdigt hat oder über schwerwiegende Verdachtsmomente ohne Erörterung hinweggegangen ist oder ob an die für eine Verurteilung erforderliche Gewissheit überspannte Anforderungen gestellt worden sind.[9]

[2] Vor Gericht und auf hoher See sind wir in Gottes Hand.
[3] Bei Inkrafttreten noch § 260 RStPO.
[4] Siehe nur *BGH*, Beschl. v. 19.08.1993, NJW 1993, 3081 (3082).
[5] Vgl. *Miebach*, in: MüKo StPO, § 261 Rn. 4
[6] *BGH*, Urt. v. 17.01.2001, NStZ 2001, 491 (492).
[7] *Miebach*, in: MüKo StPO, § 261 Rn. 52.
[8] *BGH*, Urt. v. 29.04.2015, BeckRS 2015, 15313 Tz. 10.
[9] *BGH*, Urt. v. 29.04.2015, BeckRS 2015, 15313 Tz. 9.

Im Rahmen der Beweiswürdigung ist es nicht ausgeschlossen, dass sich der Richter statistisch-mathematischer Methoden bedient, [10] die freilich auch in nachvollziehbarer Weise im Urteil dargestellt werden müssen.[11] Bedenklich ist jedoch das Hochrechnen von Verhaltensweisen aufgrund vorangegangenen Verhaltens.[12] Auch darf eine statistische Wahrscheinlichkeit allein eine weitere Beweiswürdigung nicht ersetzen,[13] anders freilich bei einem Seltenheitswert im Millionenbereich.[14]

Eine Grenze erreicht die tatrichterliche Überzeugungsbildung jedoch beim Außerachtlassen gesicherter Erfahrungssätze.[15] Gleiches gilt für die Zugrundelegung nicht begründbarer Erfahrungssätze, von dem das Tatgericht seine Überzeugung abhängig macht.[16] So hat der BGH die Erwägung des LG Berlin[17] zurückgewiesen, Fahrer bestimmter schwerer Automobile fühlten sich dort derart sicher, dass sie das Gefühl für eine mögliche Eigengefährdung ausblendeten.[18]

2. Richterliches Ermessen bei der Straffolgenfestsetzung

Im deutschen Strafprozess sind die Entscheidungen über die Schuldfrage, die entscheidend von der Beweiswürdigung (s.o. 1.) abhängt, und das Strafmaß weder personell[19] noch verfahrensmäßig[20] getrennt. Hieraus erwächst eine besondere starke Einflussmöglichkeit des Richters, da er durch die Bejahung oder Verneinung eines bestimmten Tatbestandes (bspw. Mord oder Totschlag) bereits erheblich das Strafmaß determiniert.

a) Wertungsspielräume des Tatrichters

Die Strafzumessung ist Sache des Tatgerichts.[21] In Zweifelsfällen hat das Revisionsgericht die Wertung des Tatgerichts hinzunehmen.[22]

[10] *BGH*, Urt. v. 14.12.1989, NJW 1990, 1549 (1551). *Eschelbach*, in: BeckOK StPO, § 261 Rn. 3.7 weist auf die erst unzulänglich einbezogene Wahrscheinlichkeitsforschung hin.
[11] *BGH*, Beschl. v.19. 01.2016, NStZ-RR, 118 (119).
[12] *BGH*, Urt. v. 14.12.1989, NJW 1990, 1549 (1550).
[13] *BGH*, Urt. v. 12.08.1992, NJW 1992, 2976 (2977).
[14] *BGH*, Beschl. v. 21.01.2009, NJW 2009, 1159.
[15] *Eschelbach*, in: BeckOK StPO, § 261 Rn. 3; *Miesbach*, in: MüKo StPO, §261 Rn. 90.
[16] *BGH*, Urt. v. 03.08.1982, NStZ 1982, 478 (479).
[17] *LG Berlin*, Urt. v. 27.02.2017, NStZ 2017, 471 (476).
[18] *BGH*, Urt. v. 01.03.2018, NJW 2018, 1621 (1623).
[19] So die Regelung im Deutschen Reich bis zur Emminger´schen Notverordnung v. 04.01.1924 (RGBl. I, S. 15): Geschworene entscheiden die Schuldfrage, die Berufsrichter über das Strafmaß (vgl. § 81 GVG idF v. 27.01.1877)
[20] So bspw. das US-amerikanische (Bundes-) Strafprozessrecht (vgl. Rule 32 of the Federal Rules of Criminal Procedure.
[21] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210.
[22] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210 (2211).

(1) Allgemeine Strafzumessung

§ 46 Abs. 1 Satz 1 StGB bestimmt die Schuld des Täters zum primären Maßstab für die Strafzumessung. Satz 2 ergänzt allerdings einen spezialpräventiv-resozialisierenden Blickwinkel; Absatz 2 zählt eine ganze Reihe von konkretisierenden Strafzumessungsgesichtspunkten auf, die teils auf die Tat, teils auf den Täter, teils objektiv, auf Tatschwere und -folgen sowie Vorleben des Täters, teils subjektiv auf die Gesinnung desselben bezogen sind. Ein Stufenverhältnis der Strafzwecke oder eine sonstige Halt gebenden Konkretisierung des Verhältnisses dieser zueinander existiert nicht und ist auch nicht von Verfassungswegen geboten.[23] Die rudimentäre Norm belässt dem Richter einen erheblichen Spielraum und sorgt auch nur unzureichend gegen mögliche psychologische Verzerrungen in der Person des Richters vor.[24] Eine mathematisch-schematisierende Strafzumessung ist gerade nicht vorgesehen und widerspräche der notwendigen Abwägung (vgl. § 46 Abs. 2 Satz 1).[25]

Eine ins Einzelne gehende Richtigkeitskontrolle ist ausgeschlossen; ein Urteil nur aufzuheben, wenn ein Rechtsfehler vorliegt, namentlich das Tatgericht von einem falschen Strafrahmen ausgegangen ist, seine Zumessungserwägungen in sich fehlerhaft sind oder rechtlich anerkannte Strafzwecke außer Acht lassen oder wenn sich die Strafe von ihrer Bestimmung, gerechter Schuldausgleich zu sein, soweit nach oben oder unten löst, dass ein grobes Missverhältnis von Schuld und Strafe offenkundig ist.[26]

Da § 267 Abs. 3 Satz 1 StPO lediglich die Angabe der für Strafe bestimmenden Gründe in den Urteilsgründen verlangt, erlaubt die Nichterwähnung eines Umstands nicht ohne weiteres den Schluss auf eine fehlende Berücksichtigung durch den Tatrichter, der unter Berücksichtigung der Besonderheiten des Einzelfalles entscheidet, was als wesentlicher Strafzumessungsgrund anzusehen ist.[27] Bewertungsrichtung und Gewicht dieser Strafzumessungstatsachen bestimmt in erster Linie das Tatgericht, dem hierbei von Rechts wegen ein weiter Entscheidungs- und Wertungsspielraum eröffnet ist.[28]

Für Steuerhinterziehung hat der BGH[29] ein 3-Stufen-Schema entwickelt, wonach bei einem sechsstelligen Hinterziehungsbetrag die Verhängung einer Geldstrafe nur bei Vorliegen von gewichtigen Milderungsgründen noch schuldangemessen sein kann. Bei Hinterziehungsbeträgen in Millionenhöhe kommt eine aussetzungsfähige Freiheitsstrafe nur bei Vorliegen besonders gewichtiger Milderungsgründe in Betracht. Eine Über-

[23] *BVerfG*, Urt. v. 21.06.1977, NJW 1977, 1525 (1531).
[24] Vgl. *Miebach/Meier*, in: MüKo StGB, § 46 Rn. 4.
[25] *BGH*, Urt. v. 21.02.2006, NJW 2006, 270 (271); *Miebach/Meier*, in: MüKo StGB, § 46 Rn. 88.
[26] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210.
[27] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210 (2211).
[28] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210 (2211).
[29] *BGH*, Urt. v. 02.12.2008, NJW 2009, 528 (532).

tragung dieser Grundsätze auf andere Delikte nicht möglich, auch nicht auf Untreue.[30] Im Einzelfall kann eine Verhängung von Geldstrafe ausgeschlossen sein.[31] Im Übrigen verbleibt es aber bei den aufzeigten Spielräumen für den Tatrichter.

(2) Strafrahmen

Zunächst ist festzustellen, dass schon die Strafrahmen dem Richter einen weiten Spielraum lassen. Ein typischer Rahmen ist Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe,[32] mit anderen Worten (das System der Ersatzfreiheitsstrafen berücksichtigend) fünf[33] Tage bis fünf Jahre. Das Höchstmaß liegt also beim 365-fachen des Mindeststrafrahmens, selbst beim Mindestmaß der Freiheitsstrafe (ein Monat, § 38 Abs. 2 StGB) noch beim 60-fachen. Ein anderer typischer Strafrahmen bei Verbrechen ist ein bis 15 Jahre Haft.[34]

Dieser Spielraum wird noch erheblich erweitert durch die unbenannten minder schweren sowie besonders schweren Fälle, sowie durch weder abschließende noch zwingende Regelbeispiele. Die Regelbeispielstechnik führt bspw. beim Diebstahl zu einer Verdopplung der Höchststrafe auf zehn Jahre (§ 243 Abs. 1 Satz 1 StGB), der unbenannte besonders schwere Fall des sexuellen Missbrauchs von Kindern (§ 176 Abs. 3 StGB) zu einem Strafrahmen von einem Jahr bis zu 15 Jahren statt von sechs Monaten bis zu zehn Jahren. Unbenannte minder schwere Fälle führen in den Fällen der §§ 154 Abs. 2, 226a Abs. 2 StGB zu einer um die Hälfte ermäßigten Mindest- und einer um zwei Drittel gekürzten Höchststrafe.

Im Falle der Strafmilderung gemäß § 49 Abs. 1 StGB wird der Strafrahmen auch relativ breiter; während die Höchststrafe bei zeitiger Freiheitsstrafe um lediglich ein Viertel sinkt (§ 49 Abs. 1 Nr. 2 StGB), wird die Mindeststrafe um bis zu fünf Sechstel gesenkt (§ 49 Abs. 1 Nr. 3 Var. 2 und 4 StGB).

Zudem entscheidet der Richter darüber, ob er Strafen von nicht mehr als einem Jahr bzw. Gesamtstrafen von nicht mehr als zwei Jahren als Geld- oder Freiheitsstrafe ausgestaltet (§ 40 Abs. 1 Satz 2 i.V.m. § 54 Abs 2 Satz 2 StGB). Während bei Strafen von unter sechs Monaten ein gesetzlicher Vorrang der Geldstrafe gilt (§ 47 StGB) und bei Strafen von unter einem Monat nur Geldstrafe möglich ist (§ 38 Abs. 2 StGB), ist er für den Bereich von sechs Monaten bis zu einem Jahr, bei Gesamtstrafe auch zweien, nur durch allgemeine Strafzumessungserwägungen gebunden.

[30] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210 (2212).
[31] *BGH*, Beschl. v. 16.04.2008, NJW 2008, 2057 zu § 353b StGB.
[32] §§ 223, 242, 263, 266 StGB.
[33] § 40 Abs. 1 Satz 2 StGB.
[34] §§ 146 Abs. 1, 154 Abs. 1, 226a, Abs. 1, 249 Abs. 1 StGB.

(3) Bewährung

Die Entscheidung über die Strafaussetzung zur Bewährung kann der Tatrichter schon dadurch determinieren, dass er eine Strafe von (auch knapp) über zwei Jahre verhängt. Auch wenn eine bewusste Vermeidung der Bewährungsentscheidung durch die Strafhöhe unzulässig ist,[35] lässt sich dies, sofern nicht ausdrücklich erwähnt, auch kaum nachweisen. Gleiches gilt für die bewusst niedrige Ansetzung des Strafmaßes, um noch Bewährung verhängen zu können.[36] Auch soweit eine Aussetzungsentscheidung zu treffen ist, ist sie grundsätzlich Sache des Tatrichters.[37]

Ab einer Freiheitstrafe von sechs Monaten ist zu prüfen, ob die Verteidigung der Rechtsordnung Strafaussetzung zur Bewährung entgegensteht (§ 56 Abs. 3 StGB), wenn sie also für das allgemeine Rechtsempfinden unverständlich erscheinen müsste und dadurch das Vertrauen der Bevölkerung in die Unverbrüchlichkeit des Rechts erschüttert und von der Allgemeinheit als ungerechtfertigtes Zurückweichen vor der Kriminalität angesehen werden könnte.[38] Der BGH verlangt insofern eine allseitige Würdigung von Tat und Täter.[39] Dabei hat das Tatgericht auch eine Häufung von gleichartigen Taten zu berücksichtigen.[40] Andererseits ist eine ausdrückliche Erörterung nicht erforderlich, wenn die aus dem Urteil ersichtlichen Tatsachen dies nahelegen.[41] Dies ist nicht nötig im Falle einer umfassenden und sorgfältigen Würdigung der Taten und der Täterpersönlichkeiten sowie der zahlreicher festgestellten Strafmilderungsgründe.[42]Eine demoskopische Untermauerung dieses generalpräventiven Kriteriums ist nicht üblich und auch nicht erforderlich.[43]

Ab einer Freiheitsstrafe von mehr als einem Jahr ist zusätzlich zu prüfen, ob besondere Umstände die Strafaussetzung rechtfertigen (§ 56 Abs. 2 StGB). Dieses Kriterium erweist sich als nahezu völlig offen.[44] Eine erschöpfende Darlegung aller Erwägungen ist weder möglich noch geboten; nachprüfbar darzulegen sind lediglich die wesentlichen Umstände. Die Entscheidung steht im pflichtgemäßen Ermessen des Tatrichters; seine ganz maßgeblich auf dem in der Hauptverhandlung gewonnenen persönlichen Eindruck beruhende Wertungen sind bis zur Grenze des Vertretbaren zu respektie-

[35] *Groß*, in: MüKo StGB, § 56 Rn. 11, der umgekehrt die Ermöglichung einer Bewährungsentscheidung durch Kombination von Geld- und Freiheitsstrafe für möglich hält.
[36] Ein „Mitberücksichtigen“ soll indes auch nicht rechtsfehlerhaft sein, *BGH*, Urt. v. 13.12.2001, wistra 2002, 137.
[37] *BGH*, Urt. v. 06.07.2017, NJW 2017, 3011 (3012).
[38] *BGH*, Urt. v. 06.07.2017, NJW 2017, 3011 (3013).
[39] *BGH*, Urt. v. 06.07.2017, NJW 2017, 3011 (3013).
[40] *BGH*, Urt. v. 06.07.2017, NJW 2017, 3011 (3013).
[41] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210 (2213).
[42] *BGH*, Urt. v. 14.03.2018, NJW 2018, 2210 (2213).
[43] *Groß*, in: MüKo StGB, § 56 Rn. 58.
[44] *Groß*, in: MüKo StGB, § 56 Rn. 43. Bezeichnend ist die schlichte Bejahung im Fall Sal. Oppenheim, *BGH*, Urt. v. 14. 03. 2018, NJW 2018, 2210 (2212).

ren.[45] Rechtsfehlerhaft ist, wenn keine über die Legalprognose hinausgehenden Gründe angeführt werden.[46] Ebenso, wenn der Tatsachen nicht berücksichtigt bleiben, wie etwa der Charakter eines illegalen Straßenrennens als bewusste Gefahrschaffung; ein solcher Umstand gibt der Tat ihr Gepräge und darf nicht unberücksichtigt bleiben.[47] Gleichwohl zeigt die Praxis eine geringe Filterwirkung: So wurden 2016 66,1% aller Freiheitsstrafen von mehr als einem Jahr bis zu zwei Jahre zur Bewährung ausgesetzt. Im Bereich 7-9 Monate lag der Anteil bei 78%, bei 10-12 Monate bei 76,7%.[48] Die Nichtaussetzung der Freiheitsstrafe ist die Ausnahme, nicht die Regel, die „besonderen Umstände" werden also faktisch als gewöhnliche Umstände gedeutet. Nicht nur die Häufigkeit der Strafaussetzung an sich, sondern auch der geringe Abstand zu den Bewährungsquoten bei niedrigerer Strafhöhe deuten darauf hin, dass das gesetzliche Stufenmodell unterlaufen wird.

b) Prognoseentscheidungen

Während das geltende Strafrecht die Strafzumessung weitgehend dem richterlichen Ermessen und damit seiner wertenden Betrachtung überlässt, kennt das Gesetz auch Rechtsfragen, bei welchen es einen eher empirisch-prognostischen Ansatz wählt.[49]

So verlangt § 56 Abs. 1 Satz 1 eine positive Legalprognose als Mindestbedingung für die Strafaussetzung zur Bewährung. Diese ist zu stellen, wenn nach allgemeiner forensischer Erfahrung[50] die Wahrscheinlichkeit künftigen straffreien Verhaltens größer ist als diejenige neuer Straftaten.[51] Da der Tatrichter im Regelfall über eigene Sachkunde verfügt,[52] sind Sachverständige nur ausnahmsweise heranzuziehen; so bei der Reststrafenaussetzung (§ 57 Abs. 1 Satz 1 Nr. 2 StGB) in den Fällen des § 454 Abs. 2 StPO. Dies gilt nur dann nicht, wenn zweifelsfrei der Schluss auf die fehlende Gefahr erlaubt ist[53] oder umgekehrt eine Aussetzung aussichtlos erscheint.[54]

Die Einweisung in ein psychiatrisches Krankenhaus (§ 63 StGB) sowie die Sicherungsverwahrung (§ 66 StGB) setzen eine Prognoseentscheidung voraus, die gemäß § 246a StPO der Hinzuziehung eines Sachverständigen bedarf.

---

[45] *BGH*, Urt. v. 06.07.2017, NJW 2017, 3011 (3012).
[46] *BGH*, Urt. v. 06.07.2017, NJW 2017, 3011 (3012 f.).
[47] *BGH*, Urt. v. 06.07.2017, NJW 2017, 3011 (3013).
[48] So wurden 2016 9609 von 14547 Freiheitsstrafen von 13 Monaten bis Jahre ausgesetzt, 9894 von 12908 Freiheitstrafen von 10 bis 12 Monate, 11824 von 15161 Freiheitsstrafen von 7 bis 9 Monate. Zahlen nach: *Statistisches Bundesamt*, Strafverfolgung, Fachserie 10, Reihe 3 – 2016, S. 160 f.
[49] Vgl. S*ingelnstein*, NStZ 2018, 1 (3).
[50] *Groß*, in: MüKo StGB, § 56 Rn. 24.
[51] So der BGH in st. Rspr., siehe etwa *BGH*, Beschl. v. 13.08.1997, NStZ 1997, 594.
[52] *Groß*, in: MüKo StGB, § 56 Rn. 58; *v. Heintschel-Heinegg*, in: BeckOK StGB, § 56 Rn. 39.
[53] *OLG Frankfurt a.M.*, Beschl. v. 10.07.1998, NStZ 1998, 639 (640).
[54] *v. Heintschel-Heinegg*, in: BeckOK StGB, § 57 Rn. 15.

Auch die Anordnung von Untersuchungshaft wegen Fluchtgefahr (§ 112 Abs. 2 Nr. 2 StPO) setzt eine Einschätzung der Wahrscheinlichkeit voraus, dass sich der Beschuldigte dem Verfahren entziehen werde.[55] Von Verfassungswegen ist hier ein eine intensive Auseinandersetzung mit dem Einzelfall erforderlich,[56] auch unter Berücksichtigung kriminalistischer Erfahrungen.[57]

c) Fazit

Die Festsetzung der Rechtsfolgen der Tat ist weitestgehend dem Ermessen des Tatrichters überlassen. Lediglich bei einzelnen Rechtsfragen wählt das Gesetz einen mehr empirisch-prognostischen Ansatz, ohne ihn allerdings stets verfahrensmäßig abzusichern.

III. Algorithmen

1. Technische Möglichkeiten

a) Bedeutung von Algorithmen

Moderne Technik verändert alle Lebensbereiche, nicht nur Alltag und Wirtschaft, sondern auch politische Handlungsspielräume und rechtliche Normierungsmöglichkeiten. Das Problem der Zurückdrängung tradierter Rechtsetzungsmacht durch technische (vermeintlich unpolitische) Normsetzung und einer drohenden Irrelevanz des Rechts wird für die Rechtswissenschaften zum bereichsübergreifenden Problem.[58]

Wichtiges Element der fortschreitenden Digitalisierung ist der Einsatz von Algorithmen, also von Rechenvorschriften, die derart formuliert sind, dass ihre Ausführung z.B. durch Computerprogramme möglich ist; dabei ermöglicht der Algorithmus einen Output, der aus dem seiner Rechenregeln gemäßen Verarbeitung von Rohdaten (Input) besteht.[59]

b) Konkreter Einsatz

(1) Einsatz in der deutschen Verwaltung

Technische Hilfsmittel zum Erlass von Verwaltungsakten setzt die öffentliche Verwaltung seit langem ein.[60] Dies hat auch der Gesetzgeber schon frühzeitig mitberücksichtigt.[61] Durch den zum 01.01.2017 in Kraft getretenen § 35a VwVfG[62] ist der Gesetzge-

[55] *Böhm/Werner*, in: MüKo StPO, § 112 Rn. 41.
[56] Dazu *BVerfG*, Beschl. v. 25.06.2018, BeckRS 2018, 14020 Tz. 34.
[57] *Graf*, in: Karlsruher Kommentar StPO, § 112 Rn. 16.
[58] Vgl. *Boehme-Neßler*, NJW 2017, 3030 (3031) und passim.
[59] Vgl. *Kastl*, GRUR 2015, 136 (136).
[60] *Prell*, in: BeckOK VwVfG, § 35a Rn. 2.
[61] Vgl. § 37 Abs. 4 VwVfG idF v. 25. 05. 1976.
[62] Durch Art. 20 Nr. 3 des Gesetzes zur Modernisierung des Besteuerungsverfahrens v. 18.07.2016, BGBl. I S. 1679.

ber einen Schritt weiter gegangen[63] und erlaubt den vollständig automatisierten Erlass eines Verwaltungsakts, sofern dies durch Rechtsvorschrift vorgesehen ist und weder ein Beurteilungs- noch ein Ermessensspielraum besteht.§ 35a VwVfG setzt nicht nur für vollautomatisierte Verwaltungsakte eine Grenze, sondern nach Sinn und Zweck auch für solche, bei denen lediglich die Bekanntgabe nicht vollständig automatisiert ist.[64] Umstritten ist der Einsatz selbstlernender (indeterminierter) Software.[65] Faktisch ist der Einsatz im Steuerrecht schon weit fortgeschritten.[66] Rechtsfragen der Automatisierung sind also keine rechtspolitischen Desiderate mehr, sondern solche des geltenden Rechts. Gleichwohl bedeutete ihr Einsatz im Strafrecht aktuell noch eine präzedenzlose Nutzbarmachung von Algorithmen, für die es an einer abschließenden Bewertung fehlt.

(2) Einsatz im US-Strafrecht

Vorreiter auf dem Gebiet sind die USA, wo die Nutzung solcher Systeme auch zur Forderung von Bürgerrechtlern gehörte.[67] Beispielhaft ist das System „COMPAS".[68] Die Nutzung stößt auch auf zum Teil heftige Kritik,[69] während die Gerichte bisher in seinem Einsatz keinen Rechtsverstoß gesehen haben.[70] Zugleich belegt der praktische Einsatz die Notwendigkeit, schon frühzeitig in Deutschland eine rechtspolitische Debatte darüber zu führen, ob und in welchen Grenzen eine solche Technologie auch in unseren Strafprozess inkorporiert werden soll.

2. Zulässigkeit des Einsatzes

a) Verstoß gegen das allgemeine Persönlichkeitsrecht?

Dem Einsatz von Algorithmen könnte entgegenhalten werden, er entwerte den Menschen zum bloßen Objekt eines technischen Auswertungsvorgangs, zu einem auslesbaren Datensatz. In Bezug auf den Polygraphen hatte der BGH unter Verweis auf Art. 1 GG, entschieden, ein solcher Einblick in die Seele des Beschuldigten und ihre unbewussten Regungen verletze die von § 136a StPO geschützte Freiheit der Willensent-

[63] Kritisch *Ahrendt*, NJW 2017, 537 (540).
[64] *Prell*, in: BeckOK VwVfG, § 35a Rn. 3.
[65] *Stelkens*, in: Bonk/Sachs/Stelkens VwVfG, § 35a Rn. 47.
[66] Dazu kritisch *Ahrendt*, NJW 2017, 537 (539).
[67] Siehe den von der ACLU (American Civil Liberties Union) herausgegebenen Forderungskatalog „Smart reform is possible. States Reducing Incarceration Rates and Costs While Protecting Communities", https://www.aclu.org/files/assets/smartreformispossible.pdf, S. 9 (zuletzt abgerufen am 16.08.2018).
[68] COMPAS steht für „Correctional Offender Management Profiling for Alternative Sanctions".
[69] Vgl. das Interview mit dem US-Kriminologen Barry Krisberg, http://www.taz.de/!5244806/ (zuletzt abgerufen am 15.08.2018) sowie https://www.zeit.de/gesellschaft/zeitgeschehen/2016-06/algorithmen-rassismus-straftaeter-usa-justiz-aclu (zuletzt abgerufen am 16.08.2018).
[70] Siehe das Urteil des Supreme Court of Wisconcin v. 13.07.2016, Az. 2015AP157-C, http://www.scotusblog.com/wp-content/uploads/2017/02/16-6387-op-bel-wis.pdf (zuletzt abgerufen am 16.08.2018). Der United States Supreme Court hat diesen Fall nicht zur Entscheidung angenommen, https://www.supremecourt.gov/docketfiles/16-6387.htm (zuletzt abgerufen am 16.08.2018).

schließung und -betätigung und sei im Strafverfahren unzulässig.[71] Im Anschluss daran hat das BVerfG eine derartige Durchleuchtung der Person, welche die Aussage als deren ureigene Leistung entwerte und den Untersuchten zu einem bloßen Anhängsel eines Apparates werden ließe, als Verletzung des Allgemeinen Persönlichkeitsrechts gesehen, das der Wahrheitserforschung im Strafverfahren Grenzen setze.[72] Davon ist der BGH jedoch für den Fall des Einverständnisses des Angeklagten abgerückt und sieht den Polygraphen nur noch als völlig ungeeignetes Beweismittel i.S.d. § 244 Abs. 3 Satz 2 Var. 4 StPO.[73]Selbst nach der früheren Beurteilung des Polygraphen ist hier eine Analogie abzulehnen. Der Algorithmus verarbeitet lediglich Daten, die auch dem Richter zur Verfügung stehen, und die, ob unbewusst oder nicht, durch diesen verarbeitet würden. Tatsächlich kann der Algorithmus sogar wesentlich weniger intensiv die Persönlichkeit durchleuchten als etwa ein Sachverständiger. Insofern kann der Algorithmus nicht eingriffsintensiver sein als etwa eine psychiatrische Untersuchung oder die Behandlungsuntersuchung nach § 9 Abs. 1 StVollG NRW. Ein pauschalisierendes Verbot lässt sich nicht aus dem allgemeinen Persönlichkeitsrecht herleiten.

b) Grenzen eines möglichen Einsatzes

(1) Direkter Einfluss Privater

In der Strafrechtspflege als einem Kernbereich[74] hoheitlichen Handelns ist eine Privatisierung besonders kritisch zu sehen.[75] Eine Ersetzung gesetzesgebundener, demokratisch legitimierter Entscheidungen durch einen geheimen, privaten Algorithmus, der gleichsam neben und vor die einschlägigen Normen des StGB und StPO träte, berührte das Demokratieprinzip und das Gebot der Rechtsklarheit[76] als Ausfluss des Rechtsstaatsprinzips. Letztlich erscheint ein Mitwirken Privater am Ausgang des Strafverfahrens als verfassungswidrig, sofern er nicht auf eine technische Unterstützung ohne eigene Wertungsspielräume begrenzt wird und sich in dem Rahmen hält, der durch tradierte Formen der Mitwirkung Privater wie das Sachverständigengutachten vorgezeichnet ist.

[71] *BGH*, Urt. v. 16.02.1954, NJW 1954, 649 (650).
[72] *BVerfG*, Beschl. v. 18.08.1981, NStZ 1981, 446 (447).
[73] *BGH*, Urt. v. 17.12.1998, NJW 1999, 657 (658).
[74] Vgl. *BVerfG*, Urt. v. 30.06.2009, NJW 2009, 2267 (2287): „Die Sicherung des Rechtsfriedens in Gestalt der Strafrechtspflege ist seit jeher eine zentrale Aufgabe staatlicher Gewalt. Bei der Aufgabe, ein geordnetes menschliches Zusammenleben durch Schutz der elementaren Werte des Gemeinschaftslebens auf der Grundlage einer Rechtsordnung zu schaffen, zu sichern und durchzusetzen, ist das Strafrecht ein unverzichtbares Element zur Sicherung der Unverbrüchlichkeit dieser Rechtsordnung."
[75] Vgl. zur notwendigen Differenzierung des Legitimationsniveaus *Grzeszick*, in: Maunz/Dürig, Art. 20 II Rn. 222.
[76] Ein nach privatem Ermessen abänderlicher Algorithmus böte keine Verlässlichkeit der Rechtsordnung mehr, vgl. *Grzeszick*, in: Maunz/Dürig, Art. 20 VII Rn. 50.

(2) Determinierung

Fraglich ist, in welchem Ausmaß die Entscheidungsfreiheit des Richters durch das Rechenergebnis eines Computerprogramms eingeschränkt werden darf. Die Verpflichtung des Richters zu einem von fremden Wertungen freien, von seiner persönlichen Überzeugung getragenen Urteil bindet als zunächst einfaches Recht nicht den Reformgesetzgeber.[77]

Europarechtlich ist hier Art. 22 DSGVO in den Blick zu nehmen. Art. 22 Abs. 1 verbietet vollautomatische Entscheidungen mit rechtserheblicher Wirkung gegen den Willen des Betroffenen. Es folgt ein Ausnahmenkatalog (Art. 22 Abs. 2), der unter besonderen Kautelen doch eine Vollautomatisierung erlaubt, sowie eine Rückausnahme für besondere Kategorien von Daten und wiederum eine Ausnahme von dem Verbot für diese Datenverarbeitungen (Art. 22 Abs. 4). Eine direkte Umwandlung des Ergebnisses des Algorithmus, etwa in einen Strafausspruch ohne Korrekturmöglichkeit[78] durch einen Menschen wäre tatbestandlich erfasst.

Rspr. des EGMR zur Vollautomatisierung von Verwaltungsakten existiert nicht, allerdings kann die bloße Vollautomatisierung weder materielle noch verfahrensmäßige Standards herabsetzen.[79]

Schon bei Schaffung des VwVfG[80] hat der Gesetzgeber rechtstaatliche Bedenken gegen Automatisierung gehegt und diese nur dort für zulässig erachtet, wo „keinerlei verantwortliche Wertung“ mehr erforderlich ist.[81] Fraglich ist allerdings, ob das Gebot der Einzelfallgerechtigkeit sowie das Schuldprinzip[82] gerade die Entscheidung eines Menschen fordern, oder auch einer elektronischen Entität, einer KI, zuließe. Gegenstand der hier vorliegenden Arbeit sind allerdings „bloße” Algorithmen, die unzweifelhaft keine eigene Wertungsmöglichkeit besitzen. Insofern kann diese Frage hier offenbleiben. Ein Verzicht auf einen wertenden Akt ist in der Rechtsprechung allerdings wohl schon durch Art. 92 GG ausgeschlossen, der, anders als in den Vorschriften über die Verwaltung, mit den Richtern ausdrücklich menschliche Träger der Hoheitsgewalt nennt, und die eigentliche Rechtsfindung exklusiv ihnen zuweist.[83]

[77] *Miebach*, in: MüKo StPO, § 261 Rn. 54 f; *Eschelbach*, in: BeckOK stopp, § 261 Rn. 2.
[78] Bloßes Übersetzen der Entscheidung durch einen Sachwalter in einen Verwaltungsakt genügt nicht, *v. Lewinski*, in: BeckOK DatenschutzR DS-GVO, Art. 22 Rn. 25.
[79] *Stelkens*, in: Bonk/Sachs/Stelkens VwVfG, § 35a Rn. 58.
[80] v. 25.05.1976, BGBl. I, S. 1253.
[81] BT-Drs. 07/910, S. 59. So auch *Binder*, NVwZ 2016, 960 (963), allerdings ohne Anlegen verfassungsrechtlicher Maßstäbe.
[82] Als Teil des Rechtsstaatsprinzips, *Grzeszick*, in: Maunz/Dürig, Art. 20 VII Rn. 124.
[83] Vgl. hierzu *Hillgruber*, in: Maunz/Dürig, Art. 92 Rn. 75.

c) Fazit: Grundsätzlich zulässig

Der Einsatz von Algorithmen ist jedenfalls zulässig, sofern diese keine vollständige Determinierung des Strafverfahrens bewirken und keine über die tradierten Formen hinausgehende Einbindung Privater mit sich bringen.

IV. Grundsatzentscheidung für Algorithmen

Wesentliches Argument für den Einsatz von Algorithmen ist die dadurch entstehende Objektivität, die die selbst rechtsstaatlich bedenkliche Weite des richterlichen Spielraums einhegen könnte. Die tatrichterliche Entscheidungsgewalt bei der Strafzumessung ist korrekturbedürftig, gefährdet sie doch eine gleichmäßige und sachgerechte Spruchpraxis. Zudem bedeutet die Verwendung von Algorithmen bei der Beweiswürdigung nicht mehr als die Fortschreibung des auch bisher üblichen Einsatzes empirisch-statistischer und prognostischer Methoden (s. o. II. 1. und 2. b)). Als eine Ergänzung, nicht eine Ersetzung anderer Erkenntnismethoden bieten Algorithmen eine sinnvolle Alternative. Allerdings ist das Vertrauen auf die Erfahrung und Urteilskraft der im Einzelfall rechtssprechenden Richter eine tragende Säule des Rechtsstaats. Als zu groß empfundene Wertungsspielräume sollten eher durch materielle Korrekturen eingehegt werden. Algorithmen sind daher nur unter Wahrung klarer Kautelen und möglichst schonend in das tradierte System des Strafverfahrens einzufügen.

V. Ausgestaltung des Algorithmeneinsatzes

1. Beweiswürdigung

Auf Beweisebene ist eine Einbeziehung von Algorithmen in verallgemeinernder Form schon technisch schwer vorstellbar. Vielmehr können diese bei einzelnen Fragen eine Rolle fragen, insbesondere dort, wo schon heute Sachverständigengutachten, also statistische, mathematische, empirische Erkenntnisse, einfließen. Über diese können dann auch Erkenntnisse von Algorithmen in die Verhandlung eingeführt werden. Einer gesetzlichen Neuerung bedarf es hierzu nicht, allenfalls klarstellender Regelungen für die Sachverständigen und je nach Lebenssachverhalt Regularien für datenschutzsensible oder potenziell diskriminierende (s. u. 5.) Algorithmen. An der freien Beweiswürdigung oder dem Revisionsmaßstab ergeben sich keine Änderungen. Denn so wichtig die Einbeziehung rational-wissenschaftlicher Erkenntnisse ist, so sinnvoll ist auch der Grundsatz der freien Beweiswürdigung und die Aufgabenverteilung zwischen Tatgericht und Revision, die Spielräume wirksam begrenzt (s.o. II. 1.).

2. Straffolgenfestsetzung

a) Prognoseentscheidungen

Im Bereich der Strafzumessung ist zu konstatieren, dass der Gesetzgeber manche Strafzumessungserwägung bewusst von der freien Würdigung durch den Richter (oder der Anstaltsleitung) lösen, vielmehr wissenschaftlich-prognostischen Kriterien unterstellen will (s. o. II. 2. b)). Dies gilt für die Sozialprognose bei Bewährungsentscheidungen (§§ 56 Abs. 1, 57 Abs. 1 StGB, auch i.V.m. 57a Abs. 1 StGB), für die Fluchtgefahr (§ 112 Abs. 2 Nr. 2 StPO), für den Bereich der Maßregeln der Sicherung und Besserung (§§ 80a, 246a, 275a Abs. 4 StPO) sowie für Vollzugsentscheidungen im Strafvollzug (insb. die der Anordnung des offenen Vollzuges, § 10 Abs. 1, oder von Vollzugslockerungen, § 11 Abs. 2, auch i.V.m. § 13 Abs. 1 Satz 1 StVollG NRW). Überall dort sind Algorithmen eine sinnvolle Ergänzung.

b) Wertungsentscheidungen

Bei Wertungsentscheidungen sollte die Berücksichtigung von Algorithmen unterbleiben, insbesondere beim Strafmaß.[84] Aus der Strafzumessung lassen sich keine rein spezial- oder generalpräventiven Strafquanten lösen, die isoliert zugemessen werden könnten (siehe oben II. 2. a)). Bestehende Bedenken gegen den Spielraum des Tatrichters sind

c) Implementierung

(1) Phase eins: Testphase

Für den Einsatz eines solchen Algorithmus, der zunächst nur zu Testzwecken ohne Anwendung an den Gerichten parallel zu diesen Prognosen abgibt, bedarf es umfangreicher Datenerhebungen. In anonymisierter Form werden Daten der Betroffenen erhoben, und die Prognosen des Programms dann wiederum mit der tatsächlichen Entwicklung der Betroffenen abgeglichen. Beispielhaft, von allen Beschuldigten, gegen die ein Haftbefehl wegen Fluchtgefahr beantragt wird, werden Daten gesammelt, die der Haftrichter auch auswertet, und dann nachgehalten, wer sich tatsächlich dem Verfahren entzieht. Sukzessive führt dies zu einer steigenden Genauigkeit des zunächst aus kriminologischen Hypothesen gespeisten Algorithmus.[85]

(2) Phase zwei: Fakultativer Einsatz

Sind die Ergebnisse der Testphase zufriedenstellend, wird ihre Anwendung den Gerichten freigestellt. Entscheidet sich das Gericht für eine Auswertung des Algorithmus,

[84] So auch die offizielle Empfehlung für COMPAS, siehe hierzu das Urteil des Supreme Court of Wisconcin v. 13.07.2016, Az. 2015AP157-C, http://www.scotusblog.com/wp-content/uploads/2017/02/16-6387-op-bel-wis.pdf, S. 8 (zuletzt abgerufen am 16.08.2018).
[85] So auch *Singelnstein*, NStZ 2018, 1 (3) für Predictive-Policing-Algorithmen.

würde dann ein Justizbeamter die Auswertung der Software als Sachverständiger in den Prozess einführen. Der Richter wird damit in seiner Willensbildung nicht anders beeinflusst als durch Sachverständige bisher, und die formale Struktur des Prozesses unangetastet. Eine direkte Bedienung durch den Richter ist daher abzulehnen.

Die Freischaltung des Algorithmus sollte schrittweise erfolgen. Die massenhaft erfolgenden U-Haft-, Bewährungs- und Vollzugsentscheidungen sind hier schneller analysierbar als die seltener anfallenden über die Sicherungsverwahrung und die Einweisung in ein psychiatrisches Krankenhaus. In letzteren Fällen bestehen stärkere Bedenken gegen mathematische Verfahren.[86] Ihr fakultativer Einsatz kann daher u.U. auch erst ermöglicht werden, wenn bei den anderen Entscheidungen schon Phase drei initiiert ist.

(3) Phase drei: Obligatorischer Einsatz

Erweist sich der Algorithmus in einer Langzeituntersuchung als signifikant treffsicherer als andere Prognosemethoden, ist er zwingend beizuziehen. Dabei hat er das gleiche Gewicht wie andere Sachverständigengutachten.

d) Wissenschaftliche Begleitung

Die Erkenntnisse, die aus dem Einsatz des Algorithmus entstehen, sollen auch der Wissenschaft zur Verfügung gestellt werden, sodass Kriminologie und psychiatrische Begutachtungspraxis davon profitieren.

Welche Merkmale aufgezeichnet und von dem Algorithmus verwertet werden, ist eine Frage, für die ein Expertengremium zu berufen ist. Die zu erhebenden Daten sind gesetzlich auf die Empfehlung dieses Gremiums hin zu regeln. Im Laufe der Zeit sollte hierbei eine Erweiterung erfolgen, um den Algorithmus treffsicherer zu machen.

3. Nachvollziehbarkeit

Zur Wahrung der Legitimität[87] staatlichen (s.o. III. 2. b) (1)) Strafens sind die einzusetzenden Algorithmen nachvollziehbar zu gestalten.[88] Private können für die Konstruktion eingesetzt werden, der Staat sollte aber keinesfalls eine privat betriebene Software lizensieren müssen oder gar fallbasiert nutzen.[89]So wird auch vermieden, dass die (freilich anonymisierten) Daten unsachgemäß genutzt werden, was einen Verstoß gegen das Datenschutzrecht bedeuten könnte.

[86] Vgl. *BGH*, Beschluss vom 17.02.2016, BeckRS 2016, 07672 Tz. 15.
[87] Die sich entscheidend aus der prinzipiellen Öffentlichkeit allen staatlichen Handelns speist; vgl. *Grzeszick*, in: Maunz/Dürig, Art. 20 II Rn. 24.
[88] So auch nachdrücklich S*ingelnstein*, NStZ 2018, 1 (7).
[89] Z.B. COMPAS, bei dem die Herstellerfirma auch keine näheren Angaben zum Algorithmus erteilt. Siehe hierzu auch https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html (zuletzt abgerufen am 16.08.2018).

Die für die Softwarepflege zuständige Behörde bedarf stetiger Evaluation und Kontrolle, um Fehler im System rechtzeitig erkennen zu können.

4. Keine Handlungsempfehlung

Der Algorithmus sollte allein Wahrscheinlichkeiten für Szenarien angeben. Die interne Subsumtion auf einen Vorschlag würde psychologisch den Richter viel stärker beeinflussen. Erforderlich ist eine erschöpfende Angabe aller Prognosen, z.B. bei Bewährungsentscheidungen nicht nur die Wahrscheinlichkeit für Straffälligkeit während der Bewährung, sondern auch, soweit möglich, über mögliche Auswirkungen einer Haftstrafe, also Verrohungs- und Radikalisierungseffekte, Rückfallgefahr bei Haftentlassung etc.

5. Diskriminierungsschutz

Merkmale, die Gegenstand besonderer Diskriminierungsverbote sind, dürfen nicht als solche durch den Algorithmus verarbeitet werden. Die Festlegung des genauen Kataloges, der sich an Art. 3 Abs. 3 GG zu orientieren hat, muss durch den Gesetzgeber unter Wahrung grund-, europa- und menschenrechtlicher Diskriminierungsverbote erfolgen. Art. 9 Abs. 1 DSGVO gibt hier ebenfalls einen Fingerzeig. Ob diese Fragen für den Zweck der vorbeugenden Verbrechensbekämpfung anders zu entscheiden sind,[90] kann hier dahinstehen. Eine genaue Untersuchung des Umfangs von Berücksichtigungsverboten und des etwaigen Umfangs von auch bloß mittelbarer Diskriminierung[91] muss an anderer Stelle geleistet werden.

Literaturverzeichnis

Ahrendt, Christian, Alte Zöpfe neu geflochten – Das materielle Recht in der Hand von Programmierern, NJW 2017, 537-540.

Bader/Ronellenfitsch, BeckOK VwVfG mit VwVG und VwZG, 40. Edition, München 2018.

Binder, Braun, Vollautomatisierte Verwaltungsverfahren im allgemeinen Verwaltungsverfahrensrecht?, NVwZ 2016, 960-965.

Boehme-Neßler, Volker, Die Macht der Algorithmen und die Ohnmacht des Rechts. Wie die Digitalisierung das Recht relativiert, NJW 2017, 3031-3037.

Brink/Wolff, BeckOK Datenschutzrecht, 24. Edition, München 2018.

[90] Dazu jüngst differenzierend *OVG Münster*, Urt. v. 07.08.2018 (Az.: 5 A 294/16). Ablehnend zu dieser Praxis *Liebscher*, NJW 2016, 2779 (2779).

[91] Deren Berücksichtigung im Rahmen von Art. 3 Abs. 3 GG umstritten ist, siehe *Osterloh*, in: Sachs, Art. 3 Rn. 255; ablehnend *Langenfeld*, in: Maunz/Dürig, Art. 3 III Rn. 37.

Graf (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 30. Edition, München 2018.

Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 7. Aufl. München 2013.

Heintschel-Heinegg (Hrsg.), BeckOK – StGB, 38. Edition, München 2018.

Herdegen/Scholz/Klein (Hrsg.), Maunz/Dürig – Grundgesetz – Kommentar, 82. Ergänzungslieferung, München 2018.

Joecks/Miebach (Hrsg.), Münchener Kommentar zum StGB, Band 2, 3. Aufl., München 2016.

Kastl, Graziana, Algorithmen – Fluch oder Segen? Eine Analyse der Autocomplete-Funktion der Google-Suchmaschine, GRUR 2015, 136-141.

Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur StPO, *Schneider (Hrsg.)*, Band 2, 1. Aufl., München 2016.

Liebscher, Doris, „Racial Profiling" im Lichte des verfassungsrechtlichen Diskriminierungsverbots, NJW 2016, 2779-2281.

Sachs (Hrsg.), Grundgesetz – Kommentar, 8. Aufl., München 2018.

Sachs/Schmitz (Hrsg.), Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz – Kommentar, 9. Aufl., München 2018.

Singelnstein, Tobias, Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NStZ 2018, 1-9.

Algorithmenbasierte Straftatprognosen in der Eingriffsverwaltung

Zu den verfassungsrechtlichen Grenzen und einfachgesetzlichen Möglichkeiten von „Predictive Policing“

Florian Zenner

Studentische Hilfskraft am Lehrstuhl für Öffentliches Recht, Univ.-Prof. Dr. Annette Guckelberger, Universität des Saarlandes
s8flzenn@stud.uni-saarland.de

Abstract

Erste erfolgversprechende Zahlen und der Wunsch nach einer effizienteren Personalsteuerung drängen mehr und mehr Länder zum Einsatz von Prognosesoftware in der täglichen Polizeiarbeit.[1] Doch auch wenn sich die Technik weiter zum festen Bestandteil der Gefahrenabwehr entwickelt, scheinen die rechtlichen Fragen bis heute nicht ausreichend geklärt zu sein. Der Beitrag befasst sich ausgehend von einer Begriffsbestimmung zunächst mit den technischen Grundlagen von Predictive Policing und zeigt die hierbei rechtlich relevanten Schritte und Probleme auf. Sodann wird aus der mittlerweile umfassenden Judikatur des BVerfG und den zahlreichen Literaturauffassungen ein verfassungsrechtlicher Rahmen für die Technik herausgearbeitet. In dessen Grenzen sind in einem letzten Schritt Überlegungen dazu anzustellen, auf welche Art und Weise die neuen Möglichkeiten einfachgesetzlich in die Polizeiarbeit integriert, die verfassungsrechtlichen Vorgaben konkretisiert und Bedenken ausgeräumt werden können.

I. Themenaufriss

“Nichts würde ihr ungewiß sein und Zukunft wie Vergangenheit würden ihr offen vor Augen liegen.”[2] So beschrieb einst der Mathematiker Pierre-Simon de Laplace eine Intelligenz, der es möglich wäre, anhand vorhandener Daten zukünftige Ereignisse vorherzusagen. Und auch wenn dieser „Laplacesche Dämon“[3] eher stellvertretend für die

[1] Siehe zu diesen Motiven: *GdP Direktion 4 (Südwest)*, Denkzettel Nr. 097/2016.
[2] *Laplace*, S. 2.
[3] Siehe zum Begriff etwa *Gessmann*, S. 422 „Laplace“.

erkenntnistheoretische Weltauffassung seines Namensgebers ist, kann das Bild noch in der heutigen Zeit ein neues Phänomen veranschaulichen: Predictive policing.

Die Technik, von der sich Beamte und Wissenschaftler eine „Vorhersage der Orte und Zeitpunkte zukünftiger Verbrechen“ [4] erhoffen, hielt in den letzten Jahren auch in der Bundesrepublik zunehmend Einzug.[5] Während Bayern bereits 2015 ein solches System im Dauerbetrieb hatte, zogen in den Folgejahren auch Baden-Württemberg und Nordrhein-Westfalen mit Testphasen nach.[6] Mittlerweile nutzen immerhin acht der sechzehn Bundesländer derartige Programme.[7] Unabhängige Institute[8], das BKA[9] und wohl auch die Bundesregierung[10] beobachten die Entwicklung.

Der rasante Aufschwung der Software impliziert zwar eine weitgehende Klarheit darüber, worin die Ziele ihres Einsatzes liegen, wie und ob durch die Verwendung valide Ergebnisse erzielt werden und was die technischen Grundlagen von Predictive Policing überhaupt sind. Nähert man sich dem Thema jedoch an, so ergeben sich schnell einige Probleme, die im Kern wohl genau auf solche – bis dato unbeleuchtete –[11] Fragen zurückgeführt werden können. Ehe daher der Blick zu den Problemen der Prognosesoftware und deren rechtlichen Lösungsansätzen wandern kann, ist es wichtig, den Untersuchungsgegenstand einzugrenzen und einige Überlegungen zu der vielleicht entscheidenden Frage in diesem Themenkomplex anzustellen: Was ist Predictive Policing?

II. Begriffsbestimmung

Bereits in der Herangehensweise zeichnen sich bei der Ausfüllung dieses Anglizismus deutliche Unterschiede ab. Während einige Autoren eine strafprozessuale bzw. strafrechtliche Perspektive einnehmen,[12] beobachten andere das Phänomen aus der Sicht des Polizeirechts[13]. *Singelnstein* verortete zuletzt den Untersuchungsgegenstand an der „Grenze von Polizeirecht und Strafrecht“[14]. Der Technik scheint also eine gewisse Janusköpfigkeit innezuwohnen. Denn im Moment der Programmierung kann zunächst

[4] *Belina*, MSchrKrim 2016, 85 (85).
[5] *Belina*, MSchrKrim 2016, 85 (85).
[6] *Singelnstein*, NStZ 2018, 1 (1).
[7] *Grünwald*, “Predictive Policing” – ein erfolgversprechender Ansatz zur Verbrechensbekämpfung.
[8] Vgl. etwa den Evaluationsbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht: *Albrecht/Eser/Sieber*, Predictive Policing als Instrument zur Prävention von Wohnungseinbruchsdiebstahl – Evaluationsergebnisse zum Baden-Württembergischen Pilotprojekt P4.
[9] BT-Drs. 19/1513, S. 2.
[10] Hierauf hindeutend das Eckpunktepapier der Bundesregierung für eine Strategie Künstliche Intelligenz, Stand 18.07.2018, S. 6, 10.
[11] *Merz*, ABIDA-Dossier, Januar 2016, S. 2.
[12] *Gless*, in: GS Weßlau, S. 165 ff.; *Legnaro/Kretschmann*, KrimJ 2015, 94 (94 ff.); *Meinicke*, K&R 2015, 377 (377 ff.).
[13] *Ebert*, LKV 2017, 10 (12); *Rademacher*, AöR 142 (2017), 366 (366 ff.).
[14] *Singelnstein*, NStZ 2018, 1 (6).

noch offen bleiben, ob die Software einmal der Gefahrenabwehr dienen wird oder im Rahmen der Repression zum Einsatz kommt.

Auch die ehemalige Bundesregierung erkannte dieses definitorische Problem. Sie versuchte daher den Kern der Technik freizulegen, indem sie Predictive Policing als einen mathematisch-statistischen Ansatz bezeichnete, mit dem anhand anonymer Falldaten und unter Verwendung kriminologischer Thesen weitere Straftaten berechnet werden sollen.[15] Sie verzichtete damit bewusst darauf, den Zweck des Algorithmus in die Definition mit aufzunehmen. Darüber hinaus geht aus der Umschreibung auch keine Information über die Darstellungsform der Vorhersage hervor.

Demzufolge handelt es sich bei Predictive Policing um ein sehr weites Feld, das eine ganze Reihe unterschiedlicher Vorgänge umfassen kann. Diesen ist lediglich gemein, dass sie kriminologische Überlegungen mit mathematisch-statistischen Big-Data-Technologien verknüpfen, um zukünftige Verbrechen vorhersagen zu können.[16]

III. Technische Grundlagen und rechtlich relevante Vorgänge

Nachdem nun ein erster Orientierungsrahmen gegeben ist, ist es ebenfalls notwendig, einen Blick auf die technischen Grundlagen und Möglichkeiten zu werfen. Diese bieten dann die Gelegenheit, die theoretische Weite der Definition auf der Ebene des Faktischen einer weiteren Konkretisierung zuzuführen und jene Vorgänge besser hervorzuheben, deren rechtliche Beurteilung in einem nachfolgenden Teil anstehen soll.

1. Funktionsweise

Die enorme Bandbreite der Funktionsweise verschiedener polizeilicher Vorhersagesoftware wird ebenso wie die immensen Möglichkeiten erst bei einem Blick über den Atlantik deutlich. Denn die USA, die als „Ursprungsland“[17] der Prognoseprogramme gelten, verfolgen nach Art wie auch nach Umfang eine gänzlich andere Strategie, als dies etwa in der BRD der Fall ist.

a) Stand in Deutschland

Hiesige Anbieter beschränken sich im Moment noch darauf, Tatortberichte der Polizei, Geodaten und Verkehrsinformationen bei der Verarbeitung heranzuziehen.[18] Diese Daten werden dann in altbekannte und der Software vorgegebene kriminologische Wiederholungsmuster eingeordnet, um anhand dessen die Fortführung des Musters und damit die kommenden Straftaten vorherzusagen.[19] Für die Zukunft scheint es auch

[15] BT-Drs. 18/3703, S. 3.
[16] BT-Drs. 18/3703, S. 3.
[17] *Belina*, MSchrKrim 2016, 85 (85).
[18] *Heitmüller*, Predictive Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report.
[19] *Egbert*, APuZ 2017, 17 (20); siehe zum exakten Ablauf: *Gless*, in: GS Weßlau, S. 165 (167 Fn. 10).

nicht ausgeschlossen, dass selbstlernende Programme völlig neue Zusammenhänge entdecken und damit ihre eigene Effizienz ohne menschliche Hilfe steigern können.[20]

Die in der Bundesrepublik verwendeten Algorithmen zeichnen sich also auf der Inputseite durch eine besondere Datensparsamkeit aus, auf den Gebrauch personenbezogener Daten wird gänzlich verzichtet.[21] Auf der Outputseite steht dafür allerdings „nur" ein Bruch, der die abstrakte Wahrscheinlichkeit für die künftige Begehung einer Straftat *in einem bestimmten räumlichen Bereich* beschreibt.[22] Außerdem ist zu beachten, dass die sehr stark musterbasierte Herangehensweise in ihrem Anwendungsspektrum beschränkt ist. So erfreut sie sich zwar im Rahmen des Einbruchdiebstahls, der häufig bestimmten planmäßigen Strukturen folgt, großer Beliebtheit,[23] ist allerdings dort unanwendbar, wo es an solchen Erklärungsmustern fehlt.[24]

b) Stand in den USA

Diese Abstraktheit und Musterabhängigkeit spielen in den USA indes eine immer geringere Rolle. Die dortigen Behörden haben die raumbasierte Vorgehensweise längst weiterentwickelt und versuchen, die Verbrechensvorhersage zum einen auf konkrete Personen und zum anderen auf ein breiteres Deliktsspektrum auszuweiten.[25]

Doch auch diese Outputerweiterung hat ihren Preis. Während sie nämlich auf der einen Seite ein quantitatives Mehr an Daten fordert, ist es auch nötig, qualitativ solche Daten miteinzubeziehen, die einen konkreten Personenbezug aufweisen.[26] Beispiele für schon jetzt einbezogene Faktoren wären hierbei etwa Wohnortdaten verurteilter Straftäter, sozioökonomische Daten oder auch Social-Media-Daten.[27]

c) Zwischenfazit

Die unterschiedlichen Entwicklungsstadien veranschaulichen also sehr gut, dass die hierzulande verwendete Software nur einen kleinen Bereich innerhalb der oben aufgestellten Definition nutzt. Sie zeigen allerdings auch, welche Möglichkeiten die algorithmenbasierte Straftatprognose noch offen hält und stellen uns hierbei vor die Frage, ob und wieweit ein Nachrüsten in Zukunft zulässig sein wird.

---

[20] *Rolfes*, in: FS Asche, S. 51 (57); *Singelnstein*, NStZ 2018, 1 (3); siehe zur „algorithmischen Kriminologie" allgemein *Berk*, Security Informatics 2013, 2:5.
[21] BT-Drs. 19/1513, S. 5; *Bode/Stoffel/Keim*, Variablität und Validität von Qualitätsmerkmalen im Bereich von Predictive Policing, S. 2; *Rademacher*, AöR 142 (2017), 366 (369).
[22] *Rademacher*, AöR 142 (2017), 366 (369).
[23] *Egbert*, APuZ 2017, 17 (17); *Merz*, ABIDA-Dossier, Januar 2016, S. 5.
[24] *Singelnstein*, NStZ 2018, 1 (5).
[25] Siehe zu diesen „New Versions of Predictive Policing": *Ferguson*, Washington University Law Review 94 (2017), 1109 (1142 ff.); *Perry/McInnis/Price/Smith/Hollywood*, S. xiv ff.
[26] *Gless*, in: GS Weßlau, S. 165 (172).
[27] *Rademacher*, AöR 142 (2017), 366 (370); *Singelnstein*, NStZ 2018, 1 (2).

2. Rechtlich relevante Vorgänge

Seiner Funktionsweise entsprechend ist Predictive Policing auch rechtlich als mehrstufiger Vorgang zu betrachten. So steht etwa noch lange bevor eine Prognose angestellt werden kann die *Erhebung* der Daten, deren *Verarbeitung* sich sodann anschließt.[28] Daraufhin werden *Maßnahmen* getroffen, die ebenfalls bestimmten Anforderungen unterliegen können.[29]

Anhand dieser Dreiteilung sollen im Folgenden die einzelnen Schritte näher dargestellt werden. Außerdem ist ein Blick auf die kritischen Stimmen zu werfen, deren Bedenken ebenfalls in diesem System eingeordnet werden können. Hieran wird dann die Frage angeschlossen, welche verfassungsrechtlichen Grenzen diese Probleme ziehen und wie sie einfachgesetzlich bewältigt werden können.

a) Datenerhebung

Zu Beginn jeder Prognose steht die Datenerhebung. Sie beschafft den „Rohstoff", der daran anschließend algorithmisch verarbeitet wird und stellt daher den wohl essentiellsten Schritt dar.

Das in diesem Rahmen wohl am häufigsten befürchtete Szenario ist die Missachtung datenschutzrechtlicher Vorgaben. So sehen Kritiker etwa die Gefahr, dass in Zukunft die Einbeziehung personenbezogener Daten vom einstigen Tabuthema zum zentralen Streitpunkt werden wird.[30]

b) Datenverarbeitung

Im nächsten Schritt, der Datenverarbeitung, geht es sodann darum, den gewonnenen „Rohstoff" in bekannte Muster einzusortieren bzw. neue Zusammenhänge aufzudecken.

Problematisch hierbei erscheint jedoch, dass der Blick nur auf solche Deliktsfelder gerichtet wird, die ohnehin gesellschaftlich wahrgenommen werden, da zu ihnen bereits Informationen vorliegen. Das polizeiliche Hellfeld rückt also noch stärker ins Visier, wodurch sich mittels immer weiterer gewonnener Daten der Anschein perpetuiert, Kriminalität komme allein oder zentral an diesen Orten vor.[31] Verschärft wird diese Situation noch dadurch, dass der Einsatz von Big-Data-Technologien nur dort über-

[28] Differenzierung angelegt in BVerfGE 65, 1 (47); siehe auch *Gusy*, Rn. 259.
[29] Zu dieser Dreiteilung siehe auch *Singelnstein*, NStZ 2018, 1 (6 ff.).
[30] Vgl. nur *Meinicke*, K&R 2015, 377 (380), der daran zweifelt, dass die aktuell in der BRD verwendete Software keine personenbezogenen Daten verwendet; siehe außerdem *Singelnstein*, NStZ 2018, 1 (6).
[31] *Gluba*, Predictive Policing – Eine Bestandsaufnahme, S. 11; zu Stigmatisierungseffekten allgemein siehe *Ferguson*, University of Pennsylvania Law Review 163 (2015), 327 (401 ff.).

haupt Sinn ergibt, wo auch tatsächlich viele Daten vorliegen.[32] Dies dürfte ein Ausbrechen aus dem Zirkel erschweren.

Eng damit verbunden ist die Befürchtung sog. Verdrängungs- oder Ausnutzungseffekte.[33] Denn mit fortschreitender Offenlegung der zugrunde liegenden kriminologischen Ansätze[34] könnten auch die Gegenspieler der Beamten nach einiger Zeit gewarnt sein und sich neue Strategien ausdenken, um die Software ins Leere laufen zu lassen und somit sogar von deren verzerrter Wahrnehmung zu profitieren.[35]

Das letzte auf dieser Ebene angesiedelte Problem stellt sich als Fortentwicklung der beiden zuvor genannten Befürchtungen dar und entsteht dadurch, dass häufig zu bestimmten Bevölkerungsgruppen in einer Wohngegend besonders viele Daten vorliegen. Die hierbei entstehenden Zirkel bergen dann auch die Gefahr erheblicher Diskriminierungen, wie sie etwa in den USA bereits deutlich zu beobachten waren.[36]

c) Polizeiliche Folgemaßnahmen

Sind alle Daten eingegeben und wurde eine Musterfortentwicklung erkannt, so stellt sich für die Beamten die Frage, wie sie weiter verfahren können. Hierbei werden schlicht hoheitliche Maßnahmen, die mangels Grundrechtsrelevanz auf die allgemeinen polizeilichen Aufgabennormen gestützt werden können, als weitgehend unproblematisch betrachtet.[37]

Interessanter ist dieser Bereich der polizeilichen Arbeit jedoch, wenn der Blick auf die Möglichkeit von Vorfeldmaßnahmen gelenkt wird. Es stellt sich dann die Frage, inwieweit Eingriffe, etwa zur Erlangung weiterer Informationen und zur Verifizierung oder Falsifikation einer polizeirechtlichen Gefahr, schon dann möglich sind, wenn die Software bloß die abstrakte Wahrscheinlichkeit einer solchen ausgegeben hat.[38] Die neue Technik führt also in ein altes Problemfeld, das es an späterer Stelle näher zu beleuchten gilt und für das, ebenso wie für die unter a) und b) behandelten Bedenken, eine Lösung unter verfassungsrechtlichen Gesichtspunkten zu suchen ist.

[32] *Hoffmann-Riem*, AöR 142 (2017), 1 (6 f.).
[33] *Belina*, MSchrKrim 2016, 85 (93); *Singelnstein*, NStZ 2018, 1 (4).
[34] Siehe etwa die umfassenden Ausführungen bei *Gluba*, Predictive Policing – Eine Bestandsaufnahme.
[35] Siehe zu den Auswirkungen von Prognosen auf tatsächliches Verhalten eingehend *Harari*, S. 82 ff.
[36] *Martini*, JZ 2017, 1017 (1018); *Rademacher*, AöR 142 (2017), 366 (376); *Singelnstein*, NStZ 2018, 1 (4).
[37] *Singelnstein*, NStZ 2018, 1 (7), der etwa das Einsetzen von Polizeistreifen als Beispiel nennt.
[38] Angerissen, aber unbeantwortet bei *Singelnstein*, NStZ 2018, 1 (8).

IV. Verfassungsrechtliche Rahmenbedingungen

1. Grenzen von Datenerhebung und Datenerarbeitung

Wann immer von Datenerhebung und Datenverarbeitung durch staatliche Stellen die Rede ist, kommt seit dem Volkszählungsurteil des BVerfG[39] einem Institut ganz zentrale Bedeutung zu: Dem Recht auf informationelle Selbstbestimmung.[40]

Dieses umfasst, als Ausfluss des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG), die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbart.[41] Es entfaltet also unmittelbar an jener Stelle Relevanz, an der sich die Frage nach einer Annäherung an das US-amerikanische Modell und die damit verbundene Einbeziehung personenbezogener Daten stellt. Ihre Erhebung und Verwertung wäre als Eingriff in das genannte Grundrecht zu betrachten, dessen einschneidende Qualität selbst die offene Preisgabe der Daten (etwa in sozialen Netzwerken) nicht zwangsläufig entfallen ließe.[42] Es ist also zu klären, ob und ggf. wie ein solcher Eingriff gerechtfertigt werden kann.

Bereits im Volkszählungsurteil hatte das BVerfG die grundsätzliche Einschränkbarkeit des Rechts auf informationelle Selbstbestimmung aufgrund überwiegender Allgemeinwohlbelange anerkannt.[43] Später ergänzte es, dass zur Verhinderung von Grundrechtseingriffen „ins Blaue hinein“ die Hürden verhältnismäßig höher werden müssten, je weiter der Eingriff im Vorfeld einer polizeirechtlichen Gefahr angesiedelt sei.[44] Auf dieser Grundlage bestand auch für die präventiv polizeiliche Rasterfahndung in Nordrhein-Westfalen verfassungsrechtlich gebotener Korrekturbedarf.[45]

Wo allerdings personenbezogenes Predictive Policing in diesem Rahmen einzuordnen ist, ob dessen Anwendung überhaupt mit dem „Rastern“ verglichen werden kann und was daher die Folgen für seine Zulässigkeit sind, wurde bisher noch keiner verfassungsgerichtlichen Klärung unterzogen. Die Stimmen in der Literatur gehen vielmehr in unterschiedliche Richtungen:

a) Grundrechtsschonung durch Steuerbarkeit

Nach einer Ansicht besteht bei polizeilichen Vorhersageprogrammen der entscheidende Unterschied zur Rasterfahndung darin, dass ihre Algorithmen besser steuerbar sei-

[39] BVerfGE 65, 1 ff.
[40] Siehe zur Entwicklung: *di Fabio*, in: Maunz/Dürig GG, Art. 2 Abs. 1 Rn. 173 ff.
[41] BVerfGE 65, 1 (42).
[42] Etwa dann nicht, wenn gezielt bestimmte Personen unter Heranziehung weiterer Daten untersucht werden, vgl. BVerfGE 120, 274 (345).
[43] BVerfGE 65, 1 (44); bestätigt in BVerfGE 115, 320 (345).
[44] BVerfGE 115, 320 (360 ff.).
[45] BVerfGE 115, 320 ff.; siehe hierzu: *Volkmann*, JURA 2007, 132 (132 ff.).

en und die Streubreite erheblich eingeschränkt werden könne.[46] So soll durch die sofortige Löschung nicht gefahrindizierender Daten der Eingriff gegenüber den hierbei Betroffenen entfallen.[47] Der Kreis der verbleibenden Grundrechtsträger, die durch Datenerhebung und Verarbeitung weiterhin tangiert sind, könne letztlich derart minimiert werden, dass die Effektivität der Software die Grundrechtsbelastung rechtfertige.[48]

b) Zweifache Entgrenzung des Eingriffs

Auf der anderen Seite wird jedoch entgegengehalten, dass bei der verwendeten Software im Gegensatz zur Rasterfahndung nicht einmal die Schutzrichtung im Moment der Datenerhebung klar sei. Ferner sei die Streubreite ebenfalls erhöht, da die Software bereits in einem sehr frühen Stadium ihrer Programmierung und Anwendung enorme Datenmassen benötige, um effektiv personenbezogene Prognosen anstellen zu können.[49] Eine solche zweifache Entgrenzung des Eingriffs könne schließlich vor dem Hintergrund des Rasterfahndungsurteils nicht zulässig sein, Erhebung und Verarbeitung personenbezogener Daten seien also a fortiori verfassungswidrig.[50]

c) Vergleich und Stellungnahme

Bei Betrachtung dieser Kontroverse wird schnell deutlich, dass die beiden Standpunkte sich weniger ihrem Inhalt nach, als in ihrem Bild von der Technik selbst unterscheiden. Denn es entspricht faktisch nicht dem Stand der gegebenen Wiederholungsmuster, direkt erkennen zu können, ob ein einzelner Umstand als verdächtig oder unverdächtig einzustufen ist und damit durch unmittelbares Löschen dieser Daten Grundrechte zu schonen.[51]

Ferner birgt gerade die Einbeziehung personenbezogener Daten ein erhöhtes Diskriminierungsrisiko. Zwar mag in diesem Rahmen eine selektive Wahrnehmung der Software diskriminierende Faktoren, wie etwa die ethnische Herkunft, grds. ausblenden können.[52] Gerade der Einsatz neuartiger Techniken, deren Output die berücksichtigten Faktoren nicht mehr erkennen lässt,[53] könnte die Selektion jedoch durch Kombination diverser Daten (Einkommen, Wohngegend, Versicherungsdaten etc.) wieder zu Nichte machen. In diesem Rahmen werden als Lösungsansätze zwar Kontrollalgo-

[46] *Rademacher*, AöR 142 (2017), 366 (397).
[47] Siehe zu dieser grundsätzlichen Möglichkeit BVerfGE 100, 313 (366); BVerfGE 107, 299 (328); BVerfGE 115, 320 (343); BVerwG, NVwZ 2015, 906 (907).
[48] *Rademacher*, AöR 142 (2017), 366 (399).
[49] *Singelnstein*, NStZ 2018, 1 (6).
[50] *Singelnstein*, NStZ 2018, 1 (7).
[51] *Gless*, in: GS Weßlau, S. 165 (171).
[52] So *Rademacher*, AöR 142 (2017), 366 (375).
[53] Siehe zu dieser Vorgehensweise sog. künstlicher neuronaler Netze, bei denen die zwischen In- und Output liegenden „hidden layer" nicht ausgelesen werden können: *Bibel/Kruse/Nebel*, S. 34; aus der juristischen Literatur: *Martini/Nink*, NVwZ 2017, 681 (682).

rithmen oder sich selbst erklärende KI-Systeme angeboten,[54] die hierbei angepriesenen Möglichkeiten entsprechen jedoch aktuell nicht dem Stand der polizeilichen Vorhersagesoftware[55] und vermögen die im Lernvorgang einer KI benötigten enormen Datenmassen[56] nicht zu vermindern.

Es zeigt sich also, dass personenbezogenes Predictive Policing zumindest zurzeit noch erhebliche Risiken birgt. Viele Probleme, wie die Konzentration auf „die üblichen Verdächtigen" und damit einhergehende Diskriminierungseffekte, können vielmehr sogar durch ein bewusstes Verzichten auf einen derart weitgehenden Einsatz vermieden werden. Zwar verbleibt auch bei raumbezogener Anwendung der Programme ein gewisses Diskriminierungsrisiko,[57] dieses ist jedoch verfassungsrechtlich weit weniger problematisch, solange mittelbare Rückschlüsse auf konkrete Personen(-gruppen) nicht möglich sind und damit weder Recht auf informationelle Selbstbestimmung tangiert,[58] noch Art. 3 Abs. 3 GG verletzt wird. Verbleibende lokale Stigmatisierungseffekte hingegen stellen für die Polizeiarbeit kein Novum dar. So existieren schon sehr lange polizeiliche Lagebilder, anhand derer Einsätze koordiniert werden sollen.[59]

Es bleibt daher dabei, dass in absehbarer Zeit unter den geltenden rechtlichen Maßstäben der Einsatz personenbezogener Daten zur Straftatprognose allenfalls unter sehr engen Voraussetzungen zulässig sein kann.[60] Für die Verwendung nichtpersonenbezogener Daten empfiehlt es sich, auf einfachgesetzlicher Ebene einen „digitalen Beipackzettel"[61] zu schaffen, der dem Bürger Transparenz gewährleistet und die Möglichkeit der Zurwehrsetzung gegen etwaige negative Effekte garantiert.[62] Dies ist aufgrund der RL 2016/680 nicht zuletzt auch unionsrechtlich geboten.[63]

[54] *Martini/Nink*, NVwZ 2017, 681 (682); *Rademacher*, AöR 142 (2017), 366 (377).
[55] Siehe zu den bei der Erklärung komplexer Algorithmen auftretenden Schwierigkeiten *Reichwald/Pfisterer*, CR 2016, 208 (212).
[56] Siehe hierzu *Lenzen*, S. 63.
[57] Algorithmenbasierte Entscheidungsprozesse – Thesenpapier des vzbz, S. 14, aufzurufen unter https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf, zuletzt aufgerufen am 14.08.2018.
[58] So auch *Singelnstein*, NStZ 2018, 1 (6).
[59] Siehe hierzu *Clages/Zeitner*, S. 187 f.
[60] I.E. ebenso: *Meinicke*, K&R 2015, 377 (383); *Singelnstein*, NStZ 2018, 1 (7); siehe außerdem die Aufzeichnungen zur Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18./19.03.2018, die zu einem ähnlichen Ergebnis kam, abgedruckt in: *Spiecker/Bretthauer*, G 2.4.21.
[61] *Martini*, JZ 2017, 1017 (1020); ähnlich auch *Martini/Nink*, NVwZ 2017, 681 (682), die von einem „Recht auf Einsichtnahme in die Bewertungsmaßstäbe" sprechen, aber auch auf die Schwierigkeiten beim Einsatz von künstlicher Intelligenz eingehen; *Rademacher*, AöR 142 (2017), 366 (390) nennt dieses Recht ein „Recht auf Plausibilität".
[62] Algorithmenbasierte Entscheidungsprozesse – Thesenpapier des vzbz, S. 14, aufzurufen unter https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf, zuletzt aufgerufen am 14.08.2018.
[63] Vgl. dort insb. Erwägungsgrund 38.

2. Grenzen potentieller Eingriffsbefugnisse

Ist auf den beiden ersten Ebenen ein Ergebnis erzielt, so ist verfassungsrechtlich zu beleuchten, welche Möglichkeiten polizeilichen Handelns vom Gesetzgeber geschaffen werden können, um an die vom Programm ermittelte Straftatwahrscheinlichkeit sinnvoll und zulässig anzuknüpfen. Es wird also konkret die vielfach diskutierte Frage aufgeworfen, wie weit Befugnisnormen für grundrechtsrelevantes Handeln bereits im Vorfeld der konkreten Gefahr angesiedelt sein dürfen.

a) Altbekannte Lücken

Bereits vor den technischen Meilensteinen, die im Laufe unseres Jahrzehnts gelegt wurden, gehörte dieses Feld zu den wohl umstrittensten der deutschen Polizeirechtsdogmatik.[64] Denn auch ohne moderne Informationstechnologie stand etwa die Frage im Raum, inwieweit Identitätskontrollen an sog. „gefährlichen Orten“ auch in abgeschwächten Gefahrensituationen möglich seien. Allein in diesem Beispiel wurde ausgehend von einer konkreten, über die abstrakte, bis hin zur gänzlichen Entbehrlichkeit der Gefahr alles vertreten.[65]

Auch die Aussagen des BVerfG konnten in dieses Dickicht bis heute keine echte Klarheit bringen. So verweisen die Richter immer wieder auf die erhöhten Bestimmtheitsanforderungen im Bereich der Vorfeldbefugnisse, ohne jedoch eine konkrete Systematisierung zu wagen, die letztlich zur eben geforderten Rechtssicherheit für den Bürger hätte beitragen können.[66]

In der Literatur wurden indes immer wieder derartige Versuche unternommen.[67] Hierdurch sollte zum einen der gestiegenen Relevanz der Informationsgewinnung für die Erkennung und Abwehr von Gefahren Rechnung getragen und zum anderen eine rechtsstaatlichen Grundsätzen entsprechende Dogmatik herausgearbeitet werden. Vielversprechend schien vor allem der Ansatz *Möstls*, der zwischen kausalverlaufshemmenden Maßnahmen und rein informationeller Vorfeldarbeit differenziert.[68] Während erstere sich weiterhin an der klassischen Gefahr-Störer-Dogmatik orientierten, seien die letzteren bereits aus rein logischen Erwägungen hieran nicht gebun-

[64] Siehe zum Gesamtkomplex umfassend *Schenke*, JuS 2018, 505 (505 ff.).
[65] Zu den Einzelansichten *Möstl*, DVBl. 2007, 581 (583 Fn. 17 mit Nachweisen).
[66] *Möstl*, DVBl. 2010, 808 (809 ff.), mit einer Übersicht der Rspr. des BVerfG.
[67] Siehe neben den bereits genannten etwa *Darnstädt*, DVBl. 2017, 88 (88 ff.); *Puschke/Singelnstein*, NJW 2005, 3534 (3534 ff.).
[68] *Möstl*, S. 180 ff.; *Möstl*, DVBl. 2007, 581 (582).

den,[69] was jedoch im Bereich intensiver Informationseingriffe durch entsprechende Verfahrenssicherungen auszugleichen sei.[70]

b) Änderungen durch den Einsatz von Predictive Policing

Das Problem, vor dem dieses neue Polizeirecht jedoch stand, lag auf der Hand. Denn selbst wenn hierfür neue Bezugspunkte, wie der konkrete Gefahrenverdacht oder der raum-/personenbezogene abstrakte Gefahrenverdacht entwickelt wurden, konnten die Vorwürfe schwindender Rechtssicherheit und Rechtsanwendungsgleichheit nicht unterbunden werden. Vor allem das Verlassen auf bloße Erfahrungssätze schien problematisch, stattdessen wurden „tatsachenbasierte konkrete Wahrscheinlichkeiten" auch für die Vorfeldarbeit gefordert.[71]

Es scheint allerdings bemerkenswert, dass gerade in der jüngeren Literatur die softwaregestützte Straftatprognose als Indikator für einen je nach angegebener Wahrscheinlichkeit mehr oder weniger verdichteten Gefahrenverdacht herangezogen wird.[72] Was könnte daher näher liegen, als diese Ansätze zu verknüpfen und Predictive Policing als ein Hilfsmittel ins Spiel zu bringen, das in einem solchen System aufgrund der exakt abschichtbaren Wahrscheinlichkeitswerte die gleiche Anwendung des Rechts durch die Beamten gewährleistet. Entgegen der teilweise geäußerten Befürchtungen vor freiheitsentziehenden Maßnahmen durch Softwareprognosen,[73] könnten diese damit sogar weniger Problem als Teil einer Lösung der schwierigen Frage sein, wie das polizeiliche *Informations*recht in verfassungsrechtlich einwandfreier Weise von einer faktischen auf die normative Ebene transferiert werden kann.

Dabei ist jedoch stets die soeben aufgestellte Differenzierung zu beachten. Denn ein tatsächlicher Eingriff in den Kausalverlauf, also eine nicht rein informationelle Maßnahme,[74] unterliegt Anforderungen, die auch eine Softwareprognose nicht zu erfüllen vermag. Es erscheint daher äußerst bedenklich und für die Entwicklung einer verfassungsmäßigen Vorfelddogmatik schädlich, wenn etwa vom bayerischen Gesetzgeber auch die „Unterbrechung des Kausalverlaufs"[75] nunmehr bereits vor der konkreten Gefahr ermöglicht wird. Diese sollte bei aller Informationsarbeit im Vorfeld doch stets den Anknüpfungspunkt für derartige Maßnahmen bilden.

---

[69] *Möstl*, DVBl. 2007, 581 (586); ähnlich mit Verweis auf „Sinn und Zweck" der Vorfeldmaßnahmen *Trute*, Die Verwaltung 2003, 501 (517).
[70] *Möstl*, DVBl. 2007, 581 (586).
[71] *Meyer*, JZ 2017, 429 (435).
[72] *Rademacher*, AöR 142 (2017), 366 (383).
[73] *Nobis*, StV 2018, 453 (458).
[74] Zur durchaus schwierigen Abgrenzung aufgrund mittelbar-faktischer Wirkungen von Informationsmaßnahmen siehe in Auseinandersetzung mit den Literaturauffassungen *Möstl*, S. 244 ff.
[75] *Waechter*, NVwZ 2018, 458 (461).

3. Zwischenfazit

Diese Ergebnisse spiegeln auf einer Zeitleiste betrachtet auch genau jenes Anliegen wider, das die verfassungsgerichtliche Rechtsprechung verfolgt. Denn mit einem Näherrücken an die konkrete Gefahr steigen in der hier entwickelten Einordnung letztlich auch die Möglichkeiten und werden die Hürden für Polizeibeamte herabgesetzt.

Während somit bei Datenerhebung- und Datenverarbeitung Grundrechtseingriffe gänzlich abzulehnen waren, da diese jeglichem Gefahrenverdacht noch vorverlagert sind, können beim Vorliegen entsprechender Softwareprognosen erste Informationseingriffe – vorbehaltlich einer gesetzlichen Grundlage – zulässig sein. Auch innerhalb dieses Bereiches sind Abstufungen anhand des errechneten Wahrscheinlichkeitswertes möglich. Eingriffe in den Kausalverlauf sollten jedoch der am Ende dieser Zeitleiste liegenden konkreten Gefahr vorbehalten bleiben.

V. Einfachgesetzliche Ausgestaltungsmöglichkeiten

Es verbleibt zuletzt diesen bereits sehr konkreten Rahmen auch einfachgesetzlich auszugestalten. Es sollen hier einige gesetzgeberische Möglichkeiten dargestellt werden, wie eine solche Implementierung gelingen und verbleibenden Problemen und Anliegen Rechnung getragen werden kann.

1. Einführung eines digitalen Beipackzettels

Da wie gezeigt lokale Stigmatisierungseffekte – gerade bei der Verwendung rein nichtpersonenbezogener Daten – auftreten können, ist es zunächst wichtig, den betroffenen Bürgern gegenüber transparent zu sein. Die Arbeit der Software, ihre Zielsetzung und die Relevanz für das darauf folgende hoheitliche Handeln müssen ebenso klar und verständlich dargelegt werden, wie eine Möglichkeit zur Rüge etwaiger Fehleinschätzungen bestehen muss. Auch dass die Polizeibehörden sich selbst vor eine „intransparente Blackbox“[76] gestellt und lediglich das Potential der Software[77] sehen, erscheint daher als ein enormes rechtsstaatliches Defizit, bei dem dringender Korrekturbedarf besteht.

Ein häufig diskutiertes Mittel ist hierbei die Schaffung des bereits angesprochenen digitalen Beipackzettels. Er soll in einfacher Sprache die wesentlichen Vorgänge darlegen und stellt daher insb. im Verhältnis zum Bürger ein geeignetes Medium dar.

[76] So S. 2 eines Berichts der Polizei Hamburg vom Februar 2018 zum Projekt „Prädiktionspotential schwerer Einbruchskriminalität“, aufzurufen unter https://www.polizei.hamburg/contentblob/10651848/ee06121971285e6c2dff60f29d205208/data/projektstand-02-2018-do.pdf, zuletzt aufgerufen am 14.08.2018.

[77] *Jarchow/Rabitz-Suhr*, SIAK-JOURNAL 2/2018, 15 (19), mit Bezug auf das Hamburger Forschungsprojekt „Prädiktionspotential schwerer Einbruchskriminalität“.

Dabei ist jedoch zu beachten, dass eine allzu konkrete Offenlegung verwendeter Prädikatoren und kriminalistischer Ansätze letztlich die Ergebnisse der Prognose gefährden kann.[78] Daher stehen der vollständigen Veröffentlichung des Algorithmus auch polizeiliche Interessen entgegen, die es gerade vor dem Hintergrund potentieller Ausnutzungseffekte[79] mit den Interessen der Betroffenen an möglichst umfassender Klarheit bei der Schaffung des Beipackzettels abzuwägen gilt.

Was die Polizeibeamten selbst anbetrifft, so scheint der richtige Weg eine verständnisfördernde Weiterbildung zu sein. Diese wird letztlich auch einen effizienteren und professionelleren Einsatz der Software nach sich ziehen.[80]

2. Anpassung polizeilicher Befugnisnormen

Ein letzter Aspekt zur Abrundung stellt die Anpassung der polizeilichen Befugnisnormen dar. Es wurde herausgearbeitet, dass dem Gesetzgeber etwa die Möglichkeit offen steht, die Prognosewerte in den Tatbestand bestimmter Standardbefugnisse zur Informationsgewinnung einzusetzen und damit bisher unbestimmte Rechtsbegriffe einer gewissen Rationalisierung zuzuführen. Ebenfalls gezeigt wurde jedoch, dass die Grenze dort liegt, wo die Polizei unmittelbar in den Kausalverlauf eingreift. Eine Abweichung von der klassischen Dogmatik wäre an solcher Stelle rechtsstaatlich wohl unhaltbar.

VI. Fazit

Was bleibt nun vom bereits heraufbeschworenen Orwell'schwen Schreckensszenario der Totalüberwachung?[81] Wird Predictive Policing wirklich unser gesamtes Polizeirecht umkrempeln und einer Vergeheimdienstlichung der behördlichen Arbeit Vorschub leisten? Oder gibt es vielleicht rationalere Einordnungen, die sich in das System der Gefahrenabwehr einfügen und diese sinnvoll ergänzen können?

Endgültige Antworten auf solche Fragen sind wohl der Zukunft vorbehalten. Bis dato scheint es jedenfalls unklar, wie rasant sich die Technik weiterentwickeln und wo das BVerfG die Grenze für ihren Einsatz ziehen wird. Der Beitrag sollte jedoch versuchen, mit einigen Vorbehalten gegen Predictive Policing zu brechen und die Diskussion auf eine rationale und dogmatisch orientierte Ebene zu verlagern.

Gewiss ist bei der Machtkumulation von Staat und Big-Data ein kritischer Blick angebracht. Doch ebenso wenig wie das einmal Gedachte wieder zurückgenommen werden kann,[82] werden sich neue Technologien aufgrund rechtsstaatlicher Bedenken in

[78] *Harari*, S. 82 ff. mit entsprechenden historischen Beispielen.
[79] S.o. III. 2. b).
[80] *Jarchow/Rabitz-Suhr*, SIAK-JOURNAL 2/2018, 15 (19).
[81] So etwa *Gless*, in: GS Weßlau, S. 165 (172).
[82] Frei nach *Dürrenmatts* Physikern.

Luft auflösen. Am Ende ist es an der Rechtswissenschaft auch dieses Phänomen zu erfassen und vielleicht wird sich zeigen, dass unter Berufung auf das Grundgesetz auch das Neue stets einen Platz in bewährten Strukturen findet und diese bei korrekter Herangehensweise nicht schwächen, sondern sogar stärken wird.

Literaturverzeichnis

Albrecht, Hans-Jörg/Eser, Albin/Sieber, Ulrich (Hrsg.), Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl – Evaluationsergebnisse zum Baden-Württembergischen Pilotprojekt P4, Freiburg 2017.

Belina, Bernd, Predictive Policing, MSchrKrim 2016, 85-100.

Berk, Richard, Algorithmic criminology, Secutity Informatics 2013, 2:5.

Bibel, Wolfgang/Kruse, Rudolf/Nebel, Bernhard (Hrsg.), Computational Intelligence, Wiesbaden 2011.

Bode, Felix/Stoffel, Florian/Keim, Daniel, Variabilität und Validität von Qualitätsmerkmalen im Bereich von Predictive Policing, Konstanzer Online Publikationen, April 2017, aufzurufen unter https://bib.dbvis.de/uploadedFiles/ Bode_0402496.pdf, zuletzt aufgerufen am 14.08.2018.

Clages, Horst/Zeitner, Ines – Kriminologie, 3. Auflage, Hilden 2016.

Darnstädt, Thomas, Ein personenbezogener Gefahrbegriff – Analyse der Bedingungen des Bundesverfassungsgerichts an Vorfeld-Ermächtigungen im BKA-Gesetz, DVBl. 2017, 88-96.

Ebert, Frank, Entwicklungen und Tendenzen im Recht der Gefahrenabwehr, LKV 2017, 10-17.

Egbert, Simon, Siegeszug der Algorithmen? – Predictive Policing im deutschsprachigen Raum, APuZ 2017, 17-23.

Ferguson, Andrew Guthrie, Big Data and Predictive Reasonable Suspicion, University of Pennsylvania Law Review 163 (2015), 327-410.

Ferguson, Andrew Guthrie, Policing Predictive Policing, Washington University Law Review 94 (2017), 1109-1189.

Gessmann, Martin (Hrsg.), Philosophisches Wörterbuch, 23. Auflage, Stuttgart 2009.

Gless, Sabine, Predictive Policing und operative Verbrechensbekämpfung, in: *Herzog, Felix/Schlothauer, Reinhold/Wohlers, Wolfgang (Hrsg.)*, Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächtnisschrift für Edda Weßlau, Berlin 2016, S. 165-180.

Gluba, Alexander, Predictive Policing – Eine Bestandsaufnahme, aufzurufen unter https://netzpolitik.org/wp-upload/LKA_NRW_Predictive_Policing.pdf, zuletzt aufgerufen am 14.08.2018.

Grünwald, Clemens, "Predictive Policing" – ein erfolgversprechender Ansatz zur Verbrechensbekämpfung, aufzurufen unter ttps://www.datenschutz-notizen.de/predictive-policing-ein-erfolgversprechender-ansatz-zur-verbrechensbekaempfung-0817538/, zuletzt aufgerufen am 14.08.2018.

Gusy, Christoph – Polizei- und Ordnungsrecht, 10. Auflage, Tübingen 2017.

Harari, Yuval Noah – Homo Deus – Eine Geschichte von Morgen, Sonderausgabe des pbp, Bonn 2017.

Heitmüller, Ulrike, Predictive Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report, aufzurufen unter https://www.heise.de/newsticker/meldung/Predictive-Policing-Die-deutsche-Polizei-zwischen-Cyber-CSI-und-Minority-Report-3685873.html, zuletzt aufgerufen am 14.08.2018.

Hoffmann-Riem, Wolfgang, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017), 1-42.

Jarchow, Esther/Rabitz-Suhr, Simone, Informationsmanagement bei der Polizei – Digitale Ermittlungsunterstützung in der Einbruchssachbearbeitung, SIAK-JOURNAL 2/2018, 15-20.

Laplace, Pierre-Simon de – Philosophischer Versuch über die Wahrscheinlichkeit, zit. nach *Mises, Richard von (Hrsg.)*, Leipzig 1932.

Legnaro, Aldo/Kretschmann, Andrea, Das Polizieren der Zukunft, KrimJ 2015, 94-111.

Lenzen, Manuela – Künstliche Intelligenz – Was sie kann & was uns erwartet, München 2018.

Martini, Mario, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017-1025.

Martini, Mario/Nink David, Wenn Maschinen entscheiden…, NVwZ 2017, 681-682.

Meinicke, Dirk, Big Data und Data-Mining: Automatisierte Strafverfolgung als neue Wunderwaffe der Verbrechensbekämpfung?, K&R 2015, 377-384.

Merz, Christina, Predictive Policing – Polizeiliche Strafverfolgung in Zeiten von Big Data, ABIDA-Dossier, Januar 2016, aufzurufen unter http://www.abida.de/sites/default/files/Dossier_Predictive_Policing.pdf, zuletzt aufgerufen am 14.08.2018.

Meyer, Stephan, Kriminalwissenschaftliche Prognoseinstrumente im Tatbestand polizeilicher Vorfeldbefugnisse, JZ 2017, 429-439.

Möstl, Markus – Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Tübingen 2002.

Möstl, Markus, Die neue dogmatische Gestalt des Polizeirechts, DVBl. 2007, 581-589.

Möstl, Markus, Das Bundesverfassungsgericht und das Polizeirecht, DVBl. 2010, 808-816.

Nobis, Frank, Strafrecht in Zeiten des Populismus, StV 2018, 453-464.

Perry, Walter/McInnis, Brian/Price, Carter/Smith, Susan/Hollywood, John, Predictive Policing – The Role of Crime Forecasting in Law Enforcement Operations, Washington 2013.

Puschke, Jens/Singelnstein, Tobias, Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen, NJW 2005, 3534-3538.

Rademacher, Timo, Predictive Policing im deutschen Polizeirecht, AöR 142 (2017), 366-416.

Reichwald, Julian/Pfisterer, Dennis, Autonomie und Intelligenz im Internet der Dinge – Möglichkeiten und Grenzen autonomer Handlungen, CR 2016, 208-212.

Rolfes, Manfred, Predictive Policing: Beobachtungen und Reflexionen zur Einführung und Etablierung einer vorhersagenden Polizeiarbeit, in: Fachgruppe Geoinformatik des Instituts für Geographie der Universität Potsdam (Hrsg.), Geoinformation & Visualisierung, Festschrift anlässlich der Emeritierung von Herrn Prof. Dr. Hartmut Asche, Potsdam 2017, S. 51-76.

Schenke, Wolf-Rüdiger, Polizeiliches Handeln bei Anscheinsgefahr und Gefahrverdacht, JuS 2018, 505-516.

Scholz, Rupert/Herdegen, Matthias/Klein, Hans (Hrsg.), Maunz/Dürig Grundgesetz, Band 1 Texte – Art. 5, 82. Ergänzungslieferung, München im Januar 2018.

Schweer, Thomas, „Vor dem Täter am Tatort" – Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs, Die Kriminalpolizei 1/2015, 13-16.

Singelnstein, Tobias, Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NStZ 2018, 1-9.

Spiecker, Indra/Bretthauer, Sebastian, Dokumentation zum Datenschutz Bd. 5, 68. Auflage, Baden-Baden 2018.

Trute, Hans-Heinrich, Gefahr und Prävention in der Rechtsprechung zum Polizei- und Ordnungsrecht, Die Verwaltung 2003, 501-522.

Volkmann, Uwe, Die Verabschiedung der Rasterfahndung als Mittel der vorbeugenden Verbrechensbekämpfung, JURA 2007, 132-138.

Waechter, Kay, Bayern: Polizeirecht in neuen Bahnen, NVwZ 2018, 458-462.

Gibt es in unserer datengetriebenen Wirtschaft überhaupt noch Daten ohne Personenbezug?

Die Herausforderungen des sachlichen Anwendungsbereichs des Datenschutzrechts aus der Perspektive datenverarbeitender Unternehmen

Carmen Födisch

Promovendin am Lehrstuhl für Bürgerliches Recht, Wettbewerbs- und Immaterialgüterrecht, Medien- und Informationsrecht von Herrn Prof. Dr. Andreas Wiebe, LL.M. (Virginia) an der Georg-August-Universität Göttingen
carmen.foedisch@gmx.de

Abstract

Die seit dem 25. Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO) stellt die datengetriebene Wirtschaft vor große Herausforderungen, insbesondere im Hinblick auf die Einhaltung und Umsetzung ihrer komplexen Pflichten für datenverarbeitende Unternehmen. Notwendige Voraussetzung für die Eröffnung des sachlichen Anwendungsbereichs der DSGVO ist zunächst das Merkmal des personenbezogenen Datums. Durch eine Anonymisierung der Daten kann die Anwendbarkeit der DSGVO hingegen vermieden werden. In Anbetracht der fortschreitenden Technologie erhärtet sich jedoch der Verdacht, dass es keine „wahren" anonymen Daten mehr geben wird. Der Beitrag soll aufzeigen, dass Daten zwar häufig einer Re-Identifizierung unterzogen werden können, aber im Wege einer dynamischen Auslegung und Anwendung des Datenschutzrechts trotzdem Rechtssicherheit in Bezug auf den Personenbezug eines Datums geschaffen werden kann.

I. Einleitung – Der Personenbezug von Daten als Auslöser für die Begründung von Rechten und Pflichten

Spätestens seit auch die mediale Öffentlichkeit und nicht nur der europäische Gesetzgeber die Tragweite eines unionsweiten harmonisierten und hohen Datenschutzniveaus erkannt hat, ist die Anwendbarkeit der DSGVO in aller Munde. In unserer datengetriebenen Wirtschaft ist in nahezu jedem Gesellschaftsbereich die automatisierte

Verarbeitung personenbezogener Daten angekommen.[1] Unternehmen, die personenbezogene Daten – sei es von ihren eigenen Mitarbeitern oder sei es von ihren Kunden – verarbeiten, gelten als Verantwortliche für die Datenverarbeitung i.S.v. Art. 4 Nr. 7 DSGVO und damit gleichzeitig als primärer Adressat der DSGVO.[2] Damit einher ergehen zahlreiche neue Pflichten auf Unternehmerseite, wie auch umfangreiche Rechte auf Seiten der betroffenen Personen. Während insbesondere durch die Einführung eines sog. Rechts auf Vergessenwerden (Art. 17 DSGVO) und eines Rechts auf Datenportabilität (Art. 20 DSGVO) die Betroffenenrechte in der DSGVO gestärkt wurden, müssen Unternehmen in der Anwendungspraxis die Ausübung der Betroffenenrechte nach Art. 15 ff. DSGVO nicht nur gewährleisten, sondern daneben auch eine Vielzahl an weiteren Maßnahmen umsetzen, die zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten beitragen. Das Ausmaß solcher Pflichten reicht von Dokumentationspflichten (bspw. in einem Verarbeitungsverzeichnis nach Art. 30 DSGVO), über Informations- und Meldepflichten nach Art. 13 f. DSGVO bzw. Art. 33 f. DSGVO, bis hin zu weitreichenden Anforderungen im Datenschutzmanagement (bspw. die Bestellung eines Datenschutzbeauftragten nach Art. 37 ff. DSGVO oder die Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 f. DSGVO). Zudem erlangt die Ausweitung dieser Pflichten für datenverarbeitende Unternehmen besonderen Nachdruck durch die hohen Bußgeldandrohungen in Art. 83 DSGVO im Falle eines Verstoßes.

Vor dem Hintergrund dieser Masse an zu implementierenden Maßnahmen ist die Frage nach der Anwendbarkeit der DSGVO von zentraler Bedeutung. Die Verarbeitungstätigkeit eines Unternehmens fällt eben erst dann in den sachlichen Anwendungsbereich der DSGVO nach Art. 2 Abs. 1 DSGVO, sofern personenbezogene Daten verarbeitet werden. Für Daten ohne Personenbezug gilt die DSGVO einschließlich ihrer Pflichten daher nicht.[3] In Anbetracht des digitalen Zeitalters drängt sich jedoch der Eindruck auf, dass eine trennscharfe und sinnvolle Abgrenzung von personenbezogenen zu nicht personenbezogenen Daten kaum noch erbracht werden kann.[4] In dieser Hinsicht sollte die DSGVO den künftigen technischen Herausforderungen entgegentreten können. Der ansonsten durch die DSGVO entstehende Mehraufwand für Unternehmen muss kritisch hinterleuchtet werden, da das Datenschutzrecht nicht als Innovationsbremse fungieren darf.

[1] U.a. *Roßnagel*, DuD 2016, 561 (564).
[2] Ausführlich zum Begriff des Verantwortlichen etwa *Hartung*, in: Kühling/Buchner, Art. 4 Nr. 7 Rn. 6.
[3] Prämisse des folgenden Beitrags ist es, dass sich der Aussagegehalt der Information in einem Datum auf eine natürliche Person beziehen können muss.
[4] Ebenso *Härting/Schneider*, CR 2015, 819 (821).

II. Begriffserklärungen

1. Die Legaldefinition des Art. 4 Nr. 1 DSGVO

Art. 4 Nr. 1 DSGVO bestimmt näher, wann ein personenbezogenes Datum vorliegt. Hierunter fallen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[5] Eine natürliche Person ist jedenfalls dann identifiziert, wenn die betreffenden Daten selbst Aufschluss über die Identität der Person geben oder sich ein solcher Bezug zur Person unmittelbar aus dem Inhalt oder dem Zusammenhang der Daten ohne Rückgriff auf weitere Informationen ergibt.[6] Weil aber der Begriff der Identifizierbarkeit unbestimmt ist, hat der europäische Gesetzgeber zugleich in Art. 4 Nr. 1 HS. 2 DSGVO versucht diesen zu konkretisieren. Dies soll dann der Fall sein, wenn eine natürliche Person direkt oder indirekt identifiziert werden kann, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standorten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.[7] Wie oder von wem eine solche Zuordnung zum Zwecke der Identifizierung erfolgen kann, ist dem Wortlaut der Gesetzesnorm auf den ersten Blick nicht zu entnehmen.[8]

2. Anonyme oder anonymisierte Daten

Im Hinblick auf die eingangs geschilderten Anforderungen des Datenschutzes könnte sich die Anonymisierung von Daten als Lösung für Unternehmen anbieten, um die datenschutzrechtlichen Vorgaben zu umgehen. So betont Erwägungsgrund 26 Satz 5, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten sollen. An einer ausdrücklichen Legaldefinition des Anonymisierens fehlt es – im Gegensatz zu § 3 Abs. 6 BDSG a.F. – allerdings in der DSGVO. Erwägungsgrund 26 Satz 5 führt jedoch weiter aus, dass es sich dabei um solche Informationen handelt, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder [jene] […] personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann." Anders als der deut-

[5] Obwohl bislang das Merkmal „bestimmt oder bestimmbar" statt „identifiziert oder identifizierbar" in der alten Rechtslage verwendet wurde, erfolgte die Wortlautänderung der Definition des personenbezogenen Datums in der deutschen Fassung lediglich aus redaktionellen Gründen, denn im Englischen wurden die Begriffe „identified" und „identifiable" aus Art. 2 lit. a EU-Datenschutzrichtlinie unverändert in Art. 4 Nr. 1 DSGVO übernommen, vgl. *Krügel*, ZD 2017, 455 (455); *Ernst*, in: Paal/Pauly, Art. 4 Rn. 3.

[6] *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 18; vgl. insoweit zur „bestimmten" natürlichen Person *EuGH*, Urt. v. 19.10.2016, Rn. 38, mit Anmerkung *Kühling/Klar*, ZD 2017, 24 (25).

[7] Unter Berücksichtigung des Wortlautes handelt es sich dabei um keine abschließende Aufzählung möglicher Verknüpfungen von Personen zu bestimmten Daten, so auch *Laue/Nink/Kremer*, § 1 Rn. 14.

[8] Ebenso *Hofmann/Johannes*, ZD 2017, 221 (222).

sche Gesetzgeber noch in § 3 Abs. 6 BDSG a.F. differenziert hat, wird nun auf europäischer Ebene zwischen absoluter und faktischer Anonymität (De-Anonymisierung wäre nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft möglich) in der DSGVO zumindest nicht ausdrücklich unterschieden.[9] Die Möglichkeit einer De-Anonymisierung ist aber weiterhin vorhanden. Strittig ist daher, welches verbleibende Restrisiko einer De-Anonymisierung aus datenschutzrechtlicher Perspektive zu ertragen ist.

Praktisch umgesetzt wird eine Anonymisierungsmaßnahme im Grundsatz auf zwei unterschiedliche Weisen. Sofern möglich, wird bei einer Anonymisierung in einem Datensatz der Bezug zu einer natürlichen Person entfernt, ohne dabei den weiteren Datengehalt zu verändern.[10] Unternehmen können entweder Angaben ohne Personenbezug aus einem Bestand an personenbezogenen Daten extrahieren und gesondert verarbeiten oder sie löschen jegliche Identifikationsmerkmale im Datenbestand, wodurch der Personenbezug im Ganzen entfällt.[11] Abgesehen von der Entfernung des Personenbezugs können Daten auch von vornherein bei ihrer Erhebung und Speicherung ohne Personenbezug sein (wobei dies im datengetriebenen Wirtschaftsleben eher seltener zutreffen wird).[12]

Konträr zu personenbezogenen Daten bewirkt somit eine Anonymisierung der Daten, dass die Verarbeitung außerhalb des Regelungsbereiches der DSGVO liegt. Grundsätzlich besteht aber auch die Möglichkeit einer De-Anonymisierung, wodurch eine natürlichen Person re-identifiziert werden kann. Nach jetzigem Diskussionsstand bleibt die Frage unbeantwortet, welche erforderliche datenschutzrechtliche Hürde zu nehmen ist, sodass Unternehmen in der Praxis rechtssicher von einer ausreichenden Anonymisierungsmaßnahme zur Auflösung des Personenbezugs ausgehen können.

3. Pseudonymisierung i.S.v. Art. 4 Nr. 5 DSGVO

Neben der Maßnahme der Anonymisierung trägt auch die Pseudonymisierung zu einem höheren Schutz des allgemeinen Persönlichkeitsrechts der betroffenen Person bei.[13] Anders aber als bei der Anonymisierung, die zu einer vollständigen Beseitigung des Personenbezugs führt, wird im Falle der Pseudonymisierung das Identifikationsmerkmal, welches die Zuordnung des Datums zu einer identifizierten oder identifizierbaren natürlichen Person ermöglicht, durch ein Pseudonym ausgetauscht. Diese zu-

[9] *Härting,* ITRB 2016, 36 (37).
[10] *Wójtowicz*, PinG 2013, 65 (65); durch eine Veränderung der Art und Weise der Verarbeitung (bspw. mithilfe von Verschlüsselung) können Daten anonymisiert werden ohne dabei diese selbst zu verändern, vgl. *ebd.* (67).
[11] *Gola/Klug/Körffer*, in: Gola/Schomerus, § 3 Rn. 43; ausführlich zu möglichen Anonymisierungstechniken vgl. *Artikel-29-Datenschutzgruppe,* Opinion 05/2004 on Anonymisation Techniques, WP 216.
[12] Vgl. *Hofmann/Johannes*, ZD 2017, 221 (223).
[13] *Hullen*, PinG 2015, 210 (211).

sätzlichen Informationen, ohne die das personenbezogene Datum nicht mehr einer spezifischen betroffenen Person zugeordnet werden kann, sind gesondert aufzubewahren und technischen und organisatorischen Maßnahmen gegen eine Re-Identifizierung zu unterlegen, vgl. Art. 4 Nr. 5 DSGVO. Zweck des Pseudonyms ist es, dass nur derjenige, der die diesem Kennzeichen zugrundeliegende Zuordnungsregel kennt, die Pseudonymisierung rückgängig machen kann.[14] Aufgrund dessen ist der sachliche Anwendungsbereich der DSGVO für denjenigen eröffnet, der die pseudonymisierten Daten verarbeitet.[15] Erwägungsgrund 26 Satz 2 stellt klar, dass diese „als Informationen über eine identifizierbare natürliche Person betrachtet werden."

Obwohl die Pseudonymisierung also nicht dazu führt, dass Unternehmen die Anwendbarkeit der DSGVO vermeiden können, räumt sie ihnen dennoch bestimmte Privilegien ein, indem sie Unternehmen bei der Einhaltung ihrer Datenschutzpflichten unterstützt (vgl. Erwägungsgrund 28 Satz 1). So kann beispielsweise die Pseudonymisierung dazu verhelfen, den Anforderungen an die Umsetzung von geeigneten technischen und organisatorischen Maßnahmen i.S.v. Art. 25 Abs. 1 DSGVO („data protection by design") zu genügen. Die DSGVO schafft damit Anreize für Unternehmen die Pseudonymisierung als ein Mittel zu verwenden, um die Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben zu erleichtern und mindert zugleich die Risiken für die betroffenen Personen.[16]

4. Zwischenergebnis

Für Unternehmen ist es zum einen wichtig bei der Erhebung und Speicherung der Daten zu erkennen, ob diese für sie von vornherein personenbezogen oder anonym sind. Durch eine spätere Anreicherung oder Verknüpfung der Daten mit weiteren Informationen kann auch im Nachhinein der Bezug eines Datums zu einer identifizierten oder identifizierbaren Person hergestellt werden.

Zum anderen ist es für die Anwendbarkeit des Datenschutzrechts entscheidend, sofern ein Unternehmen seine personenbezogenen Datenbestände erst im Nachhinein anonymisieren möchte, dass eine De-Anonymisierung faktisch ausgeschlossen ist, damit sich das Anonymisieren als wirksame Maßnahme zur Vermeidung des Personenbezugs erweist.

III. Fehlende Trennschärfe des Personenbezugs in Theorie und Praxis

Von diesen Definitionen ausgehend sollten sich im Grunde nach anonyme und personenbezogene Daten ausschließen. Unklar bleibt indes unter welchen Voraussetzungen

[14] *Hullen*, PinG 2015, 210 (210).
[15] *Hofmann/Johannes*, ZD 2017, 221 (223).
[16] Vgl. Erwägungsgrund 28 Satz 1.

eine natürliche Person als identifizierbar gilt. Zwar sollen nach Erwägungsgrund 26 Satz 3 in Bezug auf die Identifizierbarkeit einer natürlichen Person alle Mittel Berücksichtigung finden, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinen Ermessen wahrscheinlich genutzt werden […]“. Die vom europäischen Gesetzgeber nicht vermiedene Abstraktheit und Unbestimmtheit der Terminologie schafft für Wissenschaft und Praxis aber auch weiterhin unter Geltung der DSGVO erhebliche Rechtsunsicherheit. Das Kriterium der Identifizierbarkeit bleibt damit wesentlich für das Vorliegen von personenbezogenen und nicht personenbezogenen Daten.

1. Relevanz des Personenbezugs in der Praxis

Nur kurz soll die Relevanz einer hinreichenden Unterscheidung von personenbezogenen und anonymen Daten in der Praxis verdeutlicht werden. In unserer heutigen arbeitsteiligen Informationsgesellschaft lagern immer häufiger datenverarbeitende Unternehmen beispielsweise ihre IT-Infrastruktur aus. Abgesehen von der Möglichkeit der Auftragsdatenverarbeitung nach Art. 28 DSGVO können der Einfachheit halber anonyme Daten im Rahmen des Cloud-Computings genutzt werden, ohne dass es hierfür auf die datenschutzrechtliche Zulässigkeit nach Art. 6 Abs. 1 DSGVO ankäme.[17] Die Bestimmung des Begriffs des Personenbezugs und seine Grenzen hat damit für Unternehmen enorme Auswirkungen auf den rechtssicheren Umgang mit Daten.

2. Die Theorie des absoluten und relativen Personenbezugs unter Bezugnahme der Rechtslage vor Inkrafttreten der DSGVO

Ursprünglich stellten IP-Adressen den Aufhänger für die streitige Frage dar, wann eine Person als identifizierbar (bzw. „bestimmbar“ nach der alten Rechtslage) gilt.[18] Im Wesentlichen ging es darum, welche Anforderungen an die Zusatzinformationen zur Identifizierung der natürlichen Person zu treffen sind und inwieweit es maßgebend ist, ob Dritte den Personenbezug herstellen können, sodass eine IP-Adresse als personenbezogenes Datum einzustufen ist. IP-Adressen dienen dabei als ein gelungenes Exempel für die richtungsweisende Bedeutung des Streits um den Personenbezug, denn sobald Unternehmen vernetzte Computer nutzen, werden mittlerweile standardisiert IP-Adressen verarbeitet und in Server-Log Dateien gespeichert.[19] Heutzutage trifft dies nicht nur auf nahezu jedes Unternehmen zu, sondern oft sind Unternehmen selbst Anbieter von Online-Mediendiensten, wie es in der vom EuGH zu entscheidenden Rechtssache der Fall war.[20] Die Bejahung des Personenbezugs von IP-Adressen, obwohl

[17] Vgl. m.w.N. *Kühling/Klar*, NJW 2013, 3611 (3612 f.).
[18] Grundlegend *EuGH*, Urt. v. 19.10.2016, mit Anmerkung *Kühling/Klar*, ZD 2017, 24 (25 f.).
[19] *Bergt*, ZD 2015, 365 (365).
[20] Beim Anbieter von Online-Mediendiensten handelte es sich in der EuGH-Entscheidung allerdings um die Bundesrepublik Deutschland und um kein privatrechtliches Unternehmen.

ein Unternehmen selbst nicht über diejenigen Zusatzinformationen verfügt, die in Verbindung mit der IP-Adresse eine Identifizierung der natürlichen Person ermöglichen würden, kann somit weitreichende Konsequenzen für datenverarbeitende Unternehmen haben und muss entsprechend ebenso auf andere Datenverarbeitungsszenarien übertragen werden.

a) Absoluter Personenbezug

Die zentrale Frage nach dem Vorliegen eines personenbezogenen Datums betrifft jedoch nicht nur die Problematik der Identifizierbarkeit bei IP-Adressen, sondern ebenso verschiedenste Sachverhalte, in denen über die Anwendbarkeit des Datenschutzrechts gestritten wird. Dementsprechend haben sich schon die unterschiedlichsten Rechtsauffassungen vor Geltung der DSGVO herausgebildet.[21] Vertreter der Theorie des absoluten Personenbezugs stellen im Allgemeinen auf die objektive Möglichkeit ab, dass nicht nur der Verantwortliche selbst, sondern auch irgendein Dritter die natürliche Person identifizieren und somit einen Personenbezug herstellen kann.[22] Für datenverarbeitende Unternehmen hätte dies zur Konsequenz, dass sie nach dieser derart weitreichenden Ansicht fast immer von der Anwendbarkeit des Datenschutzrechts ausgehen müssten.

b) Relativer Personenbezug

Nach der relativen Theorie soll es bei der Beurteilung des Personenbezugs von Daten nur auf den jeweiligen Verantwortlichen ankommen.[23] Sofern also ein Unternehmen die Identität der natürlichen Person nicht mit eigenen Mitteln ermitteln kann, findet das Datenschutzrecht keine Anwendung – ergo: die Daten wären lediglich anonym. Teilweise wird eine relativierte Ansicht vertreten, dass auch dann ein Personenbezug der Daten anzunehmen sei, wenn das Unternehmen die Daten an einen Dritten übermittelt, der über das zur Identifizierung erforderliche Zusatzwissen verfügt.[24] Diesbezüglich kritisieren Vertreter der Gegenauffassung, dass es widersprüchlich sei, ein und dasselbe Datum für ein und denselben Verantwortlichen zum einen als anonym und zum anderen aber als personenbezogen im Falle des Vorliegens des Übermittlungstatbestandes zu qualifizieren.[25]

---

[21] Zum Überblick des Theorienstreits und den weiteren Ausprägungen im Einzelnen vgl. *Bergt*, ZD 2015, 365 (365 ff.).
[22] So etwa *Pahlen-Brandt*, DuD 2008, 34 (38); *Düsseldorfer Kreis*, Beschluss „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ vom 26./27. November 2009; *Heidrich/Wegener*, DuD 2010, 172 (174); *Breyer*, ZD 2014, 400 (405).
[23] U.a. *Voigt*, MMR 2009, 377 (379).
[24] U.a. *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 3 Rn. 10; *Kühling/Klar*, NJW 2013, 3611 (3615); *Dammann*, in: Simitis, § 3 Rn. 32.
[25] Vgl. *Breyer*, ZD 2014, 400 (404).

c) EuGH, Rs. C-582/14, Breyer vs. BRD

Der EuGH hat sich für einen „verschärften“ relativen Personenbezug entschieden, denn grundsätzlich soll es zwar auf das Wissen des Verantwortlichen ankommen, aber dieser muss sich unter Umständen das Wissen des Dritten zurechnen lassen.[26] Die Inanspruchnahme eines Dritten, der über Zusatzinformationen zur Identifikation der natürlichen Person verfügt, stellt nämlich nur dann ein Mittel dar, das vernünftigerweise zur Bestimmung der betreffenden Person vom Verantwortlichen eingesetzt wird, wenn der Verantwortliche über rechtliche Möglichkeiten verfügt, um diese Informationen vom Dritten zu erlangen. Genauere Anforderungen an das rechtliche Mittel lässt der EuGH aber offen.[27]

3. Aktuelle Rechtslage nach der DSGVO

a) Keine hinreichende Klärung unter Geltung der DSGVO

Der Streit des absoluten und relativen Personenbezugs währt unter Geltung der DSGVO trotz der Rechtsprechung des EuGH zur Personenbeziehbarkeit von IP-Adressen fort.[28] Allein aus dem Wortlaut des Art. 4 Nr. 1 DSGVO kann nicht entnommen werden, auf wessen Wissen, Fähigkeiten oder Mittel es konkret bei der Identifizierung der betroffenen Person ankommen soll. Umgekehrt wird ebenso in der DSGVO nicht hinreichend spezifiziert, ob im Falle eines unverhältnismäßig großen Re-Identifizierungsaufwands noch von einer Anonymisierung auszugehen ist oder diese Daten bereits einer betroffenen Person zuzuordnen sind.[29] Wegen der unscharfen Begriffe des Personenbezugs und der Anonymität bedarf es deshalb unter Bezugnahme der Erwägungsgründe einer Auslegung hinsichtlich dieser Frage unter besonderer Berücksichtigung technologischer Entwicklungen.

b) Kriterien des Einsatzes von Mitteln zur Identifizierung

Dennoch ist zu vermuten, dass der langwierige Streit der Identifizierbarkeit zumindest ein wenig Anklang in der DSGVO in Erwägungsgrund 26 gefunden hat. Danach sollen alle Mittel zur direkten oder indirekten Identifizierung der natürlichen Person berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person „nach allgemeinen Ermessen wahrscheinlich“ genutzt werden (vgl. Erwägungsgrund 26 Satz 3). Dies entspricht eben solchen Mitteln, die „vernünftigerweise“ eingesetzt werden und zumindest laut EuGH zur alten Rechtslage im Falle des Vorliegens von rechtlichen Mit-

[26] *EuGH*, Urt. v. 19.10.2016, mit Anmerkung *Kühling/Klar*, ZD 2017, 24 (28).
[27] So auch *EuGH*, Urt. v. 19.10.2016, mit Anmerkung *Kühling/Klar*, ZD 2017, 24 (28).
[28] Zustimmend *Härting*, ITRB 2016, 36 (36); von einem absoluten Verständnis in der DSGVO ausgehend hingegen *Buchner*, DuD 2016, 155 (156).
[29] Vgl. *Hofmann/Johannes*, ZD 2017, 221 (223).

teln zutrifft.[30] Die bloße Möglichkeit einer Identifizierung reicht also gerade nicht aus, denn dem Erwägungsgrund 26 ist in diesem Kontext eine einschränkende Funktion zuzusprechen.[31] Welche sonstigen Voraussetzungen aber abseits von rechtlichen Mitteln für die Annahme vorliegen könnten, dass das verantwortliche Unternehmen „vernünftigerweise" Zugriff auf die bei dem Dritten befindlichen erforderlichen Zusatzinformationen zur Identifikation der Personen nehmen kann, bleibt weiterhin vage. Fest steht lediglich, dass nicht nur das Unternehmen selbst über das zur Identifikation erforderliche Zusatzwissen verfügen muss, sondern es genügt, dass ein Dritter die Zusatzinformationen einer natürlichen Person zur Identifikation zuordnen kann.

Im Hinblick auf die Wahrscheinlichkeit, ob Mittel des Verantwortlichen oder einer anderen Person konkret eingesetzt werden, fließen alle objektiven Kriterien, wie etwa die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, in die Entscheidung ein, vgl. Erwägungsgrund 26 Satz 4. Beispielsweise besteht die Möglichkeit, dass ein Unternehmen mit unterschiedlichen, voneinander getrennten Datenbanken, diese miteinander verknüpft, sodass ohne großen technischen, zeitlichen oder finanziellen Aufwand die zugrundeliegenden Daten einen Personenbezug erhalten können (dabei kommt es nicht darauf an, ob tatsächlich das Unternehmen ein solches Vorhaben umsetzt).[32] Im Gegensatz dazu erscheint es eher unwahrscheinlich, dass ein Unternehmen Zusatzinformationen eines Dritten zur Identifikation der natürlichen Person in Anspruch nehmen wird, wenn dem Unternehmen dessen Existenz nicht einmal bekannt ist.[33]

c) Gefahr einer omnipräsenten Möglichkeit der Nutzung von Mitteln zur Identifizierung infolge des technologischen Fortschritts

Diese Annahmen geraten doch in Anbetracht des technologischen Fortschritts immer häufiger ins Wanken. Solche Kriterien des Aufwands an Zeit, Kosten und Arbeitskraft werden vor dem Hintergrund der immer leichter verfügbaren, kostengünstigen und einfach zu handhabenden Technologie womöglich nur noch selten als unverhältnismäßig erscheinen.[34] Die Gefahr, dass eine allzu weite Auslegung des Personenbezugs dazu führt, dass jede Art von Information als personenbezogenes Datum eingeordnet werden könnte, da niemals mit absoluter Sicherheit ausgeschlossen werden könne, dass es nicht einen Dritte gibt, der im Besitz von entsprechendem Zusatzwissen ist,[35] besteht ebenso in Anbetracht des schnellen technologischen Fortschritts. Der Verdacht

[30] Vgl. *Hofmann/Johannes*, ZD 2017, 221 (224).
[31] *Roßnagel*, § 3 Rn. 10.
[32] Vgl. Beispiel bei *Laue/Nink/Kremer*, § 1 Rn. 17.
[33] *Hofmann/Johannes*, ZD 2017, 221 (224).
[34] Vgl. *Hullen*, PinG 2015, 210 (211).
[35] So etwa Generalanwalt beim EuGH *Sanchez-Bordona,* Schlussanträge v. 12.5.2016, BeckRS 2016, 81027, Rn. 65.

liegt nahe, dass es immer eine spezielle intelligente Software oder einen IT-Experten geben wird, denen es gelingt, vermeintlich anonymisierte Daten doch wieder einer identifizierbaren Person zuzuordnen.[36] So können allein schon jetzt Metadaten, die dazu dienen ausgewählte Aspekte von Primärdaten zu beschreiben,[37] derartige Zusatzinformationen enthalten, dass durch sie ein Rückschluss auf die natürliche Personen im Primärdatum gewährt werden kann. Auch wenn erforderlich ist, dass die zu berücksichtigende Technologie für datenverarbeitende Unternehmen vor allem verfügbar i.S.v. zugänglich sein muss,[38] verbleibt nichtsdestotrotz eine wenig Skepsis, dass in naher Zukunft die Zugänglichkeit solcher Technologien nicht mehr eine große Herausforderung darstellen dürfte.

Die Möglichkeiten einer Re-Identifizierung schreiten derart voran und sind allgegenwertig, dass der Anonymisierung als Maßnahme zur Vermeidung des Personenbezugs zukünftig wohl nur noch wenig Raum gegeben werden kann. Dies hätte zur Folge, dass Unternehmen keinerlei Anreiz mehr hätten ihre Daten zu anonymisieren und die Anonymisierung datenschutzrechtlich de facto gegenstandslos wäre. Letztendlich ist deshalb die Sinnhaftigkeit der Anonymisierung als Maßnahme für ein Unternehmen zur Vermeidung der Personenbeziehbarkeit im Hinblick auf den technischen Fortschritt zu hinterfragen.

d) Dynamische Auslegung

Die Befürchtung eines Endes echter Anonymität[39] ist zumindest vor dem Hintergrund einer dynamischen Auslegung des Datenschutzrechts unbegründet. Im Rahmen der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, sind gemäß Erwägungsgrund 26 Satz 4 ebenso die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen. Der DSGVO wohnt damit zumindest eine gewisse Zukunfts- und Entwicklungsfähigkeit inne.[40] Ziel der DSGVO kann es nicht sein, wirtschaftliche Prozesse infolge von datenschutzrechtlichen Vorgaben zu hemmen, wenn in Anbetracht neuer technologischer Gegebenheiten Unternehmen einen ausnahmslosen Personenbezug von Daten zu befürchten haben. Stattdessen müssen die datenschutzrechtlichen Beurteilungsmaßstäbe zugleich dynamisch angepasst werden, um Rechtssicherheit zu gewährleisten.

Diese Erwägungen sind ebenso auf den „technologieneutralen“ Schutzumfang der datenschutzrechtlichen Vorschriften (vgl. Erwägungsgrund 15 Satz 1) zurückzuführen.

[36] Vgl. *Hullen*, PinG 2015, 210 (211); *Härting*, ITRB 2016, 36 (37).
[37] So m.w.N. die Definition bei *Krüger/Möllers*, MMR 2016, 728 (728).
[38] *Hofmann/Johannes*, ZD 2017, 221 (224).
[39] So etwa *Härting/Schneider*, CR 2015, 819 (822).
[40] *Hofmann/Johannes*, ZD 2017, 221 (223).

Technikneutralität bedeutet in erster Linie, dass der Rechtsrahmen der DSGVO auch auf technische Weiterentwicklungen angewendet werden kann. Zur Konsequenz hat dies aber nicht, dass je mehr technisch möglich wird, desto eher von einem Personenbezug auszugehen ist. Vielmehr soll die Auslegung des Begriffs der „nach allgemeinem Ermessen wahrscheinlich[en]“ Nutzung entsprechend der technologischen Entwicklungen „mitwandern“. Die DSGVO soll gerade auch noch in Zukunft, wenn durch neue Technologien problemlos Informationen rekonstruiert werden können, nur insoweit zum Schutz natürlicher Personen bei der Verarbeitung beitragen, wie solche Daten auch schützenswert sind.

Art. 4 Nr. 1 DSGVO ist somit dahingehend auszulegen, dass selbst in Anbetracht technologischer Möglichkeiten immer noch objektive Faktoren im Einzelfall derart überwiegen können, dass davon auszugehen ist, eine Identifikation der natürlichen Person wird nicht erfolgen. Es liegt sodann kein Personenbezug des Datums vor, obwohl eine Zuordnung zur natürlichen Person technisch möglich wäre. Die Prognose, dass die Anonymisierung im Datenschutzrecht auszusterben droht,[41] wird sich daher so nicht bewahrheiten.

IV. Fazit und Ausblick

Die Antwort auf die eingangs aufgeworfene Frage, ob Daten trotz ihres möglichen Aussagegehalts über eine natürliche Person tatsächlich keinerlei Personenbezug aufweisen können, muss zwar mit Blick auf die zu erwartenden technologischen Entwicklungen grundsätzlich verneint werden, die DSGVO kann aber dennoch den künftigen Herausforderungen standhalten.

Wenn zukünftig anzunehmen ist, dass die Technologie das Datenschutzrecht überholen und somit die Möglichkeit des Anonymisierens „aushebeln“ kann, darf auch das Datenschutzrecht die Technologie „aushebeln“ und fordern, dass nicht das Optimum an technischen Fähigkeiten als Maßstab zu gelten hat, sondern der Anwender der Technik im Mittelpunkt einer Wahrscheinlichkeitsprüfung steht. Objektive Faktoren, wie etwa die Wirtschaftlichkeit einer Identifizierungsmaßnahme, sind in jedem Einzelfall grundlegend zu berücksichtigen und ins Verhältnis zur verfügbaren Technologie zu setzen. Andernfalls würde der mit der DSGVO verfolgte Anreiz der Datenanonymisierung ins Leere laufen, wenn der europäische Gesetzgeber tatsächlich gewollt hätte, dass es im Zuge von technologischen Entwicklungen für Unternehmen kaum noch einen Bereich geben soll, in dem nicht datenschutzrechtliche Regelungen angesichts der Verarbeitung von personenbezogenen Daten eingreifen würden.

[41] So *Härting*, ITRB 2016, 36 (37).

Erst wenn sich die technologische Situation derart zugespitzt hat, dass Unternehmen nicht mehr den geringsten Aufwand für eine Re-Identifizierung erbringen müssen, können möglicherweise andere Kriterien im Hinblick auf die Eröffnung des Anwendungsbereichs der DSGVO diskutiert werden. Nicht zu Unrecht geht das Gefahrenpotential des Missbrauchs selten von einem einzelnen personenbezogenen Datum selbst aus, sondern von der Kombination und Verknüpfung mit anderen Informationen, einschließlich einer Auswertung der Daten.[42] Dahingehend muss der Begriff des personenbezogenen Datums durch den Einfluss technischer Entwicklungen immer wieder neupositioniert werden. Deshalb sollte durchaus die Diskussion um eine Abkehr von der Einteilung der Daten mit und ohne Personenbezug hin zu einer Abstufung der Daten nach der Sensibilität ihres Inhalts und der Eingriffsintensität angeregt geführt werden.[43]

Literaturverzeichnis

Artikel-29-Datenschutzgruppe, Opinion 05/2004 on Anonymisation Techniques, adopted on 10 April 2014, WP 216.

Bergt, Matthias, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts, Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365-371.

Breyer, Patrick, Personenbezug von IP-Adressen, Internetnutzung und Datenschutz, ZD 2014, 400-405.

Buchner, Benedikt, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155-161.

Düsseldorfer Kreis, Beschluss „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ vom 26./27. November 2009.

Gola, Peter / Schomerus, Rudolf (Hrsg.), BDSG Bundesdatenschutzgesetz Kommentar, 12. Aufl., München 2015.

Härting, Niko, Beiträge für die Beratungspraxis, Datenschutz-Grundverordnung – Anwendungsbereich, Verbotsprinzip, Einwilligung, ITRB 2016, 36-40.

Härting, Niko / Schneider, Jochen, Eine Rückbesinnung auf die Kern-Anliegen des Privatsphärenschutzes, CR 2015, 819-827.

[42] *Härting/Schneider*, CR 2015, 819 (820).
[43] Vgl. in diese Tendenz gehend *Härting/Schneider*, CR 2015, 819 (824).

Heidrich, Joerg / Wegener, Christoph, Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen, DuD 2010, 172-177.

Hofmann, Johanna / Paul, Johannes, DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs, Begriffserklärung der entscheidenden Frage des sachlichen Anwendungsbereichs, ZD 2017, 221-226.

Hullen, Nils, Anonymisierung und Pseudonymisierung in der Datenschutz-Grundverordnung, PinG 2015, 210-212.

Krügel, Tina, Das personenbezogene Datum nach der DS-GVO, Mehr Klarheit und Rechtssicherheit?, ZD 2017, 455-460.

Krüger, Jochen / Möllers, Frederik, Metadaten in Justiz und Verwaltung, Neue juristische Problemkategorie im Rahmen der elektronischen Aktenführung?, MMR 2016, 728-731.

Kühling, Jürgen / Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl., München 2018.

Kühling, Jürgen / Klar, Manuel, Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, 3611-3617.

Laue, Philip / Nink, Judith / Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl., Baden-Baden 2016.

Paal, Boris P. / Pauly, Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Pahlen-Brandt, Ingrid, Datenschutz braucht scharfe Instrumente, Beitrag zur Diskussion um „personenbezogene Daten", DuD 2008, 34-40.

Roßnagel, Alexander (Hrsg.), Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, Baden-Baden 2017.

Roßnagel, Alexander, Wie zukunftsfähig ist die Datenschutz-Grundverordnung?, DuD 2016, 561-565.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz Kommentar, 8. Aufl., Baden-Baden 2014.

Voigt, Paul, Datenschutz bei Google, MMR 2009, 377-382.

Wójtowicz, Monika, Wirksame Anonymisierung im Kontext von Big Data, PinG 2013, 65-69.

Die Einwilligung nach der Datenschutz-Grundverordnung

Julia Münzenmaier

Rechtsreferendarin am OLG Bamberg und
Wissenschaftliche Mitarbeiterin am Lehrstuhl für Staatsrecht, Völkerrecht, Internationales Wirtschaftsrecht und Wirtschaftsverwaltungsrecht (Prof. Dr. Pache), Universität Würzburg
julia.muenzenmaier@jura.uni-wuerzburg.de

Abstract

Die Rechtmäßigkeit der Datenverarbeitung von personenbezogenen Daten gemäß Art. 6 Abs. 1 DS-GVO knüpft hauptsächlich an die Einwilligung der betroffenen Personen zur Datenverarbeitung an. Eine solche Einwilligung ist nur entbehrlich, wenn besondere gesetzliche Erlaubnistatbestände zur Datenverarbeitung eingreifen. Im Rahmen dieses Beitrags soll untersucht werden, welche Anforderungen an die wirksame Einwilligung gestellt werden.

Art. 4 Nr. 11 DS-GVO, Art. 7 DS-GVO und zahlreiche Erwägungsgründe legen dabei bestimmte Voraussetzungen fest. So ist es zum Beispiel für eine wirksame Einwilligung elementar, dass die Einwilligung freiwillig erteilt wurde. Eine Legaldefinition bezüglich der Freiwilligkeit wird jedoch in der DS-GVO nicht getroffen, allerdings finden sich in den Erwägungsgründen nähere Anhaltspunkte hinsichtlich der Freiwilligkeit. Laut Erwägungsgrund Nr. 42 muss der Nutzer „eine echte oder freie Wahl“ haben und somit in der Lage sein, „die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“. Auch Situationen, in denen ein klares Ungleichgewicht zwischen dem für die Datenverarbeitung Verantwortlichen und der betroffenen Person besteht, können gegen das Vorliegen der Freiwilligkeit sprechen. Zudem bestehen bei bestimmten Koppelungen einer Leistung mit einer Einwilligung in die Datenverarbeitung Bedenken an die Freiwilligkeit der Einwilligung.

Anhand von Beispielen und einem Vergleich mit der früheren Rechtslage soll dargestellt werden, wann eine Einwilligung wirksam ist.

I. Einführung

Seit dem 25.05.2018 ist die Datenschutz-Grundverordnung (DS-GVO) als allgemein gültige Verordnung innerhalb der EU unmittelbar anwendbar. Diese Verordnung re-

gelt, unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen.

Grundsätzlich ist gemäß Art. 6 DS-GVO jede Datenverarbeitung zunächst verboten, soweit die betroffene Person nicht in die Verarbeitung einwilligt oder ein gesetzlicher Erlaubnistatbestand eingreift. Daher ist die Einwilligung eine der zentralen Rechtmäßigkeitsvoraussetzungen für die Datenverarbeitung (vgl. Art. 6 Abs. 1 S. 1 lit. a DS-GVO), sie wird sogar als „Maß der Rechtmäßigkeit“[1] der Datenverarbeitung bezeichnet. Manche sehen die Einwilligung deswegen auch als „entscheidenden Grundpfeiler des Datenschutzes“[2] an.

Gemäß Art. 4 Nr. 11 DS-GVO ist die Einwilligung der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

In der früheren Datenschutzrichtlinie (DSRL)[3] war die Einwilligung ähnlich definiert: Gemäß Art. 2 lit. h DSRL war die Einwilligung der betroffenen Person jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte und mit der die betroffene Person akzeptierte, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

Folglich hat sich der Wortlaut der Einwilligung kaum geändert. Im Vergleich mit der früheren Datenschutzrichtlinie ist in der DS-GVO jedoch Art. 7 hinzugekommen, der weitere Voraussetzungen für die Wirksamkeit der Einwilligung nennt. Insofern stellt die DS-GVO eine Neuerung zur früheren europäischen Rechtslage dar. Im Bundesdatenschutzgesetz (BDSG) a.F. waren allerdings schon vor Inkrafttreten der DS-GVO weitere Anforderungen an die Einwilligung zur Datenverarbeitung geregelt.

Im Folgenden soll die Rechtsnatur der Einwilligung geklärt werden und welche Anforderungen an eine wirksame Einwilligung bestehen. Zudem wird untersucht, ob die Regelungen der DS-GVO in Bezug auf die Einwilligung große Änderungen im Vergleich mit der vorherigen Rechtslage mit sich bringen.

II. Primärrechtliche Vorgaben

Die zentrale Bedeutung der Einwilligung lässt sich auf Art. 8 Abs. 2 S. 1 GrCH zurückführen, der jeder Person das Recht auf den Schutz der sie betreffenden personenbezo-

[1] *Ernst*, ZD 2017, 110 (110); *Ernst*, in: Paal/Pauly, Art. 4 Rn. 61.
[2] So *Albrecht*, CR 2016, 88 (91).
[3] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281/31 (außer Kraft seit dem 24.05.2018).

genen Daten garantiert. Demnach dürfen diese personenbezogenen Daten nur mit einer expliziten gesetzlich geregelten Grundlage oder mit der Einwilligung der betroffenen Person verarbeitet werden. Auch Art. 16 Abs. 1 AEUV garantiert den Schutz der personenbezogenen Daten, erwähnt aber im Gegensatz zu Art. 8 Abs. 2 S. 1 GrCH nicht ausdrücklich das Erfordernis einer Einwilligung zur Datenverarbeitung.

Indem Art. 5 Abs. 1 lit. a DS-GVO regelt, dass personenbezogene Daten auf rechtmäßige Weise verarbeitet werden müssen, und Art. 6 Abs. 1 lit. a DS-GVO als Voraussetzung für die rechtmäßige Datenverarbeitung die Einwilligung nennt, werden die primärrechtlichen Vorgaben umgesetzt. Die Einwilligung ist also Ausdruck der informationellen Selbstbestimmung.

III. Rechtsnatur

Die Rechtsnatur der Einwilligung war schon nach alter Rechtslage gemäß des BDSG a.F. umstritten. Einige sahen in ihr eine rechtsgeschäftliche Erklärung[4], andere eine geschäftsähnliche Handlung[5] und manche einen bloßen Realakt[6]. Die Vorschriften über Willenserklärungen sollten demnach entweder direkt oder nur entsprechend angewandt werden.

Die DS-GVO bestimmt die Rechtsnatur der Einwilligung nicht näher. Nunmehr ist sie jedoch nicht mehr nach deutschem Recht auszulegen, sondern unionsrechtlich autonom zu bestimmen.[7] Demnach wird die Einwilligung als rechtserhebliche Handlung *sui generis* gesehen,[8] weshalb die deutschen Regelungen in Bezug auf Mängel bei Willenserklärungen nicht anwendbar sind.

Die DS-GVO regelt nicht, ob bei Vorhandensein von Willensmängeln zum Beispiel die Anfechtung der Einwilligung möglich ist. Teilweise wird vertreten, in solchen Fällen auf das nationale Recht zurückzugreifen und die §§ 119, 123 BGB entsprechend anzuwenden, soweit Unionsrecht dem nicht entgegensteht.[9] Allerdings ist es konsistenter, bei einem Irrtum des Einwilligenden nicht auf analoge Anwendungen der §§ 119, 123 BGB zurückzugreifen, sondern stattdessen von einer Unwirksamkeit der Einwilligung aufgrund von fehlender Informiertheit oder Täuschung auszugehen. Wurde eine Einwilligung aufgrund einer Drohung erteilt, fehlt es ohnehin schon an der Freiwilligkeit der Einwilligung. Daher liegt zudem keine Regelungslücke vor, die für eine analoge Anwendung der §§ 119, 123 BGB erforderlich wäre.

[4] *Schild*, in: BeckOK, Art. 4 Rn. 130.
[5] *Kühling*, in: BeckOK, § 4a BDSG a.F. Rn. 33.
[6] *Zscherpe*, MMR 2004, 723 (724); *Spindler*, in: Spindler/Schuster § 4a Rn. 3.
[7] *Buchner/Kühling*, in: Kühling/Buchner, Art. 7 Rn. 1a.
[8] So *Buchner/Kühling,* in: Kühling/Buchner, Art. 7 Rn. 1a.
[9] *Stemmer*, in: BeckOK, Art. 7 Rn. 29; *Lang/Peintinger*, ELR 2013, 206 (210).

IV. Voraussetzungen der Einwilligung

Neben der Legaldefinition der Einwilligung in Art. 4 Nr. 11 DS-GVO regeln Art. 6 Abs. 1 lit. a, Art. 7 und Art. 8 DS-GVO weitere Voraussetzungen der wirksamen Einwilligung in die Datenverarbeitung. Außerdem geht eine Vielzahl von Erwägungsgründen näher auf die Anforderungen an eine Einwilligung ein.

1. Einwilligungsfähigkeit

In der DS-GVO wird nicht geregelt, wann eine Person zur Einwilligung fähig ist. Jedoch können nicht nur Volljährige wirksam in ihre Datenverarbeitung einwilligen, denn Erwägungsgrund Nr. 65 S. 3 setzt voraus, dass eine Einwilligung „im Kindesalter“[10] gegeben werden kann. Somit geht der europäische Gesetzgeber davon aus, dass Minderjährige grundsätzlich in die Verarbeitung ihrer personenbezogenen Daten einwilligen können. Demnach ist also für die Einwilligung keine (volle) Geschäftsfähigkeit nach deutschem Recht notwendig.[11]

Es ist vielmehr darauf abzustellen, ob die Minderjährigen einsichtsfähig sind.[12] Die Person muss also im konkreten Fall dazu fähig sein, die Bedeutung und Tragweite der Einwilligung zu erfassen.[13] Dabei kommt es auf eine Beurteilung des Einzelfalls an. Je weitreichender die Datenverarbeitung ist, desto älter muss das Kind in der Regel sein.

Anders ist dies bei der Einwilligung eines Minderjährigen in Bezug auf Dienste der Informationsgesellschaft gemäß Art. 8 DS-GVO. Dienste der Informationsgesellschaft sind solche Dienstleistungen, die in der Regel gegen Entgelt im Fernabsatz und auf individuellen Abruf eines Dienstleistungsempfängers erbracht werden.[14] Demnach ist bei Minderjährigen unter 16 Jahren die Datenverarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Nach Art. 8 Abs. 1 S. 3 DS-GVO können Mitgliedstaaten durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, allerdings darf diese nicht unter dem vollendeten dreizehnten Lebensjahr liegen. Von dieser Möglichkeit hat Deutschland jedoch bislang keinen Gebrauch gemacht.

[10] Die englische Fassung verwendet die Bezeichnung „as a child“.
[11] A.A. *Schild*, in: BeckOK, Art. 4 Rn. 130, der auf die Geschäftsfähigkeit abstellt.
[12] *Buchner/Kühling*, in: Kühling/Buchner, Art. 7 Rn. 67.
[13] *Stemmer*, in: BeckOK, Art. 7 Rn. 33.
[14] So die Legaldefinition in Erwägungsgrund Nr. 16 der Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, ABl. EG 1998, L 217/8, außer Kraft seit 06.10.2015, und Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. 2015, L 241/1.

Da explizit in Art. 8 DS-GVO eine Altersgrenze für bestimmte Einwilligungen festgelegt wurde, bedeutet dies im Umkehrschluss, dass in Bezug auf andere Einwilligungen keine Altersgrenze gilt.

2. Form

Grundsätzlich kann die Einwilligung formlos erklärt werden, wie Erwägungsgrund Nr. 32 klarstellt. Demnach ist eine mündliche sowie elektronische Erklärung der Einwilligung möglich. Die Formfreiheit der Einwilligung stellt eine Änderung zur vorherigen Rechtslage dar, denn nach § 4a Abs. 1 S. 3 BDSG a.F. war für die Einwilligung grundsätzlich die Schriftform erforderlich. Da allerdings gemäß Art. 7 Abs. 1 DS-GVO der Verantwortliche jederzeit in der Lage sein muss, das Vorliegen einer Einwilligung nachzuweisen, werden sich die Verantwortlichen in der Praxis häufig eine Einwilligung in Schriftform oder elektronisch in Textform geben lassen, weil eine mündliche Einwilligung kaum nachzuweisen ist.

Des Weiteren ist für die Einwilligung eine Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung notwendig. Die Einwilligung kann zwar auch konkludent erklärt werden, solange diese im jeweiligen Kontext unmissverständlich dahingehend ausgelegt werden kann, dass die betroffene Person die Datenverarbeitung akzeptiert.[15] Allerdings reichen laut Erwägungsgrund Nr. 32 Schweigen, bereits angekreuzte Kästchen oder die Untätigkeit der betroffenen Person nicht für eine wirksame Einwilligung aus. Es ist aber möglich, dass die betroffene Person ein Kästchen beim Besuch einer Internetseite anklickt und dadurch ihre Einwilligung erteilt.

Durch das Erfordernis der eindeutig bestätigenden Handlung hat die DS-GVO der „Opt-out"-Lösung („opt-out" = fehlender Widerspruch gegen die Datenverarbeitung) eine Absage erteilt. Die Einwilligung kann also nur im Rahmen einer „Opt-in"-Lösung rechtmäßig erteilt werden. Dies stellt eine Änderung zur bisherigen Rechtslage dar, denn vor dem Inkrafttreten der DS-GVO wurden „Opt-out"-Lösungen noch von dem Bundesgerichtshof toleriert.[16]

3. Informiertheit

Schon die Legaldefinition in Art. 4 Nr. 11 DS-GVO legt fest, dass eine Einwilligung nur vorliegen kann, wenn sie in „informierter Weise" abgegeben wurde. Auch nach Erwägungsgrund Nr. 32 müssen die Erklärenden ausreichend darüber informiert werden, zu welchem Zweck die Datenverarbeitung vorgenommen wird. Dient die Verarbeitung

[15] So *Franzen*, in: Franzen/Gallner/Oetker, Art. 4 Rn. 20.
[16] Vgl. BGH, NJW 2008, 3055 (Rn. 20 ff.); BGH, NJW 2010, 864 (Rn. 21 ff.); *Schantz*, NJW 2016, 1841 (1844); *Stemmer*, in: BeckOK, Art. 7 DS-GVO Rn. 83.

mehreren Zwecken, muss der Verantwortliche auf alle Verarbeitungszwecke hinweisen. Hintergrund dieser Regelung ist, dass eine Person nur dann in der Lage ist, einen freien Willen zu bilden, wenn sie alle Umstände bezüglich der Einwilligung kennt. Fehlt ein Hinweis auf die konkrete Datenverarbeitung, liegt begriffsnotwendig schon keine Einwilligung vor, weil sie nicht gemäß Art. 4 Nr. 11 DS-GVO in „informierter Weise" abgegeben wurde.

4. Zeitpunkt

Die Einwilligung muss zeitlich vor der Datenverarbeitung abgegeben werden. Wird die Einwilligung erst nach Beginn der Datenerhebung oder -verarbeitung erteilt, ist diese rechtswidrig. Dieser Mangel kann auch nicht nachträglich geheilt werden und zu einer rechtmäßigen Datenverarbeitung führen.[17]

5. Freiwilligkeit

Die Freiwilligkeit der Einwilligung ist eine der wichtigsten Voraussetzungen für die Wirksamkeit dieser. So macht schon die Legaldefinition in Art. 4 Nr. 11 DS-GVO deutlich, dass eine Einwilligung nur dann vorliegen kann, wenn sie freiwillig erteilt wurde.

Eine Legaldefinition des Begriffs Freiwilligkeit fehlt jedoch in der DS-GVO. Die vorherige Fassung der DS-GVO und die frühere Datenschutzrichtlinie verwendeten statt des Wortes „freiwillig"[18] noch den Begriff „ohne Zwang"[19]. Die neue Fassung stellt nun aber klar, dass nicht nur die Abwesenheit von Zwang gemeint ist, sondern der Nutzer bei der Abgabe der Einwilligung „freiwillig" handeln, also eine „echte oder freie Wahl"[20] haben muss.[21] Gemäß Erwägungsgrund Nr. 42 ist dies nur der Fall, wenn die betroffene Person in der Lage ist, ihre Einwilligung zu verweigern, ohne hierfür Nachteile zu erleiden.

Insgesamt ist das Vorliegen der Freiwilligkeit stets anhand des Einzelfalls zu beurteilen und kann weder pauschal verneint noch bejaht werden. Es gibt jedoch Indizien, die für die (Un-)Freiwilligkeit der Einwilligung sprechen.

Ist die Datenverarbeitung schon gesetzlich gestattet, weil die Verarbeitung zum Beispiel gemäß Art. 6 Abs. 1 S. 1 lit. b DS-GVO zur Vertragserfüllung erforderlich ist, ist fraglich, ob Raum für eine zusätzliche (freiwillige) Einwilligung in die Datenverarbeitung bleibt. So geht das Bayerische Landesamt für Datenschutzaufsicht davon aus, dass

[17] *Schild*, in: BeckOK, Art. 4 Rn. 126.
[18] In der englischen Fassung wird von „freely given" gesprochen, in der spanischen Fassung von „voluntad libre" und in der französischen Fassung von „volonté libre".
[19] Vgl. *Ernst*, in: Paal/Pauly Art. 4 Rn. 61.
[20] Erwägungsgrund Nr. 42.
[21] *Ernst*, in: Paal/Pauly, Art. 4 Rn. 69.

beim Einholen einer zusätzlichen Einwilligung einer solchen Einwilligung keine freie Entscheidung mehr zugrunde liegt.[22] Die betroffene Person hat dann nämlich keine echte Wahl, da die Datenverarbeitung auch ohne seine Einwilligung durchgeführt werden darf. Diese Auffassung des Bayerischen Landesamts für Datenschutzaufsicht ist jedoch diskutabel, da im Wege eines "erst recht"-Schlusses die Datenverarbeitung erst recht zulässig sein müsste, wenn die Verarbeitung gesetzlich gestattet ist und die betroffene Person zudem damit einverstanden ist. Selbst wenn die betroffene Person nicht einwilligen muss, kann sie mit der konkreten Form der Datenverarbeitung einverstanden sein. Auch der Wortlaut von Art. 6 Abs. 1 S. 1 DS-GVO spricht gegen die Auffassung des Bayerischen Landesamts für Datenschutzaufsicht: Demnach ist die Verarbeitung "nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen" erfüllt ist. Dies bedeutet, dass auch mehrere der in Art. 6 Abs. 1 S. 1 lit. a – f genannten Anforderungen gleichzeitig erfüllt sein können. Daraus muss man schließen, dass eine wirksame freiwillige Einwilligung auch neben einem weiteren gesetzlichen Erlaubnistatbestand vorliegen kann.

Im Folgenden werden weitere Fallkonstellationen dargestellt, bei denen das Vorliegen einer freiwilligen Einwilligung problematisch ist.

a) Klares Ungleichgewicht

Besteht ein klares Ungleichgewicht („clear imbalance") im Sinne des Erwägungsgrundes Nr. 43 S. 1 zwischen der betroffenen Person und dem Verantwortlichen und ist es in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich, dass die Einwilligung freiwillig gegeben wurde, soll diese keine gültige Rechtsgrundlage zur Datenverarbeitung liefern. Deswegen ist in Fällen eines klaren Ungleichgewichts das Vorliegen einer freiwilligen Einwilligung kritisch zu prüfen.

(1) Behörden

Der europäische Gesetzgeber geht in Erwägungsgrund Nr. 43 S. 1 davon aus, dass zwischen Behörden und betroffenen Personen grundsätzlich ein klares Ungleichgewicht besteht und die Einwilligung deswegen nicht als Rechtsgrundlage zur Datenverarbeitung dienen soll. Lässt sich zum Beispiel eine Kommune, die Schulen oder Kindergärten betreibt, eine Einwilligung für das Veröffentlichen von Fotos aus diesen Schulen oder Kindergärten geben, muss genau untersucht werden, ob die Einwilligung „in Anbetracht aller Umstände in dem speziellen Fall" (Erwägungsgrund Nr. 43 S. 1) wirklich freiwillig gegeben wurde.[23]

[22] Vgl. die Antwort des Bayerischen Amts für Landesdatenschutz auf eine Anfrage des GDD Erfa-Kreises Würzburg, Datenschutz Newsbox, Ausgabe 6 von 2018, S. 3; http://www.datakontext.com/media/pdf/23/28/77/Newsbox_6_2018dEKjlNqCDoGo6.pdf.
[23] Dieses Beispiel wurde genannt von *Leeb/Liebhaber*, JuS 2018, 534 (537).

(2) Marktbeherrschende Stellung

Verlangen marktbeherrschende Unternehmen eine Einwilligung und kann eine Person diese nicht verweigern, weil sie auf den Vertragsschluss mit dem Unternehmen angewiesen ist, gilt die Einwilligung in der Regel als nicht freiwillig erteilt. In solchen Fällen besteht nämlich üblicherweise ein klares Ungleichgewicht zwischen dem marktbeherrschenden Unternehmen und der betroffenen Person. Zudem kann die betroffene Person oftmals die Einwilligung nicht verweigern, ohne hierfür im Sinne des Erwägungsgrundes Nr. 42 Nachteile zu erleiden.

So ist es zum Beispiel problematisch, wenn die betroffene Person auf den Vertragsabschluss mit dem marktbeherrschenden Unternehmen angewiesen ist, weil dieses der einzige Stromlieferant in der Umgebung ist. Auch wenn der WLAN-Betreiber am Flughafen den Vertrag von einer Einwilligung abhängig macht, ist dies ein Indiz für die Unfreiwilligkeit der Einwilligung.[24] Die Einwilligung zur Datenverarbeitung ist ebenso bei sozialen Netzwerken wie Facebook, die den Markt beherrschen, kritisch zu bewerten: Erteilen Nutzer ihre Einwilligung nicht und müssen sich aus diesem Grund aus dem Netzwerk abmelden, erleiden sie Nachteile, weil sie dadurch den Zugriff auf ihre Kontakte verlieren.[25]

Hinsichtlich der Beurteilung der Freiwilligkeit der Einwilligung gegenüber marktbeherrschenden Unternehmen und ähnlichen Situationen von Ungleichgewicht haben sich kaum Änderungen im Vergleich zu der vorherigen Rechtslage ergeben. Schon nach BGH-Rechtsprechung wurde eine Einwilligung als nicht freiwillig angesehen, wenn sie „in einer Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung“ erklärt wurde.[26]

(3) Beschäftigungsverhältnis

Auch in sozialen Abhängigkeitssituationen wie in einem Beschäftigungsverhältnis ist die Freiwilligkeit der erteilten Einwilligung sorgfältig zu untersuchen, da dort ebenfalls häufig ein „klares Ungleichgewicht“ im Sinne des Erwägungsgrundes Nr. 43 zwischen den Beteiligten besteht.

[24] Mit diesem und weiteren Beispielen *Frenzel*, in: Paal/Pauly, Art. 7 Rn. 18. In solchen Fällen kann neben dem Kriterium des klaren Ungleichgewichts auch Art. 7 Abs. 4 DS-GVO eine Rolle spielen, wenn die beabsichtigte Datenverarbeitung über das für die Vertragserfüllung Erforderliche hinausgeht, siehe hierzu 5 b).
[25] So auch *Schantz*, NJW 2016, 1841, 1845.
[26] BGH, Urt. v. 16.7.2008 – VIII ZR 348/06, DuD 2008, 818 (820) – Payback; Urt. v. 11.11.2009 – VIII ZR 12/08, DuD 2010, 493 (495) – Happy Digits.

Vor Erlass der DS-GVO war es streitig, ob Arbeitnehmer gegenüber ihrem Arbeitgeber überhaupt in ihre Datenverarbeitung einwilligen können.[27] Der ursprüngliche Entwurf der DS-GVO der Kommission sah daher in Erwägungsgrund Nr. 34 noch vor, dass ein Beschäftigungsverhältnis stets die Freiwilligkeit der Einwilligung ausschließen würde,[28] da hierbei ein zu großes Ungleichgewicht zwischen dem Beschäftigten und dem Arbeitgeber herrschen würde. Aufgrund der untergeordneten und abhängigen Stellung des Arbeitnehmers oder Bewerbers schien der Kommission die Einwilligung allein nicht als ausreichender Schutzmechanismus.[29] In der endgültigen Fassung der DS-GVO erwähnt Erwägungsgrund Nr. 155 nunmehr explizit die Einwilligung des Beschäftigten, wodurch klargestellt ist, dass in einem Beschäftigungsverhältnis wirksam in die Datenverarbeitung eingewilligt werden kann. Auch der Schluss aus § 26 Abs. 2 BDSG ergibt, dass der Gesetzgeber nunmehr von einer wirksamen Einwilligung in einem Beschäftigungsverhältnis ausgeht.[30]

Art. 88 DS-GVO gewährt den Nationalstaaten die Möglichkeit, von Regelungen der DS-GVO im Beschäftigungskontext abzuweichen. Diese Möglichkeit hat der deutsche Gesetzgeber in § 26 Abs. 1 BDSG genutzt und die Anforderungen an die Freiwilligkeit der Einwilligung im Beschäftigungskontext genauer festgelegt: Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Gleichgelagerte Interessen können zum Beispiel dann vorliegen, wenn sich der Arbeitnehmer in eine vom Arbeitgeber zur Verfügung gestellte Geburtstagsliste einträgt. Auch wenn der Arbeitgeber die Kontodaten des Arbeitnehmers speichert und verwaltet, um diesem das monatliche Gehalt zu überweisen, kann von gleichgelagerten Interessen und somit einer freiwilligen Einwilligung in die Datenverarbeitung ausgegangen werden.

b) Koppelung der Einwilligung an andere Leistungen

Gemäß Art. 7 Abs. 4 DS-GVO muss bei der Beurteilung der Freiwilligkeit berücksichtigt werden, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Datenverarbeitung abhängig ist, obwohl diese für die Vertragserfüllung nicht erforderlich ist. Dieser

[27] Ein Überblick über den Meinungsstreit zur alten Rechtslage lässt sich gut hier finden: *Kühling*, in: BeckOK, § 4a BDSG a.F. Rn. 65; *Riesenhuber*, in: BeckOK, § 32 BDSG a.F. Rn. 36.
[28] *Buchner/Kühling*, in: Kühling/Buchner Art. 7 Rn. 6.
[29] *Riesenhuber*, in: BeckOK,§ 26 BDSG Rn. 43.1.
[30] So auch *Reichold*, in: Münchener Hdb. zum Arbeitsrecht, Bd. 1: Individualarbeitsrecht, § 96 Rn. 126.

Absatz wurde erst auf Vorschlag des Europäischen Parlaments der DS-GVO hinzugefügt, im ursprünglichen Entwurf der Kommission war ein solcher noch nicht vorhanden.[31] Allerdings sah der Vorschlag des Parlaments noch ein absolutes Koppelungsverbot vor, wonach die Koppelung eines Vertrags mit einer Einwilligung zur Datenverarbeitung, die nicht zur Vertragserfüllung erforderlich war, zwingend zur Unwirksamkeit der Einwilligung führte.[32]

Dieses absolute Koppelungsverbot wurde letztendlich nicht umgesetzt.[33] So spricht Art. 7 Abs. 4 DS-GVO nur von einem Umstand, dem „unter anderem" Rechnung getragen werden muss. Dies steht im Widerspruch zu Erwägungsgrund Nr. 43 S. 2, wonach die Einwilligung nicht „als freiwillig erteilt" gilt, wenn „die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist". Damit weist der Erwägungsgrund im Gegensatz zu Art. 7 Abs. 4 DS-GVO auf ein striktes Koppelungsverbot hin. Nichtsdestotrotz ist der Wortlaut des Art. 7 Abs. 4 DS-GVO vorrangig. Gerade weil das absolute Koppelungsverbot durch den Vorschlag des Parlaments in der Diskussion stand, zeigt der endgültige Wortlaut von Art. 7 Abs. 4 DS-GVO, dass ein striktes Verbot nicht beabsichtigt war.[34]

Laut Art. 7 Abs. 4 DS-GVO muss dem Umstand von einer Koppelung der Leistung an die Einwilligung zwar „in größtmöglichem Umfang", aber letztendlich nur „unter anderem" Rechnung getragen werden. Die Koppelung ist also nicht das einzige Kriterium zur Beurteilung der Freiwilligkeit. Zudem wäre ein absolutes Koppelungsverbot mit Art. 8 Abs. 1 und Abs. 2 GRCh unvereinbar, da dem Einzelnen als Ausdruck seiner Privatautonomie das Recht gewährt werden muss, frei über seine Daten zu verfügen.[35]

Die ursprünglich geltende Datenschutzrichtlinie kannte im Gegensatz zur DS-GVO noch keine Regelung zur Koppelung der Einwilligung mit Leistungen. Allerdings waren in § 28 Abs. 3 lit. b BDSG a.F. und § 95 Abs. 5 TKG bereichsspezifische Koppelungsverbote enthalten. Nach § 28 Abs. 3 lit. b BDSG a.F. durfte die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich war. Eine unter solchen Umständen erteilte Einwilligung war unwirksam. Somit fand das Koppe-

[31] S. *Buchner/Kühling,* in: Kühling/Buchner, Art. 7 Rn. 8.
[32] *Buchner/Kühling,* in: Kühling/Buchner Art. 7 Rn. 46, 8; Art. 7 IV des Parlamentsentwurfs, Entschließung des Parlaments v. 12.3.2014, P7_TA(2014)0212, 115.
[33] Vgl. *Heckmann/Paschke*, in: Ehmann/Selmayr Art. 7 Rn. 56, die ebenfalls von keinem absoluten Koppelungsverbot ausgehen. Ebenso *Frenzel*, in: Paal/Pauly Art. 7 Rn. 18.
[34] A.A. *Dammann*, ZD 2016, 307 (307), nach dessen Auffassung „im praktischen Ergebnis (…) ein striktes Koppelungsverbot" vorliegt.
[35] *Heckmann/ Paschke*, in: Ehmann/ Selmayr Art. 7 Rn. 56.

lungsverbot hauptsächlich bei Monopolverträgen Anwendung.[36] Von einer Unzumutbarkeit konnte nach alter Rechtslage jedoch noch nicht ausgegangen werden, wenn vergleichbare Angebote nur zu einem höheren Preis oder zu schlechteren Gesamtkonditionen zu erhalten waren.[37] Demnach durften Unternehmen die Einwilligung der betroffenen Personen mit gewissen Vorteilen „erkaufen". Allerdings war die Einwilligung unwirksam, wenn der Abschluss eines Monopolvertrags nur mit einer entsprechenden Einwilligung zur Datenverarbeitung möglich war.[38]

Nach der heutigen Rechtslage muss im Einzelfall untersucht werden, ob die betroffene Person die Einwilligung nur deswegen (und damit unfreiwillig) erteilt hat, weil die Vertragserfüllung davon abhängig gemacht wurde.

Eine Koppelung liegt zum Beispiel vor, wenn der Betrieb einer Taschenrechner-App davon abhängig gemacht wird, dass die App auf standortbezogene Daten zugreift, um lokale Werbung anzuzeigen, obwohl der Standort des jeweiligen Nutzers für das Funktionieren der App irrelevant ist. Hier sprechen die Umstände dafür, dass in einem solchen Fall die Koppelung unzulässig ist. Allerdings spielt bei der Bewertung der Freiwilligkeit auch eine Rolle, ob der Nutzer sich problemlos eine andere App als Taschenrechner installieren kann. Es muss also stets eine Beurteilung anhand des Einzelfalls erfolgen, bei dem lediglich dem Umstand der Koppelung „in größtmöglichem Umfang Rechnung getragen" wird.

Stellt die Einwilligung die Hauptleistungspflicht dar, steht Art. 7 Abs. 4 DS-GVO allerdings nicht entgegen. Ist die Einwilligung nämlich elementarer Vertragsbestandteil, ist sie nicht für die Vertragserfüllung, sondern für den Vertragsabschluss an sich erforderlich.[39] Deswegen bleibt das Geschäftsmodell „Service gegen Daten", bei dem Nutzer eine Leistung „kostenlos" im Gegenzug für die Angabe ihrer Daten bekommen, weiterhin zulässig.[40] Das Angebot ist in diesem Fall nämlich nicht als kostenlos zu bewerten, sondern stellt einen Tausch von Leistung gegen eine Lizenz zur wirtschaftlichen Verwertung personenbezogener Daten dar. Hierfür spricht auch die geplante Richtlinie über digitale Inhalte[41], nach der Daten als Entgelt angesehen werden können. Diese Richtlinie hätte keinen Anwendungsbereich mehr, wenn eine Koppelung von Daten mit anderen Vertragsleistungen generell ausgeschlossen wäre.[42] So ist es zum Beispiel zulässig, wenn eine betroffene Person gegenüber einem Unternehmer in

[36] *Gola/Klug/Körffer*, in: Gola/Schomerus, § 28 Abs. 1 lit. a a.F.
[37] *Gola/Klug/Körffer*, in: Gola/Schomerus, § 28 Abs. 1 lit. a a.F.
[38] *Gola/Klug/Körffer*, in: Gola/Schomerus, § 28 Abs. 1 lit. a a.F.
[39] *Frenzel,* in: Paal/Pauly, Art. 7 Rn. 51.
[40] A.A. *Golland*, MMR 2018, 130 (131).
[41] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM (2015) 634.
[42] *Heckmann/Paschke*, in: Ehmann/Selmayr, Art. 7 Rn. 53.

den Bezug eines Email-Newsletters einwilligt, um hierdurch einen Rabatt beim Kauf einer Ware zu erhalten.

V. Widerruf der Einwilligung

Art. 7 Abs. 3 DS-GVO gewährt den betroffenen Personen das Recht, ihre Einwilligung jederzeit zu widerrufen. Auf diese Widerrufsmöglichkeit müssen die Personen schon bei Abgabe ihrer Einwilligung hingewiesen werden.

Des Weiteren muss der Widerruf gemäß Art. 7 Abs. 3 S. 4 DS-GVO „so einfach wie die Erteilung der Einwilligung" gestaltet sein. Dies bedeutet, dass der Verantwortliche den Widerruf nicht erschweren darf, indem er bestimmte Voraussetzungen daran knüpft. Beispielsweise ist es nicht möglich, den Widerruf per E-Mail auszuschließen.

In der früheren Datenschutzrichtlinie und im BDSG a.F. war eine Widerrufsmöglichkeit noch nicht ausdrücklich erwähnt, allerdings ging man schon nach der alten Rechtslage davon aus, dass ein Widerruf der einmal erteilten Einwilligung möglich sein muss.[43]

VI. Fortgeltung von Einwilligungen nach altem Recht

In der DS-GVO findet sich keine ausdrückliche Norm zur Regelung, ob Einwilligungen, die vor dem Inkrafttreten der DS-GVO erteilt wurden, fortgelten. Allerdings legt Erwägungsgrund Nr. 171 fest, dass Datenverarbeitungen, die vor dem 25.05.2018 bereits begonnen haben, innerhalb von zwei Jahren nach Inkrafttreten der DS-GVO mit ihr in Einklang gebracht werden sollen. Beruhen die Verarbeitungen auf einer Einwilligung gemäß DSRL, ist eine erneute Einwilligung nicht erforderlich, wenn die Art der bereits erteilten Einwilligung den Bedingungen der DS-GVO entspricht.

VII. Abweichendes nationales Recht

Die DS-GVO regelt die Anforderungen an die Einwilligung zwar weitestgehend abschließend, allerdings dürfen die Nationalstaaten im bereichsspezifischen Datenschutz teilweise von der DS-GVO abweichen und spezifischere Rechtsvorschriften erlassen, wie dies zum Beispiel Art. 88 Abs. 1 DS-GVO für den Beschäftigtendatenschutz normiert. Daher gibt es in Deutschland ein spezielles Formerfordernis für die Einwilligung im Beschäftigungskontext. Gemäß § 26 Abs. 2 S. 3 BDSG bedarf die Einwilligung nämlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

[43] *Buchner/Kühling*, in: Kühling/Buchner Art. 7 Rn. 33.

Aufgrund der nationalen Abweichungsmöglichkeiten ist die Harmonisierungswirkung hinsichtlich der Einwilligung als Legitimationstatbestand überschaubar.[44]

VIII. Fazit

Durch Inkrafttreten der DS-GVO wurde die Einwilligung etwas besser geregelt und einige Voraussetzungen genauer gestaltet. Die grundlegenden Anforderungen finden sich nun in der DS-GVO und nicht mehr in einer Richtlinie und verschiedenen nationalen Gesetzen. Aufgrund der Formfreiheit ist es mittlerweile einfacher, die Einwilligung zu erteilen und diese später auch zu widerrufen. Zudem können bestimmte Anforderungen an die Einwilligung mithilfe der Erwägungsgründe leichter ausgelegt werden. Allerdings bringt die DS-GVO im Vergleich mit dem BDSG a.F. keine schwerwiegenden Änderungen in Bezug auf die Einwilligung mit sich, da schon die vorherige Fassung des BDSG einige Regelungen zur Einwilligung enthielt. Weiterhin problematisch ist die Beurteilung, wann eine Einwilligung freiwillig erteilt wurde. In der DS-GVO und in den Erwägungsgründen sind zwar Anhaltspunkte für die Bewertung der Freiwilligkeit zu finden, aber letztendlich kommt es auf eine Abwägung im Einzelfall an. Hier wird sich erst in der Praxis zeigen, unter welchen Umständen eine betroffene Person (nicht) freiwillig in die Datenverarbeitung einwilligen kann. Außerdem können die nationalen Gesetzgeber in bestimmten Bereichen von der DS-GVO abweichen, wodurch die Anforderungen an die Einwilligung nicht vollständig harmonisiert wurden.

Literaturverzeichnis

Albrecht, *Jan Philipp,* Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 88-98.

Beck'scher Onlinekommentar (Hrsg.: *Wolff, Heinrich Amadeus/ Brink, Stefan*), Datenschutzrecht – Kommentar, 24. Aufl., München 2018.

Dammann, *Ulrich,* Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307-314.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), Datenschutz-Grundverordnung – Kommentar, 2. Aufl., München 2018.

Ernst, *Stefan*, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110-114.

Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 2. Aufl., München 2018.

[44] So auch *Buchner/Kühling*, in: Kühling/Buchner, Art. 7 Rn. 71.

Gola, Peter/Schomerus, Rudolf (Hrsg.), Bundesdatenschutzgesetz – Kommentar, 12. Aufl., München 2015.

Golland, Alexander, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, 130-135.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), DS-GVO – Datenschutz-Grundverordnung – Kommentar, 2. Aufl., München 2018.

Lang, Sonja/Peintinger, Stefan, Die wirksame Einwilligung im Datenschutzrecht unter Berücksichtigung des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-GVO) vom 25. Januar 2012, ELR 2013, 206 -215.

Leeb, Christina-Maria/Liebhaber, Johannes, Grundlagen des Datenschutzrechts, JuS 2018, 534-538.

Münchener Handbuch zum Arbeitsrecht, Band 1 – Individualarbeitsrecht (Hrsg.: *Kiel, Heinrich/Lunk, Stefan/Oetker, Hartmut*), 4. Aufl., München 2018.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutzgrund-Verordnung und Bundesdatenschutzgesetz – Kommentar, 2. Aufl., München 2018.

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841-1847.

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien – Kommentar, 3. Aufl., München 2015.

Zscherpe, *Kerstin*, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, 723-727.

Die (fehlenden) Abhilfebefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach § 16 Abs. 2 BDSG

Europarechtskonforme Umsetzung oder rechtswidrige Gesetzeslücke?

Kira Schulze Lohoff | Dr. Mirko Wieczorek

Universität Köln | Landgericht Köln
K.schulze-lohoff@gmx.de | mirkowieczorek@web.de

Abstract

Zum 25.05.2018 traten sowohl die EU-Datenschutz-Grundverordnung (DS-GVO)[1] als auch die EU-Datenschutz-Richtlinie Justiz und Inneres (DSRL-JI)[2] in Kraft. Insbesondere zur Umsetzung der nicht unmittelbar anwendbaren DSRL-JI wurde das geltende nationale Recht geändert. Konkret wurde das Bundesdatenschutzgesetz (BDSG) mithilfe des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU)[3] neu gefasst. In dem so angepassten BDSG sind unter anderem Vorschriften enthalten, die die Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI) betreffen. So werden die Befugnisse dieser Aufsichtsbehörde für den Anwendungsbereich außerhalb der DS-GVO in § 16 Abs. 2 BDSG geregelt. Ob diese Vorschrift mit ihrem Fokus auf das bereits unter § 25 BDSG a.F. geltende Beanstandungsrecht die neuen/geänderten europarechtlichen Vorgaben – insbesondere nach Art. 47 Abs. 2 DSRL-JI – hinreichend umsetzt, soll in diesem Beitrag näher beleuchtet werden.

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[3] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017.

I. Einleitung

Sowohl DS-GVO als auch DSRL-JI haben das Ziel, das Datenschutzrecht in Europa vollständig zu harmonisieren und ein gleichwertiges Schutzniveau für die Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten zu gewährleisten.[4] Die DS-GVO enthält jedoch eine Vielzahl von Öffnungsklauseln und ist deshalb ein „atypischer Hybrid aus Verordnung und Richtlinie“[5]. Zudem scheint das Ziel einer durchgreifenden Modernisierung und Anpassung des europäischen Datenschutzrechts an das Internet-Zeitalter durch die sehr umfangreiche Übernahme von Gesetzestext – und damit Gesetzessystematik – der über 20 Jahre alten EU-Datenschutzrichtlinie (DSRL)[6] konterkariert zu werden.[7] Ob damit die angestrebte Vollharmonisierung und Anpassung an das Internet-Zeitalter gelungen ist, ist also fraglich, kann jedoch für die hiesige Untersuchung dahinstehen.

Das im Zuge des Inkrafttretens der DSRL-JI neu gefasste BDSG enthält jedenfalls auch zahlreiche Vorschriften (§§ 8 ff. BDSG), die den Aufgabenbereich der BfDI betreffen und die im Mittelpunkt der vorliegenden Untersuchung stehen sollen (zum Problemaufriss s. Punkt II.). Die BfDI ist als Aufsichtsbehörde zuständig für die öffentlichen Stellen des Bundes, § 9 BDSG. Dabei hat sie neben den in der DS-GVO direkt normierten Aufgaben nach § 14 BDSG die dort niedergelegten Aufgaben für die vorgenannten Stellen im Bereich Justiz und Inneres wahrzunehmen. Hierzu stehen ihr nach § 16 BDSG Befugnisse zu, von denen die (fehlenden) Abhilfe- und Durchgriffsbefugnisse nach § 16 Abs. 2 BDSG im Nachfolgenden genauer betrachtet werden sollen.

II. Problemaufriss

§ 16 BDSG enthält Regelungen zu den Befugnissen der BfDI als Aufsichtsbehörde sowohl im Anwendungsbereich der DS-GVO als auch im Anwendungsbereich der DSRL-JI und nationaler Datenschutzvorschriften. Dabei stellt § 16 Abs. 1 S. 1 BDSG lediglich eine (deklaratorische) Bezugnahme auf die unmittelbar geltenden Befugnisse der Aufsichtsbehörde gem. Art. 58 DS-GVO dar, die in § 16 Abs. 1 S. 2-4 BDSG um einige Verfahrensvorschriften ergänzt werden.[8] § 16 Abs. 2 BDSG regelt hingegen die Befugnisse der BfDI außerhalb des Anwendungsbereiches der DS-GVO, d.h. im Anwendungsbe-

[4] DS-GVO ErwGr 3.
[5] *Kühling/Martini*, EuZW 2016, 448 (449); vgl. auch *Kühling/Raab*, in: Kühling/Buchner, Einführung Rn. 2.
[6] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
[7] Vgl. bereits *Wieczorek*, DuD 2011, 476 (477 ff.); *Härting/Schneider*, ZRP 2011, 233 (233 f.); *Härting*, BB 2012, 459 (462 f.); *Schneider/Härting*, ZD 2012, 199 (200, 203); s.a. *Kühling/Raab*, in: Kühling/Buchner, Einführung Rn. 1 f. und Roßnagel, Rn. 58.
[8] Mehr dazu bei *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 4 ff.

reich der DSRL-JI und nationaler Datenschutzvorschriften. § 16 Abs. 3-5 BDSG enthält ferner einige – hier nicht relevante – Sondervorschriften.[9]

Nach § 16 Abs. 2 S. 1-3 BDSG steht der BfDI im Anwendungsbereich der DSRL-JI und nationaler Datenschutzvorschriften nur das Instrument der Beanstandung zur Verfügung. Inhaltlich entspricht dieses im Wesentlichen § 25 BDSG a.F.[10] § 16 Abs. 2 S. 1 BDSG entspricht hinsichtlich Beanstandung und Stellungnahme § 25 Abs. 1 S. 1 BDSG aF. Zur Nichtbeanstandung bzw. dem Verzicht auf eine Stellungnahme gleicht § 16 Abs. 2 S. 2 BDSG der Regelung in § 25 Abs. 2 BDSG aF. Auch § 16 Abs. 2 S. 3 BDSG ist mit § 25 Abs. 3 S. 1 BDSG aF identisch. Hinzu kommen einige weitere Befugnisse der BfDI, die den Wortlaut der schon bestehenden Vorschriften des BDSG übernehmen.[11]

Damit haben sich die Befugnisse der BfDI durch Inkrafttreten von DS-GVO, DSRI-JI und BDSG neu/DSAnpUG-EU in diesem Bereich praktisch kaum verändert. Nur in § 16 Abs. 2 S. 4 BDSG wurde das Recht der BfDI ergänzt, vor möglichen Datenschutzverstößen im Vorfeld der beabsichtigten Datenverarbeitung zu warnen. Damit wird Art. 47 Abs. 2 lit. a) DSRL-JI unmittelbar umgesetzt; Art. 47 Abs. 2 lit. b) und c) DSRL-JI finden hingegen keine Entsprechung im Gesetz.

Die Beanstandung nach § 16 Abs. 2 S. 1-3 BDSG selbst regelt ein Instrument der Aufsichtsbehörde für den Anwendungsbereich der DSRL-JI und Datenverarbeitungen, die durch weitere fachgesetzliche Vorschriften außerhalb des Anwendungsbereichs der DS-GVO, beispielsweise durch sicherheitsbehördliche Normen, geregelt werden.[12] Meist findet § 16 Abs. 2 BDSG auf den Bereich der Nachrichtendienste Anwendung.[13]

Vor dem Ausspruch einer Beanstandung sollten möglichst Beratungs- und Aufklärungstätigkeiten, wie sie in § 14 Abs. 1 S. 1 Nr. 4 BDSG und § 16 Abs. 2 S. 4 BDSG genannt werden, zu Rate gezogen werden. Dadurch soll erreicht werden, dass Verantwortliche zunächst für die Vorschriften über den Datenschutz sensibilisiert werden. Wenn diese milderen Maßnahmen nicht erfolgreich sind, soll die Beanstandung herangezogen werden, die den Abschluss der Datenschutzkontrolle darstellt.[14] Die anderen Instrumentarien zur Verwirklichung des Datenschutzes müssen aber nicht zwangsweise vor der formellen Beanstandung erfolgen.[15]

Gegenstand der Beanstandung nach § 16 Abs. 2 BDSG ist ein tatsächlicher Verstoß gegen Vorschriften des BDSG und nationale Vorschriften sowie sonstige datenschutz-

[9] Mehr dazu bei *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 30 ff.
[10] Detaillierter hierzu *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 2.
[11] Detaillierter hierzu *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 2.
[12] *Hullen/Krohm*, in: Plath, DSGVO/BDSG, §16 Rn. 13.
[13] *Körffer,* in: Paal/Pauly, DS-GVO/BDSG, § 16 Rn. 3
[14] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 10; *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 25 Rn. 1.
[15] *Dammann*, in: Simitis, BDSG § 25 Rn. 8.

rechtlich relevante Mängel bei der Verarbeitung personenbezogener Daten.[16] Es muss sich nicht um einen vorsätzlichen Verstoß handeln; vorliegen muss die objektive Feststellung des Verstoßes sowie die Zurechenbarkeit zum Verantwortungsbereich der verantwortlichen Stelle.[17] Bei unerheblichen Mängeln kann die Behörde von einer Beanstandung in dem ihr zugestandenen Ermessensspielraum absehen.[18]

Eine Beanstandung sollte inhaltlich die Darlegung des fraglichen Sachverhalts umfassen und insbesondere erläutern, was die Datenschutzbehörde hinsichtlich des Datenschutzes und der Verarbeitung personenbezogener Daten bemängelt.[19] Die BfDI legt ihre Rechtsauffassung dar und fordert den Adressaten zu einer Stellungnahme innerhalb der angemessenen Frist auf.[20] Die Beanstandung wird an die zuständige Behörde gerichtet.

Eine Beanstandung hat nicht die Rechtsnatur einer rechtsverbindlichen Weisung oder eines Verwaltungsakts.[21] Sie trifft keine rechtliche Regelung.[22] Beanstandungen können daher nicht mit Rechtsmitteln angegriffen werden. Für eine Klage der kontrollierten öffentlichen Stelle gegen eine Beanstandung durch die BfDI, die beim Verwaltungsgericht zu erheben wäre, fehlt daher das Rechtsschutzinteresse.[23]

Die Beanstandung hat eine spezifische datenschutzrechtliche Bedeutung.[24] Ihre Wirkung besteht darin, ein eingehendes Prüfungsverfahren auszulösen. Neben der Beanstandung gehören weitere Mittel zu den Einwirkungsmöglichkeiten der BfDI. Eine Beanstandung löst die Pflicht der Stellungnahme aus; diese ist durch die Stelle abzugeben, der die Beanstandung zugeleitet worden ist. Diese Stelle fordert ihrerseits die kontrollierte öffentliche Stelle zu einer Äußerung auf. Wenn sie sich der Auffassung der BfDI anschließt, kann sie Maßnahmen ergreifen, die einer Abhilfe dienen. Andererseits kann sie die Beanstandung auch einfach zurückweisen.[25] Die BfDI hat darüber hinaus beispielsweise die Möglichkeit, in einem Tätigkeitsbericht ihre Rechtsauffassung darlegen.[26]

Die Beanstandung entfaltet also keine unmittelbare Rechtswirkung, sondern allenfalls eine mittelbare. Vergleicht man § 16 Abs. 2 BDSG mit Art. 47 DSRL-JI, so zeigt sich,

[16] *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 25 Rn. 2.
[17] *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 25 Rn. 2; *Dammann*, in: Simitis, BDSG, § 25 Rn. 6.
[18] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 11; *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG § 25 Rn. 3.
[19] *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 25 Rn. 4.
[20] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 13.
[21] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 12; s. stellvertretend *BVerwG*, Beschl. v. 5.2.1992 – 7 B 15/92, CR 1993, 242 (242), Ls. Nr. 1, Rn. 2 f.; *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 25 Rn. 4.
[22] *BVerwG*, RDV 1993, 27.
[23] *Dammann*, in: Simitis, BDSG § 25 Rn. 20.
[24] *von Lewinsky*, in: Auernhammer, DSGVO/BDSG, § 16 Rn. 11.
[25] *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 25 Rn. 7
[26] *Meltzian*, in: Wollff/Brink, BeckOK DatenschutzR, BDSG 2018, § 16 Rn. 10.

dass Art. 47 DSRL-JI „wirksame Abhilfebefugnisse“ verlangt. Hier könnte zur Beanstandung mit ihrer nur mittelbaren Wirkung ein Widerspruch bestehen.[27] Vor diesem Hintergrund stellt sich die Frage, ob § 16 Abs. 2 BDSG die europarechtlichen Vorgaben des Art. 47 Abs. 2 DSRL-JI ausreichend umsetzt oder (rechtswidrig) dahinter zurückbleibt. Dabei lassen sich zahlreiche Argumente für die eine wie andere Sichtweise finden, die im Folgenden dargestellt werden sollen (Punkt III.).

III. Begutachtung der (fehlenden) Abhilfebefugnisse

1. Sichtweise des deutschen Gesetzgebers

Der deutsche Gesetzgeber hat sich dafür entschieden, die alte Regelung im Wesentlichen beizubehalten und der Aufsichtsbehörde jedenfalls keine unmittelbaren Durchgriffsbefugnisse zu geben. Die Gesetzbegründung BT-Drs. 18/11325 stellt die Ansicht des Gesetzgebers dar.[28] Darin wird erläutert, dass der BfDI bewusst keine Durchgriffsbefugnisse gegenüber Verantwortlichen gegeben werden sollen, die für die Verhütung, Ermittlung Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständig sind.[29]

Die DSRL-JI habe im Gegensatz zur DS-GVO Richtliniencharakter und lasse eine flexible Gestaltung zu, um den fachlichen Bedürfnissen der Straftatenverhütung, -ermittlung und -verfolgung sowie Gefahrenabwehr hinsichtlich der Datenverarbeitung und dem Bedürfnis nach ständiger Verfügbarkeit rechtmäßig erhobener Daten gerecht zu werden.[30] Die Letztentscheidungs- und Anordnungsbefugnis der Aufsichtsbehörde sei sensibel und komplex. Laut Gesetzgeber ist sie nicht mit den Zielen der Gefahrenabwehr und Strafverfolgung vereinbar.[31] Dies sei in dem die DS-GVO betreffenden, privaten Bereich, anders. Die effiziente Erreichung des Zwecks der Strafverfolgung und der Gefahrenabwehr überwiegt im Bereich der Polizei und Justiz nach dieser Auffassung gegenüber den Letztentscheidungs- und Anordnungsbefugnissen der BfDI.[32] Hier sieht der deutsche Gesetzgeber die vergleichsweise milden Beanstandungsmittel in § 16 Abs. 2 BDSG als ausreichend an.

2. Sichtweise der Aufsichtsbehörden

Auch die Aufsichtsbehörde selbst hatte sich in einer Stellungnahme gegenüber dem Bundestagsinnenausschuss zu der geplanten Neufassung des § 16 Abs. 2 BDSG geäu-

[27] Detailliert hierzu bereits *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 29; siehe auch *Körffer*, in: Paal/Pauly, DS-GVO BDSG § 16 Rn. 2; *Schaffland/Holthaus*, in: Schaffland/Wiltfang, DS-GVO/BDSG, § 16 Rn. 5.
[28] BT-Drs. 18/11325, S. 88.
[29] BT-Drs. 18/11325, S. 88.
[30] BT-Drs. 18/11325, S. 88.
[31] BT-Drs. 18/11325, S. 88.
[32] *Hullen/Krohm*, in: Plath, DSGVO/BDSG, §16 Rn. 13.

ßert.[33] Die BfDI kritisiert in der Stellungnahme, dass der status quo der alten Regelung erhalten bleibt und der BfDI nur die Möglichkeit einer Beanstandung bleibt. In der Stellungnahme wird darauf Bezug genommen, dass in Art. 47 Abs. 2 DSRL-JI wirksame Abhilfebefugnisse vorgesehen sind und Art. 47 Abs. 5 DSRL-JI die Verpflichtung vorsieht, die Möglichkeit einer gerichtlichen Klärung zu geben.[34]

Die Beanstandung sei im Gegensatz zu wirksamen Abhilfebefugnissen nicht verbindlich und durchsetzbar. Vertrete der Verantwortliche bzw. dessen Aufsichtsbehörde eine andere Rechtsauffassung als die Datenschutzaufsicht, bestünde keine Möglichkeit der Durchsetzung oder Einleitung einer gerichtlichen Klärung der Frage, ob die betreffende Verarbeitung rechtswidrig sei.[35] Eine wirksame Abhilfe könne die BfDI nicht schaffen. Die Aufsichtsbehörde verlangt daher wie im Anwendungsbereich der DS-GVO die Möglichkeit, verbindliche Anordnungen zu treffen.

3. Wortlaut des Gesetzes

§ 16 Abs. 2 BDSG soll die unionsrechtlichen Vorgaben der DSRL-JI umsetzen. Art. 47 Abs. 2 DSRL-JI bestimmt, dass die Aufsichtsbehörden über „wirksame Abhilfebefugnisse“ verfügen müssen. In der Vorschrift sind drei Beispiele zu finden, was unter wirksamen Abhilfebefugnissen zu verstehen ist:[36] Zunächst ist darunter die in Art. 47 Abs. 2 lit. a) DSRL-JI vorgesehene Warnung zu fassen. Die Aufsichtsbehörde kann Verantwortliche oder Auftragsverarbeiter davor warnen, dass beabsichtigte Datenverarbeitungen voraussichtlich gegen geltendes Datenschutzrecht verstoßen. Die Warnung wurde in § 16 Abs. 2 S. 4 BDSG umgesetzt. Zweitens kann die Aufsichtsbehörde gemäß Art. 47 Abs. 2 lit. b) DSRL-JI befugt sein, Verantwortliche oder Auftragsverarbeiter einschließlich der Anordnung der Berichtigung, Löschung oder Einschränkung anweisen zu können, wie bestimmte Verarbeitungsvorgänge auszuführen sind. Eine weitere wirksame Abhilfebefugnis kann nach Art. 47 Abs. 2 lit. c) DSRL-JI eine vorübergehende oder endgültige Beschränkung der Verarbeitung oder ein Verbot derselben darstellen.

Unter den beispielhaft aufgezählten wirksamen Abhilfebefugnissen in Art. 47 Abs. 2 DSRL-JI ist nicht die Beanstandung vorzufinden. Die Beanstandung kann aufgrund ihrer mangelnden Verbindlichkeit auch nicht ohne Weiteres in die Liste der Beispiele für wirksame Abhilfebefugnisse eingeordnet werden.[37] Folglich steht die Beanstandung nicht mit dem Wortlaut der umzusetzenden Vorgabe aus Art. 47 Abs. 2 DSRL-JI in Einklang.

[33] Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3. 2017, Ausschuss-Drs., 18(4)788, S. 4.
[34] Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3. 2017, Ausschuss-Drs., 18(4)788, S. 4.
[35] Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3. 2017, Ausschuss-Drs., 18(4)788, S. 4.
[36] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 24.
[37] Vgl. *Körffer,* in: Paal/Pauly, DS-GVO/BDSG, § 16 Rn. 3.

4. Wille des europäischen Gesetzgebers

Um zu ermitteln, ob die Vorgabe aus Art. 47 Abs. 2 DSRL-JI trotzdem hinreichend umgesetzt wurde, ist auch der Wille des europäischen Richtliniengebers zu betrachten. Aus den Erwägungsgründen zur DSRL-JI geht hervor, dass mit der Richtlinie beabsichtigt wurde, spezifische Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zu erlassen.[38] Mit dem Erlass der DSRL-JI wurde außerdem der Rahmenbeschluss 2008/977/JI des Rates für den Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit[39] abgelöst. Im Unterschied zu der DSRL-JI bezog sich der Rahmenbeschluss nur auf die Verarbeitung personenbezogener Daten, die zwischen Mitgliedsstaaten weitergegeben oder bereitgestellt wurden. Eine vergleichbare Vorschrift wie Art. 47 Abs. 2 DSRL-JI, die wirksame Abhilfebefugnisse vorsieht, war in dem Rahmenbeschluss nicht zu finden.[40]

Die DSRL-JI konkretisiert die Vorgaben des Rahmenbeschlusses 2008/977/JI hinsichtlich der Befugnisse der Aufsichtsbehörden.[41] Mit der DSRL-JI wurde beabsichtigt, einerseits die Ziele des Datenschutzes und andererseits die spezifischen Anforderungen und Besonderheiten im Bereich der Gefahrenabwehr und Strafverfolgung zu verwirklichen.[42] Um diesen Erfordernissen gerecht zu werden, sollten die Aufsichtsbehörden „die notwendige[n] Instrumente zur Erfüllung ihrer [datenschutzrechtlichen] Aufgaben“ erhalten. Dazu zählen „wirksame Befugnisse […], darunter Untersuchungsbefugnisse, Abhilfebefugnisse und beratende Befugnisse“.[43] Die Grenze der Befugnisse der Aufsichtsbehörden ist allerdings dort zu ziehen, wo es spezielle Vorschriften für Strafverfahren einschließlich der Ermittlung und Verfolgung von Straftaten gibt oder die Unabhängigkeit der Gerichte berührt wird.[44]

Die Verschärfung der Befugnisse der Aufsichtsbehörde im Anwendungsbereich der Datenschutzrichtlinie für Justiz und Polizei zeigt, dass der europäische Gesetzgeber

[38] DSRL-JI ErwGr 10.
[39] Rahmenbeschluss 2008/977/JI des Rates v. 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. EU 2008 L 350, 60).
[40] DSRL-JI ErwGr 6; *Art.-29-Datenschutzgruppe*, Stellungnahme 1/2013 zum Entwurf der DSRL-JI, WP 201, 26.2.2013, S. 6.
[41] Vgl. DSRL-JI ErwGr 82; *Art.-29-Datenschutzgruppe*, Stellungnahme 1/2013 zum Entwurf der DSRL-JI, WP 201, 26.2.2013, 6 f.; *Art.-29-Datenschutzgruppe*, Stellungnahme 3/2015 zum Entwurf der DSRL-JI, WP 233, 1.12.2015, 15; *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 26.
[42] Allg. DSRL-JI ErwGr 11.
[43] DSRL-JI ErwGr 82 S. 1.
[44] DSRL-JI ErwGr 82 S. 2; vgl. Rahmenbeschluss 2008/977/JI ErwGr 35 S. 3.

bewusst auch in diesem Bereich wirksame Abhilfebefugnisse forderte. Das Belassen bei einem Beanstandungsrecht, wie es der deutsche Gesetzgeber handhabt, wird der Zielsetzung des europäischen Gesetzgebers nicht gerecht.[45]

5. Historische Betrachtung

Historisch ist Art. 47 Abs. 2 DSRL-JI aus Art. 25 Abs. 2 lit. b) Rahmenbeschluss 2008/977/JI hervorgegangen.[46] Art. 25 Abs. 2 lit. b) Rahmenbeschluss 2008/977/JI verlangte, dass der Aufsichtsbehörde „wirksame Einwirkungsbefugnisse" zur Verfügung stehen.[47] Was unter wirksamen Einwirkungsbefugnissen zu verstehen ist, wurde beispielhaft aufgezählt. Zu den Mitteln der Aufsichtsbehörde zählten die Abgabe von Stellungnahmen, die Befugnis der Anordnung der Sperrung, Löschung und Vernichtung von Daten bzw. das vorläufige oder endgültige Verbot der Verarbeitung gegenüber dem für die Verarbeitung Verantwortlichen oder die Befugnis, Verwarnungen oder Ermahnungen auszusprechen bzw. die Parlamente oder andere politische Einrichtungen zu befassen. Die Vorschrift ist identisch mit Art. 28 Abs. 3 (zweiter Spiegelstrich) DSRL.[48]

Art. 47 Abs. 2 DSRL-JI verlangt hingegen nicht nur „wirksame Einwirkungsbefugnisse", sondern „wirksame Abhilfebefugnisse". Daran lässt sich festmachen, dass die Befugnisse im Gegensatz zum Rahmbeschluss direkter sein sollen. Eine mittelbare Einwirkung ist nicht ausreichend, sondern die Aufsichtsbehörde soll unmittelbar in die Lage versetzt werden, bei festgestellten Verstößen rechtskonforme Zustände wiederherzustellen. Auch vor dem Hintergrund einer historischen Betrachtung bleibt das Beanstandungsrecht also hinter den europarechtlichen Vorgaben zurück.

6. Systematische Auslegung

Systematisch ist § 16 Abs. 2 BDSG in die Regelungsstruktur der DSRL-JI und der DS-GVO einzubetten. Bei Betrachtung der Vorschriften lässt sich erkennen, dass sich die Beispiele für die Befugnisse in Art. 47 Abs. 2 lit. b) und c) DSRL-JI und Art. 58 Abs. 2 lit. d), f) und g) DS-GVO entsprechen. Diese Parallelität von DSRL-JI und DS-GVO steht im Widerspruch zum Argument des deutschen Gesetzgebers, dass die Abhilfebefugnisse in DS-GVO und DSRL-JI unterschiedlich ausgestaltet seien.[49] Damit hatte der deutsche Gesetzgeber eine flexible Handhabung bei der Umsetzung der DSRL-JI begründet, die es rechtfertigen sollte, dass in § 16 Abs. 2 BDSG eine Beanstandung anstatt einer wirksamen Abhilfebefugnis vorgesehen ist.

[45] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 29; *Körffer*, in: Paal/Pauly, DS-GVO BDSG § 16 Rn. 2; *Schaffland/Holthaus*, in: Schaffland/Wiltfang, DS-GVO/BDSG, § 16 Rn. 5.
[46] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 27.
[47] S. hierzu auch Rahmenbeschluss 2008/977/JI ErwGr 35 S. 1.
[48] Vgl. hierzu *Dieterich,* ZD 2016, 260 (263).
[49] BT-Drs. 18/11325, 88.

Als Unterschied zwischen beiden Normen ist jedoch festzustellen, dass es sich bei Art. 58 Abs. 2 lit. d), f) und g) DS-GVO um „echte“ Abhilfemittel handelt, während in Art. 47 Abs. 2 lit. b) und c) DSRL-JI lediglich „Beispiele für wirksame Abhilfebefugnisse“ aufgezählt werden. Streitig war auch schon im Anwendungsbereich der DS-GVO die unmittelbare Geltung der (Abhilfe-)Befugnisse des Art. 58 DS-GVO.[50] Eine Parallele zwischen beiden Vorschriften ist darin zu sehen, dass sowohl in Art. 47 Abs. 2 lit. a) DSRL-JI als auch Art. 58 Abs. 2 lit. a) DS-GVO präventive Abhilfebefugnisse aufgelistet sind, die die mildesten zu Verfügung stehenden Mittel darstellen.[51]

Ob die Abhilfebefugnisse in DS-GVO und DSRL-JI wirklich unterschiedlich ausgestaltet sind, lässt sich also nicht abschließend beurteilen. Zwar sind die Beispiele für die Befugnisse in Art. 47 Abs. 2 lit. b) und c) DSRL-JI und Art. 58 Abs. 2 lit. d), f) und g) DS-GVO identisch ausgestaltet, was dagegen spricht, dass die DSRl-JI den nationalen Gesetzgebern einen allzu großen Spielraum bei der Umsetzung ermöglichen sollte. Jedoch spricht der Unterschied zwischen „echten Abhilfemitteln“ in der DS-GVO und Beispielen für „wirksame Abhilfebefugnisse“ in der DSRL-JI durchaus für einen gewissen Spielraum, der sich dem nationalen Gesetzgeber durch die notwendige Umsetzung der Richtlinie in einfaches Recht eröffnet.

7. Richtlinienkonforme Auslegung

Neben dem klassischen Kanon der Auslegungsmethoden wird die Auslegung von Gesetzen mit europarechtlichem Hintergrund um die sogenannte richtlinienkonforme Auslegung ergänzt. Der EuGH stützt die Verpflichtung, nationale Normen im Anwendungsbereich der Richtlinie richtlinienkonform auszulegen, auf das Umsetzungsgebot des Art. 288 Abs. 3 S. 1 AEUV sowie ergänzend auf den Grundsatz der Gemeinschaftstreue gemäß Art. 4 Abs. 3 EUV.[52] Die Mitgliedsstaaten und die Organe als solche haben im Rahmen der ihnen nach nationalem Recht zustehenden Kompetenzen darauf hinzuwirken, dass die Zielsetzungen der Richtlinien erreicht werden. Gegenstand der richtlinienkonformen Auslegung sind Rechtsvorschriften der Mitgliedsstaaten, die in den Anwendungsbereich der Richtlinien fallen.[53]

Im Gegensatz zu den klassischen Auslegungsmethoden verfolgt die richtlinienkonforme Auslegung das Ziel, „die volle Wirksamkeit der fraglichen Richtlinie zu gewährleisten und zu einem Ergebnis zu gelangen, das mit dem mit der Richtlinie verfolgten

[50] *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 27; *Nguyen,* ZD 2015, 265 (269); *Dieterich,* ZD 2016, 260 (263).
[51] Vgl. zu Art. 58 Abs. 2 lit. a) DS-GVO *Eichler*, in: BeckOK DatenschutzR DS-GVO Art. 58 Rn. 18; *Nguyen*, in: Gola DS-GVO Art. 58 Rn. 11; *Dieterich,* ZD 2016, 260 (263): Eskalationsstufen.
[52] *EuGH*, 10.4.1984, C-14/83 (von Colson und Kamann), Slg. 1984, I-1891 Rn. 26.
[53] *Leenen*, JURA 2012, 753 (754).

Ziel in Einklang steht".[54] Im Verhältnis zu den nationalen Auslegungsmethoden sollte zunächst der primäre Zugriff anhand der nationalen Auslegungsmethoden erfolgen und erst danach eine Überprüfung anhand der Richtlinie stattfinden.[55] Es sind also erst die Grenzen einer möglichen Auslegung innerhalb der deutschen Methodenlehre zu ermitteln, die „der richtlinienkonformen Auslegung eine unübersteigbare Schranke" setzen.[56] Nicht zulässig ist eine richtlinienkonforme Auslegung contra legem.[57] Es gilt allerdings nicht der Wortlaut, sondern ein funktionelles Verständnis als absolute Grenze.[58] Die Grenzen einer contra legem- Auslegung sind erst überschritten, wenn auch die Grenzen der richterlichen Rechtsfortbildung, einer Auslegung im weiten Sinne, erreicht sind.[59] Voraussetzung einer richtlinienkonformen Rechtsfortbildung ist der Nachweis einer Lücke, d.h. einer planwidrigen Unvollkommenheit der Gesamtrechtsordnung. Dabei gilt vorzugsweise der „weite Lückenbegriff" der auf die Gesamtrechtsordnung abstellt und auch die Richtlinie als Maßstab für die Lückenfeststellung heranzieht.[60]

Die Beanstandung nach § 16 Abs. 2 BDSG hat die Wirkung, dass die an Recht und Gesetz gebundene oberste Bundesbehörde auf die datenschutzrechtliche Verletzung aufmerksam gemacht wird, und ist daher durchaus in der Lage, auf die Herstellung eines datenschutzkonformen Rechtszustandes hinzuwirken.[61] Die Befugnis kann auch nicht nur isoliert, wie bisher geschehen, sondern auch in einer Gesamtschau der sonstigen, der BfDI zur Verfügung stehenden Regelungen betrachtet werden. Die BfDI verfügt nämlich neben der Beanstandung über weitere Einwirkungsmöglichkeiten. Sie kann sich beispielsweise im Tätigkeitsbericht, gegenüber dem Bundestag oder anderweitig öffentlich äußern und auf diese Weise erheblichen Druck aufbauen und somit Einfluss auf die rechtswidrige Verarbeitung nehmen (s.o.).[62] Die Beanstandung ist daher nur ein Mittel, um den Adressaten darauf aufmerksam zu machen, dass die Verarbeitung datenschutzkonformen Grundsätzen nicht genügt, und nicht das einzige. Deshalb könnte der Beanstandung in einer Gesamtschau eine vergleichbare Wirkung attestiert werden wie einem echten Durchgriffs- und Abhilferecht.[63]

[54] *EuGH*, 24.1.2012, Rs. C-282/10 (Dominguez), Rn. 9.1. m.w.N.
[55] *Leenen*, JURA 2012, 753 (755).
[56] *Canaris*, in: FS Bydlinski, 40 (70).
[57] *EuGH*, NZA 2008, 581 Rn. 103 (Impact); siehe auch schon *EuGH*, Slg. I 2006, S. 6057 Rn. 110 (Adeneler).
[58] BGHZ 178, 27 Rn. 20 f.
[59] *Canaris*, in: FS Bydlinski, 47 (91).
[60] *Leenen*, JURA, 2012, 753 (760).
[61] Vgl. so auch *Meltzian*, in: BeckOK, DatenschutzR, Wolff/Brink, BDSG 2018 § 16 Rn. 10; BT-Drs. 18/11325, 88.
[62] *Meltzian*, in: BeckOK, DatenschutzR, Wolff/Brink, BDSG 2018 § 16 Rn. 10.
[63] Vgl. *Meltzian*, in: BeckOK, DatenschutzR, Wolff/Brink, BDSG 2018, § 16 Rn.10.

Allerdings wird bei dieser Auslegung die Wortlautgrenze überschritten. Von der gleichen Wirkweise eine Beanstandung wie einem echten Durchgriffs- und Abhilferecht auszugehen, würde verwischen, dass eine Beanstandung im Gegensatz zur Abhilfe eben nicht verbindlich und durchsetzbar ist.[64] Eine richtlinienkonforme Auslegung darf jedoch, wie bereits erörtert, nicht am Gesetzeswortlaut enden, sondern der Grundsatz der richtlinienkonformen Auslegung verlangt mehr als eine bloße Auslegung im engeren Sinne. Es hat eine Rechtsfortbildung nationalen Rechts zu erfolgen, um dem Gebot richtlinienkonformer Auslegung zu entsprechen.[65] Voraussetzung einer richtlinienkonformen Rechtsfortbildung ist eine planwidrige Regelungslücke im Sinne einer planwidrigen Unvollständigkeit des Gesetzes (s.o.).[66] Wie schon erläutert, ist auf den weiten Lückenbegriff abzustellen, der auch die Richtlinie als Maßstab für die Lückenfeststellung heranzieht.[67] Bei dem hier zu untersuchenden § 16 Abs. 2 BDSG ist die Lücke darin zu sehen, dass in der Norm nur von einem Beanstandungsrecht der Aufsichtsbehörde die Rede ist, während in Art. 47 Abs. 2 DSRL-JI wirksame Abhilfebefugnisse gefordert werden. Eine Gesetzeslücke liegt daher vor.

Problematisch ist allerdings die Planwidrigkeit der Lücke. Diese ist vom Standpunkt des Gesetzes selbst zu betrachten. Es kommt auf die Regelungsabsicht und den verfolgten Zweck des Gesetzes an.[68] Nach Ansicht der Rechtsprechung soll es für die Bestimmung der Planwidrigkeit auf den Widerspruch zwischen der konkreten Regelungsabsicht und der „konkret geäußerten, von der Annahme der Richtlinienkonformität getragenen Umsetzungsabsicht des Gesetzgebers [ankommen]“[69]. Es erfolgt also nach vorzugswürdiger Ansicht eine Aufspaltung zwischen einem Umsetzungswillen einerseits und einer konkreten Regelungsabsicht andererseits.[70] Ein genereller Umsetzungswille ist aber nicht ausreichend.[71]

Bei dem hier in Rede stehenden § 16 Abs. 2 BDSG wollte der nationale Gesetzgeber zwar die europarechtlichen Vorgaben aus Art. 47 Abs. 2 DSRL-JI umsetzen. Allerdings widersetzte er sich bewusst dem Wortlaut des Art. 47 Abs. 2 DSRL-JI, der eine wirksame Abhilfebefugnis fordert. Der fehlende Umsetzungswille des Gesetzgebers wird in der Gesetzesbegründung deutlich. Der nationale Gesetzgeber rechtfertigt seine Entscheidung damit, dass Letztentscheidungs- und Anordnungsbefugnisse der Aufsichtsbehörde mit den Zielen der Gefahrenabwehr und Strafverfolgung nicht vereinbar sei-

[64] S. stellv. Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3. 2017, Ausschuss-Drs., 18(4)788, S. 4; *Wieczorek*, in: Kühling/Buchner, § 16 Rn. 12.
[65] BGHZ 179, 27, Rn. 21.
[66] *BGH*, Urt. v. 26.11.2008 – VIII ZR 200/05, Rn. 22.
[67] *Leenen*, JURA, 2012, 753 (760).
[68] *Larenz*, Methodenlehre der Rechtswissenschaft, S. 358.
[69] *BGH*, Urt. v. 26.11.2008 – VIII ZR 200/05, Rn. 25.
[70] *Kroll-Ludwigs/Ludwigs*, ZJS 2009, 123 (126).
[71] *Kroll-Ludwigs/Ludwigs*, ZJS 2009, 123 (127); a.A. *Canaris*, in: FS Bydlinski, 47 (85).

en.[72] Der Hinweis des Gesetzgebers, dass eine spezialgesetzliche Regelung von Abhilfebefugnissen möglich wäre,[73] zeigt, dass er die fehlende Regelung einer unmittelbaren Befugnis der Aufsichtsbehörde erkannt hat. Daraus lässt sich schließen, dass es sich nicht um eine Planwidrigkeit handelt, sondern die fehlende Abhilfebefugnis dem konkreten Willen des nationalen Gesetzgebers entsprach. Die Voraussetzungen einer richtlinienkonformen Rechtsfortbildung sind somit nicht erfüllt.

IV. Fazit

Führt man sich die vorherigen Ausführungen vor Augen, bestehen Zweifel an der unionsrechtskonformen Umsetzung von Art. 47 Abs. 2 DSRL-JI. Zweck einer Abhilfebefugnis ist es, der Aufsichtsbehörde die Möglichkeit zu geben, bei festgestellten Verstößen rechtskonforme Zustände herzustellen.[74] In § 16 Abs. 2 BDSG hat der Gesetzgeber nur eine Beanstandung anstatt einer direkten Einwirkungsmöglichkeit vorgesehen. In § 16 Abs. 2 S. 4 BDSG setzt er zwar eine der in Art. 58 DS-GVO unmittelbar geregelten Befugnisse tatsächlich um, aber es handelt sich dabei leidglich um die in Art. 47 Abs. 2 lit a) DSRL-JI beispielhaft genannte Warnung. Diese ist nur ein präventives Mittel und das mildeste der genannten Befugnisse. Es wäre durchaus möglich gewesen, noch weitere Maßnahmen, die in Art. 58 DS-GVO geregelt sind, in § 16 Abs. 2 BDSG aufzunehmen. Doch dies unterließ der Bundesgesetzgeber bewusst. Er beließ es bei dem milden Beanstandungsrecht und macht damit deutlich, dass er auf eine möglichst einvernehmliche Zusammenarbeit zwischen Aufsichtsbehörde und Verantwortlichen setzt.

Historisch betrachtet wäre eine solche Regelung der Einwirkungsbefugnisse zur Umsetzung von Art. 25 Abs. 2 lit. b) des Rahmenbeschlusses 2008/977/JI unproblematisch gewesen, weil demnach nur „wirksame Einwirkungsbefugnisse“ erforderlich waren. Der aktuelle Art. 47 Abs. 2 DSRL-JI sieht aber „wirksame Abhilfebefugnisse“ vor und verlangt daher eine direkte Einflussnahme der Aufsichtsbehörde. Auch die Aufsichtsbehörde selbst kritisiert in ihrer Stellungnahme, dass der Bundesetzgeber den status quo der alten Regelung konserviert und die BfDI nur die Möglichkeit einer Beanstandung hat.[75] Die Beanstandung sei nicht als wirksame Abhilfebefugnis zu sehen, da sie nicht verbindlich und durchsetzbar ist. Vertrete der Verantwortliche bzw. dessen Aufsichtsbehörde eine andere Rechtsauffassung als die Datenschutzaufsicht, bestünde keine Möglichkeit der Durchsetzung oder Einleitung einer gerichtlichen Klärung der Frage, ob die betreffende Verarbeitung rechtswidrig ist.[76]

[72] BT-Drs. 18/11325, 88.
[73] BT-Drs. 18/11325, 88.
[74] *Selmayr,* in: Ehmann/Selmayr, DS-GVO Art. 58 Rn. 18.
[75] Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3. 2017, Ausschuss-Drs., 18(4)788, S. 4.
[76] Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3. 2017, Ausschuss-Drs., 18(4)788, S. 4.

Doch der Bundesgesetzgeber rechtfertigt die Abweichung vom Befugniskatalog der DS-GVO damit, dass die DSRL-JI Richtliniencharakter habe und eine flexible nationale Umsetzung zulässt, um den Ziele des Datenschutzes und den spezifischen Anforderungen und Besonderheiten im Bereich der Gefahrenabwehr und Strafverfolgung gerecht zu werden. Eine Letztentscheidungs- und Anordnungsbefugnis der Aufsichtsbehörde sei nicht mit den Zielen der Gefahrenabwehr und Strafverfolgung vereinbar. Eine genaue Begründung liefert der Gesetzgeber allerdings nicht.

Hinzu kommt die Erklärung des Bundesgesetzgebers, dass er das Fehlen der direkten Abhilfemöglichkeit und der damit verbundenen Problematik erkannt hat. Deshalb weist er auf die Möglichkeit der Schaffung einer spezialgesetzlichen Regelung, wie es in § 67 Abs. 2 BKAG-E seinerzeit bereits diskutiert wurde, hin. Ein spezialgesetzliches Abhilferecht müsste aber nicht zusätzlich geregelt werden, wenn schon in § 16 Abs. 2 BDSG Möglichkeiten direkter Einwirkung geschaffen würden. Dieses Argument verdeutlicht daher umso mehr die Schwäche der Vorschrift. Ferner wird durch die Argumentation verdeutlicht, dass die fehlende Regelung einer Abhilfebefugnis nicht planwidrig ist. Einer europarechtskonformen Rechtsfortbildung des § 16 Abs. 2 BDSG wird somit kein Raum gelassen.

Insgesamt ist also zu sagen, dass aufgrund der mangelnden Regelung direkter Abhilfebefugnisse in § 16 Abs. 2 BDSG die besseren Argumente dafür sprechen, dass die Vorschrift europarechtswidrig ist. Möglicherweise ist die unbefriedigende Rechtslage dem Zeitdruck der baldigen Verabschiedung des BDSG geschuldet gewesen. Eine Nachbesserung erscheint jedenfalls angezeigt, um der Rechtssicherheit Rechnung zu tragen. Um die Grenzen der mitgliedsstaatlichen Ausgestaltungsbefugnis zu definieren und Klarheit zu schaffen, könnte daher ein Vertragsverletzungsverfahren nach Art. 258 AEUV dienlich sein.

Literaturverzeichnis

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Auernhammer – Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (Hrsg.), DSGVO/BDSG, 6. Aufl., Köln 2018.

Brink, Stefan/Wolff, Heinrich Amadeus (Hrsg.), BeckOK Datenschutzrecht, 24. Edition (Stand: 01.05.2018), München.

Canaris, Claus-Wilhelm, Die richtlinienkonforme Auslegung und Rechtsfortbildung im System der juristischen Methodenlehre, in: Festschrift für Bydlinski, 2002, 47-103.

Dieterich, Thomas, Rechtsdurchsetzungsmöglichkeiten der DS-GVO – Einheitlicher Rechtsrahmen führt nicht zwangsläufig zu Einheitlicher Rechtsanwendung, ZD 2016, 260-266.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO Datenschutz-Grundverordnung – Kommentar, München 2017.

Gola, Peter (Hrsg.), Datenschutz-Grundverordnung VO (EU) 2016/679 – Kommentar, 2. Aufl., München 2018.

Gola, Peter/Schomerus, Rudolf (Hrsg.), BDSG Bundesdatenschutzgesetz, 12. Aufl., München 2015.

Härting, Niko, Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf, BB 2012, 459-466.

Härting, Niko/Schneider, Jochen, Das Dilemma der Netzpolitik, ZRP 2011, 233-236.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG – Kommentar, 2. Aufl., München 2018.

Kühling, Jürgen/Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448-454.

Kroll-Ludwigs, Kathrin/Ludwigs, Markus, Die richtlinienkonforme Rechtsfortbildung im Gesamtsystem der Richtlinienwirkungen, ZJS, 2/2009, 123-130.

Larenz, Karl, Methodenlehre der Rechtswissenschaft, 6. Auflage, 1991.

Leenen, Detlef, Auslegung von Richtlinien und richtlinienkonforme Auslegung, JURA 10/2012, 753-762.

Moos, Flemming (Hrsg.), Datennutzungs- und Datenschutzverträge, 2. Aufl., Köln 2018.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG – Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG, 3. Aufl., Köln 2018.

Roßnagel, Alexander (Hrsg.), Das neue Datenschutzrecht, Kassel 2018.

Schaffland, Hans-Jürgen/Wiltfang, Noeme (Hrsg.), Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), 2018.

Schantz, Peter/Wolff, Heinrich Amadeus (Hrsg.), Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Schneider, Jochen/Härting, Niko, Wird der Datenschutz nun endlich internettauglich? Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht, ZD 2012, 199-203.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014.

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung – Handkommentar, Baden-Baden 2017.

Wieczorek, Mirko, Informationsbasiertes Persönlichkeitsrecht, DuD 2011, 476-479.

Polizeiliche Body-Cams

Eine rechtliche Bewertung

Julien Duryn

Wissenschaftlicher Mitarbeiter, Roman Müller-Böhm, MdB
Julien.Duryn@gmail.com

Abstract

Videotechnik war schon vor der Jahrtausendwende ein Einsatzmittel, welches bei den Polizeibehörden Anklang gefunden hat. Seitdem hat sich ihr Einsatz nicht nur quantitativ erhöht. Die eingesetzten Systeme wurden um vielfältige technische Geräte ergänzt. Vergleichsweise neu ist die erstmals 2014 in Hessen eingesetzte Body-Cam. Diese kleine, meist auf der Schulter getragene Kamera wird bereits in anderen Ländern eingesetzt. Sie dient in Deutschland als neutraler Beobachter. Sie kann eine Situation ohne Vorbelastung oder Zugehörigkeit aufzeichnen und wiedergeben. Dies dient der Abschreckung und Beweissicherung, nicht aber der Überwachung der Beamten[1] in ihrem Handeln, wie in den USA.

Nach nun vier Jahren Einsatz in Hessen sind weitere Bundesländer gefolgt und neben dem erweiterten Repertoire sind auch neue Gesetze geschaffen worden. Ob diese der Technik entsprechen und die Art und Weise der Regelungen in Deutschland dem Einsatz von Body-Cams gerecht wird, soll im Folgenden nachgegangen werden.

I. Ein neues Einsatzmittel

Die Polizeien von Bund und Ländern haben eine breite Auswahl an technischen Hilfsmitteln für Maßnahmen gegenüber dem Bürger. Im Bereich der Datenerhebung ist die Aufzeichnung von Videos ein vielseitig eingesetztes Mittel. Der „klassische“ Kameraeinsatz, welcher sich dadurch auszeichnet, einen Gesamteindruck eines Areals zu liefern oder ausgemachte Objekte erfasst, ist dabei ein häufig verwendetes und bewährtes Einsatzgerät.[2]

Ein aus rechtlicher und technischer Sicht neues Einsatzmittel ist die Body-Cam. Entgegen der festen Kamera zeichnet sich die Body-Cam dadurch aus, dass sie auf einzel-

[1] Aus Gründen der besseren Lesbarkeit wird auf die geschlechtsspezifische Unterscheidung verzichtet.
[2] *Martini/Nink/Wenzel*, NVwZ – Extra 2016, 1 (4); *Arnd/Staffa*, Die Polizei 2016, 190 (191).

ne Bürger gerichtet ist und diese unmittelbar aufzeichnet. Sie kann in jeder Einsatzsituation ihres Trägers herangezogen werden und damit nahezu jedes Geschehen erfassen.

Neben der rein faktischen Wirkung auf den Bürger als Einsatzgerät, welches ihm direkt gegenüber zum Einsatz kommt, entfaltet sie auch in rechtlicher Hinsicht eine neue Dimension der Datenerfassung.

II. Intensität des Grundrechtseingriffs

Um den Einsatz von Body-Cams beurteilen zu können, ist zunächst festzustellen, in welcher Form die Rechte des Bürgers beeinträchtigt werden.

1. Aufnahmen allgemein

Personenbezogene Datenerhebungen durch ein Aufnahmegerät greifen in die Grundrechte des Bürgers ein.[3] Insbesondere sind hier das allgemeine Persönlichkeitsrecht Art. 2 I i.V.m. Art. 1 I GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung[4] und je nach Maßnahme auch Art. 13 GG, die Unverletzlichkeit der Wohnung, zu nennen.[5]

2. Aufnahmen durch Body-Cams

Die besondere Qualität der Aufnahmen durch Body-Cams liegt zunächst darin, dass sie sich zielgerichtet gegen den Adressaten einer Maßnahme richten und damit den Bürger konkret zum Gegenstand der Aufzeichnung machen.[6] Die Erfassung Einzelner wird damit, selbst bei minderer Aufzeichnungsqualität, besonders hervorgehoben.[7]

Zudem besteht bei der Body-Cam bereits aufgrund der Mobilität im Einsatz die Möglichkeit, dass sich der tragende Beamte während einer Maßnahme bewegt. Damit könnten neben dem Adressaten auch weitere unbeteiligte Bürger erfasst werden.

Es liegt nicht länger maßgeblich beim Adressaten, ob er aufgezeichnet wird. Man denke etwa an Geldautomaten, Geschäftsräume oder Bahnsteige, bei denen sich derjenige, der von einer Aufzeichnung betroffen ist, bewusst in diese Situation begibt.

Die Kamera des Beamten hingegen ist trotz Kennzeichnungspflicht nicht unmittelbar erkennbar, sodass eine Person ohne ihr Wissen aufgenommen werden kann.

---

[3] *BVerfG*, Urt. v. 11.03.2008, BVerfGE 120, 378 (397 f.); *dass.*, Beschl. v. 11.08.2009, NJW 2009, 3293 (3293); *dass.*, Beschl. v. 23.07.2007, NJW 2007, 688 (690); *BVerwG*, Urt. v. 25.01.2012, NVwZ 20212, 757 (758).
[4] Vgl. dazu das Volkszählungsurteil, *BVerfG*, Beschl. v. 09.03.1988, BVerfGE 78, 77.
[5] *BVerfG*, Beschl. v. 23.02.2007, NVwZ 2007, 688 (690); *Lachenmann*, NVwZ 2017, 1424 (1425); *Di Fabio* in: Maunz/Dürig, Art. 2 I Rn. 176; *Wysk*, VerwArch 2018, 141 (145).
[6] *Ziebarth*, Die Polizei 2017, 76 (76).
[7] *Lachenmann*, NVwZ 2017, 1424 (1425).

III. Rechtlicher Charakter der Body-Cam

Videoaufzeichnungen durch Body-Cams sind intensiver, aber auch flexibler, als durch feste Kameras. Erforderlich für die rechtliche Handhabung ist somit festzustellen, welche Funktionen ihr zukommen und aus welcher Rechtsquelle sich Regelungen ergeben.

1. Qualifikation der Maßnahme

Videoüberwachung durch Polizei- und Ordnungsbehörden werden für die Gefahrenabwehr und die Straftatverfolgung genutzt. Dieser Wechselseitigkeit aus Prävention und Repression entspringt die Qualität einer Doppelfunktionalität.[8]

Eine solche Maßnahme wird überwiegend so gehandhabt, dass nach dem Schwerpunkt zu entscheiden ist, unter welchen Bereich sie fällt.[9] Jedoch ist bei den Body-Cams gerade dieser Schwerpunkt umstritten.

2. Bisherige Handhabung

In den Begründungen zu den polizeigesetzlichen Tatbeständen der Body-Cams liegt der Schwerpunkt auf der Prävention.[10] Ihr Einsatz wirke in erster Linie deeskalierend, indem Adressaten ein größeres Risiko strafrechtlicher Verfolgung eröffnet wird. Es steht somit bei einem Body-Cam-Einsatz regelmäßig bereits fest, in welchem Umfang eine rechtswidrige Handlung vorliegt und durch wen sie begangen wird.[11]

Im Hinblick auf den Primärzweck ist bedenklich, dass der Einsatz einer Body-Cam den Schutz der Polizeibeamten nicht als Maßnahme per se durchsetzt, sondern Handlungen der Beamten und des Umfeldes lediglich dokumentiert. Sie würde damit nur mittelbar im Rahmen einer nachgelagerten Verfolgung Wirkung entfalten.[12]

Zudem sprechen Bund und Länder den Aufzeichnungen der Body-Cams eine repressive Funktion zu, indem in den Gesetzen auch die Strafverfolgung geregelt wird.[13] Folglich macht bei Prävention durch drohende Repression der Strafverfolgungsaspekt einen Schwerpunkt des Einsatzes aus und der Repressionscharakter ist nicht nur Beiwerk.[14]

---

[8] *Arzt/Schuster*, DVBl 2018, 351 (351); *Kipker*, in: Taeger, Tagungsband DSRI-Herbstakademie 2016, 121 (124); *Kipker/Gärtner*, NJW 2015, 296 (297); *Martini/Nink/Wenzel*, NVwZ – Extra, 1 (8); *Wysk*, VerwArch 2018, 141 (150).
[9] *Ehlers/Schneider*, in: *Schoch/Schneider/Bier* VwGO, § 40 Rn. 606; *Jortzig/Kunze*, Jura 1990, 294 (297).
[10] Vgl. Gesetzesbegründung § 27a BPolG, BT-Drs. 18/10939, S. 12-13; Gesetzesentwurf § 15c PolG NRW, LT-Drs. 16/12361, S. 14.
[11] *Martini/Nink/*Wenzel, NVwZ-Extra 2016, 1 (9).
[12] *Arzt/Schuster*, DVBl 2018, 351 (351).
[13] Vgl. die Tatbestände von Bund und Ländern.
[14] Vgl. *Schnabel*, NVwZ 2010, 1457 (1458); *Roggan*, NVwZ 2001, 134 (139); *Arzt/Eier*, NZV 2010, 113 (116).

Bisher regeln Bund und Länder den Einsatz der Body-Cam allein über die Polizeigesetze. Der gefahrenabwehrrechtliche Aspekt wird als so ausschlaggebend betrachtet, dass der Einsatz hauptsächlich dem Bereich der Polizeien zuzuordnen sei und entsprechend dem Grundsatz Polizei ist Ländersache[15] nach Art. 30 und 70 I GG den Landesgesetzgebern unterfällt.

Allerdings entspringt dem unklaren Gesamteindruck die Forderung nach einer strafprozessualen Grundlage.[16] Im Sinne der Rspr. des BVerfG ist die Strafverfolgungsvorsorge kompetenzmäßig dem „gerichtlichen Verfahren“ i.S.d. Art. 74 I Nr. 1 GG zuzuordnen, und damit den Regelungen der StPO.[17]

In seinem Urteil zum Kameraeinsatz der Hamburger Polizei im Stadtteil St. Pauli hat das BVerwG festgestellt, dass durch den Bund keine abschließenden Regelungen bezüglich der Strafverfolgungsvorsorge getroffen wurden.[18]

Überträgt man dies unmittelbar auf den Einsatz der Körperkameras, verbliebe die rechtliche Verordnung der gesetzlichen Grundlage für einen Body-Cam-Einsatz entsprechend § 484 IV StPO so lange im Polizeirecht, bis der Bund eine entsprechende Regelung in das Gesetz einfügt,[19] oder dies mit Absicht nicht regelt.[20]

3. Getrennte Handhabung

Eine solche Handhabung der Body-Cams wie statische Überwachungskameras im Sinne der Rspr. des BVerwG erscheint nicht der Tragweite dieses Einsatzmittels gerecht zu werden.

Eine beabsichtigte Nichtregelung erscheint bei der Gesamtwürdigung der Überwachungstatbestände der StPO nicht bezweckt. Zwar hat auch der Bund eine eigene polizeigesetzliche Grundlage für den Einsatz von Body-Cams geschaffen, jedoch lässt sich daraus allein keine bewusste Nichtregelung ableiten. Mit Blick auf den wachsenden „Trend“ unter den Ländern, die Körperkamera zu einem Bestandteil des polizeilichen Repertoires zu machen, ist zu vermuten, dass die Entwicklung noch nicht abgeschlossen ist und sich eine Positionierung der Gesetzgeber erneut verändern kann.

Statt der umfassenden Regelung durch ein Gesetz kommt hier eine getrennte Handhabung entsprechend der Verwendung einer Body-Cam-(Aufzeichnung) in Betracht.

[15] *Zöller*, NVwZ 2005, 1235 (1239).
[16] Vgl. *Schnabel*, NVwZ 2010, 1457 (1458); *Roggan*, NVwZ 2001, 134 (139); *Arzt/Eier*, NZV 2010, 113 (116).
[17] *BVerfG*, Urt. v. 27.07.2005, NJW 2005, 2603 (2605).
[18] *BVerwG*, Urt. v. 25.01.2012, NVwZ 2012, 757 (760).
[19] *Wysk*, VerwArch 2018, 141 (152); *Kipker/ Gärtner*, NJW 2015, 296 (297).
[20] *Schnabel*, NVwZ 2010, 1457 (1459); *BVerfG*, Urt. v. 27.10.1998, NJW 1999, 841 (843).

Den Gesetzgebern ist hinsichtlich des Schutzzwecks ihrer Polizeibeamten ausreichend Raum zu geben. Insofern erscheint es angemessen, den „vor Ort“-Einsatz der Body-Cam als polizeiliche Maßnahme in das Gefahrenabwehrrecht der Länder zu verorten.

Daneben ist der Fall, dass eine Body-Cam von vornherein oder während der Maßnahme repressiv ausgerichtet ist, unproblematisch als Mittel der StPO zu erfassen.[21]

Der Einsatz an sich zeichnet sich durch einen gesetzgeberisch zugrunde gelegten Präventionszweck aus. Daneben besteht die Verarbeitung im Kern aus der Sichtung und Speicherung des Materials und der Nutzung zur Strafverfolgung. Damit liegt deren Schwerpunkt klar im repressiven Bereich und es wäre eine strafprozessuale Grundlage zur Weiterverarbeitung notwendig.

Folglich ist zwischen dem Einsatz an sich und der späteren Datenverarbeitung als eigene Maßnahme zu trennen. Im Bereich der Datenverarbeitung bedeutet dies, dass entgegen der bisherigen Handhabung die Anforderungen an Bearbeiterkreis, Einsicht und Löschung zentral durch die StPO zu regeln wären.

IV. Präventive Nutzung

In allen Polizeigesetzen der Länder und dem des Bundes finden sich Regelungen zum Einsatz von Videokameras.[22] Zudem haben die Gesetzgeber Normen geschaffen oder erweitert, durch die der Einsatz der Body-Cams eine eigene Regelung findet.[23]

1. Besondere Tatbestände im Vergleich

Gemäß des Vorbehalts des Gesetzes bedarf ein staatlicher Eingriff einer parlamentsgesetzlichen Grundlage.[24] Diese bewirkt den Ausgleich zwischen dem rechtfertigenden überwiegenden Allgemeininteresse[25] und dem Grundrechtseingriff.[26]

Bei Body-Cams sind hohe Anforderungen an die Umstände des Einsatzes zu stellen, dass dieser gerechtfertigt ist und vielfach wurde hierbei schon diskutiert, wie diese auszusehen haben.[27]

[21] *Arzt/Schuster*, DVBl 2018, 351 (357).
[22] Vgl. § 27 BPolG; § 21 II PolG BW; Art. 33 I bis III PAG Bay; § 24 bis 24b ASOG Bln, § 31 BbgPolG; § 29 I bis III BremPolG; § 8 I bis IV HmbPolDVG; § 14 I bis IV HSOG; § 32 SOG MV; § 32 Nds. SOG; § 15a PolG NRW; § 27 POG RPF; § 27 I bis II SPolG; § 37 SächsPolG; § 16 SOG LSA; § 184 LVwG; § 33 PAG TH.
[23] Vgl. § 27a BPolG; § 21 V-VIII PolG BW; Art. 33 IV, VI, VIII PAG Bay; § 29 V BremPolG; § 8 V HmbPolDVG; § 14 VI HSOG; § 32a SOG MV; § 32 IV Nds. SOG; § 15c PolG NRW; § 27a POG RPF; § 27 III SPolG; § 37 II SächsPolG; § 33 VI PAG TH.
[24] *Grzeszick*, in: Maunz/Dürig, Art. 20 Rn. 75; *Huster/Rux*, in: BeckOK GG, Art. 20 Rn. 172.
[25] *Di Fabio*, in: Maunz/Dürig, Art. 2 I Rn. 181.
[26] *Wysk*, VerwArch 2018, 141 (150).

Die Uneinheitlichkeit der Polizeigesetze weckt den Verdacht, dass im Hinblick auf den schweren Grundrechtseingriff trotz der Erfahrungen seit dem ersten Einsatz 2014 bei Bund und Ländern einige Regelungen nicht alle Bedürfnisse einer ausreichenden Ermächtigungsgrundlage abdecken.

a) Beschreibung des Einsatzmittels

Auch wenn die eingesetzten Systeme untereinander ähnlich sind, benennen nicht alle Tatbestände die Body-Cam in vergleichbarer Präzision.

So haben neben dem Bund[28] von den zwölf Bundesländern, die zurzeit Body-Cams im Polizeidienst einsetzen oder zumindest ein Pilotprojekt gestartet haben[29], nur Baden-Württemberg, Bayern, Mecklenburg-Vorpommern, NRW und Rheinland-Pfalz, einen gesetzlichen Tatbestand geschaffen, der die Body-Cams auf ein konkretes Einsatzmittel beschränkt.[30] Das Mittel wird als (*Bild- und Ton-)-Aufzeichnungsgerät* bzw. *Aufnahmegerät* welches *nahe am Körper getragen wird* bezeichnet.

Die restlichen Länder verwenden zwar eigens auf die Body-Cams zugeschnittene Tatbestände, nennen aber in diesen kein konkretes Einsatzmittel,[31] sondern sprechen von der Erhebung personenbezogener Daten durch *technische Mittel (zur Bild- und Tonaufzeichnung)*.

Mit der Nennung des Einsatzmittels in einigen Tatbeständen wird einerseits der Mobilitätscharakter der Kameras verdeutlicht. Andererseits wird eine uferlose Verwendung anderer Aufnahmegeräte ausgeschlossen.

Die verbliebenen Tatbestände regeln zwar Bedingungen, aber nicht die Art der Aufnahmegeräte. Mit Blick auf die rechtlichen Grundlagen anderer Kameraeinsätze oder die Datenerhebungsgeneralklausel der Länder[32] ließe sich das konkret zu verwendende Einsatzgerät sinngemäß abgrenzen. Jedoch erscheint es wünschenswert, dass auch in den verbleibenden Landesgesetzen die Aufnahmegeräte angemessen benannt und eingegrenzt werden.

---

[27] *Kipker*, in: Taeger, Tagungsband, DSRI- Herbstakademie 2016, 121 (125 ff.); *Lachenmann,* NVwZ 2017, 1424 (1426); *Kipker/Gärtner*, NJW 2015, 296 (298); *Martini/Nink/Wenzel*, NVwZ-Extra 2016, 1 (9); *Wysk*, VerwArch 2018, 141 (150).

[28] Vgl. § 27a BPolG.

[29] Entsprechend dem Stand von August 2018.

[30] Vgl. § 21 V, VI PolG Bad.-Württ.; Art. 33 IV 1 PAG Bayern; § 15c PolG NRW; § 32a SOG M-V; § 27a POG RPF.

[31] Vgl. § 29 BremPolG; § 8 HmbPolDVG; § 14 HSOG; § 32 Nds. SOG; § 28 SPolG; § 37 SächsPolG; § 33 PAG TH.

[32] § 21 I BPolG; § 20 PolG BW; Art. 31 PAG Bay; § 18 ASOG; § 30 BbgPolG; § 28 BremPolG; § 6 HmbPolDVG; § 13 HSOG; § 27 SOG M-V; § 31 Nds SOG; § 26 POG RPF; § 26 SPolG; § 36 SächsPolG; § 15 SOG LSA: § 179 LVwG SH; § 32 PAG TH.

b) Einsatzzweck

In allen Tatbeständen findet sich eine vergleichbare Beschreibung der Zweckbestimmung der Body-Cam im Polizeieinsatz. Der *Schutz für die Polizeibeamten oder Dritte*.

Das gefährdete Rechtsgut wird auch nahezu einheitlich benannt. Die meisten Tatbestände sehen eine Gefahr für *Leib oder Leben* bzw. *die körperliche Unversehrtheit* vor.

Bayern erfasst darüber hinaus eine Gefahr für die *Freiheit* einer Person. Der Bund schließt die *Freiheit* der Person und das *Eigentum* mit ein.

Bremen, Niedersachsen, das Saarland und Thüringen knüpfen nicht an ein ausdrücklich genanntes Rechtsgut, sondern an ein Schutzbedürfnis für die Polizeibeamten an.[33]

c) Gefahrenschwelle und -Prognose

Bei der Qualität der Gefahr ist in den meisten Gesetzen von einer *Gefahr* die Rede. NRW und das Saarland fordern weiter eine *konkrete* Gefahr.[34]

Im Bremer Polizeigesetz ist explizit nur von *Umständen* die Rede[35], Niedersachsen, Thüringen und Sachsen knüpfen allein an den Umstand der Eigensicherung bzw. des Verdachts der Straftatbegehung an, ohne eine Gefahr explizit vorauszusetzten.[36]

Bezüglich der Beurteilung, ob ein Gefahrenmoment auch vorliegt, finden sich wiederum Unterschiede in den Polizeigesetzen.

Während der baden-württembergische, nordrheinwestfälische und rheinlandpfälzische Tatbestand von *Tatsachen die eine Annahme rechtfertigen* spricht[37], verlangt der des Bundes *tatsächlich bestehende Anhaltspunkte*.[38]

Bayern verlangt die *Erforderlichkeit* des Einsatzes und Mecklenburg-Vorpommern darüber hinaus eine *mit an hinreichender Wahrscheinlichkeit zu erwartende Erforderlichkeit*.[39] Dementsprechend hat ein Beamter nach seinem Ermessen zu beurteilen, ob eine Gefahr vorliegt.

Eine konkrete Gefahr ist aber selbst dort zu fordern, wo sie im Gesetzestext nicht ausdrücklich erwähnt wird.

Im Hinblick auf die hohen Anforderungen an Body-Cams und dem Schutzzweck, insbesondere hinsichtlich der Verhältnismäßigkeit einer polizeilichen Maßnahme, spre-

[33] Vgl. § 29 V 1 BremPolG; „Eigensicherung“ in §32 IV 1 Nds. SOG; § 27 III1 SPolG; § 33 VI 1 PAG TH.
[34] Vgl. § 15c I 1PolG NRW; § 27 III 1 SPolG.
[35] Vgl. § 29 V 1 BremPolG.
[36] Vgl. § 32 IV 1 Nds. SOG; § 37 II 1 SächsPolG; § 33 VI 1 PAG TH.
[37] Vgl. § § 21 V 1 PolG BW; § 15c I 1 PolG NRW; § 27a I POG RPF.
[38] Vgl. § 27a I BPolG.
[39] Vgl. Art. 33 IV 1 PAG Bay; § 32a I 1 SOG MV.

chen auch in diesem Fall die Umstände dafür, dass auch ohne explizite Nennungen der Tatbestände eine konkrete Gefahr benötigt ist.[40]

d) Konkretisierung der Maßnahme

In den Gesetzen wird unterschiedlich geregelt, welche Art von Maßnahme von der Polizei durch eine Body-Cam aufgezeichnet werden darf.

(1) Einsatz im öffentlichen Bereich

Einige Tatbestände der Länder knüpfen an bestimmte polizeiliche Standardmaßnahmen an. Hessen sieht den Einsatz bei Identitätsfeststellungen vor. Bremen und Niedersachsen beschränken den Einsatz auf Kontroll- und Anhaltesituationen im öffentlichen Verkehrsraum. Thüringen sieht den Einsatz sowohl bei Personen-, als auch bei Fahrzeugkontrollen vor.[41]

In den übrigen Gesetzen ist keine Maßnahme vorgesehen, bei denen eine Aufzeichnung erfolgen soll. Hierbei ist allerdings zu beachten, dass der Einsatz bei Maßnahmen zur Gefahrenabwehr erfolgt.

Gerade um einen wirksamen Einsatz zu schaffen, erscheint es kontraproduktiv, den Einsatz, auf einzelne Standardmaßnahmen zu beschränken, da sonst die Situationen, die anderen Maßnahmen unterworfen sind oder allein durch die Generalklauseln der Länder gelöst werden können, nicht erfasst werden.[42]

Stattdessen erscheint es sachgerecht, an das polizeiliche Ermessen für jede Vorüberlegung des Einsatzes der Body-Cams anzuknüpfen. Hinsichtlich dieser Prognose regeln die Länder dies nach den Wortlauten zwar leicht voneinander abweichend, jedoch ist einheitliche Aussage dieser Formulierungen, dass der Beamte vor einem Body-Cam-Einsatz sein Ermessen zu gebrauchen hat. Dies erscheint bezüglich der Bestimmtheit der Einsatzschwelle ausreichend.

(2) Einsatz im Bereich privater Lebensführung

Die Aufzeichnung durch Body-Cams begleitet den Beamten durch die Maßnahme. Dabei ist denkbar, dass die Maßnahme einer Ortsverlagerung unterliegt, für die eine kontinuierliche Aufnahme ihrem Tatbestand nach nicht gestattet ist.[43]

Dies kommt insbesondere bei Bereichen der Privatsphäre in Betracht, in die im Gegensatz zur Intimsphäre zwar auch eingegriffen werden kann, dies aber nur unter strengen Anforderungen an die Verhältnismäßigkeit gestattet ist.[44]

[40] Vgl. *Schenke*, JuS 2018, 505 (506).
[41] Vgl. § 29 V 1 BremPolG; § 14 VI 1 HSOG; § 32 IV 1 Nds. SOG; § 33 VI 1 PAG TH.
[42] *Martini/Nink/Wenzel*, NVwZ-Extra 2016, 1 (10).
[43] *Ziebarth*, Die Polizei 2017, 76 (78).

Eine Eingrenzung zum Einsatz in Wohnungen oder allgemein dort, wo die Sozialsphäre endet und Privat- oder sogar die Intimsphäre[45] beginnt, erscheint daher notwendig.

Das BPolG enthält diesbezüglich keinen Tatbestand. Allerdings erstreckt sich der Aufgabenbereich der Bundespolizei typischerweise auf Bereiche, die der Sozialsphäre zuzuordnen sind.[46] Kritische Situationen, etwa öffentliche Toiletten oder Umkleiden im Duty-Free Bereich, lassen sich der Intimsphäre zuordnen. In diese ist ein Eingriff ausgeschlossen,[47] womit ein besonderer Tatbestand für die Bundespolizei nicht notwendig ist.

Nur drei Landestatbestände regeln Einsätze innerhalb von Wohnungen.[48]

Bayern und NRW verlangen dafür eine *dringende Gefahr*. Entsprechend der Voraussetzungen des Eingriffs in die Sozialsphäre ist davon auszugehen, dass hier an die bedeutenden Rechtsgüter, die schon in den Tatbeständen genannt werden, anzuknüpfen ist.[49]

Die in den Gesetzen verdeutlichte Schwelle wird der benötigten Schwelle für einen rechtfertigungsfähigen Eingriff in die Privatsphäre gerecht und damit dem Bedürfnis nach den erhöhten Anforderungen an die Rechtfertigung.

Problematisch erscheinen daneben die Gesetze der Länder, die einen Body-Cam-Einsatz innerhalb von Wohnungen überhaupt nicht regeln.

Ob an dieser Stelle die allgemeinen Datenerhebungsregelungen der Polizeigesetze oder die Tatbestände anderer technischer Überwachung herangezogen werden können, erscheint höchst fraglich.

Wenn bereits die Tatbestände, welche einen Wohnungseingriff explizit vorgeben, ohne eine erhöhte Schwelle für den Eingriff als nicht rechtfertigungsfähig erscheinen, vermögen dies auch nicht die Gesetze ohne einen konkreten Tatbestand für einen Eingriff in die Bereiche der privaten Lebensführung.

Nicht geregelte Tatbestände erlauben somit keinen Eingriff in die Privatsphäre. Folglich ist ein Einsatz einer Body-Cam in der Wohnung ohne besondere gesetzliche

[44] *Di Fabio*, in: Maunz/Dürig, Art. 2 I Rn. 159.
[45] *BVerfG*, Urt. v. 15.01.2970, BVerfGE 27, 344 (351); *vgl. auch: Di Fabio, in: Maunz/Dürig, Art. 2 I Rn. 158.*
[46] Vgl. § 1 I BPolG.
[47] *Di Fabio*, in: Maunz/Dürig, Art. 2 I Rn. 158.
[48] Art. 33 IV 3 PAG Bay; § 32a III 1 SOG MV; § 15c II 1 PolG NRW.
[49] Vgl. *Arzt/Schuster*, DVBl 2018, 351 (353).

Ermächtigungsgrundlage ein unrechtmäßiger Eingriff in den Schutzbereich des Kernbereichs privater Lebensführung.[50]

e) Aufnahmebeginn

Die meisten Länder sehen keinen besonderen Tatbestand für einen Aufnahmebeginn vor,[51] oder umschreiben diesen nur als *kurzfristige* bzw. *kurzzeitige* Aufnahme.[52]

Um dem Bedürfnis gerecht zu werden, nicht nur eine Situation aus einem Geschehnis herauszugreifen, sondern den gesamten Tathergang zu erfassen, geht mit dem Einsatz der Body-Cams die vielumstrittene Funktion des Prerecordings einher, der vorherigen Aufnahme durch die Körperkamera.

Bei diesem wird die Kameraaufzeichnung durch einen eingebauten Speicher festgehalten, welcher nur von geringer Kapazität ist und daher automatisch nach dem entsprechenden Intervall überschrieben wird. Eine dauerhafte Speicherung der Aufnahme erfolgt erst, sobald ein Beamter diese manuell auslöst.

Rheinland-Pfalz verbietet das Prerecording ausdrücklich.[53] Der Bund, Baden-Württemberg und Mecklenburg-Vorpommern sehen in ihren Tatbestanden ausdrücklich eine Intervallspeicherung vor, die 30 bzw. 60 Sekunden andauert und von welcher in eine kontinuierliche Aufnahme gewechselt werden kann.[54]

Es wird die Voraufzeichnung tatbestandlich von der kontinuierlichen Aufzeichnung abgegrenzt. Allerdings finden sich nach dem Wortlaut keine besonderen Anforderungen an die kurzzeitige Aufnahme. Baden-Württemberg und Mecklenburg-Vorpommern trennen dagegen in den jeweiligen Tatbeständen nicht zwischen der anlassbezogenen und der kontinuierlichen Aufnahme, sondern legen fest, dass sich eine Aufzeichnung nach 60 Sekunden selbst überschreiben muss, es sei denn, es liegt eine Gefahr für Leib oder Leben vor. Ähnliches findet sich in den Regelungen der übrigen Länder, die von einer *kurzzeitigen* oder *kurzfristigen* Aufnahme sprechen, die aber an dieselben Anforderungen geknüpft sind, wie kontinuierliche Aufnahmen.

(1) Besonderheit des Prerecordings

Beim Prerecording handelt es sich wie bei der anlassbezogenen Aufzeichnung um einen Grundrechtseingriff.

[50] Vgl. § 21 III PolG BW; *Ziebarth*, Die Polizei 2016, 76 (77).
[51] Vgl. die Tatbestände von Hamburg, Niedersachsen, NRW, Sachsen und Thüringen.
[52] Vgl. Art. 33 IV 1 PAG Bay; § 29 VI 1 BremPolG; § 14 VI 1 HSOG; § 27 III 1 SPolG.
[53] Vgl. § 27a III POG RPF.
[54] Vgl. §§ 27a III 1 BPolG; 21 VI 1, VIII PolG BW; 32a I 1 SOG M-V.

Im Rahmen einer Vorabaufnahme erfolgt diese jedoch nicht allein gegenüber Adressaten einer polizeilichen Maßnahme, sondern erfasst jeden Bürger, der dem Beamten begegnet.

Diese Aufzeichnung erfolgt daher mit hoher Wahrscheinlichkeit in einem weitaus größeren Ausmaß, als es die begleitende Maßnahme tut. Dagegen ist sie aber auch von kürzerer Dauer, da der Beamte kein besonderes Ziel anvisiert.

Eine solche Aufzeichnung ist in ihrer Intensität damit zwar geringer, als die kontinuierliche Aufzeichnung, allerdings geht von ihr auch eine informationell schwerwiegende Wirkung aus,[55] sodass sie als „Vorstufe“ zur späteren Aufzeichnung zu qualifizieren ist.[56]

(2) Anforderungen an eine Prerecording Funktion

Folglich benötigt ein solcher Eingriff eine entsprechende Ermächtigungsgrundlage.

Um durch das Prerecording keine unbegrenzte Aufnahme zu schaffen, erscheint eine Begrenzung des Aufnahmeintervalls auf 30 Sekunden wie im Bundestatbestand oder auf 60 Sekunden wie in einigen Ländern sinnvoll. Somit schafft man Aufnahmen in handhabbaren und vor allem löschbaren Größen, um den Eingriff in die Grundrechte des unbeteiligten Bürgers potentiell so gering wie möglich zu halten. Zwar bleibt das Restrisiko, dass Unbeteiligte Teil dieser Aufnahme werden, jedoch scheint dies gerechtfertigt, sofern diese nur eine untergeordnete Rolle im Fokus der Kamera einnehmen und bei einer Aufzeichnung auch nur teilweise in ihrer Handlung erfasst werden.

Zudem ist eine Transparenzregelung notwendig.[57] Insbesondere ist einem Adressaten vor einem Wechsel vom Prerecording zur dauerhaften Aufnahme der entsprechende Hinweis und die Relevanz im Hinblick auf die Datenerhebung anzuzeigen.

Diese Transparenz gegenüber dem Bürger wird im Hinblick auf die Geeignetheit des Prerecordings, der Prävention, kritisiert. So würde beim Hinweis, dass eine Kamera eine Vorabaufnahme tätige, diese aber ohne besondere Vorkommnisse überschrieben werden, die Aufzeichnung keine abschreckende oder deeskalierende Wirkung gegenüber dem Adressaten entfalten.[58]

Dies vermag allerdings nicht zu überzeugen. Insbesondere das Mittel der Body-Cam und die angedrohten Konsequenzen, die sich für den Adressaten ergeben können, erzielen, dass dieser sein Folgeverhalten in ein kritischeres Licht gerückt sieht. Somit er-

[55] *Lachenmann*, NVwZ 2017, 1424 (1427); *Arzt/Schuster*, DVBl 2018, 351 (352); *Kipker*, in: Taeger, Tagungsband DSRI-Herbstakademie 2016, 121 (124).
[56] *Parma*, DÖV 2016, 809 (811).
[57] *Lachenmann*, NVwZ 2017, 1224 (1427).
[58] *Kipker*, in: Taeger, Tagungsband, DSRI- Herbstakademie 2016, 121 (131).

reicht die kritisierte „verbale Auseinandersetzung ohne qualifizierte Folge“[59] jedenfalls, dass der Adressat sein Verhalten zumindest überdenkt.

(3) Umsetzung von Bund und Ländern

Der Bund erscheint mit seiner expliziten Nennung eines „Bereitschaftsbetriebes“, die bisher effektivste Variante einer Grundlage für eine Voraufzeichnung geschaffen zu haben. Zwar sieht der Bundesgesetzgeber keine erhöhte Schwelle für den vorbeugenden Body-Cam-Einsatz vor, jedoch grenzt er diesen auf die Situation vor der Maßnahme ein und restringiert zudem den Eingriff auf maximal 30 Sekunden.

Im Hinblick auf Baden-Württemberg und Mecklenburg-Vorpommern, werden die Tatbestände weder in deklaratorischer Hinsicht gerecht, noch wird den Polizeien eine Handhabung ermöglicht, die dem Zweck des Prerecordings entsprechen würde. Streng genommen ist den Tatbeständen zufolge überhaupt nicht von Prerecording im eigentlichen Sinne auszugehen. Die Regelungen entscheiden lediglich über die Dauer der Aufzeichnung durch eine Body-Cam und damit zwei Arten der Aufnahme für eine Situation[60]. Eine kurzfristige Aufzeichnung dürfte demnach nur unter den Umständen begonnen werden, die für eine später zu speichernde Aufzeichnung gelten.

Folglich formulieren die Länder bisher keine besondere Anforderung, was das dortige Prerecording grundlagenlos erscheinen lässt.

2. Zwischenergebnis

Durch die Tatbestände der Länder werden zumeist die wichtigsten Grundlagen für den Einsatz der Body-Cams erfasst und geregelt. Diesbezüglich erscheint es auch angemessen, dass im Rahmen seiner Einschätzungsprärogative der Landesgesetzgeber einen weiten Spielraum hat, die Regelungen der landesspezifischen Bedürfnisse oder Erfordernisse anzupassen.

Sofern der präventive Einsatz der Body-Cams den Polizeigesetzen der Länder und des Bundes konsequent zugesprochen werden soll, ist von diesen zu fordern, anhand der verfassungsrechtlich bedenklichen Lücken in den Gesetzen den Nachholbedarf umzusetzen und die Polizeigesetze klarer auf das Mittel Body-Cam zuzuschneiden.

V. Repressive Nutzung

Neben der präventiven Seite des Body-Cam-Einsatzes stellt sich noch die Frage, wie die Verarbeitung von Body-Cam-Aufzeichnungen im Nachgang zu regeln wäre. Hierbei geht es vor allem um Pflichten und Rechte durch einen Tatbestand für die Datenverarbeitung.

[59] Vgl. Fn. 58.
[60] *Parma*, DÖV 2016, 809 (811).

Dazu müsste die Verwertung entweder unter die Regelung eines bereits existierenden Tatbestandes fallen (1.) oder es müsste ein neuer geschaffen werden (2.).

1. Bestehende Tatbestände

Die StPO enthält bereits eine Vielzahl an Regelungen, die tatbestandliche Voraussetzung für Maßnahmen der Ermittlungsbehörden und damit u.a. auch der Polizei schaffen.

Bezüglich der Auswertung der Daten von Körperkameras kommen die §§ 100a-h StPO in Betracht. Zwar setzen die meisten Überwachungsbefugnisse der Ermittlungsbehörden einen Anfangsverdacht voraus,[61] welcher im Rahmen der Auswertung der Body-Cam-Aufnahme regelmäßig gegeben sein dürfte. Jedoch eignet sich keine der Normen tatbestandlich als Grundlage für die Verwertung von Aufzeichnungen einer Körperkamera.[62]

Diese Hürde ergibt sich ebenfalls bei den Verwertungsregelungen der Staatsanwaltschaft für Daten ihrer Ermittlungsbehörden in §§ 161 und 163b StPO. Zudem handelt es sich um eine Beweissicherung und keine erforderliche repressive Identifikation.[63]

§ 81b StPO entspricht bereits nach seinem Zweck zur Durchführung des Strafverfahrens eine erkennungsdienstliche Maßnahme weder der Zielrichtung noch dem Umfang des Einsatzmittels der Body-Cam.[64]

Somit zieht sich durch alle potentiellen Tatbestände, insbesondere derer, die bereits eine Videoaufzeichnung zum Gegenstand haben, das Problem, dass die dortigen Anforderungen nicht der intensiven Aufnahmen einer Body-Cam entsprechen.

Folglich bildet die aktuelle StPO keine taugliche Grundlage für den repressiven Einsatz der Body-Cams.

2. Anforderungen eines neuen Tatbestandes

Dementsprechend müsste für die Datenverarbeitung eine eigene Regelung in der StPO geschaffen werden. Bezüglich dieser stellt sich die Frage, welche Anforderungen an einen Verwertungstatbestand zu stellen sind.

Hinsichtlich der Datenerhebung durch Body-Cams ist ein besonderer Schwerpunkt auf die Regelung von Datenspeicherung, -verarbeitung, und -löschung zu legen.

---

[61] Vgl. *Zöller*, NVwZ 2005, 1235 (1239); *Arzt/Schuster*, NVwZ 2005, 351 (357); *Roggan*, NVwZ 2001, 134 (138).
[62] *Parma*, DÖV 2016, 809 (814); *Hegmann*, in: BeckOK StPO mit RiStBV und MiStra, § 100h Rn. 7.
[63] *Arzt/Eier*, NZV 2010, 113 (117).
[64] *Arzt/Eier*, NZV 2010, 113 (117); dagegen: *Knape/Becker*, Die Polizei 2007, 348 (351) jedoch bezüglich der Überwachung des Verkehrsraums.

Eine besondere Rolle spielen dabei die Fragen, wer über eine Speicherung und die Verarbeitung entscheidet, wie lange gespeichert werden darf und welchen Zugriff Beamte, Betroffene und Unbeteiligte haben.

Dafür sind die bereits getroffenen Regelungen von Bund und Ländern heranzuziehen.

a) Zugriffsregelung

Eine rein automatisierte Verarbeitung der Daten ist nicht vorgesehen, insbesondere da die Body-Cam keine Übertragung der Daten auf einen Server vorsieht, sondern dies manuell geschehen muss, sodass im Prozess der Datenverarbeitung an mehreren Stellen Beamte mitwirken.

Es erscheint bereits problematisch, wer bei Auswertungen mit Daten in Berührung kommen darf.

In den Polizeigesetzen ist dies gar nicht oder uneinheitlich geregelt.[65] Allein Mecklenburg-Vorpommern und NRW setzen konkrete Personen(kreise) voraus. [66]

In NRW darf eine Löschung der Aufnahme nur durch den aufzeichnenden Beamten mit Zustimmung seines Vorgesetzten erfolgen.[67]

Positiv ist hervorzuheben, dass NRW damit den Personenkreis abgrenzt und einen unbeschränkten Zugriff auf Daten tatbestandlich ausschließt. Jedoch birgt der Einbezug des aufnehmenden Beamten das Risiko, dass hier Manipulationen Raum gegeben wird.[68]

Zudem ist im Gesetz von NRW in der besonderen Situation des Einsatzes in einer Wohnung ein Richtervorbehalt vorgesehen. Davon kann nur bei *Gefahr im Verzug* abgewichen werden und selbst dann ist die richterliche Entscheidung unverzüglich nachzuholen.[69]

Mecklenburg-Vorpommern regelt nur den besonderen Umstand des Body-Cam-Einsatzes in Wohnungen und die angeschlossene Auswertung bzw. die Ausnahmeregelungen bei *Gefahr im Verzug*. Hier entscheiden die Behördenleitung bzw. ein beauftragter Beamter.[70]

Auch hier erscheint das Abgrenzen eines Personenkreises in Anbetracht der Sensibilität der Daten angemessen. Jedoch beschränkt sich die gesetzliche Regelung auf den

[65] So auch *Martini/Nink/Wenzel*, NVwZ-Extra 2016, 1 (11).
[66] § 32a VII 3, 4 SOG MV; § 15c IV 3, VI 1, 2 PolG NRW.
[67] § 15c IV 3 PolG NRW.
[68] *Lachenmann*, NVwZ 2017, 1424 (1428).
[69] § 15c VI 1, 2 PolG NRW.
[70] § 32a VII 2, 4 SOG MV.

besonderen Einsatz innerhalb von Wohnungen. Eine ausdrückliche Regelung über die Verwertung der „einfachen“ Aufzeichnungen durch die Body-Cam im Regelfall liegt nicht vor. Angesichts der Vergleichbarkeit der Situationen könnte hier jedoch Entsprechendes für den „Normalfall“ des Einsatzes gelten. Die Art der Aufzeichnung bleibt gleich, lediglich das Aufgezeichnete ist unterschiedlich. Wenn demnach bei einer prekären Situation, ohne richterliche Entscheidung, die Behördenleitung oder ein speziell ausgewiesener Beamter über eine Löschung entscheidet, dann könnte dies auch für den Regelfall gelten.

Darüber hinaus wird eine externe Prüfstelle gefordert, die damit eine unabhängige und weniger beeinflussbare Auswertung gewährleisten soll.[71]

Allerdings erscheint eine besondere Stelle zur Datenauswertung nicht erforderlich.[72] Entscheidend ist allein der Gesichtspunkt, dass der Personenkreis auf wenige Entscheidungsträger begrenzt wird. Eine externe Verarbeitung ist mit einer erhöhten Auswertungszeit verbunden, was gerade hinsichtlich des repressiven Zwecks ein Hindernis darstellt.

In einer strafprozessualen Regelung wird jedenfalls die Angabe zu machen sein, welcher Beamte mit einer Aufzeichnung in Berührung kommt und in Folge dessen eine Löschung veranlassen und durchführen darf.[73]

b) Speicherfristen

Schließlich bedarf es einer tatbestandlichen Befristung für die Datenverarbeitung von Body-Cam-Aufzeichnungen. Allerdings herrscht auch diesbezüglich tatbestandliche Vielfalt in den Polizeigesetzen.

Wie lange eine Aufzeichnung gespeichert werden darf, ist uneinheitlich geregelt. Ob im Gesetz eine Speicherdauer von 14 Tagen, 30 Tagen[74] oder zwei Monaten[75] vorgesehen wird, erscheint nicht problematisch.

Neben einer möglichen Einwirkung eines Betroffenen ist auch die faktische Umsetzung, also die Auswertungsmöglichkeit aus tatsächlicher Perspektive für den Zeitraum zu berücksichtigen. Eine sofortige Auswertung und damit verbundene sofortige Löschungsmöglichkeit scheidet schon aufgrund der praktischen Umsetzbarkeit aus.[76]

---

[71] Vgl. *Martini/Nink/Wenzel*, NVwZ-Extra 2016, 1 (10); *Kipker/Gärtner*, NJW 2015, 296 (297) sprechen von einer Treuhandstelle.
[72] So auch *Lachenmann*, NVwZ 2017, 1424 (1428).
[73] Vgl. *Martini/Nink/Wenzel*, NVwZ-Extra 2016, 1 (11).
[74] Vgl. hier § 27a POG RPF; so auch *Lachenmann*, NVwZ 2017, 1424 (1428) bezüglich der Angemessenheit von 30 Tagen.
[75] Vgl. hier die Tatbestände von Bayern, Bremen, Sachsen.
[76] Vgl. *Arzt*, Stellungnahme v. 13.01.2015, NRW LT-Drs. 16/5923, S. 13.

Stattdessen sollte der vom Gesetzgeber festgelegte Zeitraum berücksichtigen, dass hinsichtlich der Situationen in den Ländern und den Einsatzgebieten der Bundespolizei eine Aufzeichnung angemessen ausgewertet werden kann. Zudem ist Betroffenen eine angemessene Einwirkungsmöglichkeit einzuräumen.[77]

Folglich erscheint eine gesetzliche Regelung wie in Hamburg und Thüringen, welche gar keinen Zeitraum enthalten, nicht ausreichend.

Bisher wird die Löschungspflicht in allen Gesetzestatbeständen, außer in Hamburg und Thüringen, durch eine Ausnahme durchbrochen. Diese greift dann ein, sobald Aufzeichnungen von vornherein oder bei der Auswertung zu repressiven Zwecken genutzt werden sollen.

Allein der Bund ordnet eine maximale Speicherdauer trotz einer repressiven Nutzung von sechs Monaten im Gesetz an, in den restlichen Gesetzen ist die repressive Nutzung unbegrenzt.

Diesbezüglich erscheint eine zu enge zeitliche Begrenzung zwar nicht zielführend, jedoch besteht die Gefahr, dass ohne eine feste Beschränkung Daten auf lange Sicht gespeichert bleiben, sofern einer Ermittlung nicht abgeschlossen ist.

Die Regelung des Bundes von einer maximalen Speicherdauer von einem halben Jahr eröffnet einerseits die Möglichkeit einer effektiven Datenauswertung zu repressiven Zwecken und andererseits einen Schutz der Betroffenen vor einer anhaltenden Verarbeitung ihrer Daten, sodass diese eine taugliche Vorlage für den Tatbestand in der StPO darstellt.

c) Betroffenenrechte

Neben einer Kenntlichmachung eines Body-Cam-Einsatzes, sodass bereits Transparenz bei der Aufnahme besteht, sind dem Betroffenen im Nachgang der Aufnahme Mitwirkungs- und Einsichtsrechte einzuräumen.[78] Es stellt sich allerdings die Frage, in welchem Umfang dies für die Betroffenen auszugestalten ist.

In den Polizeigesetzen von Bund und Ländern selbst finden sich derartige Regelungen nicht. Allenfalls sind derartige Betroffenenrechte in den Datenschutzgesetzen vorzufinden.[79]

Zumindest erscheint es für die strafprozessuale Grundlage erforderlich, dass im Rahmen der polizeilichen Maßnahme samt Aufzeichnung der Betroffenenkreis darauf

[77] Vgl. *Arzt*, Stellungnahme v. 13.01.2015, NRW LT-Drs. 16/5923, S. 13.
[78] *Kipker/*Gärtner, NJW 2015, 296 (299); *Kipker*, in: Taeger, Tagungsband, DSRI- Herbstakademie 2016, 121 (135); *Martini/Nink/Wenzel*, NVwZ-Extra, 1 (11).
[79] Vgl. dazu §§ 5, 18 DSG NRW.

hinzuweisen ist, dass im Nachgang eine Aufzeichnung eingesehen werden kann.[80] In praktischer Hinsicht erscheint es allerdings notwendig, dass eine Einsichtnahme eine vorherige Sichtung voraussetzt, sodass die Betroffenen untereinander keine Aufzeichnungen weiterer Personen einsehen können oder wirksame Unkenntlichmachungen vorzunehmen sind.

Insbesondere wird kritisiert, dass nach aktuellen Regelungen gegenüber unbeteiligten Dritten, welche jedoch auch Teil einer Aufnahme wurden, nicht im gleichen Umfang die Einsicht gewährt wird, wie den Adressaten einer Maßnahme, obwohl die Qualität des Eingriffes in beiden Fällen gleichbleibt.[81]

d) Einfluss europäischen Datenschutzrechts

Seit dem 25.05.2018 gilt die Datenschutzgrundverordnung. Mit dieser wurden bezüglich der Erhebung und Verarbeitung personenbezogener Daten teilweise Regelungen weiterentwickelt, aber auch neu eingeführt. Damit stellt sich auch die Frage, ob sich hier ein Einfluss auf die Datenerhebung durch Body-Cams und deren spätere Auswertung ergibt.

Hier ist zunächst festzustellen, dass Datenerhebungen der Polizei als Ermittlungsbehörde Maßnahmen darstellen, welche unter abschließendes Sekundärrecht der EU fallen.[82] Während demnach zivile Aufzeichnungen unter die DSGVO fallen, ist deren Anwendungsbereich für die Body-Cam-Aufzeichnungen nicht eröffnet.[83]

VI. Ausblick

Die Body-Cam ist als Einsatzmittel auf den Schultern deutscher Polizeibeamten angekommen. Laut der Länder zeigt sie beim Bürger Wirkung und schafft den Ansatz einer informationellen Ausgeglichenheit.

Jedoch erscheint die bisherige Handhabung noch unausgereift und die Tatbestände bedürfen Nachholung. Körperkameras sind der nächste Schritt, personenbezogene Daten zu erheben und zu speichern, was aufgrund der Intensität besonderes Augenmerk auf Voraussetzungen und Grenzen bedarf.

Bisher wurde diese Aufgabe nicht abschließend gelöst. Insbesondere entsteht der Eindruck, dass die Landesgesetzgeber ihre Regelungen zwecks ihrer Gesetzgebungskompetenz auf eine Präventionswirkung zuschneiden, die faktisch gar nicht erreicht wird.

---

[80] *Kipker/Gärtner*, NJW 2015, 296 (300).
[81] Vgl. hier NRW, wo Unbeteiligte auf das IFG verwiesen werden; dazu *Arzt/Schuster*, DVBl 2018, 351 (356).
[82] Vgl. Hier Art. 1 I EU-RL 2016/680 v. 27.04.2016 für die Verhütung, Aufdeckung oder Verfolgung von Straftaten […].
[83] *Martini/Nink/Wenzel*, NVwZ-Extra 2016, 1 (11).

Bevor nun durch eine voreilige Handhabung der Body-Cams Wölfe in Schafspelzen ihren festen Einzug in die Polizeigesetze finden, ist die Qualität der Body-Cam zu der der bisherigen Videotechnik klar abzugrenzen und es liegt an den Parlamenten, Regelungen zu schaffen, die dem Einsatz der Körperkameras angemessen sind und ihn effektiv möglich machen.

Ein entscheidender Schritt ist ein strafprozessualer Tatbestand mit klarem Regelungshintergrund hinsichtlich der gesamten Verwertung personenbezogener Daten, was durch die bisherige Rechtslage nicht erreicht wird.

Literaturverzeichnis

Arnd, Heiko/Staffa, Valerie, Einsatz von Bodycams bei der Polizei Rheinland-Pfalz, Die Polizei 2016, 190-196.

Arzt, Clemens, Stellungnahme für die Anhörung des Innenausschusses im Landtag von Nordrhein-Westfalen 13. Januar 2015, Drucksache 16/5923 vom 20. Mai 2014.

Arzt, Clemens/ Schuster, Susanne, Bodycam-Einsatz jetzt auch in NRW, DVBl 2018, 351-358.

Arzt, Clemens/Eier, Jana, Section Control und allgemeine Videoüberwachung im Straßenverkehr – Neue und alte Maßnahmen ohne Rechtsgrundlage, NZV 2010, 113-119.

Epping, Volker/ Hillgruber, Christian (Hrsg.), BeckOK Grundgesetz – Kommentar, 37. Edit., München 2018.

Graf, Jürgen-Peter (Hrsg.), BeckOK StPO mit RiStBV und MiStra – Kommentar, 29. Edit., München 2018.

Jortzig, Manuela/Kunze, Wolfgang, Rechtsschutz gegen Maßnahmen der Ermittlungsbehörden, Jura 1990, 294-299.

Kipker, Dennis-Kenji/Gärtner, Hauke, Verfassungsrechtliche Anforderungen an den Einsatz polizeilicher „Body-Cams“, NJW 2015, 296-301.

Knape, Michael/Becker, Reiner, Bildaufnahmen und -aufzeichnungen im Rahmen der technischen Verkehrsüberwachung, Die Polizei 2007, 384-354.

Lachenmann, Matthias, Einsatz von Bodycams durch Polizeibeamte, NVwZ 2017, 1424-1430.

Martini, Mario/Nink, David/Wenzel, Michael, Bodycams zwischen Bodyguard und Big Brother, NVwZ-Extra 2016, 1-18.

Maunz, Theodor/Dürig, Günther (Bgr.), Grundgesetz Kommentar, 82. Lief., München 2018.

Parma, David, Rechtsgrundlagen für den Einsatz von „Body-Cams“, DÖV 2016, 809-819.

Roggan, Fredrik, Die Videoüberwachung von öffentlichen Plätzen Oder: Immer mehr gefährliche Orte für Freiheitsrechte, NVwZ 2001, 134-141.

Schenke, Wolf-Rüdiger, Polizeiliches Handeln bei Anscheinsgefahr und Gefahrenverdacht, JuS 2018, 505-516.

Schnabel, Christoph, Polizeiliche Videoüberwachung öffentlicher Räume nach § 8 III HbgPolDVG am Beispiel der Reeperbahn-Entscheidung des OVG Hamburg, NVwZ 2010, 1457-1461.

Schoch/Schneider/Bier (Hrsg.), Verwaltungsgerichtsordnung Kommentar, 33. EL., München 2017.

Taeger, Jürgen (Hrsg.), Smart World - Smart Law? Weltweite Netze mit regionaler Regulierung, Tagungsband DSRI-Herbstakademie 2016, Edewecht 2016.

Wysk, Peter, Tausche Freiheit gegen Sicherheit?, Verwaltungsarchiv 2018, 141-162.

Ziebarth, Wolfgang, Polizeiliche Body-Cams in Baden-Württemberg, Die Polizei 2017, 76-81.

Zöller, Mark A., Möglichkeiten und Grenzen polizeilicher Videoüberwachung, NVwZ 2005, 1235-1241.

Braucht der Hausfriedensbruch im Strafrecht ein „digitales Update“?

Henrik Nolte

Student der Rechtswissenschaften im 4. Semester an der Eberhard Karls Universität Tübingen
henrik.nolte26@googlemail.com

Abstract

Um IT-Systeme besser vor Hackerangriffen und unbefugter Benutzung zu schützen, hat der Bundesrat erst jüngst wieder eine Gesetzesinitiative zur Schaffung eines neuen Straftatbestands des „digitalen Hausfriedensbruchs“ aufgegriffen. Der vorliegende Beitrag untersucht, ob die Einführung eines „digitalen Hausfriedensbruchs“ in rechtlicher und rechtstatsächlicher Hinsicht erforderlich ist.

I. Der Bundesratsvorschlag „digitaler Hausfriedensbruch“

Die fortschreitende Digitalisierung zeigt ihre Gefahren immer deutlicher: Zunehmend häufen sich Cyberangriffe auf Internetportale oder kritische Infrastrukturen wie etwa auf Elektrizitäts- oder Wasserwerke sowie auf Industrie- oder Telekommunikationsanlagen, die zu wirtschaftlichen Schäden in Milliardenhöhe führen können. Ausgeführt werden derartige Angriffe mit Hilfe sogenannter Botnetze. Dabei handelt es sich um technische Systeme, die mit Schadprogrammen infiziert und zu einem großen Netzwerk zusammengeschlossen werden. Cyberkriminellen ist es mit Hilfe von Botprogrammen möglich, den Zusammenschluss der befallenen Systeme fernzusteuern, mittels gebündelter Rechenleistung Angriffe durchzuführen und sensible Daten von Computernutzern in privaten Haushalten und Unternehmen auszuspähen.

Es stellt sich die Frage, ob hierbei Strafbarkeitslücken bestehen und das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme verletzt wird, dessen Schutz das Strafrecht und europarechtliche Vorgaben gewähren sollen. Deshalb hat das Bundesland Hessen zuletzt im April 2018 über den Bundesrat einen Gesetzentwurf in den Bundestag eingebracht, der einen neuen Straftatbestand des „digitalen Hausfriedensbruchs“ einführen und IT-Systeme besser vor Hackerangriffen und unbe-

fugter Benutzung schützen soll.[1] Der Gesetzentwurf überträgt den Rechtsgedanken des Hausfriedensbruchs nach § 123 StGB und des unbefugten Gebrauchs eines Fahrzeugs nach § 248b StGB in die digitale Welt.[2] Demnach soll jeder, der gegen oder ohne den Willen des Berechtigten in ein technisches System eindringt oder ein solches unbefugt in Gebrauch nimmt, gleichermaßen strafbar sein. Der vorgeschlagene Entwurf des § 202e Abs. 1 StGB lautet wie folgt:

> *(1) Wer unbefugt*
>
> *1. sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft,*
>
> *2. ein informationstechnisches System in Gebrauch nimmt oder*
>
> *3. einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt,*
>
> *wird mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Die Tat nach Satz 1 ist nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen.*

Der vorliegende Beitrag stellt die technischen Grundlagen von Botnetzen dar und geht der Frage nach, ob die Einführung eines „digitalen Hausfriedensbruchs“ aufgrund bestehender Strafbarkeitslücken, mangelnden Rechtsgüterschutzes und europarechtlicher Vorgaben erforderlich ist. Abschließend wird geklärt, ob der vorgeschlagene Straftatbestand das vom Gesetzgeber erstrebte Ziel tatsächlich erreichen kann und wie er gegebenenfalls zielgerichteter formuliert werden könnte.

II. Botnetze – technische und begriffliche Grundlagen

Botnetze sind technische Systeme, die mit Schadprogrammen infiziert und zu einem großen Netzwerk zusammengeschlossen wurden. Die eingesetzte Schadsoftware bezeichnet man als Roboterprogramme bzw. Botprogramme oder „Bots“.[3] Sie werden von Kriminellen, auch „Botmaster“ genannt, über Server ferngesteuert und als Werkzeug für Straftaten missbraucht. Als Bot kommt jedes System in Betracht, das mit dem Internet verbunden ist. Dazu gehören neben PCs und Smartphones zunehmend auch internetfähige Autos, Spielzeuge oder Haushaltsgeräte.[4]

[1] BT-Drs. 19/1716, s. auch schon BT-Drs. 338/16.
[2] BT-Drs. 19/1716, S. 5
[3] Kurz für das englische Wort „Robot“.
[4] *BKA*, Bundeslagebild 2016, S. 15.

Ziel des Aufbaus eines Botnetzes ist es, die Rechenleistung und Bandbreite möglichst vieler IT-Systeme zu bündeln und für eigene Zwecke zu nutzen. Automatisiert können Bots, gesteuert durch den Botmaster, unerkannt Spam-Emails versenden oder groß angelegte Cyberangriffe gegen Internetseiten oder Unternehmen durchführen oder zum Schürfen von Bitcoins eingesetzt werden. Mittlerweile können Dritte sogar Botnetze zur Begehung von Straftaten mieten.[5]

Die Infektion von Opfersystemen (sog. Spreading) kann auf verschiedene Wege erfolgen. Häufig werden sog. Trojaner[6] verwendet, um Botprogramme einzuschleusen. Zunehmend gelangen Botprogramme auch durch bloße „Drive-By-Infection“, den Aufruf einer mit Schadsoftware präparierten Website oder E-Mail, auf technische Systeme.[7] Schließlich kann die Schadsoftware auch so gestaltet sein, dass sie über das Internet nach weiteren Systemen sucht, die über keine Zugangsvorkehrungen verfügen oder große Schutzlücken im Betriebssystem aufweisen, um diese mit Botprogrammen zu infizieren. Betrachtet man den Ablauf von der Erstellung eines Botnetzes bis hin zu dessen Einsatz, lassen sich im Wesentlichen drei technische Schritte unterscheiden:[8]

Schritt 1: Herstellung einer speziellen Schadsoftware, die meist als „Botprogramm“ bzw. „Botware“ bezeichnet wird.

Schritt 2: Infektion technischer Systeme mit dieser Schadsoftware (sog. „Spreading“) und Kontaktaufnahme des aktiven Programms mit Servern über das Internet. Das System wird zum ferngesteuerten „Bot“.

Schritt 3: Empfang von Befehlen durch Server und deren Ausführung durch die Bots.

Infiziert die Botware ein IT-System und wird dort installiert, stellt dies die maßgebliche Handlung des „digitalen Haufriedensbruchs“ dar, auf die sich der Gesetzesentwurf bezieht.

III. Strafrechtliche Behandlung von Botnetzen *de lege lata*

Im Folgenden soll die Phase des „Spreadings“ nach Maßgabe des geltenden Strafrechts bewertet werden, da sich der „digitale Hausfriedensbruch“ in diesem Schritt vollzieht.

1. „Elektronischer Hausfriedenbruch“, § 202a StGB

Nach § 202a StGB macht sich strafbar, wer sich oder einem anderen unbefugt Zugang zu Daten, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders ge-

[5] *BKA*, Bundeslagebild 2016, S. 9; *Buermeyer/Golla*, K&R 2017, 14 (14).
[6] Programme, die als nützliche Anwendung getarnt sind, jedoch Schadsoftware enthalten.
[7] *BKA*, Bundeslagebild 2016, S. 13 mit Fn. 20; *Roos/Schumacher*, MMR 2014, 377 (378 mit Fn. 8).
[8] *Busching*, Digitaler Hausfriedensbruch, S. 491; *Mavany*, KriPoZ 2016, 106 (108).

sichert sind, unter Überwindung der Zugangssicherung verschafft. Diese Vorschrift wird zuweilen bereits als „elektronischer Hausfriedensbruch“ bezeichnet,[9] weshalb die Einführung eines „digitalen Hausfriedensbruchs“ besonders angezweifelt wird.[10]

a) „Unbefugt Zugang zu Daten verschaffen“

Zur Verwirklichung des § 202a StGB ist es notwendig, dass der Täter sich unbefugt Zugang zu Daten verschafft. Dies ist der Fall, wenn sich der Täter eine Position verschafft, aus der er auf Daten des Systems zugreifen kann.[11] Eine Zugriffsmöglichkeit des Täters auf Daten durch Botprogramme wird von der Literatur fast einhellig mit der Begründung bejaht, dass der Täter kein Interesse an einem Botprogramm hätte, das nicht in der Lage ist, sich Zugang zu Daten zu verschaffen.[12] Schließlich sei der Botmaster zur Begehung weiterer Straftaten auf Systemdaten angewiesen.

Diese Annahme erfasst jedoch nicht alle Fälle, in denen sich Cyberkriminelle fremder IT-Systeme bemächtigen. Bezweckt der Botmaster das Ausspähen von Passwörtern oder Kontodaten, sind Botprogramme so programmiert, dass sie auf Befehl Daten des Systems ausspähen und dem Botmaster Zugang zu den Informationen gewähren. Unter diesen Umständen ist eine Strafbarkeit gemäß § 202a StGB gegeben.

Allerdings ist die Intention des Botmasters oftmals nicht das Ausspähen von Daten, sondern die, wie ein „Trittbrettfahrer“ die Rechenleistung des fremden Systems zu nutzen, etwa für das Ausführen anderer Befehle wie z.B. die Durchführung von DDoS-Angriffen[13] oder das Schürfen von Bitcoins. Dazu programmiert der Täter Botprogramme so, dass sie selbst die notwendigen Informationen ermitteln und diese nicht an den Botmaster weiterleiten.[14] Das zeigt sich zum einen daran, dass Botnetze immer größer werden und der Täter ausschließlich auf die Rechenleistung der infizierten Hardware, nicht aber auf eine Flut einzelner Systemdaten zugreifen will. Außerdem werden vermehrt internetfähige Alltagsgegenstände wie z.B. Kühlschränke oder Soundanlagen zum Opfer von Botprogrammen, an deren (System-)Daten der Täter überhaupt kein Interesse hat. In diesen Fällen kann der Täter zwar Befehle geben, er wird aber mangels Interesse und entsprechender Programmierung keine Zugangsmöglichkeit zu Daten des befallenen Systems haben. In diesem Fall ist eine Strafbarkeit nach § 202a StGB nicht gegeben.

---

[9] *Ernst*, NJW 2007, 2661 (2661); *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 18.
[10] *Buermeyer/Golla*, K&R 2017, 14 (15); *Mavany*, KriPoZ 2016, 106 (109).
[11] *Fischer*, StGB, § 202a Rn. 10; *Hilgendorf*, in: LK, § 202a Rn. 16; jeweils m.w.N.
[12] *Buermeyer/Golla*, K&R 2017, 14 (14); *Busching*, Digitaler Hausfriedensbruch, S. 492; *Golla*, Risiken und Nebenwirkungen, S. 166.
[13] Distributed-Denial-of-Service, dabei wird ein Server gezielt mit so vielen Anfragen einzelner Bots bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und schlimmstenfalls zusammenbricht.
[14] So ebenfalls nur: *Dietrich*, Besonderen Sicherung, S. 137.

Deshalb besteht bei Bot-Angriffen häufig keine Strafbarkeit nach § 202a StGB. Ob sich der Täter bereits durch das Einschleusen von Botprogrammen unbefugt Zugang zu Daten verschafft, hängt vielmehr von deren Konfiguration und Einsatzzweck ab.

b) „Besondere Zugangssicherung“

Erlangt der Täter durch das das Einschleusen eines Botprogramms hingegen zugleich Zugang zu den Daten des Systems, hängt eine Strafbarkeit nach § 202a StGB ferner davon ab, ob die Daten „besonders gegen unberechtigten Zugang gesichert“ sind und der Täter diese Sicherung aktiv überwunden hat.

Eine *besondere* Zugangssicherung liegt nach herrschender Meinung vor, wenn der Berechtigte Vorkehrungen getroffen hat, die objektiv geeignet und subjektiv dazu bestimmt sind, den Zugriff auf Daten zu verhindern oder zumindest erheblich zu erschweren, wobei sich in der Sicherung sein Interesse an der Geheimhaltung manifestieren muss.[15] Eine für jedermann ohne großen Aufwand überwindbare Sicherung oder gar eine rein symbolische Manifestation des Geheimhaltungswillens genügt nicht.[16] Aus dem Begriff der Sicherung ergibt sich ferner, dass sie zum Tatzeitpunkt bestehen und einen Angriff in der konkreten Situation abwehren können muss.[17]

Aus diesem Grund stellen Firewalls grds. keine Zugangssicherung im Sinne des § 202a StGB dar,[18] da diese nur als „Torwächter“ fungieren, die darüber entscheiden, ob auf dem Computer installierte Programme Internetzugriff erhalten oder nicht. Firewalls können deshalb die Installation von Programmen nicht verhindern.[19]

Davon zu unterscheiden sind Antivirenprogramme. Sie stellen eine wirksame Zugangssicherung gem. § 202a StGB dar.[20] Schleust der Täter Botprogramme in Endgeräte wie Laptops oder Computer ein und erlangt damit eine Zugangsmöglichkeit zu den dort gespeicherten Daten, geschieht dies in den meisten Fällen durch die Überwindung eines auf dem jeweiligen Gerät installieren Antivirenprogramms. Beachtlich ist, dass sich knapp 15 % aller Computernutzer in Deutschland ohne aktive Antivirensoftware im Internet bewegen.[21] Damit ist jeder sechsten Person der strafrechtliche Schutz versagt, da sich Angreifer in diesen Fällen mangels Überwindung einer besonderen Zugangssicherung nicht nach § 202a StGB strafbar machen.

---

[15] BT-Drs. 16/3656, S. 10; ferner *Ernst*, NJW 2003, 3233 (3236); *Graf*, in: MüKo, § 202a Rn. 35; *Lenckner/Eisele*, in: Schönke/Schröder, § 202a, Rn. 14.

[16] *Fischer*, StGB, § 202a, Rn. 9; *Graf*, in: MüKo, § 202a Rn. 32; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, Rn. 550.

[17] *Graf*, in: MüKo, § 202a Rn. 32; *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 8.

[18] So auch (ohne Begründung) *BGH*, NStZ 2016, 339 (340).

[19] So *Stam*, ZIS 2016, 547 (549); wohl auch *Dietricht*, Besondere Sicherung, S. 384; *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 14.

[20] *Stam*, ZIS 2016, 547 (549).

[21] *https://de.statista.com/statistik/daten/studie/226942/umfrage/anteil-der-verbraucher-ohne-aktives-antivirenprogramm/.*

Weshalb aber ein ungeschütztes Opfer keinen staatlichen Schutz bekommen soll, das geschützte ihn hingegen „oben drauf“, vermag das Erfordernis einer vorhandenen Zugangssicherung nicht zu erklären. Vielmehr ist es gerade die Aufgabe des Strafrechts, angesichts der komplexen digitalen Welt auch unwissende und technisch nicht affine Personen zu schützen. Das viktimodogmatisch[22] geprägte Merkmal der Zugangssicherung führt daher de lege lata zu erheblichen Strafbarkeitslücken.

c) Phänomen „Internet der Dinge“

Eine neue Dimension erlangt die Problematik der Zugangssicherung im Rahmen der technischen Entwicklungen seit dem Jahr 2015. Bis dato war es üblich, dass Botprogramme auf Notebooks oder PCs installiert wurden. Das hatte für die Täter den Nachteil, dass die Geräte vom Nutzer ständig ausgeschaltet wurden und damit nicht zuverlässig erreichbar waren. Neuerdings werden aber auch Alltagsgegenstände wie Autos, Fernseher, Kühlschränke oder Uhren mit dem Internet verbunden. Dieses rasant wachsende Phänomen der digitalen Vernetzung von Gegenständen wird als „Internet der Dinge“ (Internet of Things, kurz IoT) bezeichnet. Es verwundert nicht, dass zunehmend IoT-Geräte in das Visier der Botmaster gelangen, zumal diese im Gegensatz zu PCs ständig erreichbar sind.

In Bezug auf das Merkmal der Zugangssicherung ist problematisch, dass die meisten IoT-Geräte über keine oder nur unzureichende Schutzmechanismen verfügen und allenfalls standardisierte Passwörter verwenden.[23] Außerdem sind für eine Kaufentscheidung des Kunden normalerweise nur die Gerätefunktionalität, der damit verbundene Komfortgewinn und der Kaufpreis ausschlaggebend. Die IT-Sicherheit von IoT-Geräten spielt dagegen bisher keine oder nur eine untergeordnete Rolle.[24] Von einer Manifestation des Geheimhaltungswillens, wie es das Merkmal der Zugangssicherung nach § 202a StGB verlangt, kann daher nicht gesprochen werden. Selbst im Falle einer Sicherung ist es den Tätern oftmals ein Leichtes, die werkseitigen Standardkennwörter für die jeweiligen Modelle ausfindig zu machen.[25] Das Überwinden einer Zugangssperre durch standardisierte Kennwörter reicht für das Merkmal einer besonderen Zugangssicherung nach § 202a StGB nicht aus, da die Täter keine erhöhte deliktische Energie aufwenden.[26] Auch manifestiert die Verwendung von Standardkennwörtern

[22] Der viktimodogmatische Ansatz geht davon aus, dass das unvorsichtige und leichtfertige Opfer keinen strafrechtlichen Schutz verdient; vgl. näher *Amelung*, GA 1977, 1 (1 f.).
[23] *BKA*, Bundeslagebild 2016, S. 25; *BSI*, Lage der IT-Sicherheit 2017, S. 16.
[24] *BSI*, Lage der IT-Sicherheit 2017, S. 16.
[25] Ein Beispiel neben zahlreichen anderen Websites: *http://www.routerpasswords.com/.*
[26] BT Dr. 12/6500; *Hilgendorf*, in: LK, § 202a Rn. 36; *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 14; a.A. *Ernst*, NJW 2003, 3233 (3236).

nicht das Geheimhaltungsinteresse des Berechtigten, da dieses Interesse allenfalls durch eine Änderung der Passwörter deutlich wird.[27]

Somit besteht bei IoT-Geräten häufig keine besondere Zugangssicherung. Das Einschleusen von Botprogrammen in Geräte des Internets der Dinge ist deshalb meist nicht von § 202a StGB erfasst.

2. Strafbarkeit nach dem Bundesdatenschutzgesetz

Neben einer Strafbarkeit aus dem StGB kommen die Normen des BDSG zu einem vergleichbaren Ergebnis. Nach § 42 I BDSG macht sich strafbar, wer gewerbsmäßig personenbezogene Daten einer großen Zahl von Personen ohne Berechtigung einem Dritten vermittelt oder auf eine andere Art und Weise zugänglich macht. Nach § 42 II BDSG macht sich strafbar, wer nicht allgemein zugängliche personenbezogene Daten ohne Berechtigung verarbeitet oder durch unrichtige Angaben erschleicht und dabei mit Bereicherungs- oder Schädigungsabsicht handelt.

Sind PCs mit Botprogrammen infiziert, die so programmiert sind, dass sie Daten ausspähen und dem Täter Zugriff auf diese gewähren, kann dieses Verhalten häufig die Strafbarkeit nach § 42 BDSG begründen, da sich auf dem PC regelmäßig personenbezogene Daten befinden. Werden Botprogramme hingegen in IoT-Geräte eingeschleust, ist es eine Frage des Einzelfalls, ob auch personenbezogene Daten betroffen sind. Während solche z.B. bei internetfähigen Fernsehern mit integrierter Kamera und Mikrofon anfallen können, speichern Maschinen, Anlagen oder „intelligente“ Haushaltsgeräte meist keine oder nur allgemeine, oft aber nicht personenbezogene Daten,[28] so dass insoweit Strafbarkeitslücken bestehen.

3. Unbefugtes Abfangen von Daten, § 202b StGB

Nach § 202b StGB macht sich strafbar, wer sich mittels technischer Anlagen unbefugt Daten verschafft, die sich nicht im öffentlichen elektronischen Übertragungsvorgang befinden. Geschützt sind damit die Inhalte aller elektronischen Datenübermittlungsvorgänge wie z.B. E-Mail, WLAN oder Bluetooth.[29] Erfolgt die Infektion mit Botprogrammen beispielsweise dadurch, dass von einem infizierten E-Mailserver alle ein- und ausgehenden E-Mails abgefangen und mit maliziösem Anhang weitergeleitet werden, wurde auf eine Datenübertragung zugegriffen und § 202b StGB verwirklicht.[30]

[27] *Hilgendorf*, in: LK, § 202a Rn. 36; *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 14.
[28] *Kochheim*, Cybercrime, Rn. 457 mit Fn. 553.
[29] *Lenckner/Eisele*, in: Schönke/Schröder, § 202b Rn. 3; *Graf*, in: MüKo, § 202b Rn. 9.
[30] *Mavany*, KriPoZ 2016, 106 (109); *Roos/Schumacher*, MMR 2014, 377 (379).

4. Strafbarkeit nach §§ 303a, 303b StGB

Schließlich kann durch die Infektion eine Strafbarkeit nach § 303a StGB in Betracht kommen. Taugliche Tathandlungen sind das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von *gespeicherten* Daten. Geschütztes Rechtsgut ist das Interesse des Berechtigten an der unversehrten Verwendbarkeit der gespeicherten Daten.[31] Nicht geschützt ist die Integrität eines Systems an sich.

a) Veränderung von Daten, § 303a StGB

Deshalb liegt ein tatbestandliches Verändern von Daten nur dann vor, wenn eine Funktionsbeeinträchtigung von Daten herbeigeführt und dadurch deren Informationsgehalt geändert wird.[32] Regelmäßig werden Botprogramme die Startroutine des Systems umschreiben und eine Datenveränderung bewirken, um einen Neustart des Computers zu überleben oder Protokolle ändern, um ihre Existenz auf dem System zu kaschieren oder um Zugriff auf das Internet und die Ressourcen des Systems zu erlangen.[33]

Zunehmend werden jedoch auch Schadprogramme eingesetzt, die keine Veränderung an *gespeicherten* Daten herbeiführen (sog. „fileless malware“) und von Antivirenprogrammen nicht erkannt werden.[34] Die Besonderheit dieser „fileless malware“ besteht darin, dass sie sich nicht auf der Festplatte, sondern im Arbeitsspeicher des Systems einnistet, wo Daten nur vorübergehend verfügbar und daher tatbestandlich nicht „gespeichert“ sind. Durch das Einnisten dieser Form von Botprogrammen wird der inhaltliche Aussagewert von *gespeicherten* Daten nicht verändert, so dass § 303a StGB insoweit nicht greift.[35]

b) Qualifikation, § 303b StGB

Zudem kann eine Computersabotage nach § 303b StGB in Betracht kommen, wenn eine Datenverarbeitung erheblich gestört wird, die für einen anderen von wesentlicher Bedeutung ist. Das ist der Fall, wenn die Funktionsfähigkeit der jeweiligen Einrichtung von einem ungestörten Ablauf ganz oder überwiegend abhängig ist.[36] Alleine die Installation eines Botprogramms bleibt aber regelmäßig unbemerkt und dürfte daher zu keiner erheblichen Störung einer Datenverarbeitung führen.

Bemerkenswert ist, dass § 303b StGB eine erhebliche Störung von IoT-Geräten oft nicht erfasst. Bei IoT-Geräten kommt es darauf an, ob deren Datenverarbeitung für die

[31] *Wieck-Noodt*, § 303a Rn. 2; *Stam*, ZIS 2017, 547 (551).
[32] BT Dr. 10/5058, S. 35; *Wolf* in LK, § 303a, Rn. 27; *Heine*, NStZ 2016, 441 (443).
[33] *Buermeyer/Golla*, K&R 2017, 14 (15); *Heine*, NStZ 2016, 441 (444); *Mavany*, KriPoZ 2016, 106 (109).
[34] BT-Drs. 19/1716, S. 4; *Bär*, in: Graf/Jäger/Wittig, § 303a Rn. 20.
[35] Hierzu nur: *Bär*, in: Graf/Jäger/Wittig, § 303a Rn. 20.
[36] BT-Drs. 16/3656, S. 13; *Schultz*, DuD 2006, 778 (783).

Lebensgestaltung der betroffenen Personen von wesentlicher Bedeutung ist.[37] Diese Frage wirft erhebliche Abgrenzungsprobleme auf. Während ein Kühlschrank als System von wesentlicher Bedeutung für die Lebensgestaltung angesehen werden kann, ist ein völliger Ausfall von vernetzten Fernsehern, Radios oder Soundanlagen nicht von § 303b StGB erfasst. Damit gewährt § 303b StGB nur bedingt Schutz vor Angriffen auf IoT-Geräte.

IV. Unzureichender Rechtsgüterschutz

Es zeigt sich, dass das bestehende Strafrecht im Bereich der Botnetz-Kriminalität bedeutsame Strafbarkeitslücken beim Schritt der Infizierung aufweist. Die Notwendigkeit der Einführung des § 202e StGB-E kann sich daher auch aus einem bislang unzureichenden Rechtsgüterschutz ergeben. Nach dem aktuellen Entwurf reichen die bisher vom Strafrecht geschützten Rechtsgüter nicht aus, um den Schutz des „*Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*“ hinreichend zu gewähren.

Das sog. „Computergrundrecht“ ist Ausfluss des allgemeinen Persönlichkeitsrechts und bewahrt den Lebensbereich des Grundrechtsträgers vor staatlichen Zugriffen im Bereich der Informationstechnik. In seiner wegweisenden Online-Durchsuchungs-Entscheidung[38] hob das BVerfG hervor, dass der Einzelne dem System persönliche Daten anvertraue oder bereits durch dessen Nutzung liefere.[39] Die Fülle dieser personenbezogenen Informationen könnten bei einem Zugriff auf das System einen Einblick in wesentliche Teile der Lebensgestaltung einer Person geben.[40] Müsste der Einzelne aber befürchten, dass seine persönlichen Daten erhoben und verarbeitet werden, könnte dies dazu führen, dass er sein Nutzungsverhalten und damit seine Persönlichkeitsentfaltung anpasst.[41]

Deshalb schützt das Grundrecht das Interesse des Nutzers, dass seine vom System erfassten Daten in der Gesamtheit vertraulich bleiben.[42] Folglich sind auch nur solche IT-Systeme geschützt, die personenbezogene Daten speichern und bei einem Zugriff einen Rückschluss auf die Persönlichkeit des Nutzers zulassen.

Vom Entwurf erfasst sind nach Absatz 6 des § 202e StGB-E jedoch nicht nur Systeme, die „*zur Verarbeitung personenbezogener Daten geeignet und bestimmt*“ sind, sondern auch Systeme, die „*wirtschaftlichen Zwecken*“ dienen oder zu den „*Bereichen Energie, Transport und Verkehr sowie Ernährung*“ zu zählen sind. Geschützt sind daher

[37] BT-Drs. 16/3656, S. 22.
[38] BVerfGE 120, 274 – Online-Durchsuchungen.
[39] *BVerfG*, NJW 2008, 822 (827).
[40] *BVerfG*, NJW 2008, 822 (827).
[41] *BVerfG*, NJW 2008, 822 (824).
[42] *BVerfG*, NJW 2008, 822 (827).

auch vernetzte Industriemaschinen oder Verkehrssysteme, aber auch Haushaltsgeräte, selbst wenn diese keine personenbezogenen Daten erheben oder speichern.

Insofern deckt sich der Gesetzesentwurf nur im Wortsinn mit dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, da er die „Integrität" dieser Systeme gewährleistet. Inhaltlich geht er jedoch über den Grundrechtsschutz hinaus, indem er die Integrität *aller* IT-Systeme gewährleistet. Damit dient § 202e StGB-E gleichsam dem vorverlagerten Schutz vor Beeinträchtigungen der IT-Infrastruktur.

Zwar schützt § 202a StGB das „formalisierte Interesse an der Geheimhaltung von Daten" und damit ebenfalls genau das, was hinter dem vom BVerfG postulierten Grundrecht steht.[43] Da der digitale Hausfriedensbruch jedoch inhaltlich über den Schutz dieses Grundrechts hinausgeht, bleibt auch das Schutzgut des § 202a StGB hinter dem des § 202e StGB-E zurück. Der umfassende Schutz eines IT-Systems wird auch nicht durch § 303a StGB gewährleistet, weil dadurch nur das Interesse des Berechtigten an der unversehrten Verwendbarkeit der gespeicherten Daten geschützt ist. Ebenfalls genügt es nicht, auf das Interesse der Betreiber und Nutzer am störungsfreien Funktionieren der Datenverarbeitung (§ 303b StGB) abzustellen, da das Einschleusen von Botprogrammen häufig unbemerkt bleibt und nur selten zu einer Funktionsbeeinträchtigung der Datenverarbeitung führt.

Das Rechtsgut der „Integrität aller IT-Systeme" und der damit einhergehende Schutz vor Beeinträchtigungen der IT-Infrastruktur ist daher von einer Lücke im aktuellen Strafrecht betroffen, die durch die Einführung des § 202e StGB-E geschlossen würde.

V. Umsetzung europarechtlicher Vorgaben

Der „digitale Hausfriedensbruch", der das Rechtsgut der „Integrität aller IT-Systeme" umfassend schützen soll, verdeutlicht zugleich die unzureichende Umsetzung europarechtlicher Vorgaben im deutschen Strafrecht. Denn das Übereinkommen des Europarats über Computerkriminalität (Cybercrime-Konvention)[44] und die EU-Richtlinie über Angriffe auf Informationssysteme[45] sind bislang nicht vollumfänglich umgesetzt, auch wenn der Gesetzgeber bereits im Jahr 2007 den § 202a StGB geändert hat, um eben diese Vorgaben vollständig umzusetzen.[46]

[43] *Busching*, Digitaler Hausfriedensbruch, S. 494; *Mavany*, KriPoZ 2016, 106 (112).
[44] Abgedruckt in BGBl. 2008 II Nr. 30, 1242.
[45] Richtlinie 2013/40/EU, ABl. EU L 218, 8.
[46] BT-Drs. 16/3656, 1; BT-Drs. 16/5449, 1; *Ernst*, NJW 2007, 2661 (2661); *Graf*, in: MüKo, § 202a Rn. 1; *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 1.

Art. 2 Cybercrime-Konvention

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

Eine nahezu wortgleiche Regelung findet sich in Art. 2 der EU-Richtlinie über Angriffe auf IT-Systeme. Zum einen soll durch die Vorgaben der Tatsache Rechnung getragen werden, dass Terroranschläge auch in der „digitalen Welt“ möglich sind, indem beispielsweise IT-Systeme oder kritische Infrastrukturen über das Internet angegriffen werden.[47] Andererseits soll die Verwendung von Botnetzen, die Störung des Betriebs von IT-Systemen sowie das Abfangen oder die Veränderung von Daten bekämpft werden.[48] Nach den oben dargelegten Feststellungen ist zweifelhaft, dass diese europarechtlichen Vorgaben bereits hinreichend im deutschen Recht umgesetzt sind.

Zwar kann die Verwendung von Botnetzen von zahlreichen Straftatbeständen erfasst werden. So können z.B. DDoS-Angriffe oder Angriffe auf kritische Infrastrukturen, das Schürfen von Bitcoin oder das Erlangen von Daten je nach Einzelfall gem. §§ 202a, 202b, 303a und 303b StGB strafbar sein.[49]

Dennoch basieren die bestehenden Normen anders als die Cybercrime-Konvention und die EU-Richtlinie, die als Rechtsgut die Systemintegrität schützen, weiterhin nur auf dem Schutz der Integrität von Daten und weisen insofern eine andere Schutzrichtung auf. Auch ist der europarechtlich geforderte Schutz von Systemen nicht zwingend mit dem oben angeführten Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme gleichzusetzen. Während das Grundrecht primär nur auf den Schutz solcher Systeme abstellt, die einen Rückschluss auf die Persönlichkeit des Nutzers zulassen, kennt der europarechtlich geforderte Schutz diese Einschränkung nicht.

Schließlich zielen die europarechtlichen Vorgaben primär auf die Sicherheit der IT-Infrastruktur ab und gehen damit inhaltlich über die konkrete Beeinträchtigung von Grundrechten mit Strafcharakter hinaus. Ferner wird nach jetzigem Recht nur in den Fällen eine Strafbarkeit begründet, in denen mit dem Zugang zu einem IT-System auch

[47] Erwägungsgründe 3 f. Richtlinie 2013/40/EU, ABl. EU L 218, 8.
[48] Erwägungsgründe 5, 6 f. Richtlinie 2013/40/EU, ABl. EU L 218, 8.
[49] Siehe hierzu ausführlich: *Roos/Schumacher*, MMR 2014, 377 (377).

der Zugang zu Daten einhergeht. Zwar gehen häufig mit einem solchen Zugriff auch ein Zugang auf die dort gespeicherten Daten einher.[50] Gleichwohl sind bedingt durch entsprechend programmierte Botprogramme Fallkonstellationen möglich, in denen der Täter zwar Zugriff auf das System erlangt, aber nicht auch Zugang zu Daten.[51] Ebenso kann es vorkommen, dass der Täter zwar Zugang zu Daten hat, dafür aber keine besondere Zugangssicherung überwinden musste und daher hinsichtlich § 202a StGB straflos ausgeht.[52]

Ein umfassender Schutz der Systemintegrität, wie es die Cybercrime-Konvention und die EU-Richtlinie vorsehen, ist *de lege lata* also nicht gegeben. Die Einführung des § 202e StGB-E ist daher erforderlich, um beide europarechtlichen Vorgaben vollständig umzusetzen.

VI. Bewertung

Die Anforderungen, die die bestehenden Normen an die Strafjustiz in Fällen der Botnetz-Kriminalität stellen, können die Gerichte kaum erfüllen. Erst jüngst hob der BGH ein Urteil auf, das die Strafbarkeit eines Täters nach § 202a StGB wegen Nutzung eines Botnetzes vorsah, weil die Sachaufklärung unzureichend und unschlüssig war.[53] Ob und inwiefern zum Zeitpunkt der Tathandlung eine Zugangssicherung bestand, konnte nicht hinreichend geklärt werden. Die Einführung des § 202e StGB-E würde dazu führen, dass die strafprozessualen Anforderungen gesenkt und sich keine derartigen Beweisprobleme mehr ergeben würden. Zwar drängt sich bei einer Erweiterung des Strafgesetzbuchs alleine zum Zweck der Beweiserleichterung im rechtstaatlichen Strafprozess größtmögliche Zurückhaltung auf, dennoch ist die Einführung des § 202e StGB- E gerade auch aufgrund der festgestellten Strafbarkeitsdefizite letztlich der Einschätzung des Gesetzgebers überlassen.

Zwar ist der Entwurf des „digitalen Hausfriedensbruchs“ dem Vorwurf ausgesetzt, lediglich symbolischer Natur zu sein. Jedoch weist § 202e StGB-E ebenso wie auch alle anderen Strafrechtsnormen in seiner „generalpräventiven Funktion“[54] eine symbolische Tendenz auf. Dieser Charakter erscheint insbesondere angesichts der aufgeführten Strafbarkeitsdefizite und dem unzureichenden Rechtsgüterschutz legitim.

[50] *Gercke*, ZUM 2007, 282 (283); *Gröseling/Höfinger,* MMR 2007, 549 (551).
[51] *Gercke*, ZUM 2007, 282 (283); *ders.*, Schriftl. Stellungnahme zur Anhörung des Rechtsausschusses, S. 6, abrufbar unter: *http://bundestag.de/ausschuesse/a06/anhoerungen/15_Computerkriminalitaet/*; *Gröseling/Höfinger,* MMR 2007, 549 (551).
[52] Die Möglichkeit der Einschränkung der Strafbarkeit durch das Erfordernis einer Zugangssicherung ist zwar explizit in beiden europarechtlichen Vorgaben vorgesehen. Dennoch erscheint das Merkmal angesichts der zunehmend komplexen digitalen Welt nicht mehr zeitgemäß und vermag nicht zu erklären, warum nur das sich schützende Opfer strafrechtlichen Schutz erhalten soll.
[53] *BGH*, NStZ 2016, 339.
[54] *Roxin*, AT I, § 3 Rn. 26 f.

Problematisch ist allein, dass der Bundesratsentwurf eine besonders weite Strafbarkeit begründet und in seiner aktuellen Fassung auch sozialadäquates Verhalten erfasst, da der Wortlaut des § 202e StGB-E keineswegs auf die Bekämpfung von Botnetzen beschränkt ist. Erfasst ist vielmehr jede unbefugte Nutzung eines IT-System, sofern diese nur geeignet ist, „berechtigte Interessen“ eines anderen zu beeinträchtigen. Die Annahme eines ausschließlichen Gebrauchsrechts verkennt aber die technische Realität. Angesichts der Omnipräsenz von IT-Systemen ist der Kontakt mit ihnen im Alltag unausweichlich, so dass der Entwurf eine völlig unüberschaubare Bandbreite an Verhaltensweisen erfasst. Nach dem aktuellen Entwurf würde sich beispielsweise strafbar machen, wer in einem Bus aus Spaß vor jeder Haltestelle auf den Halte-Knopf drückt.[55] Ist ein solches Verhalten in der Nutzungsverordnung des Busses untersagt, macht sich derjenige strafbar, da er nach § 202e StGB-E Abs. 1 Nr. 1 ein IT-System in Gebrauch genommen bzw. beeinflusst hat. Das Drücken ist auch geeignet, berechtigte Interessen des Busfahrers und anderer Mitfahrer zu beeinträchtigen, da diese nicht unnötig an jeder Haltestelle anhalten wollen. Im Ergebnis wird deutlich, dass der Tatbestand des § 202e StGB-E im Hinblick auf den strafrechtlichen Bestimmtheitsgrundsatz in Art. 103 II GG bedenklich weit gefasst ist und insofern nicht geeignet ist, die gesetzgeberischen Intentionen verfassungskonform umzusetzen.

VII. Eigener Gesetzesvorschlag

Im Gegensatz zur Einführung der expansiven Regelung des § 202e StGB-E ist ein minimalinvasiver Eingriff in das Strafgesetzbuch erforderlich, der auf das Einschleusen von Programmen in IT-Systeme beschränkt ist und die Fälle erfasst, die von §§ 202a und 303a StGB nicht gedeckt sind.

Entgegen des Vorschlags von Buermeyer/Golla[56], wonach als Ergänzung in § 202c StGB bestraft werden soll, „wer eine Straftat vorbereitet, indem er Programmcode auf ein informationstechnisches System ohne Einwilligung des Berechtigten in der Absicht aufbringt, diesen ausführen zu lassen“, sollte dieses Verhalten in einem eigenen Straftatbestand pönalisiert werden. Zum einen liegt der Schwerpunkt nämlich im Einschleusen der Schadsoftware selbst, da bereits hierbei ein hohes kriminelles Gefährdungspotential liegt. Zum anderen könnte dann auch der Wunsch des aktuellen Gesetzesentwurfes berücksichtigt werden, wonach bereits der Gebrauch eines IT-Systems strafrechtlich geschützt sein soll.

Um eine Ausdehnung der Strafbarkeit auf offensichtlich nicht strafwürdige Fälle zu verhindern, könnte eine unbefugte Ingebrauchnahme so beschränkt werden, dass sie

[55] Dieses und noch weitere Beispiele: *Biselli*, Digitaler Hausfriedensbuch: Netzpolitik.org; weitere absurde Beispiele auch bei: *Buermeyer/Golla,* K&R 2017, 14 (16 f.).
[56] *Buermeyer/Golla*, K&R 2017, 14 (18).

nicht im Wege der Datenübermittlung (§ 202b) erfolgen darf und damit die Fälle abdeckt, in denen der Täter die Systeme nicht selbst infiziert, aber die Botprogramme mietet und über Server fernsteuert.

Schließlich könnte durch die Einführung einer Qualifikation für gewerbsmäßige oder bandenmäßige Begehung verdeutlich werden, dass sich die Einführung eines „digitalen Hausfriedensbruchs" gegen professionelle Strukturen richtet.[57] Der hier vorgeschlagene Entwurf könnte als Vorbereitungs-Straftat wie folgt lauten:

„(1) Wer unbefugt

1. einen Programmcode in ein informationstechnisches System einschleust, um diesen ausführen zu lassen oder

2. ein informationstechnisches System im Wege der Datenübermittlung in Gebrauch nimmt,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwerer Strafe bedroht ist.

(2) Mit Freiheitsstrafe bis zu drei Jahren wird bestraft, wer gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach Absatz 1 verbunden hat, handelt."

VIII. Ergebnis

Die Einführung eines digitalen Haufriedensbruchs ist aufgrund von bestehenden Strafbarkeitslücken, einem mangelnden Rechtsgüterschutz und europarechtlichen Vorgaben erforderlich. Der Gesetzesentwurf dient der Bekämpfung von Botnetz-Kriminalität und stellt das computertechnische Eindringen in ein IT-System unter Strafe. In dieser Phase bestehen aufgrund neuster technischer Entwicklungen hinsichtlich §§ 202a und 303a StGB Strafbarkeitslücken, die durch die Einführung des § 202e StGB-E geschlossen würden. Darüber hinaus schützt der „digitale Hausfriedensbruch" nicht nur personenbezogene Daten, sondern die Integrität *aller* IT-Systeme und dient dem Schutz eines Rechtsguts, das durch das jetzige Strafrecht nicht gewährleistet wird. Auch hinsichtlich europarechtlicher Vorgaben erscheint die Einführung eines § 202e StGB-E erforderlich, da die bestehenden Straftatbestände nur auf den Schutz von Daten, nicht aber des Systems als solches abstellen und damit hinter den internationalen Vorgaben zum Schutz der Integrität und Verfügbarkeit von Systemen zurückbleiben.

In seiner aktuellen Form begründet der Entwurf des § 202e StGB jedoch eine expansive Strafbarkeit und erfasst auch offensichtlich nicht strafwürdiges Verhalten. Daher

[57] So der Vorschlag von *Golla/v. zur Mühlen*, JZ 2014, 668 (674) in Bezug auf § 202c StGB.

wurde ein alternativer Gesetzesvorschlag ausgearbeitet, der die gesetzgeberischen Intentionen berücksichtigt. Im Ergebnis kann der Hausfriedensbruch im Strafgesetzbuch ein „digitales Update“ vertragen.

Literaturverzeichnis

Amelung, Knut, Irrtum und Zweifel des Getäuschten beim Betrug, GA, 1977, S. 1-17.

Biselli, Anna, „Digitaler Hausfriedensbruch: Hessen will neuen Straftatbestand gegen bereits illegale Botnetze einführen“: in: Netzpolitik.org; abrufbar unter: https://netzpolitik.org/2016/digitaler-hausfriedensbruch-hessen-will-neuen-straftatbestand-gegen-bereits-illegale-botnetze-einfuehren/.

Buermeyer/Golla, „Digitaler Hausfriedensbruch – Der Entwurf eines Gesetzes zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme“, K&R, 2017, S. 14-18.

Bundeskriminalamt, (BKA) Bundeslagebild Cybercrime, 2016.

Bundesamt für Sicherheit in der Informationstechnik, (BSI) Lage der IT-Sicherheit in Deutschland, 2017.

Busching, Michael, „Gesetzesentwurf zum sog. „Digitalen Hausfriedensbruch“: Notwendige Schließung von Strafbarkeitslücken oder Symbolgesetzgebung?“, Schweighofer/Kummer/Hötzendorfer/Sorge (Hrsg.), Trends und Communities der Rechtsinformatik, Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017, Wien 2017, S. 489-496.

Dietrich, Ralf, Das Erfordernis der besonderen Sicherung im StGB am Beispiel des Ausspähens von Daten, § 202a StGB, Dissertation, Berlin 2009.

Dietrich, Ralf, „Die Rechtsschutzbegrenzung auf besonders gesicherte Daten des § 202a StGB“, NStZ, 2011, S. 247-254.

Ernst, Stefan, „Hacker und Computerviren im Strafrecht“, NJW, 2003, S. 3233-3239.

Ernst, Stefan, „Das neue Computerstrafrecht“, NJW, 2007, S. 2661-2666.

Fischer, Thomas (Verf.), Strafgesetzbuch und Nebengesetze, Kommentar, 65. Aufl., München 2018.

Gercke, Marco, „Die Entwicklung des Internetstrafrechts im Jahr 2006“, ZUM, 2007, S. 282-293.

Golla, Sebastian, „Risiken und Nebenwirkungen bei der Fortbildung des Internetstrafrechts – Datenhehlerei, Digitaler Hausfriedensbruch und alternative Regelungsansät-

ze“, Stiftung der Hessischen Rechtsanwaltschaft, Die Internetkriminalität boomt: Braucht das Strafgesetzbuch ein Update?, 2017, S. 153-181.

Golla/von zur Mühlen, „Der Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei“, JZ, 2014, S. 668-674.

Graf/Jäger/Wittig (Hrsg.), Wirtschafts- und Steuerstrafrecht, Kommentar, 2. Aufl., München 2017.

Gröseling/Höfinger, „Hacking und Computerspionage – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität“, MMR, 2007, S. 549-553.

Heine, Sonja, „Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining“, NStZ, 2016, S. 441-446.

Hilgendorf/Valerius, Computer- und Internetstrafrecht: ein Grundriss, 2. Aufl., Berlin 2012.

Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Band 3, §§ 185-262, München 2003.

Kochheim, Dieter, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, München 2015.

Laufhütte, Rissing-van Saan, Tiedemann (Hrsg.), Strafgesetzbuch: Leipziger Kommentar, 6. Band, 12. Aufl., Berlin 2009.

Manavy, Markus, „Pferde, Würmer, Roboter, Zombies und das Strafrecht? Vom Sinn und Unsinn neuer Gesetze gegen den sog. digitalen Hausfriedensbuch“, KriPoZ, 2016, S. 106-112.

Roos/Schumacher, „Botnetze als Herausforderung für Recht und Gesellschaft – Zombies außer Kontrolle?“, MMR, 2014. S. 377-378.

Roxin, Claus, Strafrecht – 1: Grundlagen, der Aufbau der Verbrechenslehre, 4. Aufl., München 2006.

Schönke/Schröder (Hrsg.), Strafgesetzbuch Kommentar, 29. Aufl., München, 2014.

Schultz, Alexander, „Neue Strafbarkeiten und Probleme“, DuD, 2006, S. 778-784.

Stam, Fabian, „Die Strafbarkeit des Aufbaus von Botnetzen“, ZIS, 2017, S. 547-552.

Alle Internetseiten wurden zuletzt am 04.06.2018 aufgerufen.

Staatliche Förderung des Breitbandausbaus

Rechtliche Instrumente und Grenzen

Emanuel Kollmann

BakerMcKenzie
emanuel.kollmann@gmail.com

Abstract

Der Breitbandausbau ist eines der wichtigsten infrastrukturpolitschen Projekte unserer Zeit. Der vorliegende Beitrag untersucht die im Koalitionsvertrag von 2018 vorgeschlagenen Maßnahmen zur Förderung des Breitbandausbaus im Hinblick auf den Ausbau einer leistungsfähigen Glasfaserinfrastruktur. Der Autor zeigt, dass dem Staat verschiedene Instrumente zur Förderung des Breitbandausbaus zur Verfügung stehen, die meist daran gekoppelt sind, dass der Betreiber der betreffenden Glasfaserinfrastruktur seinen Wettbewerbern diskriminierungsfrei Zugang zu dem Netz gewährt.

I. Einleitung

1. Der Ausbau leistungsfähiger Breitbandnetzwerke als politisches Ziel

„An die Weltspitze im Bereich der digitalen Infrastruktur" – mit diesem Ziel geht die Bundesregierung in die aktuelle Legislaturperiode. Spätestens 2025 sollen die dafür erforderlichen Glasfasernetze flächendeckend Empfangsgeschwindigkeiten im Gigabit-Bereich bereitstellen.[1]

Erreicht werden soll dieses Ziel mit einem bunten Strauß von Maßnahmen. Geplant sind u.A. ein Förderfonds für Gigabitnetze, Anreize zum Netzausbau durch Anpassungen der Marktregulierung und ein rechtlich abgesicherter Anspruch auf einen Zugang zum schnellen Internet ab dem Jahr 2025.[2]

Auch die EU-Kommission legt in ihrer Strategie für einen digitalen Binnenmarkt das Ziel fest, dass bis 2025 alle Privathaushalte einen Internetzugang mit einer Empfangsgeschwindigkeit von mindestens 100 Mbit/s erhalten sollen.[3]

[1] CDU/CSU/SPD Koalitionsvertrag „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land." v. 12.03.2018, S. 37.
[2] CDU/CSU/SPD Koalitionsvertrag „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land." v. 12.03.2018, S. 37 f.
[3] *Klotz/Hofmann*, N&R 2017, 2 (6).

2. Rechtsrahmen

Die telekommunikationsrechtlichen Rahmenbedingungen sind stark europarechtlich geprägt. Die Rahmenrichtlinie (RRL)[4], Genehmigungsrichtlinie (GRL)[5], Zusammenschaltungsrichtlinie (ZRL)[6] und Universaldienstrichtlinie (URL)[7] bilden zusammen den sogenannten einheitlichen Rechtsrahmen.[8]

Der einheitliche Rechtsrahmen befindet sich momentan in Überarbeitung. Die Kommission hat 2016 einen Vorschlag für einen „Kodex für elektronische Kommunikation" (KommE-Kodex)[9] vorgelegt, der die vier Richtlinien zusammenführen und inhaltlich weiterentwickeln soll.[10] Ein wesentliches Ziel der Reform soll eine verstärkte Anreizsetzung für Investitionen in schnelle Netze sein.[11]

Das Gesetzgebungsverfahren befindet sich auf der Zielgeraden. Am 29. Juni 2018 wurde die finale Entwurfsfassung nach Abschluss der Trilog-Verhandlungen (Kodex-E) veröffentlicht.[12] Die Abschlussabstimmung im Parlament ist für November 2018 vorgesehen.

Verfassungsrechtlich werden die Rahmenbedingungen durch Art. 87 f GG vorgegeben. Dieser legt fest, dass der Bund flächendeckend angemessene und ausreichende Dienstleistungen im Bereich der Telekommunikation gewährleistet (sog. Gewährleistungsauftrag, Art. 87 f Abs. 1 GG), diese Dienstleistungen werden durch private Anbieter erbracht (Privatwirtschaftlichkeitsgebot, Art. 87 f Abs.2 GG).[13] Dies betrifft nicht nur die Erbringung von Telekommunikationsdienstleistungen, sondern auch den Aufbau und Betrieb der zugrundeliegenden Netze.[14]

Umgesetzt werden die europa- und verfassungsrechtlichen Vorgaben auf nationaler Ebene einfachrechtlich im Telekommunikationsgesetz (TKG).

3. Kein staatlicher Netzbetrieb

Das Privatwirtschaftlichkeitsgebot steht einem Netzausbau durch die öffentliche Hand entgegen.[15] Der Bund darf zwar Anteile an der Deutschen Telekom AG halten, jedoch

[4] RL 2002/21/EG.
[5] RL 2002/20/EG.
[6] RL 2002/19/EG.
[7] RL 2002/22/EG.
[8] ErwGr. 5 RRL.
[9] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation, COM(2016) 590 final.
[10] *Neumann*, N&R 2016, 262 (263).
[11] ErwGr. 3 Kodex-E.
[12] Vorschlag v. 29.6.2018 – 10692/18.
[13] *Möstl*, in: Maunz/Dürig GG, Art. 87 f Rn. 2.
[14] *Möstl*, in: Maunz/Dürig GG, Art. 87 f Rn. 33.
[15] *Möstl*, in: Maunz/Dürig GG, Art. 87 f Rn. 33.

kommt dieser im Vergleich zu ihren Wettbewerbern keine Sonderstellung mehr zu. Beide werden von Art. 87 f Abs. 2 GG gleichermaßen als „privatwirtschaftlich“ bezeichnet.[16] Der Ausbau der Glasfasernetze muss unter den Bedingungen des Wettbewerbs durch den Markt vorgenommen werden.

Die dem Staat verbleibenden Möglichkeiten der Förderung von Breitbandausbauprojekten und deren rechtlicher Rahmen sollen im Folgenden insbesondere in Bezug auf den angestrebten Ausbau der Glasfaserinfrastruktur dargestellt werden.

II. Finanzielle Förderung

Zur direkten Förderung des privaten Breitbandausbaus will die Bundesregierung u.A. die Erlöse aus der Vergabe der UMTS- und 5G-Lizenzen bereitstellen.[17] Diese Erlöse stehen innerhalb Europas den Mitgliedsstaaten zu[18] und fließen in Deutschland in den Bundeshaushalt.[19] Sie können daher vom Bund für ein Förderprogramm verwendet werden.

Ein Förderprogramm findet seine Grenzen im Beihilferecht der Union (Art. 107 ff. AEUV), denn finanzielle Zuschüsse zu privaten Breitbandausbauprojekten fallen unter den Beihilfebegriff des Art. 107 Abs. 1 AEUV, auch dann, wenn sie durch ein Ausschreibungsverfahren ermittelt werden.[20] Von dem Begriff erfasst werden nämlich alle staatlichen Maßnahmen, die bestimmten Unternehmen wirtschaftliche Vorteile gewähren und damit den unternehmerischen Leistungswettbewerb und die Handelsströme im Binnenmarkt verfälschen.[21] Diese sind grundsätzlich mit dem Binnenmarkt unvereinbar und verboten. Eine (enge) Ausnahme liegt lediglich dann vor, wenn das staatliche Handeln dem eines marktwirtschaftlich handelnden Kapitalgebers entspricht (dies hat die Kommission bislang allerdings bloß in einem einzigen Fall bejaht).[22]

Beihilfen können aber dennoch mit dem Binnenmarkt vereinbar sein, wenn sie einen der Tatbestände des Art. 107 Abs. 3 AEUV erfüllen, insbesondere von einer Verordnung i.S.v. Art. 107 Abs. 3 lit. e AEUV gedeckt sind (sogenannte Freistellungsverordnung). Eine solche hat die Kommission mit der Allgemeinen Gruppenfreistellungsverordnung (AGVO)[23] erlassen. Investitionsbeihilfen für den Ausbau der Breitbandversorgung sind unter den Voraussetzungen des Art. 52 Abs. 2 – Abs. 7 AGVO mit dem

[16] *Möstl*, in: Maunz/Dürig GG, Art. 87 f Rn. 47.
[17] CDU/CSU/SPD Koalitionsvertrag „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land.“ v. 12.03.2018, S. 37.
[18] *Klotz/Hofmann*, N&R 2017, 2 (6).
[19] *BVerfG*, NJW 2002, 2020 (2020).
[20] Leitlinien der EU für die Anwendung der Vorschriften über staatliche Beihilfen im Zusammenhang mit dem schnellen Breitbandausbau, 2013/C 25/01, Rn. 12.
[21] *Mestmäcker/Schweitzer*, in: Immenga/Mestmäcker AEUV, Art. 107 Rn. 1.
[22] *Kliemann/Stehmann*, in: von der Groeben/Schwarze/Hatje AEUV, Art. 107 Rn. 771.
[23] VO (EU) 651/2014.

Binnenmarkt vereinbar und von der Anmeldepflicht freigestellt.[24] Es gelten u.A. folgende Voraussetzungen:

Es muss ein Marktversagen und ein entsprechendes soziales Bedürfnis bestehen, dass die Freistellung rechtfertigt.[25] Es darf daher keine bestehende oder unter Marktbedingungen zu erwartende konkurrierende Infrastruktur zu dem geförderten Ausbau vorliegen.[26]

Der Betreiber des geförderten Netzes muss Wettbewerbern für mindestens sieben Jahre Zugang zu den aktiven und passiven Infrastrukturen auf Vorleistungsebene im Sinne einer physischen Entbündelung[27] gewähren.[28] Hiermit soll es Drittbetreibern ermöglicht werden, mit dem ausgewählten Netzbetreiber in Wettbewerb zu treten.[29] Die Preise für diesen Zugang müssen sich u.A. auf Preisfestsetzungsgrundsätze der nationalen Regulierungsbehörde stützen.[30]

Die Freistellung gilt nicht für Beihilfen, die eine Schwelle von 70 Mio. Euro Gesamtkosten pro Vorhaben überschreiten.[31] Beihilfen, die diese Schwelle überschreiten, müssen gem. Art. 108 Abs. 3 AEUV bei der Kommission angemeldet und auf ihre Vereinbarkeit mit Art. 107 AEUV überprüft werden. Für Beihilfen zum Breitbandausbau ist insbesondere Art. 107 Abs. 3 lit. c AEUV einschlägig, der Beihilfen zur Förderung der Entwicklung gewisser Wirtschaftszweige vom Beihilfeverbot ausnimmt. Die Kommission hat zu ihrer Entscheidungspraxis Leitlinien[32] erlassen. Diese stellen ähnliche Anforderungen wie die AGVO auf. Insbesondere bestehen Vorgaben dahingehend, dass der Förderungsempfänger offenen Zugang auf Vorleistungsebene gewähren[33] und die Preise für diesen Zugang auf die Preisfestsetzungsgrundsätze der nationalen Regulierungsbehörden stützen muss.[34]

Insgesamt legt die Kommission in ihrer Entscheidungspraxis Wert darauf, dass private Investitionen nicht durch öffentliche Investitionen verdrängt werden und andere Anbieter die vom Staat finanzierte Infrastruktur diskriminierungsfrei nutzen können.

[24] Art. 52 Abs. 1 AGVO.
[25] *Nowak*, in: Immenga/Mestmäcker AGVO, Art. 52 Rn. 9.
[26] Art. 52 Abs. 3 AGVO.
[27] Physische Entbündelung ermöglicht den Zugang zur Teilnehmerleitung und versetzt die Übertragungssysteme von Wettbewerbern in die Lage, direkt darüber zu übertragen, (Art. 2 Nr. 139 AGVO).
[28] Art. 52 Abs. 5 AGVO.
[29] *Nowak*, in: Immenga/Mestmäcker AGVO, Art. 52 Rn. 12.
[30] Art. 52 Abs. 6 AGVO.
[31] Art. 4 Abs. 1 lit. y AGVO.
[32] Leitlinien der EU für die Anwendung der Vorschriften über staatliche Beihilfen im Zusammenhang mit dem schnellen Breitbandausbau, 2013/C 25/01.
[33] Leitlinien der EU für die Anwendung der Vorschriften über staatliche Beihilfen im Zusammenhang mit dem schnellen Breitbandausbau, 2013/C 25/01, Rn. 78 g.
[34] Leitlinien der EU für die Anwendung der Vorschriften über staatliche Beihilfen im Zusammenhang mit dem schnellen Breitbandausbau, 2013/C 25/01, Rn. 78 h.

Alle Betreiber sollen gleichermaßen Zugang zur subventionierten Infrastruktur erhalten. Zudem soll sichergestellt sein, dass die Vorleistungspreise angemessen bleiben.[35]

Der Bund hat diese Vorgaben in der NGA-Rahmenregelung umgesetzt.[36] Diese wurde von der Bundesregierung gemäß Art. 108 Abs. 3 AEUV notifiziert und von der Kommission genehmigt.

Eine direkte Förderung des privatwirtschaftlichen Breitbandausbaus durch die öffentliche Hand im Rahmen der Grenzen des EU-Beihilferechts ist möglich. Zu beachten sind allerdings dessen Vorgaben, insbesondere die Verpflichtung des geförderten Netzbetreibers, anderen Anbietern diskriminierungsfrei Zugang zu der geförderten Netzinfrastruktur zu gewähren (sog. „Open Access“).

III. Rahmenbedingungen und Regulierung

1. Einleitung

Der Markt für Telekommunikationsinfrastruktur, in dessen Umfeld der Ausbau breitbandiger Glasfaserinfrastruktur stattfindet, ist einer strengen Regulierung der Bundesnetzagentur (BNetzA) unterworfen.

Das telekommunikationsrechtliche Marktregulierungsverfahren läuft im Wesentlichen wie folgt ab: Die BNetzA legt die zu untersuchenden Märkte fest (Marktdefinition, § 10 TKG) und untersucht sodann, ob auf diesen Märkten wirksamer Wettbewerb besteht oder Unternehmen über beträchtliche Marktmacht verfügen (Marktanalyse, § 11 TKG). Basierend auf diesen Erkenntnissen kann die BNetzA gemäß § 13 Abs. 1 S. 1 TKG in einer Regulierungsverfügung eine oder mehrere marktmachtabhängige Verpflichtungen auferlegen. Dazu gehören Zugangsverpflichtungen (§ 21 TKG) und Entgeltregulierung (§ 30 TKG).[37]

Primäres Ziel der Regulierung ist die Schaffung und Aufrechterhaltung von Wettbewerb.[38] Dies ist notwendig, da im Telekommunikationsmarkt regelmäßig ein Unternehmen, welches das ehemals staatliche Telekommunikationsnetz übernommen hat, über beträchtliche Marktmacht – bis hin zum Monopol – verfügt.[39] Deshalb kann diesem auferlegt werden, anderen Wettbewerbern die Mitnutzung seiner Netzinfrastruktur zu gestatten (Zugangsverpflichtung) und dafür nur Preise zu verlangen, die von der BNetzA zu genehmigen sind (Entgeltgenehmigung). Ein freies Wettbewerbsumfeld

[35] *Klotz/Hofmann*, N&R 2017, 2 (9).
[36] Rahmenregelung der Bundesrepublik Deutschland zur Unterstützung des Aufbaus einer flächendeckenden Next Generation Access (NGA)-Breitbandversorgung vom 15. Juni 2015.
[37] Im Übrigen: § 19 TKG (Diskriminierungsverbot), § 20 TKG (Transparenzverpflichtung), § 23 TKG (Standardangebot, § 24 TKG (getrennte Rechnungsführung), § 39 TKG (Entgeltregulierung bei Endnutzerleistungen).
[38] *Kühling/Schall/Biendl*, Rn. 152.
[39] *Correa*, in: Walden, S. 26.

setzt auch mehr Anreize für Investitionen, als ein monopolistischer aber auch als ein zu stark regulierter Markt. Es sollte daher nur dort reguliert werden, wo kein wirksamer Wettbewerb besteht.[40] Es gilt deswegen das Prinzip, dass die Regulierung nur dann eingreift, wenn die Marktaufsicht durch das allgemeine Wettbewerbsrecht unzureichend ist.[41] Dem KommE-Kodex liegt in weiten Teilen die Annahme zugrunde, dass der Breitbandausbau am besten durch eine zurückhaltende Regulierung zu fördern sei.[42]

2. Berücksichtigung bei Regulierungsentscheidungen

Bei ihren Regulierungsentscheidungen hat die BNetzA die Regulierungsziele des § 2 Abs. 2 TKG zu berücksichtigen. Zu diesen gehört auch „*die Beschleunigung des Ausbaus von hochleistungsfähigen öffentlichen Telekommunikationsnetzen der nächsten Generation*“ (§ 2 Abs. 2 Nr. 5 TKG). Eine Berücksichtigung des Breitbandausbaus bei der Marktregulierung ist daher bereits jetzt möglich.[43]

a) Beispiel: Die Regulierung der Teilnehmeranschlussleitung

Bespielhaft dafür sind insbesondere Regulierungsentscheidungen der BNetzA in Bezug auf Zugang zur Teilnehmeranschlussleitung (TAL).

Bei der TAL handelt es sich um die Kabelverbindung zwischen dem Hauptverteiler (HVt) und dem Hausanschluss der Nutzer. Üblicherweise kommen hier noch Kupferkabel zum Einsatz. Die TAL ist für den Wettbewerb auf dem Endnutzermarkt von großer Bedeutung, da der Aufbau doppelter Infrastrukturen dort unwirtschaftlich ist und so ein natürliches Monopol durch den Infrastrukturbetreiber besteht.[44] Um dem zu begegnen, wurde der Telekom Deutschland GmbH (TDG) als Betreiberin der TAL schon früh die Verpflichtung auferlegt, Wettbewerbern entbündelten Zugang[45] zur TAL zu gewähren.[46] Ziel ist die Förderung des Wettbewerbs auf den Großhandels- und Endkundenmärkten.[47] Die Verpflichtung ermöglicht den Wettbewerbern, sich mit ihren Produkten gegenüber der TDG zu differenzieren.[48] So wird auch ein Breitbandausbau durch Wettbewerber der TDG ermöglicht.[49] Die wirtschaftliche Bedeutung ist immens:

[40] *Correa*, in: Walden, S. 27; *Kopf/Vidal*, MMR 2018, 22 (25) fordern sogar einen weitgehenden Abbau der Marktregulierung.
[41] § 10 Abs. 2 S. 1 TKG.
[42] *Neumann*, N&R 2016, 262 (264); *Madiega*, S. 5.
[43] *Gärditz*, in: Scheurle/Mayen TKG, § 2 Rn. 34.
[44] *Correa*, in: *Walden*, S. 38.
[45] Entbündelter Zugang ist die Bereitstellung des Zugangs in der Weise, dass die Nutzung der gesamten Kapazität der Netzinfrastruktur ermöglicht wird (Anhang II lit. c ZRL).
[46] *Geppert/Attendorn*, in: Geppert/Schütz BeckTKG-Komm, § 21 Rn. 218; vgl. zur Entwicklung der Zugangsverpflichtung *Knapp/Weißenfels*, N&R 2014, 130 (130 f.).
[47] *Geppert/Attendorn*, in: Geppert/Schütz BeckTKG-Komm, § 21 Rn. 4.
[48] *Knapp/Weißenfels*, N&R 2014, 130 (132).
[49] *Knapp/Weißenfels*, N&R 2014, 130 (131).

75% der Breitbandanschlüsse werden weiterhin über das Netz der TDG verwirklicht, die aber selbst nur einen Marktanteil von 50% in diesem Bereich hat.[50]

Die TDG plant seit 2012 in den Kabelverzweigern (KVz)[51] sogenannte Vectoring-Technologie einzusetzen. Dabei werden Interferenzen zwischen benachbarten Kupferdoppeladern algorithmisch herausgerechnet, um die verfügbare Bandbreite deutlich zu erhöhen. Dies erfordert die leitungsübergreifende Verwaltung aller Kabel eines Kabelbündels, so dass eine Gewährung von entbündeltem Zugang an Wettbewerber zu den einzelnen TAL nicht mehr möglich ist.[52]

Die BNetzA erlaubte auf Antrag der TDG mit Beschluss vom 1. September 2016 (Vectoring-II-Entscheidung)[53] den Einsatz der Vectoring-Technologie in den KVz. Die Verpflichtung, entbündelten Zugang zur TAL zu gewähren, blieb bestehen, die TDG kann den Zugang jedoch ablehnen, wenn sie den KVz mit Vectoring ausbaut. Zugangsnachfrager können die Verweigerung wiederum abwenden, wenn sie den KVz selbst mit Vectoringtechnologie erschließen. Im Gegenzug müssen jeweils virtuelle Ersatzprodukte für den entbündelten Zugang angeboten werden.[54]

Gerechtfertigt wurde die Einschränkung des entbündelten Zugangs im Ergebnis damit, dass der Einsatz der Vectoring-Technologie den Regulierungszielen der Beschleunigung des Ausbaus von hochleistungsfähigen Telekommunikationsnetzen der nächsten Generation dient.[55]

Die Entscheidung der BNetzA traf auf nicht unerhebliche Kritik.[56] Insbesondere wurde bemängelt, dass das Regulierungsziel des Ausbaus von hochleistungsfähigen öffentlichen Telekommunikationsnetzen der nächsten Generation (§ 2 Abs. 2 Nr. 5 TKG) nicht ausreichend mit den anderen Regulierungszielen, insbesondere der Sicherstellung eines chancengleichen Wettbewerbs (§ 2 Abs. 2 Nr. 2 TKG) in Einklang gebracht worden sei. Negative Effekte für den Breitbandausbau wurden gesehen, da für Wettbewerber kein eigener Netzausbau unabhängig vom Vorleistungsprodukt der TDG mehr möglich sei.[57] Darüber hinaus führe der Fokus auf eine Übergangstechnologie zu innovations- und investitionsdämpfenden Effekten. Die Vectoring-Entscheidung wird

[50] *Dialog Consult/VATM*, S. 12.
[51] Die KVz liegen zwischen HVt und Hausanschluss.
[52] *Herrmann/Heilmann*, N&R 2017, 154 (154).
[53] *BNetzA*, Beschl. v. 1.9.2016 – Bk 3g-15/004.
[54] *BNetzA*, Beschl. v. 1.9.2016 – Bk 3g 15/004 Ziff. 1.1.1 des Tenors i.V.m. Anlage 2.
[55] *Herrmann/Heilmann/Werkmeister*, N&R 2016, 130 (132).
[56] Siehe z.B. das gemeinsame Schreiben von mehreren deutschen und europäischen Verbänden an den zuständigen EU-Kommissar, abrufbar unter http://www.vatm.de/index.php?eID=tx_nawsecuredl&u=0&g=0&t=1533030790&hash=c59ee7f098ddeef4b8077a24a535c15bfc2675c6&file=uploads/media/2016-04-20_Verb%C3%A4ndeschreiben_zur_Vectoring-Problematik_DEU.pdf
[57] *Herrmann/Heilmann*, N&R 207 154 (156).

dementsprechend auch als Grund für den schleppenden Ausbau mit FttH/B[58]-Anschlüssen gesehen.[59] Festzustellen ist jedenfalls, dass der überwiegende Anteil des Ausbaus von FttH/B-Infrastruktur von den Wettbewerbern und nicht der TDG durchgeführt wurde.[60]

Dennoch wird Vectoring in der Literatur zumindest als sinnvolle Übergangstechnologie bis zum substantiellen Ausbau von FttH/B angesehen.[61]

Die Debatte zeigt die Grenzen der Berücksichtigung des Breitbandausbaus bei der Regulierung unter Berufung auf die allgemeinen Regulierungsziele. Das Regulierungsziel der Beschleunigung des Ausbaus von hochleistungsfähigen öffentlichen Telekommunikationsnetzen der nächsten Generation ist immer mit den anderen Regulierungszielen – insbesondere dem Regulierungsziel Sicherstellung eines chancengleichen Wettbewerbs (§ 2 Abs. 2 Nr. 2 TKG) – in Einklang zu bringen. Die Ziele sind gleichwertig.[62] Eine grenzenlose Förderung des Breitbandausbaus ist auf diesem Wege daher nicht möglich.

b) Die Regulierung der Glasfasernetze

Wie im Rahmen der allgemeinen Regulierung zukünftig Modelle entwickelt werden können, um den Ausbau von Glasfaserinfrastruktur zu fördern, ist Gegenstand einer umfangreichen Debatte. Die Bundesregierung plant für breitbandige Glasfasernetze die bestehende ex-ante-Regulierung durch eine ex-post Regulierung zu ersetzen, wenn die Betreiber Open Access gewähren.[63]

Bereits jetzt werden Glasfaserinfrastrukturen regulatorisch teilweise anders behandelt als herkömmliche (Kupfer-)Kabel. So unterliegen die Zugangsentgelte für reine Glasfaser-TAL beispielsweise nur der nachträglichen Regulierung gemäß § 38 TKG, während die Kupfer-TAL der Genehmigungspflicht gemäß § 31 TKG unterworfen sind.[64] Begründet wird dies damit, dass so flexibler auf die Besonderheiten der Glasfaser-TAL reagiert werden könne, die ggf. auch höhere Vorleistungspreise rechtfertigen.[65]

Die Glasfasernetze sollen – anders als das Kupfernetz der TDG – nicht durch ein Staatsmonopol, sondern im Wettbewerb errichtet werden. Daher wird vorgeschlagen, die Regulierung auf ihre wettbewerbssichernde Funktion zurückzufahren und dem

[58] Glasfaseranschlüsse bis in die Gebäude (Fibre to the Home/Building)
[59] *Europäischer Rechnungshof*, Rn. 47 ff.
[60] *BREKO*, S. 1.
[61] *Knapp/Weißenfels*, N&R 2014, 130 (138).
[62] *Gärditz*, in: Scheurle/Mayen TKG, § 2 Rn. 19.
[63] CDU/CSU/SPD Koalitionsvertrag „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land." v. 12.03.2018, S. 38.
[64] *BNetzA*, Beschl. v. 1. 9. 2016 – Bk 3g 15/004 Ziff. 1.8 des Tenors.
[65] *BNetzA*, Beschl. v. 1.9.2016 – Bk 3g 15/004 S. 319.

Wettbewerb wieder eine größere Bedeutung einzuräumen.[66] Eine Regulierung soll insbesondere dann unterbleiben, wenn der (marktmächtige) Netzbetreiber seinen Wettbewerbern diskriminierungsfreien Zugang zur Infrastruktur gewährt (Open Access). Der BNetzA verbleibt in diesem Modell lediglich die Rolle einer Schiedsrichterin.[67]

Konkrete Rechtsgrundlagen für einzelne Regulierungserleichterungen bestehen nach geltender Rechtslage allerdings nicht[68], lediglich die Berücksichtigung der Besonderheiten von zukunftsfähigen Netzen wird im Rahmen der Regulierung an einigen Stellen vorgeschrieben.[69] Sie sind daher nur im allgemeinen Regulierungsverfahren unter Berufung auf das Regulierungsziel des § 2 Abs. 2 Nr. 5 TKG möglich. Dieses muss jedoch mit dem Regulierungsziel des Wettbewerbs in Einklang gebracht werden. Da Ziel jeder Regulierungserleichterung ist, dem Unternehmen im konkreten Fall den Wettbewerbsdruck zu nehmen, um den Ausbau von Netzen zu erleichtern, werden diesem Modell nach jetzigem Recht durch das Regulierungsziel des Wettbewerbs klare Grenzen gesetzt.

c) Die Regelungen im Kodex-E

Der Kodex-E verfolgt als wesentliches Ziel die Förderung des Breitbandausbaus.[70] Erstmals wird auch auf europäischer Ebene ein Regulierungsziel zur Förderung von Datenverbindungen mit sehr hoher Kapazität eingeführt.[71] Auch das Regulierungsziel der Nutzerrechte ist ausdrücklich mit Bezug auf „Festnetz und Mobilfunkdatenverbindungen mit sehr hoher Kapazität“ formuliert.[72] Der Kodex-E behält allerdings ausdrücklich die Gleichrangigkeit der Regulierungsziele bei.

Das Regulierungsverfahren soll angepasst, ansonsten aber unverändert bleiben.[73] Neu sind eine Reihe expliziter Rechtsgrundlagen für die Berücksichtigung des Breitbandausbaus im Rahmen der Regulierung.

(1) Berücksichtigung bei der allgemeinen Regulierung

Die nationalen Regulierungsbehörden haben zukünftig die Aufgabe, Erhebungen zur Breitbandinfrastruktur und deren voraussichtlicher Entwicklung durchzuführen.[74] Die Ergebnisse dieser Untersuchung sollen im Rahmen der Marktregulierung – beispiels-

[66] *BNetzA*, Konsultationsdokument, S. 36; *BREKO*, S. 6.
[67] *BREKO*, S. 7
[68] *Gärditz*, in: Scheurle/Mayen TKG, § 2 Rn. 34.
[69] §§28 Abs. 1 S. 2, 30 Abs. 3 S. 3, 32 Abs. 3 Nr. 3 S. 2 TKG.
[70] ErwGr. 3 Kodex-E.
[71] Art. 3 Abs. 2 lit. a Kodex-E.
[72] Art. 3 Abs. 2 lit. d Kodex-E.
[73] *Klotz/Hofmann*, N&R 2017, 2 (6).
[74] Art. 22 Kodex-E.

weise bei der Marktdefinition – berücksichtigt werden.[75] Auch bei der Auferlegung von Entgeltgenehmigungsverpflichtungen sollen Anreize für den Ausbau neuer und verbesserter Netze geschaffen werden.[76]

(2) Regulierungsfreistellung Art. 74 Kodex-E

Unternehmen, die neue Bestandteile von Netzwerken mit sehr hoher Kapazität errichten, können von Regulierung freigestellt werden, wenn bestimmte Voraussetzungen erfüllt sind (Art. 74 Abs. 2 UAbs. 2 Kodex-E).

Zu diesen Voraussetzungen gehören die Verpflichtung, Open Access zu den Netzbestandteilen zu gewähren[77] und das Angebot der Ko-Investition an Betreiber elektronischer Kommunikationsnetzwerke.[78]

Art. 74 Kodex-E war im Gesetzgebungsverfahren eine der umstrittensten Normen.[79] Kritisiert wurde insbesondere der Ansatz, dass Netzausbau eher durch Zurückhaltung bei der Auferlegung regulatorischer Verpflichtungen gefördert werden könne.[80] Das Parlament lehnte den Vorschlag der Kommission ab, dass bei Vorliegen der Voraussetzungen des Art. 74 KommE-Kodex zwingend die Regulierungsfreistellung eintrete.[81] Auch in der Literatur traf dieser Vorschlag im Hinblick auf den Wettbewerb, der durch die Regulierung eigentlich gesichert werden soll, auf Kritik.[82]

Die Norm hat in den Trilogverhandlungen eine weitgehende Überarbeitung erfahren. Bereits der Anwendungsbereich wurde erheblich eingeschränkt: Nach dem Kommissionsentwurf sollte die Möglichkeit der Regulierungsfreistellung noch für alle neuen Netzbestandteile gelten, die zum Aufbau von Netzen mit sehr hoher Kapazität beitragen.[83] Die finale Fassung sieht nur noch die Anwendung auf FttH/B-Glasfaserinfrastruktur vor.[84] Die Vorgabe, dass die freigestellte Infrastruktur gegenüber Angeboten der Ko-Investition offen sein müsse, wurde über deren gesamte Lebensdauer ausgedehnt.[85] Die Zugangsrechte von nicht an der Ko-Investition beteiligten Wettbewerbern wurden erweitert.[86] Schlussendlich wurde den Regulierungsbehörden

[75] Art. 62 Abs. 3 Kodex-E.
[76] Art. 72 Abs. 1 UAbs. 2 Kodex-E.
[77] Art. 74 Abs. 1 UAbs. 2 lit. a Kodex-E.
[78] Art. 74 Abs. 1 UAbs. 2 lit. b Kodex-E.
[79] *Madiega*, S. 7 ff. zum Stand der Diskussion.
[80] *Neumann*, N&R 2016, 262 (264); *Madiega*, S. 5.
[81] *Madiega*, S. 7.
[82] *Neumann*, N&R 2016, 262 (270).
[83] Art. 74 Abs. 1 lit. b KommE-Kodex.
[84] Art. 74 Abs. 1 Kodex-E.
[85] Art. 74 Abs. 1 UAbs. 2 lit. a Kodex-E.
[86] Art. 74 Abs. 1 UAbs. 2 lit. d Kodex-E sieht jetzt ausdrücklich vor, dass Zugangsnachfrager Zugang zu den neuen Netzbestandteilen erhalten sollen.

eine deutlich größere Rolle zugewiesen und ausdrücklich die Möglichkeit eröffnet, von der Regulierungsfreistellung zum Schutz des Wettbewerbs abzusehen.[87]

(3) Wholesale-only Anbieter Art. 77 Kodex-E

Art. 77 Kodex-E sieht für Telekommunikationsanbieter, die sich rein auf das Vorleistungsgeschäft konzentrieren und kein Endkundengeschäft haben, ein vereinfachtes Regulierungsmodell vor.[88] Wenn die Voraussetzungen des Art. 77 Abs. 1 Kodex-E vorliegen, kann die Regulierungsbehörde lediglich Zugangs- und Nichtdiskriminierungsverpflichtungen auferlegen.[89] Hintergrund der Regelung ist, dass derartige Unternehmen, selbst dann, wenn sie über beträchtliche Marktmacht verfügen, keinen Anreiz haben, zwischen einzelnen Zugangsnachfragern zu diskriminieren, um die eigene Stellung auf den Endnutzermärkten zu verbessern.[90]

Auch im Rahmen von Art. 77 Kodex-E verbleibt der Regulierungsbehörde allerdings die Möglichkeit, zum Schutz des Wettbewerbs weitere Verpflichtungen aufzuerlegen.[91]

(4) Fazit

Der Kodex-E erleichtert die Berücksichtigung des Breitbandausbaus im Rahmen der Regulierung erheblich. Neben allgemeinen Vorgaben erweitert er den „Instrumentenkasten“ der Regulierungsbehörde um einige Maßnahmen, die direkt Anreize für den Infrastrukturausbau setzen sollen.

3. Nutzung von Infrastrukturen

a) Allgemeines

Ein wesentlicher Kostenfaktor beim Ausbau von Telekommunikationsnetzen ist der Aufbau von baulichen Anlagen, in denen Kommunikationsnetze ausgebaut werden können (sog. passive Infrastrukturen).[92] Der Ausbau von Netzwerken kann daher wesentlich vergünstigt werden, wenn bereits bestehende Strukturen genutzt werden können.

[87] Art. 74 Abs. 3 Kodex-E.
[88] *Neumann*, N&R 2016, 262 (270).
[89] Art. 77 Abs. 2 Kodex-E.
[90] *Neumann*, N&R 2016, 262 (270).
[91] Art. 77 Abs. 4 Kodex-E.
[92] ErwGr. 172 Kodex-E.

b) Die Regelungen des DigiNetzG

(1) Nutzung passiver Infrastrukturen

Die §§ 77 a ff. TKG[93] enthalten Regelungen für die Mitnutzung öffentlicher Versorgungsnetze zur Verlegung von Kommunikationsnetzen. So sollen Synergien nutzbar gemacht werden[94] und der eigenwirtschaftliche Ausbau von Netzen ermöglicht werden. Der Begriff der „öffentlichen Versorgungsnetze" umfasst auch die Telekommunikationsnetze selbst[95], sodass „symmetrische" Mitnutzungsansprüche bestehen.

Es bestehen Ansprüche auf die Erteilung von Informationen (§ 77 b Abs. 2 TKG) und Vor-Ort-Untersuchungen passiver Infrastrukturen (§ 77 c Abs. 2 TKG) sowie die Mitnutzung öffentlicher Versorgungsnetze (§ 77 d Abs. 2 TKG). Diese Ansprüche können bei Vorliegen eines der Gründe des § 77 g Abs. 2 TKG versagt werden.

Daneben besteht ein Anspruch auf Koordinierung von Bauarbeiten und Mitverlegung gemäß § 77 i Abs. 3 TKG. Betreiber von öffentlichen Telekommunikationsnetzen können von Betreibern öffentlicher Versorgungsnetze, die aus öffentlichen Mitteln finanzierte Bauarbeiten ausführen, verlangen, dass diese Bauarbeiten zur Mitverlegung von Telekommunikationsinfrastruktur koordinieren. Der Anspruch ist nur durch das Tatbestandsmerkmal der Zumutbarkeit begrenzt.

(2) Die Überbauproblematik

Die Regelungen sind von der Praxis akzeptiert[96] und daher ein geeignetes Mittel zur Förderung des Breitbandausbaus.

Gleichzeitig wurde durch die Regelungen jedoch ein erhebliches Investitionsrisiko geschaffen: Bei jeder Investitionsentscheidung über ein Glasfaserprojekt muss berücksichtigt werden, dass ein Wettbewerber direkt im Anschluss parallele Netzinfrastrukturen errichten kann (sog. Überbau), indem er sich auf die Ansprüche der §§ 77 b ff. TKG stützt und sich so Investitionskosten spart, die der erste Investor tragen musste.

Die Ansprüche gemäß §§ 77 b bis d TKG können zwar versagt werden, wenn bestehende Glasfasernetze, die einen diskriminierungsfreien, offenen Netzzugang zur Verfügung stellen, überbaut werden.[97] Dies wird von der BNetzA jedoch äußerst eng und restriktiv ausgelegt.[98] Ein Versagensgrund besteht nur, wenn eine bestehende FttH/B-

[93] In der Fassung durch das Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze (DigiNetzG) vom 4. November 2016, BGBl. I S. 2473.
[94] *Biendl*, N&R 2018, 19 (19).
[95] § 3 Nr. 16 lit. a lit. aa TKG.
[96] Jedenfalls, wenn man die Anzahl der anhängig gemachten Streitentscheidungsverfahren bei der BNetzA zugrunde legt; vgl. *Biendl*, N&R 2018, 19 (20).
[97] § 77 g Abs. 2 Nr. 7 TKG.
[98] Vgl. die Analyse der Entscheidungen der zuständigen Beschlusskammer 11 von *Biendl*, N&R 2018, 19 (21).

Infrastruktur dupliziert wird. Nicht ausreichend ist der Überbau einer im Aufbau befindlichen Glasfaserverbindung, oder einer, die nur ein einzelnes Objekt anbindet.[99]

Im Rahmen des Anspruchs auf Baustellenkoordinierung und Mitverlegung (§ 77 i Abs. 3 TKG) wird die Problematik des Überbaus überhaupt nicht berücksichtigt. Die BNetzA verweist insoweit lediglich auf die Entscheidung über den Kostenausgleich gemäß § 77 n TKG.[100] Dies ist insoweit kritisch, als dabei nur „Kosten der Koordinierung von Bauarbeiten" vom Anspruchsgegner verlangt werden können.[101] Zweifelhaft ist, ob darunter auch ein Ausgleich für den Vorteil des Wettbewerbers fällt, der die Baustelleninvestition des Erstinvestors mit nutzt.[102]

Dieses Problem wurde inzwischen vom Gesetzgeber aufgegriffen. Geplant ist, den Anspruch gem. § 77 i Abs. 3 TKG ebenfalls zu versagen, wenn ein Glasfasernetz überbaut wird, dass einen diskriminierungsfreien, offenen Netzzugang zur Verfügung stellt.[103] Dadurch könnte das Problem zumindest entschärft werden.

c) Nutzungsrechte im Kodex-E

Auch der Kodex-E enthält Vorgaben zur Nutzung physischer Infrastrukturen.

Gemäß Art. 70 Kodex-E kann die Regulierungsbehörde marktmächtigen Unternehmen die Verpflichtung auferlegen, Zugang zu wesentlichen Teilen physischer Infrastruktur zu gewähren, um die Entwicklung eines nachhaltig wettbewerbsorientierten Marktes auf der Endkundenebene zu sichern. Dies soll sogar vorrangig vor der Zugangsverpflichtung zu Netzbestandteilen selbst (Art. 71 Kodex-E) gelten[104], denn Art. 71 Abs. 2 UAbs. 2 Kodex-E sieht insoweit ausdrücklich vor, dass die Regulierungsbehörde prüft, ob die alleinige Anwendung von Art. 70 zur Erreichung der Regulierungsziele ausreicht.[105] Eine derartige Rangfolge enthielt der einheitliche Rechtsrahmen nicht. Die Bedeutung der physischen Infrastruktur wird unter Geltung des Kodex-E daher erhöht.[106]

Im Übrigen erleichtert Art. 44 Abs. 1 Kodex-E auch die Anordnung der sogenannten Kolokation von Netzbestandteilen, die auf öffentlichen oder privaten Grundstücken errichtet sind. Die Regulierungsbehörde kann die gemeinsame Unterbringung und ge-

[99] *BNetzA*, Beschl. v. 6.10.2017 Bk11-17/004 Rn. 96. 103.
[100] *BNetzA*, Beschl. v. 18.7.2017 Bk11-17/002 Rn. 92 f.
[101] § 77 i Abs. 4 S. 2 TKG.
[102] *Biendl*, N&R 2018, 19 (23).
[103] Entwurf eines fünften Gesetzes zur Änderung des Telekommunikationsgesetzes, abrufbar unter https://cdn.netzpolitik.org/wp-upload/2018/08/DigiNetzG-TKG-Novelle.pdf
[104] Sog. primäre Zugangsverpflichtung vgl. *Scherer/Heinickel*, MMR 2017, 71 (75).
[105] Der Kommissionsentwurf ging ursprünglich sogar noch weiter: Gemäß Art. 71 Abs. 1 KommE-Kodex sollte die Auferlegung von Zugangsverpflichtungen zu Netzinfrastruktur nur möglich sein, wenn Maßnahmen nach Art. 70 Kodex-E für die Erreichung der Regulierungsziele nicht ausreichen sollten.
[106] *Neumann*, N&R 2016, 262 (267) bezeichnet dies als wichtigste Änderung im Kodex-E.

meinsame Nutzung der installierten Netzbestandteile und zugehörigen Einrichtungen vorschreiben. Die Vorgängerregel Art. 12 Abs. 2 RRL setzt dafür noch voraus, dass eine Verdoppelung der Infrastrukturen "wirtschaftlich ineffizient oder praktisch unmöglich" wäre. Diese Voraussetzung ist weggefallen.[107]

IV. Individueller Anspruch auf schnelles Internet

Die Bundesregierung plant, spätestens zum Jahr 2025 einen rechtlich abgesicherten Anspruch auf breitbandigen Internetzugang einzuführen.[108] Die genaue Ausgestaltung des Anspruchs ist noch unklar[109], allerdings legt die Formulierung das Instrument des Universaldienstes als Mittel zur Förderung des Breitbandausbaus nahe, denn Rechtsgrundlagen, die Netzbetreiber zu einem Netzausbau zu verpflichten, bestehen ansonsten nicht.[110]

Zweck des Universaldienstes ist, Telekommunikationsunternehmen zu verpflichten, allen Nutzern bestimmte Dienste erschwinglich zur Verfügung zu stellen. Der Universaldienstmechanismus steht für den Fall bereit, dass eine freiwillige Erfüllung dieses Versorgungsauftrages nicht erfolgt. [111]

Unter den Universaldienst fällt gemäß § 78 Abs. 2 Nr. 1 TKG auch „der Anschluss an ein öffentliches Telekommunikationsnetz an einem festen Standort, der […] die Datenkommunikation mit Übertragungsraten ermöglicht, die für einen funktionalen Internetzugang ausreichen".

Der Begriff des funktionalen Internetzugangs wird dahingehend konkretisiert, dass „dabei die von der Mehrzahl der Teilnehmer vorherrschend verwendeten Technologien [zu berücksichtigen sind]".[112] Eine bestimmte Bandbreite ist auf europäischer Ebene nicht festgelegt.[113] Relevant für die Ermittlung der Mindestbandbreite ist die Mehrheit der tatsächlich vorhandenen Internetanschlüsse im Markt. § 78 Abs. 2 Nr.2 TKG verlangt daher lediglich den Anschluss an ein Breitbandnetz mit einer grundlegenden Übertragungsrate, die im Markt weit verbreitet ist.[114]

Dem Gesetzgeber ist auch die Einführung eines Breitbanduniversaldienstes mit Bandbreiten im Gigabitbereich verwehrt. Dies ergibt sich zum einen aus den verfassungsrechtlichen Vorgaben des Art. 87 Abs. 2 GG. Dieser erfordert nämlich eine Um-

[107] *Scherer/Heinickel*, MMR 2017, 71 (73).
[108] CDU/CSU/SPD Koalitionsvertrag „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land." v. 12.03.2018, S. 38.
[109] *Neumann/Sickmann*, N&R Beil. 1/2018, 1 (2 f.).
[110] *VG Köln*, MMR 2007, 198 (199).
[111] *Kühling/Schall/Biendl*, Rn. 610.
[112] Art. 4 Abs. 2 Hs. 2 URL.
[113] ErwGr. 8 S. 6 URL.
[114] Vorgeschlagen werden 2 Mbit/s, s. *Windthorst*, in: Scheurle/Mayen TKG, § 78 Rn. 26a.

setzung des Gewährleistungsauftrages (Abs. 1) durch Private nach den Grundsätzen der Wirtschaftlichkeit und einer am Gewinnprinzip orientierten Tätigkeit.[115] Ausweislich der Gesetzesbegründung ist der staatliche Handlungsauftrag nicht auf den Ausbau einer optimalen Infrastruktur ausgerichtet, sondern zielt nur auf die Gewährleistung einer flächendeckenden Grundversorgung ab.[116] Dazu zählt ein Breitbandinternetzugang im Gigabitbereich jedoch nicht.

Ein Handeln jenseits der Legitimation des Art. 87 f GG ist bei einem Eingriff in Grundrechte der Telekommunikationsunternehmen, wie ihn eine Universaldienstverpflichtung darstellt, nicht gerechtfertigt. Ein Universaldienst, der Bandbreiten weit über der Grundversorgung vorschreibt, wäre daher verfassungswidrig.

Auch europarechtliche Vorgaben stehen einer derartigen Universaldienstverpflichtung entgegen. Die in Art. 32 URL enthaltenen Regelungen für die Fortentwicklung der Universaldienste auf nationaler Ebene sind abschließend und gelten nur für „zusätzliche […] weitere Dienste“ und nicht für eine qualitative Ausweitung der bereits in der Richtlinie geregelten Dienste.[117]

Die Neuregelung des Universaldienstes in Art. 79 ff. Kodex-E erlaubt ebenfalls keine Ausweitung: Die Bandbreite des Universaldienstes soll sich weiterhin an den der Mehrheit der Nutzer zur Verfügung stehenden Anschlüssen orientieren und darüber hinaus an den Erfordernissen der von der Mehrheit der Endnutzer genutzten Dienste, die in Annex V des Kodex-E aufgeführt sind. Den Mitgliedsstaaten steht darüber hinaus kein Spielraum zu.[118]

Der Universaldienst ist auf sein sozialpolitisches Ziel beschränkt: Sobald Internetanbindungen einer bestimmten Bandbreite der Mehrheit der Nutzer zur Verfügung stehen, kann als Universaldienstverpflichtung angeordnet werden, dass jeder Nutzer das Recht auf eine solche Anbindung hat. Telekommunikationsanbieter können jedoch nicht verpflichtet werden, Bandbreiten oberhalb dessen, was im Markt vorhanden ist, bereit zu stellen. Zur Förderung des Breitbandausbaus ist der Universaldienst allenfalls ergänzend geeignet.

V. Fazit

Die vorliegende Betrachtung zeigt, dass dem Gesetzgeber ein gut bestückter Instrumentenkasten zur legislativen Förderung von privaten Breitbandprojekten zur Verfügung steht. Neben einer direkten finanziellen Förderung steht insbesondere die Berücksichtigung im Rahmen der Marktregulierung im Fokus, deren Möglichkeiten durch

[115] *BVerfG*, NVwZ 2004, 329 (331).
[116] Begr. RegE BT-Drucks. 12/7269 S. 5.
[117] ErwGr. 46 S. 1 URL; *Fetzer*, MMR 2011, 707 (711).
[118] Art. 82 Abs. 1 S. 1 Kodex-E.

den Kodex-E noch deutlich erweitert werden. Auch die Regelungen des DigiNetzG zur Mitnutzung von Infrastrukturen erweisen sich als wirksames Mittel. Insoweit ist allerdings die Entwicklung der Überbau-Problematik zu beobachten.

Durch eine Bevorzugung im weiteren Sinne wird der Betreiber der Glasfaserinfrastruktur meist verpflichtet, umfassende Zugangsrechte an Wettbewerber zu gewähren (Open Access). Dies ist sowohl Voraussetzung für eine unmittelbare finanzielle Förderung (Art. 52 Abs. 5 AGVO), für die Regulierungsfreistellung nach dem Kodex-E (Art. 74 Abs. 1 UAbs. 2 lit. a Kodex-E) als auch für den Schutz vor Überbau bei der Nutzung passiver Infrastrukturen (§ 77 g Abs. 2 Nr. 7 TKG).

Eine Breitband-Universaldienstverpflichtung kann dagegen allenfalls ergänzend zu den genannten Instrumenten genutzt werden.

Literaturverzeichnis

Biendl, Michael, Vorfahrt für den Netzausbau, N&R 2018, 19-26.

Bundesnetzagentur, Konsultationsdokument Fragen der Entgeltregulierung bei FttH/B-basierten Vorleistungsprodukten mit Blick auf den Ausbau hochleistungsfähiger Glasfaserinfrastrukturen, abrufbar unter:
https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktregulierung/massstaebe_methoden/ftth_fttb_Ausbau/ftth_fttb_Ausbau-node.html

Geppert/Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl., München 2013.

BREKO, Regulierungskonzept zur Beschleunigung des Glasfaserausbaus (FTTB/FTTH) in Deutschland, abrufbar unter:
https://brekoverband.de/breko-strategiepapier-glasfaser-zukunft

Dialog Consult/VATM, 19. TK-Marktanalyse Deutschland 2017, abrufbar unter:
http://www.vatm.de/vatm-marktstudien.html

Europäischer Rechnungshof, Sonderbericht, Der Breitbandausbau in den EU-Mitgliedstaaten, abrufbar unter:
https://www.eca.europa.eu/de/Pages/DocItem.aspx?did=45796

Fetzer, Thomas, Breitbandinternet als Universaldienst? MMR 2011, 707-711.

Herrmann, Danielle/ Heilmann, Stefan/ Werkmeister, Christoph, Das Telekommunikationsrecht im Jahr 2015, N&R 2016, 130-140.

Herrmann, Danielle/ Heilmann, Stefan, Das Telekommunikationsrecht im Jahr 2016, N&R 2017, 154-165.

Immenga/Mestmäcker (Hrsg.), Wettbewerbsrecht, Band 3. Beihilfenrecht/ Sonderbereiche Kommentar zum Deutschen und Europäischen Kartellrecht, 5. Aufl., München 2016.

Klotz, Robert/ Hofmann, Michael, Entwicklung des Unionsrecht in den Netzwirtschaften im Jahr 2016.

Knapp, Sven/ Weißenfels, Andrea: „Vectoring" – Technischer Segen oder regulatorischer Fluch? N&R 2014, 130-138.

Kopf, Wolfgang/Vidal, Miguel, Perspektiven der TK-Regulierung, MMR 2018, 22-25.

Kühling, Jürgen/ Schall*, Tobias/ Biendl, Michael,* Telekommunikationsrecht, 2. Aufl., Heidelberg 2014.

Madiega, Tambiama, EU electronic communications code and co-investment, EPRS Briefing February 2018, EPRS BRI(2018) 614693.

Maunz/Dürig (Begr.), Grundgesetz Kommentar, 82. EL, München 2018.

Neumann, Andreas, Der Kommissionsvorschlag für einen europäischen Kodex für die elektronische Kommunikation, N&R 2016, 262-272.

Neumann, Andreas/ Sickmann, Jörn, Schaffung eines rechtlich abgesicherten Anspruchs auf einen Zugang zum schnellen Internet in: N&R Beilage 1/2018, 1-12.

Scherer, Joachim/Heinickel, Caroline, Ein Kodex für den digitalen Binnenmarkt, MMR 2017, 71-77.

Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz, 3. Aufl., München 2018.

von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 3: Art. 106 bis 173 AEUV, 7. Aufl., Baden-Baden 2015.

Walden, Ian (Hrsg.): Telecommunications Law and Regulation, Oxford 2012.

Social Bots im Wahlkampf

Das UrhG als Handhabe gegen „Meinungsroboter“?

Oliver Wolf, LL.M.

Kanzlei Plutte, Mainz
oliver.wolf@posteo.de

Abstract

Obgleich Social Bots keine neue Erscheinung sind, drangen sie erst durch die US-amerikanische Präsidentschaftswahl 2016 in das Bewusstsein einer breiteren Öffentlichkeit. In Deutschland wurde das Thema zunächst nur zögerlich aufgegriffen. Spätestens jedoch seitdem sich eine Vermengung mit der Problematik der sog. „Fake News“ abzeichnet, ist das Thema auch in Deutschland auf die Tagesordnung gerückt. Blieb es anfangs bei Verpflichtungserklärungen der Parteien, keine Social Bots einzusetzen,[1] wird inzwischen dafür plädiert, die Materie einer gesetzlichen Regelung zuzuführen.[2] Das zeigt, dass das Thema inzwischen politisch durchaus ernst genommen wird.

Die Untersuchung erläutert, was Social Bots sind und wie sie funktionieren (I.). Dabei wird auf das Gefährdungspotenzial (II.), aber auch auf nützliche Anwendungsfelder (III.) eingegangen. Sie zeigt, dass Bots bei abstrakter Betrachtung zwar nicht sanktionierbar sind, dass der Einsatz bestimmter Techniken allerdings das Datenbank- bzw. Datenbankwerkrecht verletzen kann (IV.).

I. Begriffsbestimmung und Funktionsweise

1. Bots

Bots (Kurzform für engl. *robot*) sind im weitesten Sinne Computerprogramme, die eingesetzt werden, um zeitaufwendige Aufgaben automatisiert vorzunehmen.[3] Ein alltägliches Beispiel für den Einsatz solcher Bots sind Internetsuchmaschinen: Der Index, in dem alle Webseiten eingetragen sind, die der Suchmaschine bekannt sind, wird nicht etwa von Menschenhand angelegt. Vielmehr sind autonom handelnde Bots „unterwegs“, die sich durch die über Verlinkungen aufgefundenen Seiten arbeiten und die gefundenen Informationen zusammentragen. Der typische Verwendungszweck von

[1] *Bender/Oppong*, FAZ-Online v. 07.02.2017.
[2] *Rosenbach/Traufetter*, Spiegel-Online v. 21.01.2017.
[3] *Micklitz/Schirmbacher*, in: Spindler/Schuster, 14. Teil, § 4 UWG Rn. 338.

Bots liegt also dort, wo sehr große Mengen von Daten in kurzer Zeit nach einem bestimmten Muster bearbeitet werden sollen.

2. Social Bots

Die Bot-Technik kann aber auch genutzt werden, um massenhaft menschliches Verhalten in sozialen Netzwerken nachzuahmen. Von einem Social Bot ist dann die Rede, wenn das Programm auf die Interaktion mit Menschen ausgerichtet ist.[4] Social Bots sind so programmiert, dass sie tausende Nutzeraccounts von sozialen Netzwerken wie Facebook oder Twitter[5] steuern und mit anderen Nutzern interagieren können. Das bedeutet, sie können vorgefertigte Nachrichten posten, auf bestimmte Schlagworte mit vorgefertigten Textbausteinen reagieren oder Beiträge anderer Nutzer „retweeten", also weiterverbreiten.

Darunter gibt es simplere Varianten, die permanent und massenhaft Nachrichten versenden. Diese sind auch für Laien leicht zu erkennen, da eine auch nachts unterbrechungsfreie und in regelmäßigen Zeitabständen stattfindende Aktivität nicht dem Verhalten eines menschlichen Nutzers entspricht. Komplexere Social Bots sind demgegenüber auch für Experten nur schwer auszumachen, da bspw. ihr Aktionsverhalten an den tatsächlichen Tagesablauf eines Menschen angepasst ist und sie sogar in der Lage sind, „Unterhaltungen" zu führen. In beiden Fällen lässt sich der Betrieb eines Social Bots mit einem relativ geringen technischen und finanziellen Aufwand bewerkstelligen. 1.000 gefälschte Nutzeraccounts werden ab 45 US-Dollar angeboten.[6] Die Software – also der eigentliche Bot – zur Steuerung von bis zu 10.000 Accounts kostet ca. 500 US-Dollar. [7]

3. Steuerung über Programmierschnittstellen

Funktionieren kann die massenhafte Steuerung verschiedener Accounts über Programmierschnittstellen (APIs).[8] Dabei handelt es sich, vereinfacht gesagt, um Zugriffsstellen, über die der Datenspeicher des jeweiligen Dienstes – also auch die zu dem jeweiligen Nutzeraccount gehörigen Daten – abgerufen werden kann. Dadurch ist es möglich, den Dienst auf verschiedenen Wegen zugänglich zu machen. So besteht Flexibilität, kompatible Programme für verschiedene Plattformen (bspw. Webseite, Handy-App oder auf dem PC installiertes Programm) zu erstellen, die auf denselben Datenbestand zurückgreifen können. Die Betreiber sozialer Netzwerke haben ein Interesse daran, diesen Zugang frei zur Verfügung zu stellen. Denn wenn bspw. Fitnesstracker-Apps das letzte Training automatisch posten oder neue Beiträge eines Bloggers automatisch

[4] *Ferrara/Varol/Davis/Menczer/Flammini*, Communications of the ACM 2016, 96.
[5] Soweit nicht anders dargelegt, bezieht sich die Darstellung im Folgenden auf Twitter.
[6] *Hegelich*, S. 2.
[7] *Hegelich*, S. 3.
[8] Dazu ausführlich *Hawker*, S. 1 ff.

verlinkt werden, dient das der Verbreitung des eigenen Dienstes und kann damit zumindest potenziell zu höheren Werbeeinnahmen führen.

II. Der „Bot-Effekt“ und der Vergleich zu konventionellen Medien

Gerade mit Blick auf politische Wahlkämpfe zeigt sich, dass Social Bots mehr sind als bloße technische Spielerei oder schlichtes Kommunikationsmittel. Vielmehr können sie erhebliche Auswirkungen auf die politische Debatte haben, die *Hegelich* unter dem Begriff „Bot-Effekt“ zusammenfasst.[9] Werden Social Bots so programmiert, dass Meldungen in tausendfacher Ausführung verbreitet werden oder dass automatisch auf gewisse Schlagworte reagiert wird, kann bei den übrigen Nutzern der Eindruck entstehen, dass bestimmte Meinungen von besonders vielen Menschen vertreten werden bzw. als teilens- und diskutierenswert erachtet werden (sog. „trending topics“). Das ist zwar an sich keine neue Erscheinung. Schon vor dem Zeitalter sozialer Netzwerke gab es bspw. Zeitungen, die einflussreicher bzw. auflagenstärker waren oder Fernsehsendungen mit höheren Einschaltquoten, sodass die dort vertretenen Ansichten einen höheren Verbreitungsgrad hatten. Man könnte somit zu dem Ergebnis kommen, dass die Debattenkultur auch im Wahlkampf keiner Gefährdung ausgesetzt ist, mit der sie nicht schon seit Jahrzehnten umzugehen gelernt hat. Indes bestehen mehrere wesentliche Unterschiede hinsichtlich des Beeinflussungspotentials von Social Bots zu den klassischen Medien.[10]

1. Filterblase

Bei den Inhalten, die den Nutzern angezeigt werden, handelt es sich nicht um rundfunkartig-linear verbreitete Meldungen. Vielmehr sind diese individuell auf den jeweiligen Nutzer zugeschnitten und hängen von verschiedenen Faktoren ab, insbesondere auch davon, was gerade die „trending topics“ sind.

Hierauf können Social Bots einen verzerrenden Einfluss haben, sodass ein Vergleich mit konventionellen Medien nicht greift. Bliebe man beim Beispiel der Printmedien, wäre die Beeinflussung eher damit zu vergleichen, dass am Zeitungskiosk bestimmte Blätter nur schwer sichtbar sind, weil der Kiosk vom politischen Gegner mit Zeitungen eigener Couleur überfrachtet wurde: Gegenläufige Auffassungen sind dann zwar noch auffindbar. Der Leser wird aber nicht darauf aufmerksam gemacht und muss gezielt danach suchen (sog. „Filterblase“[11]).

[9] *Hegelich*, S. 4 ff.
[10] *Hegelich*, S. 4.
[11] S. dazu *Pariser*, S. 10 ff.; krit.: *Stark*, MMR 2017, 721 (722).

2. Verzerrung des Meinungsbildes

Durch künstlich aufgeblähte Meinungen droht zum einen die Entstehung einer „Schweigespirale“.[12] So kann es passieren, dass die Anhänger der Mehrheitsmeinung davon absehen, diese zu äußern, weil sie den Eindruck haben, lediglich für die Minderheit zu stehen. Zum anderen kann ein „virtueller Herdentrieb“ entstehen, wenn bisher schweigende Anhänger einer Mindermeinung sich plötzlich in „bester Gesellschaft“ wähnen und zu der Überzeugung kommen, ihre eigene Ansicht entspräche dem, was „die Leute auf der Straße“ denken. Der hier zu den konventionellen Medien bestehende Unterschied liegt in den minimalen Ressourcen, die erforderlich sind, um erhebliche Verzerrungen des Meinungsbildes herbeizuführen.

3. Einfluss der „Trends“ auf politische Strategien

Schließlich besteht ein wesentliches Problem in dem vermeintlich zuverlässigen Abbild, das eine Analyse der kommunizierten Inhalte über die in der Gesamtbevölkerung vertretenen Ansichten ergibt. Es lässt sich leicht ermitteln wieviel Prozent aller „Tweets“ sich mit einem bestimmten Thema auseinandersetzen. Ab einer bestimmten Größe wird das Thema im Wahlkampf schwerlich ignoriert werden können. Wenn diese Zahlen aber, wie oben beschrieben, künstlich aufgebläht und tatsächlich nicht repräsentativ sind, droht die Bevorzugung von Partikularinteressen oder eine verzerrte Wahrnehmung über die Bedürfnisse, Ängste und Prioritäten der Bevölkerung.[13]

III. Anwendungsszenarien außerhalb des Meinungskampfes

Es darf gleichzeitig nicht übersehen werden, dass dieselbe Technik auch im Bereich der Kommunikation von Unternehmen zu Kunden eingesetzt werden kann. Insoweit ist festzuhalten, dass der häufig – auch hier – verwendete Begriff der „Meinungsroboter“ unpräzise ist. Die Einsatzszenarien sind vielfältig: Beispielsweise werden „Robo-Advisors“ im Bereich der Finanzanlagenberatung eingesetzt. So können Kunden, für die eine klassische Anlageberatung nicht erschwinglich wäre, aufgrund der günstigen Kostenstrukturen Zugang zu derartigen Dienstleistungen erhalten.[14] Die Bundesagentur für Arbeit setzt schon jetzt Chatbots ein, um Jugendliche an das Thema Berufswahl heranzuführen und bedient auf diesem Weg mehrere zehntausend Anfragen täglich.[15]

[12] *Kreutzer*, FAZ-Online v. 26.08.2014.
[13] *Hegelich*, S. 3.
[14] *Baumanns*, BKR 2016, 366 (366 ff.).
[15] *Bös/Marx*, FAZ-Online v. 30.01.2017.

Im gesamten Bereich der Kundenkommunikation liegen nützliche Anwendungsmöglichkeiten für Social Bots auf der Hand.[16]

IV. Juristische Einordnung von Bots

Im Folgenden wird gezeigt, dass Social Bots bei abstrakter Betrachtung keine Verbotsgesetze verletzen. Angesichts der positiven Anwendungsszenarien wird erörtert, dass eine abstrakte Zweckbestimmung, die zur Schaffung eines Verbotsgesetzes erforderlich wäre, nicht möglich ist. Schließlich wird dargelegt, dass es Fälle gibt, in denen Social Bots Normen des UrhG verletzen und daher rechtswidrig sind.

1. Keine Rechtswidrigkeit bei abstrakter Betrachtung

Das Gesetz kennt zwar Fälle, in denen bereits die Erstellung von Computerprogrammen Straftatbestände erfüllt. Diese sind jedoch nicht einschlägig.

a) Kein Abstellen auf Inhalte

Bei der juristischen Einordnung der Social Bots ist zunächst hervorzuheben, dass nicht auf die Inhalte abgestellt werden kann, die über die Social Bots verbreitet werden.[17] Inhalte, die als Schmähkritik oder unwahre Tatsachenbehauptung nicht von der Meinungsfreiheit gedeckt sind, sind unabhängig vom Kommunikationskanal rechtswidrig, was hier keiner weiteren Vertiefung bedarf.[18] Ebenso verhält es sich mit Äußerungen strafbaren Inhalts. Entsprechend ist auch kein Raum für solche Verbotsnormen, deren Tatbestand zwar durch die Programmierung von Software erfüllt werden kann, deren Voraussetzung aber das Vorhandensein bestimmter Inhalte ist. So ordnen etwa §§ 86a Abs.1 Nr.2, 130 Abs.2 Nr.3, 131 Abs.1 Nr.3 StGB Verbote der Herstellung von Gegenständen an, die Kennzeichen verfassungswidriger Organisationen enthalten[19], bzw. stellen Schriften volksverhetzenden oder gewaltverherrlichenden Inhalts unter Strafe. Wenngleich ein Social Bot zur Übermittlung derartiger Inhalte genutzt werden kann, liegt darin kein zwingender Programmbestandteil. Vielmehr kann der Bot mit beliebigen und wechselnden Inhalten „bestückt“ werden. Ein Verbot der abstrakt betrachteten Software lässt sich hieraus entsprechend nicht ableiten.

b) Zweck der Software

Daneben bestehen Verbotsnormen, die nicht auf den Inhalt, sondern auf den Zweck des Programmes abstellen. § 202c Abs.1 Nr.2 StGB verbietet die Herstellung (und an-

[16] Insoweit unzutreffend *Dankert/Dreyer*, K&R 2017, 73 (75), die den Standpunkt vertreten, Social Bots entfalteten ihr Potenzial dort, wo sie über die technisch vermittelte Steuerung ihrer Aktivitäten täuschen.
[17] Dazu und zur verfassungsrechtlichen Einordnung *Dankert/Dreyer*, K&R 2017, 73 (73).
[18] S. dazu etwa *BVerfG*, Beschl. v. 25.10.2012 - 1 BvR 901/11, NJW 2013, 217 (218); *Rixecker*, in: MüKoBGB, Anh. § 12 Rn. 170 ff., *Libertus*, MMR 2018, 20 (25).
[19] Differenzierend *Liesching*, MMR 2010, 309 (312 f.).

dere Handlungsweisen) von Computerprogrammen, die dem Zweck des Ausspähens oder Abfangens von Daten dienen. Diese Norm gilt gem. § 303a Abs. 3 StGB entsprechend für Computerprogramme, die dem Zweck der Datenveränderung dienen. § 108b Abs.2 iVm § 95a Abs. 3 Nr.3 UrhG verbietet die Herstellung von Vorrichtungen zur Umgehung technischer Maßnahmen zum Kopierschutz, wovon insbesondere auch Software erfasst ist.[20] Diese Normen sind evident nicht einschlägig. Wie dargelegt, werden die Daten, die die Social Bots abrufen, über die Programmierschnittstelle zur Verfügung gestellt, wobei auch keine technischen Maßnahmen umgangen werden. Auch hieraus lässt sich somit kein Verbot ableiten.[21]

2. Keine brauchbare Abgrenzung zwischen „guten" und „schlechten" Bots

Mit Blick auf mögliche zukünftige Gesetzgebung muss festgehalten werden, dass eine abstrakte Zweckbestimmung, die zur Normierung eines Verbotsgesetzes erforderlich wäre, enorme Schwierigkeiten aufwirft. Ein Zweck, der alle Social Bots erfasst, die den „Bot Effekt" hervorrufen und dessen Einstufung als unzulässig nicht mit etablierten Grundsätzen kollidiert, ist nicht ersichtlich. Die teilweise vertretene[22] Differenzierung zwischen „wohlwollenden" und „bösartigen" Bots führt daher nicht weiter.

c) Identitätstäuschung

Eine Identitätstäuschung ist Social Bots nicht zwingend immanent. Kommen Social Bots etwa im Servicebereich zum Einsatz, ist dem Gegenüber zumindest klar, in wessen Lager der Bot zu verorten ist. Das gilt auch dann, wenn die Frage der Täuschung auf die Eigenschaft "Mensch" bezogen wird.[23]

Daneben ist aber auch zu beachten, dass keine gesetzliche Klarnamenpflicht besteht. Vielmehr sieht § 13 VI TMG grundsätzlich eine Verpflichtung von Diensteanbietern vor, die Nutzung ihrer Dienste anonym oder unter einem Pseudonym zu ermöglichen. Zudem ist gerade auch die anonyme Meinungsäußerung von Art. 5 GG geschützt.[24]

d) Autonomes Tätigen von Äußerungen

Wie anfangs dargelegt, sind nicht alle Social Bots zu Kommunikation mit dem Gegenüber in der Lage. Allerdings eint sie unabhängig vom konkreten Einsatzgebiet das Merkmal, dass sie autonom Äußerungen tätigen.

---

[20] *LG Frankfurt a.M.*, Urt. v. 31.05.2006 - Az. 2-06 O 288/06, MMR 2006, 766; *LG Köln*, Urt. v. 6.09.2006 - Az. 28 O 178/06, MMR 2006, 412 (415); *Ohst/Wandtke*, in: Wandtke/Bullinger, PK-UrhR, § 95a UrhG Rn. 71.

[21] A.A.: *Libertus*, S. 23.

[22] So etwa *Volkmann*, MMR 2018, 58 (59 m.w.N.).

[23] So aber *Milker*, ZUM 2017, 216 (218 f.).

[24] *BGH*, Urt. v. 23.06.2009 - VI ZR 196/08, MMR 2009, 608 (612 f.); den grundrechtlichen Schutz automatisierter Meinungsäußerungen zutreffend bejahend *Dankert/Dreyer*, K&R 2017, 73 (75).

Die autonome Tätigung von Äußerungen wird aber als solche von der Rechtsprechung nicht beanstandet. In seiner Autocomplete-Entscheidung[25] befasste sich der BGH mit der Frage, welcher Aussagegehalt einer automatisierten Aussage beizumessen ist. Dabei wurde die generelle Zulässigkeit automatisierter Aussagen offenkundig unterstellt. Angesichts der unter III. beschriebenen Anwendungsmöglichkeiten wäre eine andere Einordnung auch vollkommen verfehlt.

e) „Manipulation und Desinformation“

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag nimmt eine Differenzierung vor. Demnach ist zwischen „unterstützenden Bots“ und „Social Bots“ zu unterscheiden. Um Social Bots handele es sich nur, wenn sie dem Zweck der Manipulation und der Desinformation dienen. [26] Die „unterstützenden Bots“ dürften demnach jene sein, die unter die in III. beschriebenen Anwendungsfelder fallen.

Allerdings ist diese Abgrenzung weder zutreffend noch hilfreich. Das Element der „Desinformation“ würde dazu führen, dass Bots, die ausschließlich Meinungen verbreiten, nicht von der Definition erfasst werden. Eine „Desinformation“ kann denknotwendig nur Materien betreffen, die einem Beweis zugänglich sind. Dem Beweis als wahr oder unwahr zugänglich sind aber nur Tatsachenbehauptungen.[27] „Desinformierende“ Meinungen existieren nach dem Verständnis des Art. 5 Abs. 1 S.1 GG nicht. Vielmehr sind Meinungen unabhängig davon, ob sie rational oder emotional, begründet oder grundlos sind und ob sie von anderen für nützlich oder schädlich, wertvoll oder wertlos gehalten werden.[28] Der unerwünschte „Bot-Effekt“ kann aber auch durch solche Bots erzeugt werden, die reine Meinungsäußerungen verbreiten.

Auch der Begriff der „Manipulation“ liefert, ebenfalls angesichts des Art.5 Abs.1 S.1 GG, kein brauchbares Abgrenzungskriterium. Denn er übersieht, dass die Beeinflussung des öffentlichen Diskurses geradezu Motiv und Zweck der Meinungsfreiheit ist.[29] Daneben erschließt sich auch nicht, wie sich eine Abgrenzung zu aktivem Campaigning rechtfertigen sollte. Wenn sich etwa eine Partei im Wahlkampf auf Social Media fokussiert und ihr Wahlkampfteam entsprechend besetzt, tut sie das ebenfalls mit dem Ziel, die Wahrnehmung des Diskurses in sozialen Netzwerken zu beeinflussen. In diesem Zusammenhang darf nicht übersehen werden, dass Social Bots auch fungieren könnten, um eine gewisse Waffengleichheit zwischen kleineren Parteien oder NGOs und Personal- bzw. Finanzstärkeren Akteuren herzustellen.

[25] *BGH*, NJW 2013, 2348 (2349).
[26] *Kind/Bovenschulte/Ehrenberg-Silies/Jetzke/Weide*, S. 4, dem schließt sich *Steinbach*, ZRP 2017, 101 (102) offenbar an.
[27] St. Rspr. s. etwa *BGH*, NJW 2003, 1308 (1309 f.).
[28] BVerfGE 93, 266, 289.
[29] *Dankert/Dreyer*, S. 74 m.w.N.

3. Rechtswidrigkeit von Bots in besonderen Fällen

Aus dem Gesagten folgt indes nicht, dass Social Bots nur im Falle rechtsverletzender oder strafbarer Inhalte rechtswidrig sein können. Vielmehr zeigt sich bei genauerer Betrachtung der technischen Abläufe komplexerer Social Bots, dass Tatbestände des UrhG erfüllt sein können.

a) Zugriff auf „Streams“ als Funktionsvoraussetzung komplexer Bots

Bei jenen Social Bots, die auf das Verhalten anderer Nutzer reagieren, können sich Ansatzpunkte aufgrund der Zwischenspeicherung von „Streams“ ergeben. Bei den Streams handelt es sich, vereinfacht gesagt, um Datenpakete. Die darin enthaltenen Daten entsprechen dem, was dem („echten“) Nutzer nach dem Login angezeigt würde, also insbesondere einer Aneinanderreihung von Beiträgen anderer Nutzer.

Diese Streams werden von Twitter über die Programmierschnittstellen zur Verfügung gestellt, um es Dritten zu ermöglichen, auf sie zur Umsetzung gewollter Automatisierungsvorgänge zuzugreifen.

Den jeweiligen Datensatz ruft der Social Bot ab und analysiert ihn, um auf neue Trends oder einzelne Nutzerbeiträge zu reagieren, etwa durch „Retweeten“ oder Kommentieren. Zu dieser Analyse ist in technischer Hinsicht mindestens eine Zwischenspeicherung des Streams im Arbeitsspeicher erforderlich. Vorschriften des UrhG können dann verletzt werden, wenn es sich um einen Stream handelt, der als Datenbankwerk iSd. § 4 Abs.2 S.1 UrhG, oder als Datenbank iSd. § 87a Abs.1 S.1 UrhG zu qualifizieren ist und dessen Nutzung nicht im Einklang mit den Nutzungsbedingungen der Plattform steht.

b) Schutz der „Streams“ als Datenbank bzw. Datenbankwerk

Das UrhG schützt nicht nur einzelne Werke. Schutzgegenstand kann auch die konkrete Zusammenstellung verschiedener Elemente als Datenbank nach § 87a Abs. 1 S.1 UrhG bzw. als Datenbankwerk iSd. § 4 Abs.2 UrhG sein. Die beiden Rechte, Leistungsschutzrecht an einer Datenbank einerseits und das Urheberrecht an einem Datenbankwerk andererseits, bestehen unabhängig voneinander mit verschiedenem Schutzgegenstand, wobei ersteres das Ergebnis ihrer Investitionsleistung schützt, während letzteres das Ergebnis einer persönlichen geistigen Schöpfung durch Auswahl und Anordnung einzelner Elemente zum Gegenstand hat.[30] Beide können bei den von den Nutzern sozialer Netzwerke generierten Inhalten einschlägig sein.[31]

[30] *BGH*, Urt. v. 24. 5. 2007 - I ZR 130/04, GRUR 2007, 685, 687 f. – Gedichteliste I.
[31] *Reinemann/Remmertz*, ZUM 2012, 216 (220).

(1) Datenbank, § 87a, 87b UrhG

Datenbanken sind besonders geschützt wenn es sich um eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen handelt, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert.

i. Sammlung von unabhängigen Elementen, die einzeln zugänglich sind

Der „Stream" stellt eine Sammlung von Daten dar. In ihm wird eine Vielzahl von Tweets gebündelt. Die Tweets stellen auch unabhängige Elemente dar. Die Unabhängigkeit ist gegeben, wenn sich die Elemente voneinander trennen lassen, ohne hierdurch in ihrem Informationsgehalt beeinträchtigt zu werden.[32] Die Besonderheit von „Tweets" besteht gerade darin, eigenständige Aussagen auf 140 Zeichen zu komprimieren.

ii. Systematische Anordnung und einzelne Zugänglichkeit

Die Elemente sind überdies systematisch bzw. methodisch angeordnet und einzeln zugänglich. Das erfordert insbesondere, dass sie einzeln recherchierbar sind, wobei sich die Anordnung auch erst über den Zugang durch eine Software ergeben kann.[33] Twitter stellt eine Programmierschnittstelle zum gezielten Suchen und Abrufen von Tweets nach umfangreichen Suchkriterien zur Verfügung.[34]

iii. wesentliche Investition

Schließlich liegt auch eine wesentliche Investition iSd. § 87a Abs 1 S.1 UrhG vor. Dabei ist auf die Beschaffung, Überprüfung oder Darstellung der Datenbankelemente abzustellen. Zu berücksichtigen sind sowohl sichtende, beobachtende und auswertende Tätigkeiten, als auch die Kosten des Ermittelns und Aufbereitens von Daten, der dazu eingesetzten Computerprogramme sowie der kontinuierlichen Pflege und Aktualisierung der Datenbestände einschließlich der Personalkosten.[35] Nicht zu berücksichtigen sind hingegen Kosten der Erzeugung der in der Datenbank enthaltenen Daten.[36]

Die Kosten für die Beschaffung der Daten stellen eine Investition in diesem Sinne dar. Darunter fallen nämlich auch Kosten für Software, die es Dritten ermöglicht, Daten in eine Datenbank einzugeben.[37] Zwar sind die Daten als solche für Twitter kostenlos, da die Tweets von den Nutzern eingestellt werden. Twitter trägt jedoch die Kosten

[32] *Thum/Hermes*, in: Wandtke/Bullinger, PKUrhR, § 87a UrhG Rn. 12.
[33] *Vohwinkel*, in: BeckOK UrhR, § 87a UrhG Rn. 32 f.
[34] https://developer.twitter.com/en/docs/tweets/search/overview/standard abgerufen am 15.08.2018.
[35] *Vohwinkel*, Rn. 53 f.
[36] *Witte*, in: Auer-Reinsdorf/Conrad, Handbuch IT- und Datenschutzrecht, § 6 Rn. 29.
[37] *Vohwinkel*, Rn. 41.

für die Bereitstellung der Infrastruktur, die es den Nutzern ermöglicht, eigene Inhalte zu erstellen. Hinzu kommen die Kosten für die Überprüfung des Datenbankinhalts. Dazu zählen Kosten, die bei der Kontrolle der vorhandenen Daten während des Betriebes entstehen bzw. bevor diese in die Datenbank eingestellt werden.[38] Die von den Nutzern eingestellten Tweets werden laufend überprüft. So erfolgt bei entsprechender Meldung etwa eine Überprüfung auf sog „sensible Inhalte", bei denen jeder Nutzer selbst festlegen kann, ob ihm diese angezeigt werden sollen.[39] Daneben arbeitet Twitter an Tools, die Tweets missbräuchlichen Inhalts in der Reichweite beschränkt.[40]

Diese Investitionen sind auch wesentlich. Das ist immer dann anzunehmen, wenn Sie nicht ganz unbedeutend, da nicht von jedermann zu erbringen, sind.[41] Wenngleich sich nicht im Einzelnen feststellen lässt, welcher der oben benannten Punkten welche Kosten verursacht, darf bei Twitter unterstellt werden, dass die Beobachtung und Auswertung der Tweets, sowohl darauf, was gerade „trending" ist, aber auch die Löschung rechtswidriger Inhalte, die Kennzeichnung „sensibler Inhalte", die Evaluierung der Benutzerfreundlichkeit der individuell ausgewählten Tweets etc. erheblicher finanzieller Mittel bedarf.

iv. Verletzungshandlung, § 87b Abs.1 S.2 UrhG

Die Verletzungshandlung des § 87b Abs.1 S liegt in der Vervielfältigung der Datenbank insgesamt oder eines nach Art oder Umfang wesentlichen Teiles der Datenbank. Dabei steht die Vervielfältigung eines unwesentlichen Teils jener eines wesentlichen Teils gem. § 87b Abs.1 S.2 UrhG gleich, wenn sie wiederholt und systematisch erfolgt und einer normalen Auswertung der Datenbank zuwiderläuft oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigt werden.

Eine Vervielfältigungshandlung liegt vor. Wie bereits dargelegt, können die fortgeschrittenen Funktionen von Social Bots, also solche, die sich als Reaktion auf Beiträge anderer Nutzer äußert, nur durch eine Analyse der Streams erfolgen. Diese Analyse wiederum kann nur funktionieren, wenn die Streams gespeichert werden, mindestens also im Zwischenspeicher reproduziert werden.[42]

Jeder einzelne Stream stellt eine selbständige Datenbank dar.[43] Entsprechend liegt im Zugriff auf User-Streams eine Zwischenspeicherung der gesamten Datenbank vor.

Auch wenn nicht der gesamte Stream abgerufen wird, liegt in jedem Fall eine wiederholte, systematisch erfolgende Vervielfältigung iSd. § 87b Abs. 1 S.2 UrhG vor. Die-

[38] *Vohwinkel*, Rn. 47 f.
[39] Https://help.twitter.com/de/rules-and-policies/media-settingsabgerufen am 15.08.2018.
[40] https://help.twitter.com/de/safety-and-security/tweet-visibility, abgerufen am 15.08.2018.
[41] *Vohwinkel*, Rn. 53.
[42] *Hawker*, S. 75.
[43] *Thum/Hermes,* Rn. 95; *Witte*, Rn. 15.

se ist gegeben, wenn nach und nach in Erfüllung eines Gesamtplans kleine Teile nutzbar gemacht werden, die sich insgesamt zu einem wesentlichen Teil hochrechnen.[44] Unterstellt man, dass der Social Bot so programmiert ist, keine wesentlichen Informationen zu verpassen, bzw. auf festgelegte Themen auf eine bestimmte Weise zu reagieren, ist eine permanente Auswertung der stetig wachsenden Datenbank erforderlich, sodass früher oder später ein wesentlicher Teil ausgewertet ist.

Diese beeinträchtigt auch die berechtigten Interessen des Datenbankherstellers unzumutbar. Dabei ist eine wirtschaftliche Betrachtungsweise erforderlich. Eine unzumutbare Beeinträchtigung ist angesichts des investitionsschützenden Charakters des Datenbankschutzes insbesondere dann anzunehmen, wenn deren Amortisation beeinträchtigt ist.[45] Durch den Bot-Einsatz ist der Fortbestand des gesamten Dienstes gefährdet. Zwar führen die gefälschten Nutzerprofile zunächst zumindest scheinbar zu einer Erhöhung der Nutzer und damit der Werbeeinnahmen. Mittel- bis Langfristig droht jedoch ein gegenteiliger Effekt: Wenn der Dienst nämlich für „echte“ Nutzer uninteressant wird, weil er von Social Bots infiltriert ist, kehren sich die Nutzer ab und mit ihnen die Werbeeinnahmen. Der Reiz sozialer Netzwerke besteht gerade darin, dass Menschen miteinander kommunizieren. Werden diesen jedoch nach dem Login keine von Menschen geposteten Inhalte, sondern zu einem nicht unerheblichen Teil Bot-Nachrichten angezeigt, verliert der Dienst für Nutzer den Reiz.

(2) Datenbankwerk, § 4 Abs.2 S.1 UrhG

i. Werkscharakter

Daneben sind zumindest die jeweiligen „User Streams“ als Datenbankwerke zu qualifizieren. Die dazu erforderliche geistige Schöpfung, durch die sich das Datenbankwerk von der bloßen Datenbank unterscheidet, liegt in der Auswahl und Anordnung bereits bestehender Elemente.[46] Die Auswahl und Anordnung erfolgt durch die für jeden User Stream individuelle Zusammenstellung der für ihn relevanten Tweets. In die Auswahl fließen verschiedene Kriterien wie die Interessen des jeweiligen Nutzers, welchen Personen er folgt, sein Standort, die Aktualität des Themas sowie der Zeitraum, über den das Thema bereits „trending“ ist.[47] Daran ändert sich auch nichts angesichts des Umstandes, dass die praktische Umsetzung der Anordnung nicht durch menschliche, redaktionelle Auswahl, sondern aufgrund eines Algorithmus zustande kommt. Computergenerierte Werke sind nämlich dann schutzfähig, wenn die Gestaltung des Erzeugnisses noch auf einen geistigen Schöpfungsakt zurückgeführt werden kann, wenn also

[44] *Vohwinkel*, § 87b UrhG Rn. 15; a.A.: *Wiebe*, in: Spindler/Schuster, Recht der elektronischen Medien, § 87a UrhG Rn. 13.
[45] *Dreier*, in: Dreier/Schulze, UrhG, § 87b Rn. 16.
[46] *Taeger/Rolfs*, in: Kilian/Heussen, Computerrechts-Handbuch, Teil 2, 20.6 Rn. 26.
[47] https://help.twitter.com/de/using-twitter/twitter-trending-faqs, abgerufen am 15.08.2018.

die Maschine nur Hilfsmittel ist.[48] Das ist hier der Fall. Der Schöpfungsakt ist der eigentlichen Umsetzung vorgeschaltet und liegt in der Auswahl und Gewichtung der relevanten Faktoren, die zur Zusammenstellung des konkreten User Streams herangezogen werden. Diese Auswahl erfolgt nicht beliebig. Vielmehr bestimmt sie über Erfolg oder Misserfolg eines sozialen Netzwerks. Erfolgreich wird das soziale Netzwerk nämlich nur sein, wenn dem jeweiligen Nutzer Beiträge angezeigt werden, von denen er sich angesprochen fühlt und die für ihn hilfreich sind. Gerade durch die Filterung der zunächst unübersichtlichen Datenflut aller möglichen Beiträge anderer Nutzer wird das für Twitter charakteristische Nutzererlebnis erzeugt.

Auch die zur Annahme einer persönlichen Schöpfung weiterhin erforderliche Eigentümlichkeit ist gegeben. Diese ist anzunehmen, wenn die Sammlung in ihrer Struktur, die durch Auswahl oder Anordnung des Inhalts der Datenbank geschaffen worden ist, einen individuellen Charakter hat.[49] Eine bestimmte Gestaltungshöhe ist hierbei nicht erforderlich.[50] Anders als etwa bei einem Telefonbuch[51] oder Musik-Chartlisten[52] gibt es für den dem einzelnen Nutzer angezeigten Stream keine zwingende oder von vornherein feststehende Anordnung, die nur geringen Spielraum für individuelle Gestaltung ließe. Vielmehr sind die Entscheidungsprozesse, die dieser Auswahl zugrunde liegen, sehr komplex. Nicht nur das Ob, sondern auch das Wie der oben beschriebenen Faktoren fließt hier ein. Es ist gerade diese konkrete Anordnung, die die Eigentümlichkeit des Netzwerks ausmacht und das es – neben eher gestalterischen Eigenheiten – von anderen Netzwerken abgrenzt.

ii. Unzulässigkeit der Vervielfältigungshandlung, § 55a

Aufgrund der Qualifikation als Datenbankwerk iSd. § 4 Abs.2 UrhG ist die Zulässigkeit von Vervielfältigungshandlungen nach den § 55a UrhG zu beurteilen. Demnach ist dem berechtigten Benutzer die Vervielfältigung der Datenbank gestattet, soweit dies für dessen übliche Benutzung erforderlich ist. Dabei stellt die Zwischenspeicherung im Arbeitsspeicher eine hinreichende Vervielfältigungshandlung dar.[53]

Von den nach § 55a UrhG zur Vervielfältigung Berechtigten kommt bei der online-Nutzung alleine die Variante desjenigen infrage, „dem ein Datenbankwerk aufgrund eines mit dem Urheber oder eines mit dessen Zustimmung mit einem Dritten geschlos-

[48] *Schulze*, in: Dreier/Schulze, § 2 UrhG Rn. 8.
[49] *Ahlberg*, in: BeckOK UrhR, § 4 UrhG Rn.32.
[50] *BGH*, Urt. v. 24. 5. 2007 - I ZR 130/04, GRUR 2007, 685 (687 f.) – Gedichteliste I.
[51] *BGH*, Urt. v. 06.05.1999 - I ZR 199/96, GRUR 1999, 923 (924) – Tele-Info-CD.
[52] *BGH*, Urt. v. 21.07.2005 - I ZR 290/02, GRUR 2005, 857 (858) – Hitbilanz.
[53] *Grübler*, in: BeckOK UrhR, § 55a UrhG Rn. 5.

senen Vertrags zugänglich gemacht wird“, da die ersten beiden Varianten auf die Existenz eines körperlichen Vervielfältigungsstücks abstellen.[54]

Entsprechend ist die Frage der üblichen Benutzung in diesem Sinne anhand der vertraglichen Vereinbarung zu beurteilen.[55] Wie dargelegt, verbietet *Twitter* zwar nicht grundsätzlich die automatisierte Nutzung des Dienstes. Vielmehr legen die Automatisierungsregeln die Bedingungen für die Verwendung von Bots fest. Deren Akzeptanz ist Voraussetzung der Nutzung des Dienstes. Diese Regeln verbieten unter anderem den Betrieb von mehreren Accounts mit demselben Nutzungszweck.[56] Genau dies ist jedoch bei typischen social bots der Fall.

Der Betreiber des Bots verstößt somit gegen die Lizenzbedingungen und überschreitet den von § 55a UrhG gesteckten Rahmen zulässiger Vervielfältigungshandlungen.

c) zivilrechtliche Folgen, § 97 UrhG

Soweit die Verletzungshandlungen nach deutschem Recht zu beurteilen sind, ergeben sich die Folgen aus § 97 UrhG. Demnach begründen Verstöße gegen das Urheberrecht und verwandte Schutzrechte zunächst einen Beseitigungs- und Unterlassungsanspruch (§ 97 Abs.1 UrhG). Im Falle vorsätzlichen oder fahrlässigen Handelns ergibt sich ein Schadensersatzanspruch (§ 97 Abs.2 UrhG). Rechtfertigungsgründe dürften sich in den dargestellten Konstellationen schwerlich begründen lassen.

Die Aktivlegitimation läge in derartigen Fällen ausschließlich bei Twitter als dem Verletzten. Insoweit muss es wohl eher als unwahrscheinlich angesehen werden, dass die hier aufgeworfenen Fragen jemals durch ein deutsches Gericht entschieden werden. Denn aus praktischer Sicht besteht für Twitter kaum ein Bedürfnis, sich dieser Instrumente zu bedienen. Schneller und zielführender ist es aus deren Sicht, die jeweiligen Accounts zu deaktivieren.

d) Strafrechtliche Folgen, §§ 106, 108 UrhG

§ 106 Abs.1 UrhG sieht den Straftatbestand der unerlaubten Verwertung urheberrechtlich geschützter Werke vor. Datenbanken werden nach § 108 Abs.1 Nr.8 UrhG durch den Straftatbestand des unerlaubten Eingriffs in verwandte Schutzrechte geschützt. Für beide sieht § 108a UrhG eine erhöhte Strafe im Falle gewerbsmäßigen Handelns vor.

(3) Antragsdelikt

Soweit kein gewerbsmäßiges Handeln vorliegt, handelt es sich bei den Straftatbeständen gem. § 109 UrhG um relative Antragsdelikte. Wie bereits zu den zivilrechtlichen

[54] *Dreier*, in: Dreier/Schulze, § 55a UrhG, Rn. 5.
[55] *Dreier*, in: Dreier/Schulze, § 55a UrhG, Rn.7.
[56] https://help.twitter.com/de/rules-and-policies/twitter-automation, abgerufen am 15.08.2018.

Folgen dargelegt, ist fraglich, ob es für Twitter sinnvoll ist, derartige Probleme auf dem Rechtsweg zu lösen, wenn technische Maßnahmen einfacher umzusetzen sind.

Allerdings kann an die Stelle des Strafantrages gem. § 109 Abs.1 UrhG auch die Bejahung eines besonderen öffentlichen Interesses durch die Strafverfolgungsbehörde treten. Je nach Konstellation wird sich dieses, insbesondere in Wahlkampfzeiten vor wichtigen Bundes- oder Landtagswahlen, durchaus bejahen lassen.

(4) Verstoß gegen § 55a UrhG nur bei AGB-Verletzung

Nicht übersehen werden darf dabei, dass ein Vorgehen nach § 106 UrhG an die Verletzung des § 55a UrhG und damit, wie oben dargelegt, an einen Lizenzverstoß anknüpft. Möglich wäre ein Vorgehen entsprechend nur, wenn die jeweilige Plattform die Nutzung von Bots verbietet bzw. die Bots selbst gegen die AGB verstoßen. Dass dies nicht ohne weiteres der Fall ist, zeigt sich daran, dass es sich Facebook etwa in Punkt 2.3 seiner Nutzungsbedingungen[57] vorbehält, den automatisierten Zugriff zu erlauben. Auch bei Twitter ist automatisiertes Posten grundsätzlich erlaubt.[58]

(5) Identifizierung der Betreiber kaum möglich

Auch in praktischer Hinsicht wird es schwierig sein, die Verwender der Social Bots zu identifizieren. Die unmittelbar Handelnden bleiben häufig anonym oder agieren aus dem Ausland. Ansatzmöglichkeiten bieten sich freilich, wenn der Verwender offen kundtut, Social Bots einzusetzen oder einsetzen zu wollen.

V. Fazit

Die Untersuchung hat gezeigt, dass entsprechend aufkommender Bestrebungen, die Materie der Social Bots einer gesetzlichen Regelung zuzuführen, durchaus bereits Instrumentarien bestehen, gegen diese vorzugehen. Neben der praktischen Schwierigkeit, dass der Betreiber in vielen Fällen nicht zu ermitteln ist, ist aber auch fraglich, ob der hier aufgezeigte Weg rechtspolitisch gangbar ist. Zwar ruft der Einsatz von Social Bots wohl zu Recht Skepsis hervor, da er schwerlich mit den tradierten Vorstellungen von Wahlkampf und Meinungsmarkt in Einklang zu bringen ist. Allerdings kann das UrhG langfristig nicht der Regelungsort für Maßnahmen zur Aufrechterhaltung der Debattenkultur sein. Dies gilt insbesondere angesichts dessen, dass die Rechtswidrigkeit von der Frage abhängt, ob das jeweils genutzte Medium in seinen allgemeinen Geschäftsbedingungen die Verwendung von Social Bots verbietet bzw. eine Erlaubnis im Einzelfall erteilt hat.[59] Eine Erlaubnis kann aber gerade im Interesse eines sozialen Netzwerks liegen, wenn dieses, etwa in der Startup-Phase, zunächst um jeden Preis die

[57] Https://de-de.facebook.com/terms, abgerufen am 15.08.2018.
[58] https://help.twitter.com/de/rules-and-policies/twitter-automation, abgerufen am 15.08.2018.
[59] Daran krankt im Übrigen auch der Gesetzesentwurf zum „digitalen Hausfriedensbruch“, BT-Drs. 19/1716.

Nutzerzahl steigern möchte. Vor noch größere Schwierigkeiten wäre man gestellt, wenn das jeweilige soziale Netzwerk eigene politische Präferenzen umsetzt und einzelnen Akteuren ausdrücklich erlaubt wird, Bots einzusetzen, anderen aber nicht.

Angesichts dessen ist die zu beobachtende Diskussion begrüßenswert. Erforderlich ist die Formulierung eines eindeutigen Willens durch den Gesetzgeber auf dieser Grundlage. Die unter III. dargelegten Anwendungsszenarien und die unter IV. 2. c) gezeigten Abgrenzungsschwierigkeiten zu sonstigen Aktivitäten in der Debatte, bzw. dem Wahlkampf zeigen, dass ein Einschreiten nur maßvoll erfolgen sollte.

Literaturverzeichnis

Ahlberg/Götting, (Hrsg.), BeckOK Urheberrecht, 21. Edition, München 2018.

Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Baumanns, Charlotte, FinTechs als Anlageberater? Die aufsichtsrechtliche Einordnung von Robo-Advisory, BKR 2016, 366-375.

Bender, Justus/Oppong, Marvin: Frauke Petry und die Bots, FAZ-Online v. 07.02.2017, https://www.faz.net/aktuell/politik/digitaler-wahlkampf-frauke-petry-und-die-bots-14863763.html, abgerufen am 15.08.2018.

Bös, Nadine/Marx, Uwe, Berufsberatung per Whatsapp, FAZ-Online v. 30.01.2017, https://www.faz.net/aktuell/beruf-chance/arbeitswelt/chatbot-der-arbeitsagentur-berufsberatung-per-whatsapp-14764096.html.

Dankert, Kevin/Dreyer, Stephan, Social Bots – Grenzenloser Einfluss auf den Meinungsbildungsprozess?, K & R 2017, 73-75.

Dreier/Schulze (Hrsg.), Urheberrechtsgesetz, 5. Aufl., München 2015.

Ferrara, Emilio/Varol, Onur/Davis, Clayton/Menczer, Filippo/Flammini, Alessandro: The Rise of Social Bots, Communications of the ACM 2016, 96-104.

Hawker, Mark, The developer's guide to social programming: building social context using Facebook, Google friend connect, and the Twitter API, Boston 2011.

Hegelich, Simon: Invasion der Meinungs-Roboter, Berlin 2016.

Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 34. EL, München 2018.

Kind, Sonja/Bovenschulte, Marc/Ehrenberg-Silies, Simone/Jetzke, Tobias/Weide, Sebastian, Thesenpapier zum öffentlichen Fachgespräch »Social Bots – Diskussion und Validierung von Zwischenergebnissen« am 26. Januar 2017 im Deutschen Bundestag, Onli-

neveröffentlichung, 2017, abrufbar unter https://www.tab-beim-bundestag.de-/de/aktuelles/20161219/Social%20Bots_Thesenpapier.pdf.

Kreutzer, Tobias, Auch im Netz regiert die Schweigespirale, FAZ-Online v. 26.08.2014, https://www.faz.net/aktuell/feuilleton/medien/studie-auch-im-netz-regiert-die-schweigespirale-13118570.html, angerufen am 15.08.2018.

Libertus, Michael, Rechtliche Aspekte des Einsatzes von Social Bots de lege late und de lege ferenda, MMR 2018, 20-26.

Liesching, Marc, Hakenkreuze in Film, Fernsehen und Computerspielen – Verwendung verfassungsfeindlicher Kennzeichen in Unterhaltungsmedien, MMR 2010, 309-313.

Milker, Jens: »Social-Bots« im Meinungskampf, ZUM 2017, 216-222.

Pariser, Eli, The Filter Bubble, London 2011.

Reinemann, Susanne/Remmertz, Frank, Urheberrechte an User-generated Content, ZUM 2012, 216-227.

Rosenbach, Marcel/Traufetter, Gerald: Betreiben von Social Bots soll unter Strafe stehen, Spiegel-Online v. 21.01.2017, https://www.spiegel.de/netzwelt/netzpolitik/social-bots-laender-wollen-gegen-meinungsroboter-im-internet-vorgehen-a-1130937.html, abgerufen am 15.08.2018.

Säcker/Rixecker/Oetker/Limperg (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7. Aufl., München 2015.

Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl., München 2015.

Stark, Birgit, Meinungsbildung im Netz: Die Macht der Algorithmen, MMR 2017, 721-722.

Steinbach, Armin: Social Bots im Wahlkampf, ZRP 2017, 101-105.

Volkmann, Viktor, Hate Speech durch Social Bots, MMR 2018, 58-63.

Wandtke/Bullinger (Hrsg.), Praxiskommentar zum Urheberrecht, 4. Aufl., München 2014.

Token und tokenisierte Rechte

Blockchainpositionen als Wertpapierersatz

Johannes Arndt/Valentin Tribula

Lehrstuhl Prof. Dr. Matthias Jacobs, Bucerius Law School
johannes.arndt@law-school.de
valentin.tribula@law-school.de

Abstract

Tokenisierung stellt einen zentralen Anwendungsbereich der Blockchain-Technologie dar. Dabei wird zwischen *Utility Token* und *Security Token* unterschieden, wobei sich letztere in *Debt Token* und *Equity Token* unterteilen lassen. Die privatrechtlichen Fragestellungen im Zusammenhang mit der Übertragbarkeit der einzelnen *Token* bzw. der Rechte und Forderungen aus ihnen wurden bisher kaum behandelt. Im Anschluss an eine Einführung in die Blockchain-Technologie sowie einem Überblick über die verschiedenen Arten von *Token* sollen die Fragen der Übertragbarkeit vor allem vor dem Gesichtspunkt der Vergleichbarkeit mit Wertpapieren diskutiert werden.

I. Einleitung

Bitcoin ist die bekannteste Anwendung der innovativen Blockchain-Technologie. Bitcoin ist ein reines Zahlungsmittel und vermittelt keinerlei Rechte gegenüber einer zentralen Instanz. Davon zu unterscheiden sind sogenannte *Token*, die zwar ebenfalls dezentral, also ohne Zuhilfenahme einer zentralen, buchführenden Stelle übertragen werden, aber einen Anspruch gegen eine Person geben, die den *Token* ursprünglich herausgegeben hat (im Folgenden: Emittent). Der Herausgabe-Vorgang wird – in Anlehnung an den Aktienrechtlichen *IPO* (*Initial Paper Offering*) – *ICO* (*Initial Coin Offering*) genannt. Dieser Beitrag soll die bislang vernachlässigten privatrechtlichen Fragestellungen in diesem Zusammenhang beleuchten. Während die Übertragung von Bitcoins und anderen reinen Kryptowährungen in einer anderen Arbeit beleuchtet wird,[1] soll es hier um die Übertragung des mit dem *Token* verknüpften Rechts gehen.

[1] Johannes Arndt beschäftigt sich im Rahmen seiner Dissertation mit der Frage, ob eine Bitcoin-Transaktion ein Rechtsgeschäft ist. Die bisherigen Ergebnisse liegen dieser Arbeit zugrunde. Danach besteht an Bitcoins ein absolutes Registerrecht, welches analog § 873 Abs. 1 BGB rechtsgeschäftlich übertragen wird. Siehe dazu auch *Jacobs/Arndt*, Bitcoins in der Zwangsvollstreckung (im Erscheinen).

II. Funktionsweise und Anwendungsfälle der Blockchain-Technologie

1. Funktionsweise einer Blockchain

Die Blockchain ist eine Datei, in der Transaktionen über virtuelle Werteinheiten abgebildet werden. Die Blockchain-Technologie ist also ein Buchhaltungssystem. Informationen werden in aneinandergereihten Datenblöcken (*blocks*) gespeichert, deren Verkettung anhand digitaler Fingerabdrücke (sog. *Hash-Werte*) geschieht.[2] Die Blockchain protokolliert in chronologischer Weise Transaktionen. Sie erlangt ihren Namen aus der kryptographischen Verkettung einzelner *blocks* zur *block-chain*. Die *blocks* lassen sich im Nachhinein nicht mehr ändern.

Die Blockchain ist auf allen an der jeweiligen Blockchain teilnehmenden Rechnern gespeichert (*Distributed Ledger Technologie – DLT*). Die Rechner bilden auf diese Weise ein *Peer-to-Peer*-Netzwerk, in dem sie untereinander ohne zentrale Zwischenstelle Transaktionen vornehmen. Die Teilnehmer können die Berechtigung der jeweils Verfügenden leicht überprüfen. Somit besteht ständig Konsens über die Richtigkeit der Blockchain, Vertrauen in eine höhere Instanz ist nicht notwendig. Um falsche Informationen auf einer Blockchain protokollieren zu können, bedürfte es der Kontrolle von über fünfzig Prozent der gesamten Rechenstärke des Systems.[3]

Transaktionen können nur mithilfe eines Schlüsselpaares vorgenommen werden. Dieses Paar besteht aus einem öffentlichen Schlüssel, der als Transaktionsziel dient und mit einer Kontonummer vergleichbar ist, sowie einem privaten Schlüssel, den nur der jeweilige Teilnehmer kennt und der als Passwort fungiert. Durch den privaten Schlüssel kann der Teilnehmer Transaktionen über Werteinheiten legitimieren, die zuvor an den korrespondierenden öffentlichen Schlüssel transferiert wurden.[4] Daraus resultiert exklusive Verfügungsmacht des Erwerbers.

Es ist wichtig sich zu vergegenwärtigen, dass es der Blockchain-Eintrag ist, der die Verfügungsmacht über die Werteinheit vermittelt. Er tut das zwar in Verbindung mit dem Schlüsselpaar. Dieses Schlüsselpaar ist aber nicht die Werteinheit selbst. Das ergibt sich bereits aus der Tatsache, dass es beliebig oft vervielfältigt werden kann. Zudem wird es bei einer Transaktion nicht übertragen.

2. Anwendungsfälle

Eine Blockchain kann größtmögliche Sicherheit schaffen und aufgrund ihrer Dezentralität jedenfalls theoretisch durch das Vermeiden einer Vermittlungsinstanz gleichzeitig

[2] *Welzel/Eckert* et al., S. 8 ff.
[3] *Antonopoulos*, S. 213 ff.
[4] *Martini/Weinzierl*, NVwZ 2017, 1251 (1251 ff.).

effizient und kostensparend arbeiten. Diese Charakteristika eröffnen ein weites Feld von Anwendungsmöglichkeiten in der Wirtschaft und im öffentlichen Sektor.

Aus wirtschaftlicher Sicht ist die Blockchain besonders als Technologie hinter Kryptowährungen wie dem Bitcoin oder Ethereum bekannt. Großes Potenzial zeigt sie weiterhin als Abwicklungsinstrument im Rahmen von *Smart Contracts*, die Vertragsvorgänge automatisieren. Beispielsweise wird so eine Zahlung in Kryptowährungen initiiert, sobald eine zuvor festgelegte Bedingung eintritt.[5] Die Möglichkeit, fälschungssichere chronologische Aufzeichnungen zu speichern, versuchen IBM und Walmart zu nutzen, indem sie testweise an einem transparenten Lebensmittelsystem arbeiten.[6] Dabei könnten Produzent, Konsument oder andere *Stakeholder* ohne großen Aufwand jeden Produktionsschritt nachvollziehen, den das jeweilige Produkt durchlaufen hat. Auch im pharmazeutischen Bereich findet die Blockchain erste Anwendungen bei der Kontrolle von Krankenakten.[7]

Im öffentlichen Sektor wird ebenfalls versucht, das Potenzial der Blockchain-Technologie zu nutzen. Denkbar ist unter anderem der Einsatz als Grundbuch.[8] Ferner hat die Cagliari Universität in Italien angekündigt, die Diplome ihrer Absolventen mittels der Ethereum-Blockchain auszugeben.[9] In beiden Fällen würde der Abruf der entsprechenden Daten erleichtert, da der Weg zur entsprechenden Verwaltungsstelle entfiele.

III. Tokenisierung

Immer mehr werden außerdem sog. *Token* ausgegeben, die technisch wie Kryptowährungen funktionieren, aber zusätzlich ein Recht des jeweiligen Inhabers gegenüber dem Emittenten repräsentieren.

Es wird allgemein zwischen verschiedenen *Token* unterschieden.[10] Die Unterscheidung erfolgt aufgrund des jeweils repräsentierten Rechts und ist auch aus rechtlicher Sicht relevant. Den *Token* gemeinsam ist, dass sie in einem ersten Schritt von einem Emittenten im Rahmen eines *ICO* ausgegeben werden.

1. ICO

Unternehmen stellen *Token* im Rahmen eines *Initial Coin Offering* (*ICO*) aus. Sie werden gegen eine finanzielle Gegenleistung, meist in Form von Kryptowährungen, er-

[5] Zur rechtlichen Einordnung von *Smart Contracts* siehe *Kaulartz*/*Heckmann*, CR 2016, 618 (618 ff.); zu weiteren Anwendungsmöglichkeiten siehe *Eschenbruch*/*Gerstberger*, NZBau 2018, 3 (3).
[6] IBM v. 22.08.2017.
[7] NewsBTC v. 11.09.2018.
[8] Getestet wird dies unter anderem in Schweden und Georgien, siehe dazu *Grau* sowie *Nimfuehr*.
[9] *Morris*, UToday.
[10] *Dietsch*, MwStR 2018, 546 (546); *Krüger*/*Lampert*, BB 2018, 1154 (1155); *Borkert* ITRB 2018, 39 (42).

worben. Dies geschieht auf der Basis von *Smart Contracts*: Sofern Einheiten einer Kryptowährung an die Adresse des Emittenten transferiert werden, erhält der Absender im Gegenzug automatisch einen entsprechenden Betrag der *Token*. Sobald die *Token* emittiert sind, hat der Emittent keinen Einfluss mehr auf Verfügungen über sie. Folglich hat der Inhaber absolute Herrschaftsmacht über den *Token*.[11] Dieser Herausgabevorgang stellt eine Alternative zum aktienrechtlichen *Initial Paper Offering* (*IPO*) sowie zu Crowdfunding-Plattformen dar.[12]

2. Arten von Token

Allgemein werden *Utility Token* und *Security Token* unterschieden, wobei die exakten Bezeichnungen mitunter unterschiedlich genutzt werden. *Security Token* lassen sich in *Debt Token* und *Equity Token* unterteilen. Andere Erscheinungsformen, wie auch Mischformen, sind denkbar. Schon deshalb muss ein *Token* im Einzelfall anhand seiner beabsichtigten Funktionalität bewertet werden.

a) Utility Token

Utility Token gewähren dem Erwerber einen Anspruch gegen den Aussteller auf Zugang zu einer (Dienst-)Leistung oder auf ein Produkt. Dabei steht die Gegenleistung von Anfang an fest und wird nicht verzinst. Dem Erwerber ist es erst möglich, die Forderung fällig zu stellen, sobald der Emittent in der Lage ist, die versprochene Leistung zu erfüllen – der Erwerber tritt somit in Vorleistung. Utility *Token* sind mit einem Gutschein vergleichbar.

b) Security Token

Bei dem Erwerb von *Security Token* handelt es sich um eine finanzielle Investition. Es wird zwischen *Equity* und *Debt Token* unterschieden.

(1) Equity Token

Equity Token sind als Eigenkapital zu klassifizieren, das der Erwerber leistet. Sie stehen für Unternehmensanteile oder anderes Eigenkapital, bspw. in Form von Sacheigentum.[13] Aus der Inhaberschaft können Mitspracherechte oder Dividenden resultieren. Der Erwerber ist – wie bei einem herkömmlichen Unternehmensanteil – am unternehmerischen Risiko beteiligt.

[11] Zur rechtlichen Einordnung dieser Verfügungsmacht siehe Fn. 1.
[12] Zum Verhältnis von *ICO* und *IPO* siehe auch *Vogel*/*Müller*/*Luthiger*/*Ljubicic*, AG 2017, 333 (333).
[13] *Wilmoth*, StrategicCoin.

(2) Debt Token

Debt Token sind mit klassischen Anleihen vergleichbar.[14] Der Erwerber stellt Fremdkapital zur Verfügung, welches zumeist für den Unternehmensaufbau genutzt wird. Im Gegenzug werden ihm Zinsen versprochen. Der *Token* repräsentiert in diesem Sinne den Anspruch des Fremdkapitalgebers auf Rückzahlung und Verzinsung.

c) Reichweite der Untersuchung

Diese Einordnung der *Token* hat vor allem aufsichtsrechtlichen Ursprung.[15] Für diesen Beitrag sollen *Utility Token* und *Debt Token* betrachtet werden, durch die jeweils allein ein schuldrechtlicher Anspruch repräsentiert wird. Die Betrachtung von *Equity Token* verdient indes besonders vor dem Hintergrund des Finanzmarkt- und Unternehmensrechts einen eigenen Beitrag.

IV. Steuer- und aufsichtsrechtliche Einordnung verschiedener Token

Während das Phänomen der *Token* bisher kaum aus privatrechtlicher Perspektive beleuchtet wurde, hat das Thema aus steuer- und aufsichtsrechtlicher Perspektive bereits Aufmerksamkeit erregt. Das liegt zum einen an der höheren unmittelbaren Relevanz für die beteiligten Personen und zum anderen daran, dass der EuGH sich hierzu bereits geäußert hat.

Vor dem Hintergrund regulatorischer Aspekte ist vor allem das *ICO* relevant. Es können sich etwa Fragen nach der Anwendbarkeit des Finanzmarktrechts oder dem Bestehen von Bewilligungspflichten, aber auch steuerrechtliche Fragen ergeben.

Die Bundesaufsicht für Finanzdienstleistung (BaFin) befasst sich mit der regulatorischen Einordnung von *Token* im Bereich der Wertpapieraufsicht in einem offiziellen Hinweisschreiben.[16] Demnach ist zur Einordnung und Bewertung eines *Token* unabhängig von dessen Bezeichnung eine Einzelfallprüfung vor dem Hintergrund der Voraussetzungen der einschlägigen Normen des WpHG, WpPG sowie der MiFID II notwendig. Eine Einordnung als Wertpapier zieht die Möglichkeit der Anwendung der im Bereich der Wertpapieraufsicht anwendbaren Rechtsnormen mit sich. Dazu gehören unter anderem das WpHG, WpPG sowie die MAR und die Finanzmarktverordnung (MiFIR).

Die schweizerische Finanzmarktaufsicht FINMA nimmt eine Unterteilung in *Currency Token*, *Utility Token* und *Security* Token vor und trifft ihre Entscheidung über die Einordnung als Effekten auf der Basis dieser Kategorien.[17] Trotzdem betont sie, dass im

[14] *Dietsch*, MwStR 2018, 546 (548).
[15] Siehe sogleich IV.
[16] *BaFin*, Bonn 2018.
[17] *FINMA*, Bern 2018.

Einzelfall zu prüfen ist, ob *Token* als Effekten zu qualifizieren sind. Ist dies der Fall, ergeben sich die Rechtsfolgen, wie etwaige Prospektpflichten, aus den Finanzmarktgesetzen.

Auch die U.S. Securities and Exchange Commission (SEC) nimmt im Falle eines *ICO* Einzelfallbetrachtungen anhand des Inhalts und des Zwecks der emittierten *Token* vor.[18] Grundsätzlich liegt dieser Bewertung jedoch die Annahme zu Grunde, dass es sich bei *Token*, die im Rahmen eines *ICO* emittiert werden, um Wertpapiere handelt. Kryptowährungen unterfallen nicht dem Wertpapierbegriff des SEC. Aus der Einordnung als Wertpapier resultiert auch im Bereich der amerikanischen Finanzmarktaufsicht die Anwendbarkeit entsprechender Finanzmarktgesetze. So ist etwa der Handel von Wertpapieren im Grundsatz ausschließlich mit entsprechender Lizenz gestattet.

Der EuGH hat sich aus steuerrechtlicher Sicht im Hedqvist-Urteil zur Thematik des Umtausches der Kryptowährung Bitcoin in konventionelle Währungen geäußert.[19] Er hatte zu entscheiden, ob ein Umtausch konventioneller Währungen in Bitcoin und umgekehrt als steuerbare sonstige Leistung der Mehrwertsteuer unterfällt. Indem er dies unter Anwendung des Art. 135 Abs. 1 Buchst. e MwStSystRL verneinte, stellte er den Bitcoin Devisen gleich. Diese Aussagen sind analog auf andere Kryptowährungen anwendbar.[20] Einen Rückschluss auf *Security Token* oder *Utility Token* lässt dies allerdings nicht zu.

V. Privatrechtliche Einordnung des Ersterwerbs von Token

Die Einordnung von *Token* und durch *Token* repräsentierter (im Weiteren: *tokenisierter*) Rechte aus privatrechtlicher Sicht ist besonders für die Verknüpfung des *Token* mit dem darin repräsentierten Recht relevant. Folgend soll vor dem Hintergrund der voranstehend getroffenen Kategorisierung die Rechtsnatur von *Utility Token* und *Debt Token* erläutert werden. Beide *Token*-Arten repräsentieren eine Forderung des Inhabers gegen den Emittenten und werden im Rahmen eines *ICO* ausgestellt. Die Rechtsausübung soll nach Vorstellung der Parteien regelmäßig nur unter Vorlage des *Token* möglich sein.

Dabei ist der *Utility Token* auf Zugang zu einer Leistung oder einem Produkt gerichtet, der *Debt Token* auf den Anspruch auf Rückzahlung und Verzinsung des Darlehensbetrags. Ein *Token* wird in der Regel nicht namensgebunden ausgestellt,[21] vielmehr steht das Recht, die Leistung einzufordern, nach Absicht der Parteien dem jeweiligen Inhaber des *Token* zu. Der *Token* legitimiert ihn zur Forderung, gleichzeitig dient er als

[18] *SEC* v. 25.07.2017; *SEC* v. 11.12.2017.
[19] EuGH, Urt. v. 22.10.2015, MMR 2016, 201.
[20] *BMF* v. 27.02.2018.
[21] Ggf. ist es aber für Ersterwerb und jeden weiteren Erwerb notwendig, gewisse Daten an den Emittenten zu ermitteln.

Verifizierung für den Emittenten, dass die jeweilige Person auch tatsächlich einen Anspruch hat.

1. Vergleichbarkeit von Token mit Urkunden

Gerade weil zur Rechtsausübung die Vorlage des *Token* erforderlich ist, liegt ein Vergleich von *Utility Token* und *Debt Token* zu Wertpapieren nahe. In diesem Kontext werden vor allem Inhaberschuldverschreibung nach §§ 793 ff. BGB relevant.

Ein Wertpapier ist eine Urkunde, die ein privates Recht in der Weise verbrieft, dass zu dessen Geltendmachung die Innehabung der Urkunde erforderlich ist.[22] Innerhalb der Wertpapiere gemäß §§ 793 ff. BGB ist zwischen Inhaberpapieren, Orderpapieren und Rektapapieren zu unterscheiden.[23] Jedes setzt eine Urkunde voraus.

Qua Parteivereinbarung wäre es zumindest theoretisch denkbar, dass die Vorlage des *Token* wie bei einem Schuldschein im Sinne des § 952 Abs. 1 BGB zur Rechtsausübung nicht notwendig sein soll. Unabhängig davon bedarf auch ein Schuldschein der Urkundenqualität des *Token*.

a) Direkte Anwendung

Bei einem *Token* müsste es sich folglich um eine Urkunde handeln, damit §§ 793 ff. BGB beziehungsweise § 952 Abs. 1 BGB direkt anwendbar sind. Der Urkundenbegriff richtet sich nach der für das Beweisrecht der ZPO anerkannten Definition. Eine Urkunde ist demnach eine durch Schriftzeichen verkörperte Gedankenerklärung.[24] Bei einem *Token* handelt es sich allerdings um eine virtuelle Einheit, welche nicht verkörpert ist. Damit handelt es sich bei einem *Token* nicht um eine Urkunde.

b) Analoge Anwendung

Möglicherweise sind die Vorschriften aber analog auf *Token* anzuwenden, wenn Blockchain-Einträge im Rahmen dieser Vorschriften mit Urkunden vergleichbar sind.

Die Möglichkeiten und Herausforderungen digitaler Technologien sind vom Gesetz bisher in weiten Teilen nicht erfasst. Dabei handelt es sich um technologische Konzepte, deren Ausgestaltung und Wirkung zur Zeit der Gesetzesgestaltung nicht planbar war. Dass *Token* bewusst nicht von §§ 793 ff. BGB beziehungsweise von § 952 Abs. 1 BGB erfasst sein sollen, ist vor diesem Hintergrund nicht anzunehmen.

Die analoge Anwendung der §§ 793 ff. BGB auf Registereinträge wurde bereits mit Blick auf Globalurkunden gemäß § 9a DepotG diskutiert und abgelehnt.[25] Als Begrün-

[22] *Gursky*, S. 2; *Gehrlein*, in: BeckOK BGB, § 793 Rn. 1; *Habersack*, in: MüKo BGB, Vor § 793 Rn. 5 ff.
[23] *Habersack*, in: MüKo BGB, Vor § 793 Rn. 14 ff.; *Marburger*, in: Staudinger, Vor § 793 Rn. 6 ff.
[24] *BGH*, Urt. v. 28.11.1975, NJW 1976, 294 (294).
[25] *Habersack*, in: MüKo BGB, § 793 Rn. 5; dazu kritisch: *Casper*, in: *Leible*/*Lehmann*/*Zech*, S. 173 ff.; für eine Ablösung der Globalurkunde durch Wertrechte auch: *Habersack*/*Mayer*, WM 2004, 1678 (1678).

dung wird vor allem angeführt, dass Registereinträge nicht gemäß der sachenrechtlichen Vorschriften übertragen werden.[26] Diese Begründung leuchtet ein, da eine Analogie voraussetzt, dass die angestrebte Rechtsfolge überhaupt für den Tatbestand passt, auf den die Vorschriften analog angewendet werden sollen. Rechtsfolge der §§ 793 ff. BGB ist aber gerade, dass auch die verbriefte Forderung gemäß den Regeln des Sachenrechts übertragen werden kann.[27] So soll ein höherer Verkehrsschutz durch die Möglichkeit eines gutgläubigen Erwerbs erreicht werden.[28] Resultat ist eine höhere Verkehrsfähigkeit.

Das Argument lässt sich nicht auf *Token* übertragen. Denn nach der hier vertretenen Ansicht, werden Blockchain-Einträge gem. §§ 873 ff. BGB übertragen.[29] Voraussetzung ist neben der Einigung auch ein Publizitäts-Akt, die Eintragung in die Blockchain. Diesen Realakt kann der Verfügende ohne Mitwirkung einer buchführenden Stelle tätigen, während bei den bisher diskutierten Registereinträgen eine buchführende Stelle die Übertragung vornehmen muss, auch wenn dies automatisiert geschehen mag. Im Rahmen der §§ 873 ff. BGB genießt ein gutgläubiger Erwerber denselben Schutz wie im Falle eines Inhaberpapiers. Denn der gutgläubige Erwerb ist auch im Falle von abhandengekommen Sachen möglich. Während § 935 BGB hierfür explizit eine Gegen-Ausnahme regelt, enthalten §§ 892 f. BGB von vornherein keine Ausnahme für abhandengekommene Buchpositionen.

Die analoge Anwendung der §§ 793 ff. BGB würde also im Falle von *Token* zu einer Rechtsfolge führen, die mit der im Falle von Urkunden vergleichbar ist. Denn auch an *Token* besteht ein Recht, welches rechtsgeschäftlich nach den Regeln des Sachenrechts übertragen wird. Mit der Übertragung des *Token* beabsichtigen die Parteien auch den Übergang der *tokenisierten* Forderung. Das Recht aus dem *Token* folgt dann dem Recht am *Token*. Ebenso ist der umgekehrte Fall, dass das Recht am *Token* dem Recht aus dem *Token* folgt, analog § 952 BGB möglich.

Im Rahmen der §§ 793 ff. BGB bedarf die Urkunde schließlich gemäß § 793 Abs. 2 BGB der Unterzeichnung durch den Aussteller. Es genügt abweichend von § 126 BGB ein Faksimile. *Token* sind allerdings vom Emittenten in keiner Weise, auch nicht in Form eines Faksimile, unterschrieben. Das kommt schon mangels Körperlichkeit aus tatsächlichen Gründen nicht Betracht. Allenfalls denkbar wären digitale Signaturen. Die Frage der Unterzeichnung kann jedoch dahinstehen. Denn im Rahmen des § 807 BGB finden die §§ 793 Abs. 2, 798-806 BGB keine Anwendung.[30] Die Anwendbarkeit zumin-

[26] *Habersack*, in: MüKo BGB, Vor § 793 Rn. 37.
[27] *Habersack*, in: MüKo BGB, § 793 Rn. 29 ff.
[28] *Gursky*, S. 9; *Vogel*, in: BeckOGK BGB, § 793 Rn. 140; *Habersack*/*Ehrl*, ZfpW 2015, 312 (343).
[29] Siehe Fn. 1.
[30] *Habersack*, in: MüKo BGB, § 807 Rn. 15.

dest der §§ 793 Abs. 1, 794, 796 und 797 BGB ist somit in entsprechender Anwendung dieser Vorschrift auch ohne Unterzeichnung gewährleistet. Da es an einer Unterschrift fehlt, müssen *Utility Token* und *Debt Token* deshalb regelmäßig in entsprechender Anwendung des § 807 BGB als Inhaber-*Token* behandelt werden.

Vergleichbare Wertpapiere im Sinne des § 807 BGB sind etwa Eintrittskarten zu Sport- und Kulturveranstaltungen, sofern diese nicht namensgebunden sind, sowie Einzelfahrscheine im öffentlichen Nahverkehr.[31] Gleiches gilt für Gutscheine und Briefmarken, aber auch für Casino-Jetons.

Blockchain-Einträge sind somit mit Urkunden vergleichbar. Sofern also die weiteren Voraussetzungen der §§ 793 ff. BGB beziehungsweise des § 952 Abs.1 BGB gegeben sind, sind diese analog auf *Token* anzuwenden. Entscheidend sind hierfür die jeweiligen Vertragskonstellationen und Parteiabreden, hilfsweise die Umstände des Einzelfalls unter Einbeziehung der objektiven Interessenlage.

2. Ersterwerb von Token und in ihnen tokenisierter Rechte

Die Voraussetzungen für den Ersterwerb eines *Token* und dem repräsentierten Recht bestimmen sich nach dessen Rechtsnatur. Diese hängt maßgeblich von der Parteivereinbarung ab. Theoretisch könnte ein *Token*, wie bereits erwähnt, als Schuldschein im Sinne des § 952 Abs. 1 BGB ausgestaltet werden. Dies hätte zur Folge, dass das Recht am *Token* dem Recht aus dem *Token* folgt.[32] Eine selbstständige Verfügung über den *Token* wäre nicht möglich. Der erste Gläubiger wird also mit Vertragsschluss Inhaber der *tokenisierten* Forderung und mit Ausstellung des *Token* unverzüglich Inhaber dessen.

Der Emittent zielt im Rahmen des klassischen *ICO* jedoch darauf ab, zum Zwecke der gesteigerten Verkehrsfähigkeit – und damit in Parallele zu Wertpapieren – die *Token* als Inhaber-*Token* auszustellen. Eine Namensbindung spielt bei *Token* deshalb üblicherweise keine Rolle. Sie entsprechen daher regelmäßig Inhaberschuldverschreibungen, beziehungsweise – mit Blick auf die Absenz einer Unterschrift des Emittenten – Inhabermarken im Sinne des § 807 BGB.

Damit die §§ 793 ff., 807 BGB Anwendung finden, müssten die Parteien außerdem einen Begebungsvertrag geschlossen haben und aus dem *Token* müsste ein Leistungsversprechen an den Inhaber hervorgehen.

c) Begebungsvertrag

Analog zu den §§ 793 ff. BGB müssen Emittent und Erwerber im Rahmen der Ausstellung von *Token* einen Begebungsvertrag schließen. Indem dieser die schuldrechtliche

[31] *Schödel*, in: Dauner-Lieb/Langen, § 807 Rn. 4; *Marburger*, in: Staudinger, § 807 Rn. 5.
[32] *Gursky*, in: Staudinger § 952 Rn. 3, 17.

Forderung begründet und zugleich dem Erwerber die Inhaberschaft am *Token* verschafft, vereint er schuldrechtliche und dingliche Elemente in einem Vertrag.[33]

Der Vertrag kommt durch zwei übereinstimmende Willenserklärungen zustande. Dabei ist das Anbieten der *Token* im Rahmen des *ICO* durch den (späteren) Emittenten und das Einrichten eines *Smart Contracts* als Automatisierungsprozess im Hintergrund regelmäßig als *offerta ad incertas personas* zu klassifizieren.[34] Denn das Angebot richtet sich an jedermann, der die vom Aussteller geforderten Bedingungen – meist in Form der Zahlung eines Preises in Kryptowährung – erfüllt.[35] Dies ist vergleichbar mit dem Vertragsschluss beim Warenautomaten.[36] Dem kann eine Identitätsprüfung vorgeschaltet sein, durch die der Emittent gegebenenfalls *Know-Your-Costumer*-Regelungen erfüllt und aufgrund derer der Emittent erst Zugang zu der Blockchain gewährt.[37]

Die (konkludente) Willenserklärung des Erwerbers ist in der Überweisung der Kryptowährung zu sehen. Der Zugang ist regelmäßig nach § 151 BGB entbehrlich.[38]

d) Leistungsversprechen

Schließlich muss aus dem *Token* ein Leistungsversprechen hervorgehen. Der Emittent muss sich also im Rahmen des Begebungsvertrages dazu bereit erklärt haben, eine Leistungspflicht zu übernehmen. Gegenstand ist dementsprechend eine Leistung im Sinne des § 241 Abs. 1 BGB.

(1) Übernahme einer Leistungspflicht

Der Inhalt der repräsentierten Forderung entspricht – abhängig von der versprochenen Leistung – der Forderung aus einem Dienstvertrag (§§ 611 ff BGB), aus einem Werkvertrag (§§ 631 ff. BGB), aus einem Kaufvertrag (§§ 433 ff. BGB) oder aus einem Darlehensvertrag (§§ 488 ff. BGB).[39] Der Emittent wäre demnach jeweils Dienstleister, Werkunternehmer, Verkäufer oder Darlehensnehmer. Im Grundsatz lässt sich jede dieser schuldrechtlichen Forderungen *tokenisieren*. Der Anspruch des Emittenten auf Bereitstellung der vereinbarten Menge an Kryptowährung erfüllt der Erwerber unmittelbar durch Zahlung der Kryptowährung. *Tokenisiert* wird der Gegenanspruch des Erwerbers gegen den Emittenten, der sich beim *Utility Token* regelmäßig auf eine Dienst-

[33] *Marburger*, in: Staudinger, § 793 Rn. 14; *Gursky*, S. 19.
[34] Zur Situation bei Warenautomaten: *Kaulartz*/*Heckmann*, CR 2016, 618 (618); *Berger,* in: Jauernig BGB, § 929 Rn. 4.
[35] *Bork*, in: Staudinger § 145 Rn. 8.
[36] *Ellenberger*, in: Palandt, § 145 Rn. 7; *OLG Düsseldorf*, Urt. v. 16.10.1986, ZMR 1987, 328 (328).
[37] Interesse an einer Bonitäts-Prüfung dürfte regelmäßig nicht bestehen, da die Schuld des Erwerbers unmittelbar erfüllt wird.
[38] Vgl. Fn. 36.
[39] Zur schuldrechtlichen Einordnung von Verträgen mit Kryptowährungen als Entgelt siehe *Beck*/*König*, JZ 2015, 130 (130).

leistung, ein Werk oder ein Produkt, beim *Debt Token* auf Rückzahlung des Darlehensvertrages und dessen Verzinsung erstreckt. Der konkrete Inhalt des Leistungsversprechens ist regelmäßig Auslegungsfrage (§§ 133, 157 BGB).

(2) Verpflichtung gegenüber dem Inhaber

Weiterhin muss der Wille des Emittenten die Absicht umfassen, sich gegenüber jedem berechtigten Inhaber des *Token* verpflichten zu wollen. Dieser Wille muss aus dem Inhalt der Willenserklärung vor dem Hintergrund der Verkehrssitte ausreichend deutlich hervorgehen.[40] Ein *Token* ist aufgrund der Blockchain-Technologie einem einzelnen Benutzer zugeordnet. Dass mit dem *Token* gehandelt wird, ist durchaus üblich und in der Regel vertraglich gestattet. Außerdem kommt es dem Emittenten wohl nicht darauf an, an eine spezielle Person zu leisten, sondern vielmehr, von seiner Leistungspflicht frei zu werden, sobald er erfolgreich geleistet hat. Die Blockchain-Technologie gewährleistet dies, indem die exklusive Verfügungsmacht wiederum auf den Emittenten übergeht, sobald dieser geleistet hat.

3. Zwischenfazit

Die §§ 793 ff. BGB sowie der § 952 Abs. 1 BGB sind hinsichtlich der Urkundenähnlichkeit analog auf *Token* und in ihnen *tokenisierte* Rechte anwendbar. Die Vorlagepflicht sowie die Eigenschaft als Inhaber-*Token* haben zur Folge, dass *Token* regelmäßig als Schuldverschreibungen im Sinne der §§ 793 ff. BGB, beziehungsweise als Inhabermarke im Sinne des § 807 BGB, einzuordnen sind. Denkbar, aber bisher unüblich ist auch eine Ausgestaltung der *Token* als Schuldverschreibung analog § 952 Abs. 1 BGB.

VI. Weiterveräußerung von Token und in ihnen tokenisierter Rechte

Oft werden die *Token* nach Ausgabe auf Online-Marktplätzen oder vergleichbaren Plattformen gehandelt. Nachdem die ursprüngliche Ausgabe als Ersterwerb des *tokenisierten* Rechts erläutert wurde, ist nun ein Blick auf den Zweiterwerb zu werfen.

Für den Übergang der Forderung ist entscheidend, ob nach Parteivereinbarung das Recht aus dem *Token* dem Recht am *Token* folgen soll – wie bei Inhaberpapieren wie den Inhaberschuldverschreibungen gemäß §§ 793 ff. BGB – oder umgekehrt – wie bei Schuldscheinen gemäß § 952 Abs. 1 BGB.

1. Recht aus dem Token folgt Recht am Token

Bei Inhaberpapieren folgt das Recht aus dem Papier dem Recht am Papier.[41] Da auf Wertpapiere wie auf *Token* Sachenrecht Anwendung findet, gelingt die Übertragung

[40] *Marburger*, in: Staudinger, § 793 Rn. 7.
[41] *Oechsler*, in: MüKo BGB, § 929 Rn. 15.

der *tokenisierten* Forderung automatisch durch die Übertragung des *Token* nach den sachenrechtlichen Vorschriften der §§ 873 ff. BGB.[42]

Zwar ist eine separate Abtretung der schuldrechtlichen Forderung nach den §§ 398, 413 BGB wohl unabhängig vom *Token* möglich.[43] Aufgrund der Notwendigkeit der Vorlage dessen zur Rechtsausübung wird dem Zessionar jedoch die alleinige Abtretung der Forderung regelmäßig keinen Mehrwert bringen.

2. Recht am Token folgt Recht aus dem Token

Im Gegensatz dazu folgt bei Schuldscheinen das Recht am *Token* dem Recht aus dem *Token*.[44] Wird die Forderung schuldrechtlich nach den §§ 398, 413 BGB abgetreten, so folgt dem automatisch die Inhaberschaft am *Token* gemäß § 952 Abs. 1 BGB.[45]

Ebenso verhält es sich bei Rektapapieren. Diese sind Wertpapiere, die in der Urkunde eine namentlich benannte Person als berechtigt ausweisen. Bei wirksamer Abtretung der *tokenisierten* Forderung gemäß der §§ 398, 413 BGB wird zugleich das Recht am *Token* analog § 952 Abs. 2 BGB übertragen.[46] Rekta-*Token* spielen allerdings schon deshalb eine untergeordnete Rolle im Kontext der *Token*, weil die Ausweisung eines Namens oder einer dem Namen möglicherweise gleichgestellten eindeutigen Kennzeichnung des Erwerbers bei Ausgabe eines *Token* im Rahmen eines *ICO* bisher nicht stattfindet.

VII. Fazit

Auf *Utility Token* und *Debt Token* finden die §§ 793 ff. BGB beziehungsweise der § 952 Abs. 1 BGB analog Anwendung, weil Blockchain-Einträge mit Urkunden vergleichbar sind. Abhängig von der Rechtsnatur des *Token* wird dieser entweder nach sachenrechtlichen Vorschriften gemäß der §§ 873 ff. BGB übertragen, wobei in diesem Fall die *tokenisierte* Forderung automatisch der Inhaberschaft am *Token* folgt. Oder der Übergang des *Token* geschieht gemäß § 952 BGB und folgt damit dem Übergang der *tokenisierten* Forderung, der durch Abtretung gemäß §§ 398, 413 BGB erfolgt. Entscheidend sind dabei vor allem der Parteiwille sowie die Umstände des Einzelfalls unter Berücksichtigung der Verkehrssitte. Die Bewertung von *Equity Token* wird den Rechtsanwender vor weitere Herausforderungen stellen und verdient in der Zukunft besonderes Augenmerk.

---

[42] *Klinck* in: BeckOGK BGB, § 929 Rn. 28; *Gursky*, S. 9, 113.
[43] BGH Urt. v. 14.05.2013, NZG 2013, 903.
[44] *Klinck* in: BeckOGK BGB, § 929 Rn. 27.
[45] *Gursky* in: Staudinger § 952 Rn. 3, 17.
[46] *Gursky* in: Staudinger § 952 Rn. 5, 17.

Literaturverzeichnis

Antonopoulos, Andreas M., Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2. Aufl., Sebastopol 2015.

Beck/König, Bitcoin: Der Versuch einer vertragstypologischen Einordnung von kryptographischem Geld, JZ 2015, 130.

Gsell/Krüger/Lorenz/Reymann (Hrsg.), Beck-Online Großkommentar BGB (BeckOGK BGB), München 2018.

Borkert, Christian, Crowdfunding goes Blockchain – Teil 1, ITRB 2018, 39-43.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) – Initial Coin Offering: Hinweisschreiben zur Einordnung als Finanzinstrumente, Bonn 2018.

Bundesministerium für Finanzen (BMF), E-Mail v. 27.02.2018 – aufgerufen am 15.09.2018 unter: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2018-02-27-umsatzsteuerliche-behandlung-von-bitcoin-und-anderen-sog-virtuellen-waehrungen.pdf?__blob=publicationFile&v=1.

Dauner-Lieb/Langen (Hrsg.), BGB Schuldrecht Band 2, 3. Aufl., Baden-Baden 2016.

Dietsch, David, Umsatzsteuerliche Einordung von Initial Coin Offerings, MwStR 2018, 546-551.

Eidgenössische Finanzmarktaufsicht FINMA – Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICO), Bern 2018.

Eschenbruch /Gerstberger, Smart Contracts, NZBau 2018, 3-8.

Grau, Netzwoche, Artikel v. 20.06.2016 – Schweden integriert Blockchain beim Grundbuchamt, aufgerufen am 15.09.2018 unter: https://www.netzwoche.ch/news/2016-06-20/schweden-integriert-blockchain-beim-grundbuchamt.

Gursky, Karl-Heinz, Wertpapierrecht, 3. Aufl., Heidelberg 2007.

Habersack/Ehrl, Börsengeschäfte unter Einbeziehung eines zentralen Kontrahenten, ZfpW 2015, 312-349.

Habersack/Mayer, Globalverbriefte Aktien als Gegenstand sachenrechtlicher Verfügungen?, WM 2000, 1678-1684.

IBM, Pressemitteilung v. 22.08.2017 – IBM announces Major Blockchain Collaboration with Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane

Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide., aufgerufen am 15.09.2018 unter: https://www-03.ibm.com/press/us/en/pressrelease/53013.wss#release.

Kaulartz/Heckmann, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, 618-624.

Stürner (Hrsg.), Jauernig Bürgerliches Gesetzbuch (Jauernig BGB), 17. Aufl., München 2018.

Krüger/Lampert, Augen auf bei der Tokenwahl – privatrechtliche und steuerliche Herausforderungen im Rahmen eines Initial Coin Offering, BB 2018, 1154-1160.

Leible/Lehmann/Zech (Hrsg.), Unkörperliche Güter im Zivilrecht, Tübingen 2011.

Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251-1259.

Morris, UToday, Artikel v. 20.07.2018 – Italian Universtity to Register Degrees on Ethereum Blockchain, aufgerufen am 15.09.2018 unter: https://u.today/italian-university-to-register-degrees-on-ethereum-blockchain.

Säcker/Rixecker/Oetker/Limperg (Hrsg.), Münchener Kommentar zum BGB (MüKo), Band 6, 7. Aufl., München 2017.

Säcker/Rixecker/Oetker/Limperg (Hrsg.), Münchener Kommentar zum BGB (MüKo), Band 7, 7. Aufl., München 2017.

NewsBTC, Artikel v. 11.09.2018 – UK Meds Signs Deal with Stratis to Use Blockchain in Online Pharmacy Industry, aufgerufen am 15.09.2018 unter: https://www.newsbtc.com/2018/09/11/uk-meds-signs-deal-with-stratis-to-use-blockchain-in-online-pharmacy-industry/.

Nimfuehr, Artikel v. 03.12.2017 – Blockchain application land register: Georgia and Sweden leading, aufgerufen am 15.09.2018 unter: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c.

Palandt Otto (Begr.), Bürgerliches Gesetzbuch, 74. Aufl., München 2015.

SEC – Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Washington D.C. 2017.

SEC, Pressemitteilung v. 11.12.2017 – Statement on Cryptocurrencies and Initial Coin Offerings, zu finden unter: https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11#_ftn5.

J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, §§ 139-163, 13. Aufl., Berlin 2010.

J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, §§ 779-811, 13. Aufl., Berlin 2009.

J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, §§ 925-984, 13. Aufl., Berlin 2004.

Welzel/Eckert – Mythos Blockchain: Herausforderung für den öffentlichen Sektor, Berlin 2017.

Wilmoth, StrategicCoin, Artikel – 3 Types of ICO Tokens, aufgerufen am 15.09.2018 unter: https://strategiccoin.com/3-types-ico-tokens/.

Vogel/Müller/Luthiger/Ljubicic, ICO vs. IPO?, AG 2017, 333-334.