ZIS
Zeitschrift für Internationale Strafrechtsdogmatik
http://www.zis-online.com

AUSGABE 9/2020
S. 397 - 450
15. Jahrgang

Inhalt

ISSN
1863-6470

Einleitung zur ZIS-Sonderausgabe „Strafverfolgung und Digitalisierung in Wissenschaft und Praxis“

Von Prof. Dr. Dr. **Milan Kuhli**, Hamburg, Prof. Dr. **Janique Brüning**, Kiel

In der Februar-Ausgabe dieses Jahres veröffentlichte die ZIS unsere Sonderausgabe zum Thema „Strafrecht und Digitalisierung in Wissenschaft und Praxis“[1] mit Beiträgen von Prof. *Dr. Susanne Beck*, LL.M. (Universität Hannover), Prof. *Dr. Kai Cornelius* (Universität Heidelberg), Wiss. Mit. *Lasse Quarck* (Universität Kiel), LOStA PD *Dr. Ralf Peter Anders* (Universität Hamburg) sowie Rechtsanwalt *Dr. Frédéric Schneider* (Hamburg). Es war das Ziel der Initiatorin und des Initiators, mit der genannten Ausgabe Beiträge zusammenzuführen, die den Austausch zwischen Wissenschaftlerinnen und Wissenschaftlern sowie Praktikerinnen und Praktikern im Bereich des Strafrechts und der Digitalisierung widerspiegeln.

An diese Idee knüpft auch vorliegende Sonderausgabe an, die sich dem Thema „Strafverfolgung und Digitalisierung in Wissenschaft und Praxis“ widmet. Wie sich dem Titel dieser Ausgabe entnehmen lässt, liegt der Fokus dabei stärker auf der Strafverfolgung, wenngleich thematische Überschneidungen zwischen den Ausgaben nicht in Abrede zu stellen sind. Die Frage, welche Herausforderungen, Möglichkeiten, Grenzen oder Chancen sich aus der digitalen Transformation für den Bereich der Strafverfolgung ergeben, bildete den Gegenstand eines wissenschaftlichen Workshops, der im Januar 2020 von der Initiatorin und dem Initiator dieser Sonderausgabe an der Universität Hamburg veranstaltet wurde. Die vorliegende Sonderausgabe beinhaltet die schriftlichen Ergebnisse dieses Workshops.[2]

Akad. Rätin a.Z. *Dr. Georgia Stefanopoulou*, LL.M. (Universität Hannover) widmet sich in ihrem Beitrag den Grundzügen eines sog. „Kommunikationsstrafrechts“,[3] zu dessen Katalysatoren sowohl die Greifbarkeit als auch die Unkontrollierbarkeit der digitalen Kommunikation zählen; vor diesem Hintergrund beleuchtet *Stefanopoulou* mögliche Anpassungserfordernisse des strafprozessualen Grundsatzes in dubio pro reo. Wiss. Mit. *Hannah Ofterdinger* (Universität Hamburg) untersucht in ihrem Aufsatz die normativen und tatsächlichen Grundlagen und Grenzen einer algorithmenbasierten Strafzumessung.[4] Prof. *Dr. Stefan Harrendorf* (Universität Greifswald), *Pia Müller* (Universität Greifswald) und *Antonia Mischler* (Wiesbaden) befassen sich aus kriminologischer Perspektive mit politisch extremer Kommunikation in den Social Media.[5] Prof. *Dr. Manfred Heinrich* (Universität Kiel) widmet sich in seinem Beitrag strafprozessualen Ermittlungsmaßnahmen, die das Internetsurfen und das Cloud Computing zum Gegenstand haben.[6] Die Frage, ob der Einsatz von Lügendetektorsoftware im Strafprozess aufgrund des technischen Fortschritts in Zukunft rechtmäßig sein könnte, wird von Prof. *Dr. Sönke Gerhold* (Universität Bremen) in den Blick genommen.[7]

Die Veranstaltung des genannten Workshops sowie die Publikation der vorliegenden Beiträge wären nicht möglich gewesen, wenn wir nicht auf vielfältige Weise unterstützt worden wären. Hierfür möchten wir allen Beteiligten sehr herzlich danken. Dies gilt vor allem für die Autorinnen und Autoren, die die Publikation der Beiträge in inhaltlicher Weise erst möglich gemacht haben. Darüber hinaus danken wir dem Verbund Norddeutscher Universitäten, der die Durchführung dieses Projektes durch eine großzügige finanzielle Zuwendung unterstützt hat. Ein großer Dank gebührt schließlich auch den Teams unserer Lehrstühle, die uns bei der Durchführung der Veranstaltung und bei der Vorbereitung der Publikation wertvolle Hilfe geleistet haben. Herrn Prof. *Dr. Thomas Rotsch* möchten wir herzlich für die freundliche Bereitschaft danken, die vorliegenden Beiträge in einer ZIS-Sonderausgabe zu publizieren.

Den Leserinnen und Lesern wünschen wir eine anregende Lektüre!

[1] Vgl. zur Konzeption der genannten Sonderausgabe: *Kuhli/Brüning*, ZIS 2020, 39.
[2] Die schriftliche Fassung des Referats von LOStA PD *Dr. Ralf Peter Anders* wurde bereits in der ersten Sonderausgabe veröffentlicht (vgl. ZIS 2020, 70).
[3] *Stefanopoulou*, ZIS 2020, 398.
[4] *Ofterdinger*, ZIS 2020, 404.
[5] *Harrendorf/Müller/Mischler*, ZIS 2020, 411.
[6] *Heinrich*, ZIS 2020, 421.
[7] *Gerhold*, ZIS 2020, 431.

Grundzüge eines Kommunikationsstrafrechts: Materie, Prozess, in dubio pro reo

Von Akad. Rätin a.Z. Dr. **Georgia Stefanopoulou**, LL.M. (HU Berlin), Hannover

I. Strafrecht in vernetzten Gesellschaften

Als den „höchsten Gattungsbegriff" des Verbrechens, als „die oberste Einheit für alle Phänomene des Strafrechts" und als das „feste Knochengerüst" des Straftatsystems feiert *Gustav Radbruch* 1903 den Handlungsbegriff.[1] Auch heute noch gehört der Begriff der Handlung neben jenem der Zurechnung zu den Grundelementen des materiellen Strafrechts.[2] Diese Sichtweise lässt sich systematisch auf Theorien zurückführen, wonach menschliches Handeln das fundamentale „Letztelement" sozialer Systeme darstellt.[3] Dieser Auffassung steht eine kommunikationstheoretische Betrachtung gegenüber, die vor allem durch *Niklas Luhmanns* Gesellschaftstheorie Bekanntheit erlangt hat.[4] Kommunikation ist nach *Luhmann* der „basale Prozess sozialer Systeme", die allerdings als Handlung übersetzt bzw. getarnt wird, um die eigene Komplexität zu reduzieren.[5] Mit anderen Worten, Handlung stellt aus Gründen der Vereinfachung sozialer Interaktionen lediglich eine „Camouflage der Kommunikation"[6] dar.[7] Kommunikation lässt sich als Handlung beschreiben, damit sie als hypostasiertes Ereignis anschlussfähiger wird.[8] So scheint die Hypostasierung der Kommunikation durch Übersetzung in Handlungen, also in körperliches Verhalten,[9] der interessanterweise von *Radbruch* selbst in einem anderen Zusammenhang (nämlich seiner Kritik der naturhistorischen Methode) konstatierten Schwäche des Denkens Rechnung zu tragen, Immaterielles und Abstraktes aufzuarbeiten, ohne sich dabei stellvertretender Vorstellungen zu bedienen.[10]

Sollte die Neigung, an das Materiale anzuknüpfen, eine Schwäche des Denkapparats sein,[11] dürfte diese Schwäche in der heutigen vernetzten Gesellschaft allerdings weniger ausgeprägt sein als in der vordigitalen Zeit.[12] Die gegenwärtig sich dramatisch weiter evolvierende Netzgesellschaft ist eine der digitalen Kommunikation, die durch Virtualität und Mehrdimensionalität, insbesondere auch durch eine Abkoppelung von den physikalischen Grenzen von Zeit und Raum gekennzeichnet ist.[13] Digitale Kommunikation ist kontinuierlich und stellt ein allgegenwärtiges Phänomen dar.[14] Tweets, E-Mails, Blogs, gepostete Bilder und Selfies, Online-Chats werden andauernd produziert und sind wesentlicher Teil unserer sozialen Existenz sowie konstitutives Element unserer digitalen Kultur.[15] Damit erscheint *Luhmanns* Überzeugung, dass Kommunikationsprozesse das Fundament sind, auf dem die soziale Realität aufgebaut wird,[16] durch die Strukturen des sozialen Lebens im digitalen Zeitalter eine gewisse Bestätigung zu erfahren. Auf jeden Fall steht Kommunikation im Alltag der Netzgesellschaft expliziter, drastischer und offensichtlicher im Vordergrund als in der nichtdigitalen Welt der (in der Kommunikationswissenschaft häufig so genannten) „Gutenberg-Galaxis"[17]. Durch den globalen Siegeszug des Internets wurde Kommunikation bereits in ihrer Immaterialität greifbar und in ihrer Allgegenwärtigkeit sichtbar.

Sind Kommunikationen heute gesellschaftlich präsenter und die Gesellschaft unmittelbar prägender als in der nichtdigitalen Zeit (zum Teil spricht man sogar von einem kulturell nicht mehr beherrschbaren Kommunikations-Overflow),[18] dürfte es kaum überraschend sein, dass Kommunikationen auch eine größere Strafrechtsrelevanz erlangen. Hate Speech in sozialen Netzwerken, Internet-Mobbing, Fake News und Social Bots stellen Paradebeispiele für „entfesselte Kommunikation"[19] dar, die strafrechtliche Dimension erlangen kann. Internetbeleidigungen und Volksverhetzung im Netz und Social-Media-Plattformen stellen einen beträchtlichen Teil der Netzrealität dar.[20] Neben den Beleidigungsdelikten ist auch an Phänomene wie Sexting und Cyber-Grooming zu denken, also an sexuell motivierte Anbahnungskommunikation mit Minderjährigen. Kommunikation über Sexualität, darunter fällt vor allem die Pornografie, kann unter den technischen Bedingungen des Internets unkontrollierbare Auswirkungen entfalten.[21] Haben wir also vorher festgestellt, dass die Digitalisierung Kommunikationen greifbarer und

---

[1] *Radbruch*, Der Handlungsbegriff in seiner Bedeutung für das Strafrechtssystem, 1903, S. 71 f.
[2] *Ast*, Handlung und Zurechnung, 2019, S. 11.
[3] *Luhmann*, Soziale Systeme, 1987, S. 192.
[4] *Luhmann* (Fn. 3), S. 192.
[5] *Luhmann* (Fn. 3), S. 191 f; *Schuldt*, Systemtheorie. Theorie für die vernetzte Gesellschaft, 2017, S. 47 f.
[6] *Schuldt* (Fn. 5), S. 48.
[7] *Luhmann* (Fn. 3), S. 192; *Schuldt* (Fn. 5), S. 48.
[8] *Schuldt* (Fn. 5), S. 48.
[9] Allgemein zur Handlung als Körperverhalten siehe *Ast* (Fn. 2), S. 15.
[10] *Radbruch* (Fn. 1), S. 34 f., *Radbruch* setzt sich mit *Jherings* naturhistorischer Methode auseinander. Zu *Jherings* naturhistorischer Methode, siehe *Kroppenberg*, Die Plastik des Rechts, Sammlung und System bei Rudolf v. Jhering, 2015, S. 17 ff.
[11] So *Radbruch* (Fn. 1), S. 34.
[12] Vgl. *Meinel/Sack*, Digitale Kommunikation, Vernetzen, Multimedia, Sicherheit, 2009, S. 12.
[13] *Meinel/Sack* (Fn. 12), S. 12.
[14] *Meinel/Sack* (Fn. 12), S. 12; *Stalder*, Kultur der Digitalität, 4. Aufl. 2019, S. 137.
[15] *Stalder* (Fn. 14), S. 137.
[16] *Luhmann* (Fn. 3), S. 193.
[17] *Stalder* (Fn. 14), S. 9, der Begriff stammt ursprünglich von McLuhan, The Gutenberg-Galaxy – The Making of Typographic Man, 1962.
[18] *Schuldt* (Fn. 5), S. 102.
[19] *Schuldt* (Fn. 5), S. 102.
[20] Eine Entwicklung, die schon am Anfang der Nuller-Jahre festgestellt wurde, siehe *Sieber*, ZRP 2001, 97; vgl. auch *Bremer*, MMR 2002, 147.
[21] *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 67. Aufl. 2020, § 184 Rn. 25, der allerdings auch zu Recht auf die teilweise irrationale Angstverbreitung hinsichtlich der Gefahren der digitalen Kommunikation hinweist.

sichtbarer macht, stellen wir nun fest, dass die Digitalisierung Kommunikation zugleich entfesselt und unkontrollierbar macht. Greifbarkeit und Unkontrollierbarkeit der digitalen Kommunikation stellen die entscheidenden Katalysatoren für die Entwicklung eines, wie ich hier sagen möchte, *Kommunikationsstrafrechts* dar.

Mit der Einführung dieses Terminus ist keine grundsätzliche Abkehr vom Handlungsbegriff als dem Ausgangspunkt des Straftatsystems − oder in *Radbruchs* Worten – als dem „festen Knochengerüst“[22] der Verbrechenslehre beabsichtigt. Kommunikationsstrafrecht soll nicht generell an die Stelle des in unserem strafrechtwissenschaftlichen Bewusstsein fest verankerten Handlungsstrafrechts treten, sondern als spezielle Bezeichnung jenes Phänomenbereichs fungieren, bei dem das Moment der Kommunikation vor allem wegen der besonderen technischen, „digitalen“ Rahmenbedingungen explizit und greifbar im Vordergrund steht, so dass seine „Zerlegung“ in einzelne Handlungen[23] nicht nur nicht nötig, sondern sogar wenig geeignet für die Bestimmung der angemessenen Reichweite der Strafbarkeit ist. Sieht man z.B. im Falle des Cyber-Groomings die Kommunikation als zentrales Moment des deliktischen Vorgangs, erkennt man das Hauptproblem, das die lange kontrovers diskutierte Einführung einer Versuchsstrafbarkeit in vielen Fällen mit sich bringen kann,[24] nämlich die Unbestimmtheit hinsichtlich des unmittelbaren Ansetzens. Versuchte Kommunikation im Sinne von § 176 Abs. 6 StGB könnte so wenig bestimmbar und nachweisbar sein wie eine versuchte (und deswegen straflose) Beleidigung, da sie stark absichtsabhängig ist. Der strafbare Kommunikationsversuch erscheint schneller als der Versuch einer Handlung, die dafür eher Anhaltspunkte bietet (oder zu bieten scheint), im kritischen Licht des Vorwurfs, auf ein Verdachts- oder Gesinnungsstrafrecht hinauszulaufen.[25] Die Auffassung des Delikts im üblichen handlungsbezogenen Vokabular kaschiert in gewissem Maße die Konturlosigkeit eines Kommunikationsversuchs und verleitet, wenn nicht zu dogmatischen Fehlern, so doch womöglich zu kriminalpolitischen.

Unter dem Begriff „Kommunikationsstrafrecht“ soll eine Reihe von Delikten, die bisher durch die Begriffe „Computer-, Internet- oder Informationsstrafrecht“[26] erfasst wurden, zusammengeführt und durch die Entwicklung von allgemeinen, die einzelnen Delikte übergreifenden Prinzipien systematisch aufgearbeitet werden. Als gemeinsamer Bezugspunkt der Merkmale und der Erscheinungsformen der Straftaten soll das Moment der digitalen Kommunikation fungieren.[27] Maßgebend für die Leistungsfähigkeit eines Kommunikationsstrafrechts ist die Ausarbeitung eines strafrechtlichen Kommunikationsbegriffs – als Äquivalent zum strafrechtlichen Handlungsbegriff −, der sich an ein allgemeines Kommunikationskonzept anknüpfen lässt.[28]

II. Intransparente digitale Kommunikation und Strafverfahrensrecht

Die Entstehung des neuen Rechtsgebiets „Kommunikationsstrafrecht“, das hier in seinen Grundzügen lediglich angedeutet wird – die Ausarbeitung dieses Rechtsgebiets stellt ein größeres Unterfangen dar und ihm soll eine eigene Untersuchung gewidmet werden −, ist nicht das einzige Unternehmen, das die Digitalisierung der Gesellschaft und die „Besonderheit vernetzter Interaktionen“[29] nahe legen. Den Besonderheiten digitaler Kommunikation sollte auch das Strafverfahrensrecht angepasst werden. In diesem Zusammenhang bilden vor allem die Intransparenz, die Undurchschaubarkeit und Unberechenbarkeit der digitalen Kommunikation den Ausgangspunkt für Überlegungen zur Anpassung und Änderung.[30] In seinem Spätwerk „Die Gesellschaft der Gesellschaft“ schrieb *Luhmann* 1997 „[d]ie Autorität der Quelle mit all den erforderlichen sozialstrukturellen Absicherungen […] wird entbehrlich, ja durch Technik annulliert und ersetzt durch die Unbekanntheit der Quelle“.[31] Wie Recht *Luhmann* hatte, kann man heute in zweierlei Hinsicht feststellen: erstens in der durch Algorithmen ermöglichten Mensch-Computer-Kommunikation,[32] hier erzeugen Kalküle und Rechenvor-

[22] *Radbruch* (Fn. 1), S. 72.
[23] *Luhmann* (Fn. 3), S. 193.
[24] Zur Diskussion statt vieler *Dessecker*, KriPoZ 2019, 282.
[25] Abgesehen davon, dass schon die Strafbarkeit des vollendeten Delikts stark auf die Gesinnung des Täters abstellt. In Abkehr von der Regel, dass Vorbereitungshandlungen straflos sind, wird im Rahmen des § 176 Abs. 4 Nr. 3 StGB wegen der verwerflichen Absicht des Täters, später eine Straftat zu begehen, d.h. hier, das Kind später zu sexuellen Handlungen zu bringen, eine Vorbereitungshandlung bestraft, vgl. *B. Heinrich*, KriPoZ 2017, 4, in seiner treffenden Kritik zum heutigen Zustand der Kriminalpolitik in Deutschland; ähnlich *Lederer*, LTO v. 3.12.2019, abrufbar unter https://www.lto.de/recht/hintergruende/h/cybergrooming-sexualstrafrecht-internet-kinder-vorbereitung-versuch-strafbarkeit/ (2.9.2020); vgl. auch *Fischer* (Fn. 21), § 176 Rn. 15, der zu Recht darauf hinweist, dass der Tatbestand Vorbereitungshandlungen erfasst, die als solche von außen nicht erkennbar sind; vgl. *Renzikowski*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 3. Aufl. 2017, § 176 Rn. 54.
[26] Siehe *Eisele*, Computer- und Medienstrafrecht, 2013; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 3. Aufl. 2020.
[27] Vgl. zum Handlungsbegriff *Ast* (Fn. 2), S. 11.
[28] Vgl. zum Handlungsbegriff *Ast* (Fn. 2), S. 11.
[29] *Beck*, in: Fischer/Hoven (Hrsg.), Schuld, 2017, S. 289.
[30] Zur Intransparenz der Kommunikation s. *Schuldt* (Fn. 5), S. 100.
[31] *Luhmann*, Die Gesellschaft der Gesellschaft, 1997, S. 309; siehe dazu auch *Schuldt* (Fn. 5), S. 100; von Quellen der Unbestimmtheit in der technisierten Gesellschaft spricht *Bruno Latour*, *Latour*, Eine neue Soziologie für eine neue Gesellschaft, 2007, S. 50 ff.
[32] In der Kommunikationswissenschaft bildet Algorithmizität eine von drei Merkmalen der digitalen Kultur, *Stalder* (Fn. 14), S. 13; allgemein zu den Besonderheiten der Mensch-Computer-Kommunikation *Röhner/Schütz*, Psychologie der Kommunikation, 2. Aufl. 2016, S. 110 f.

gänge unbestimmter Herkunft[33] neue Formen von Kommunikationsrealitäten, zweitens in der Anwendung von Verschlüsselungstechnologie zur Anonymisierung der IP-Adressen von Kommunikationspartnern sowie zur Chiffrierung von Nachrichten in komplexen Kryptosystemen.[34]

1. Neujustierungen des Zweifelsgrundsatzes

Anpassungsversuche des Strafverfahrensrechts angesichts dieser Intransparenz und Undurchschaubarkeit digitaler Kommunikation sind in den letzten Jahren bereits unternommen worden. Die bisher eingeführten Änderungen des Strafverfahrensrechts orientieren sich allerdings hauptsächlich an dem Ziel der effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrensrechts.[35] Die Anonymisierung der Quelle der Kommunikation und ihres Inhalts stellt die Verfolgung von Straftaten im Internet vor große Herausforderungen.[36] Darknet und Dark-Messenger dienen nicht nur als Foren für Whistleblower und politisch Verfolgte in autoritären Regimen, sondern bilden auch abgeschottete Bereiche des Internets, in denen kriminelle Foren entstehen können und Ermittlungen der Strafverfolgungsorgane erschwert sind.[37] Vor diesem Hintergrund sind neue Eingriffsmaßnahmen wie die Online-Durchsuchung und die Quellen-TKÜ eingeführt worden, damit verdeckte und mit technischen Mitteln praktizierte Kriminalität effektiv mit denselben Mitteln bekämpft wird, d.h. auch verdeckt und mit dem Einsatz von Technik.[38] Die Unbestimmtheit und Intransparenz der digitalen Kommunikation hat also bisher lediglich als Legitimation für die Erweiterung der Ermittlungsbefugnisse fungiert.

Damit sind sie in ihrer Relevanz für grundlegende Änderungen des Strafverfahrensrechts bislang nur verkürzt oder einseitig (eben aus der Ermittlungsperspektive) wahrgenommen worden. Pseudonyme, Passwörter, Verschlüsselungen und Anwendung von virtuellen Kryptowährungssystemen können oft zu Beweisschwierigkeiten führen. Außer der Kryptografie und der Verschlüsselungstechnik verstärken die Abwesenheit von raum-zeitlichen Face-to-Face-Interaktionen[39] sowie der ubiquitäre Zugang zum Internet die Intransparenz der digitalen Kommunikation und können Zweifel hinsichtlich der Sachlage und der Kommunikationsquelle auslösen. Vor diesem Hintergrund beschränkt sich die Bedeutung von Unbestimmtheit und Intransparenz digitaler Kommunikation nicht auf den Bereich der Überwachungsbefugnisse, sondern erstreckt sich auch auf den Bereich der Urteilsfindung und konkreter auf den Bereich der Anwendung des Zweifelssatzes. Führen Anpassungen der Ermittlungs- und Überwachungsmethoden an die Besonderheiten der digitalen Kommunikation zur Intensivierung von Eingriffen in die Grundrechte von Verdächtigen einerseits, können andererseits Änderungen im Bereich der Anwendung des Zweifelgrundsatzes zur Stärkung der Rechtsposition des Beschuldigten führen. Der Grundsatz „in dubio pro reo" könnte zu einem wichtigen Sicherungssystem aufgebaut werden, das einen gewissen (und aus Fairnessgesichtspunkten auch gebotenen) Ausgleich für die auf Ermittlungsebene stattfindenden Eingriffsintensivierungen bietet.[40]

Drei verbreitete Auffassungen hinsichtlich der Reichweite des Zweifelsgrundsatzes im Strafprozess sollten in diesem Zusammenhang überdacht werden: erstens die These, dass der in dubio pro reo-Grundsatz für einzelne Indizien nicht in Betracht kommt,[41] zweitens die Auffassung, dass der in dubio pro reo-Grundsatz bei unerreichbaren Beweismitteln keine Anwendung findet[42] und drittens die Auffassung, dass der in dubio pro reo-Grundsatz bei Verfahrensfehlern der Ermitt-

[33] *Baecker*, Studien zur nächsten Gesellschaft, 2007, S. 18.

[34] Zur Verschlüsselungstechnologie und Kryptografie siehe *Meinel/Sack* (Fn. 12), S. 314; zur Verschlüsselungstechnologie im Darknet *Rückert*, Politische Studien 69 (2018), 12.

[35] Siehe dazu *Freiling/Safferling/Rückert*, JR 2018, 9.

[36] Weitere Schwierigkeiten bei der Verfolgung der Straftäter entstehen durch den Auslandsbezug der Straftaten im Internet, dazu *Sieber* (Fn. 20), S. 98.

[37] *Krause*, NJW 2018, 678 f.; siehe auch Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen, BR-Drs. 443/19, S. 1. Die anonyme und verschlüsselte Kommunikation kann vor einem staatlichen Panoptismus schützen und die Bewahrung der Intimsphäre gewährleisten, empirische Untersuchungen zeigen allerdings, dass ein großer Teil der Websites im Darknet strafrechtsrelevant ist, so *Bachmann/Arslan*, NZWiSt 2019, 241 (242) mit weiteren Hinweisen; siehe auch hinsichtlich des Rechtsradikalismus den Bericht von *Röhlig*, bento v. 19.9.2019, abrufbar unter https://www.bento.de/politik/rechtsextreme-auf-telegram-warum-der-messenger-bei-identitaeren-und-neonazis-beliebt-wird-a-bc1b4560-9a92-4a8b-b718-c1455ae76df1 (2.9.2020); ausführlicher zu den Strafverfolgungsschwierigkeiten *Safferling/Rückert*, in: Konrad-Adenauer Stiftung – Analyse & Argumente, 2018, S. 1 f; *Rückert* (Fn. 34), S. 12 ff.

[38] In diesem Zusammenhang ist die Rede von einer „Waffengleichheit mit den Cyber-Kriminellen", *Rückert* (Fn. 34), S. 19. Ausführlich zu den neuen Maßnahmen *Freiling/Safferling/Rückert* (Fn. 35), S. 9 ff.

[39] Zu den Unterschieden zwischen Face-to-Face/direkter Individualkommunikation und digitaler Kommunikation siehe *Röhner/Schütz* (Fn. 32), S. 107 ff.

[40] Zur Kompensation „staatliche[n] Informationsvorsprung[s]" nach intensiven verdeckten Ermittlungen durch den Aufbau von Sicherungssystemen *Beulke/Swoboda*, Strafprozessrecht, 14. Aufl. 2018, Rn. 232.

[41] BGHSt 36, 286 (289 ff.); BGH NStZ 2001, 609; *Schmitt*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, Kommentar, 63. Aufl. 2019, § 261 Rn. 29; *Beulke/Swoboda* (Fn. 40), Rn. 490; *Zopfs*, Der Grundsatz „in dubio pro reo", 1999, S. 277; *Walter*, JZ 2006, 340 (347 f.); *Volk*, NStZ 1983, 422 (424); *Stree*, JZ 1974, 299; *Grünwald*, in: Barth (Hrsg.), Festschrift für Richard M. Honig zum 80 Geburtstag 3. Januar 1970, 1970, S. 53 (65 f.); *Schwabenbauer*, Der Zweifelsgrundsatz im Strafprozessrecht, 2012, S. 60.

[42] BGHSt 49, 112 (122 f.); *Walter* (Fn. 41), S. 349; *Schwabenbauer* (Fn. 41), S. 64.

lungsbehörden oder des Tatgerichts nicht gilt.[43] Während die Nichtanwendung des Zweifelssatzes bei Verfahrensfehlern immer wieder der Kritik[44] ausgesetzt ist, hat die erste Annahme bezüglich der Indiztatsachen und der unerreichbaren Beweismittel bisher wenig Widerspruch[45] erfahren. Beide Thesen wurzeln in demselben fest etablierten Gedanken, dass der Zweifelsgrundsatz keine Beweiswürdigungsregel ist, sondern lediglich eine Entscheidungsregel.[46] Eine Abkehr von beiden Thesen verlangt ein radikales Umdenken, was die Verortung des in dubio pro reo-Grundsatzes innerhalb der Urteilsfindung betrifft. Dies soll hier an der Problematik von Behauptungen gezeigt werden, die sich auf Indizien beziehen, d.h. auf Tatsachen, die einen Schluss auf sog. Haupttatsachen zulassen.[47]

2. Der in dubio pro reo-Grundsatz bezüglich einzelner Indizien

Vor dem Hintergrund des ubiquitären Zugangs zum Internet und der Omnipräsenz digitaler Kommunikationstechnik kann man beispielhaft an folgende Konstellation denken: Der Angeklagte behauptet, dass er nicht allein Zugang zu dem von den Ermittlungsbehörden mit einer Spähsoftware (Staatstrojaner)[48] infiltrierten Rechner hatte. Sein Behaupten wird von ihm glaubhaft substantiiert, aber trotz umfassenden Aufklärungsversuchs lässt sich das Behauptete weder ausschließen noch erweisen. Es bleibt mit Zweifeln behaftet. Nach herrschender Auffassung wäre der in dubio pro reo-Grundsatz in diesem Fall nicht anwendbar. Wäre in dubio pro reo hier anwendbar − so die Begründung −, würde etwas Ungewisses und nur Wahrscheinliches unberechtigterweise als wahr unterstellt.[49] Man fragt sich allerdings, wie dieses Argument mit der Wahrunterstellung beim Beweisantrag nach § 244 Abs. 3 S. 2 StPO als „Vorwegnahme des Zweifelsgrundsatzes“[50] zu vereinbaren ist.[51] Es gilt nämlich nach herrschender Meinung beim Beweisantrag, dass Hilfs- oder Indiztatsachen als wahr unterstellt werden können.[52]

Auch mit der herrschenden Meinung, wonach belastende Indizien immer bewiesen sein müssen, damit sie der Urteilsfindung zugrunde gelegt werden dürfen,[53] lässt sich der Ausschluss des Zweifelsgrundsatzes bei nicht erwiesenen Tatschen nicht vereinbaren. Ein entlastender Umstand, der nicht erwiesen wird, ist in der Regel auch als belastendes Indiz formulierbar.[54] Man kann sagen, der Beschuldigte war möglicherweise nicht der einzige Nutzer des Rechners, man kann aber dasselbe auch aus der Perspektive des Beschuldigten negativ formulieren, etwa: der Beschuldigte war möglicherweise der einzige Nutzer des Rechners. Das Nichterwiesene ist nach beiden wertenden Richtungen offen. Eine fehlende Entlastung wird oft eine potenzielle Belastung einschließen, so dass eine Unterscheidung zwischen Entlastungs- und Belastungsindizien hinsichtlich der Anwendung des in dubio pro reo-Grundsatzes kaum zu überzeugen vermag.[55] Der Zweifelsgrundsatz sollte vielmehr auf alle Indizien anwendbar sein. Erst dadurch erfüllt der Grundsatz seine Hauptaufgabe, wie sie oft in der Literatur formuliert wird, dass „von mehreren Sachverhalten, die bei dieser Sachlage möglich erscheinen, für die Entscheidung von dem Sachverhalt ausgegangen [wird], der für den Angeklagten am günstigsten ist“.[56]

Schaut man sich die Aufgabe genauer an, „von mehreren möglichen Sachverhalten den günstigsten als Ausgangspunkt der Entscheidung auszuwählen“, stellt man Folgendes fest: Hierin kommt zuerst unweigerlich die Funktion des in dubio pro reo-Grundsatzes als Entscheidungsregel zum Ausdruck. Die Entscheidung bei Ungewissheit wird also erst ermöglicht, wenn der für den Beschuldigten günstigste Sachverhalt fest-

[43] *Schmitt* (Fn. 41), § 136a Rn. 33; *Kleinknecht*, NJW 1966, 1537 (1544).

[44] *Jahn*, Gutachten C zum 67. Deutschen Juristentag, 2008, C 108 f.; *Ambos*, StV 2009, 151; *Beulke/Swoboda* (Fn. 40), Rn. 143; *Michael*, Der Grundsatz in dubio pro reo im Strafverfahrensrecht, 1981, S. 7; *Lüderssen*, in: Kohlmann (Hrsg.), Festschrift für Ulrich Klug zum 70. Geburtstag, 1983, S. 527 (538); vgl. auch *Müller*, Behördliche Geheimhaltung und Entlastungsvorbringen des Angeklagten, 1992, S. 80.

[45] Kritisch *Tenckhoff*, Die Wahrunterstellung im Strafprozeß, 1980, S. 147 ff.; S. 150; *ders.*, JR 1978, 348 (349); *Herdegen*, NStZ 1984, 337 (342 ff.).

[46] So BGHSt 49, 112 (122 f.); BGH NStZ 2001, 609; *Schmitt* (Fn. 41), § 261 Rn. 26; *Schwabenbauer* (Fn. 41), S. 64; *Walter* (Fn. 41), S. 349; *Volk* (Fn. 41), S. 423.

[47] *Beulke/Swoboda* (Fn. 40), Rn. 405.

[48] Zu der Überwachung „laufender Kommunikation“ im Rahmen der Quellen-TKÜ mittels eines sog. Staatstrojaners ausführlich *Freiling/Safferling/Rückert* (Fn. 35), S. 6.

[49] *Walter* (Fn. 41), S. 348.

[50] *Herdegen* (Fn. 45), S. 340; *Grünwald* (Fn. 41), S. 65, der allerdings die Wahrunterstellung hinsichtlich Indiztatsachen ablehnt. Die Nichtanwendung des in dubio pro reo-Grundsatzes für Indiztatsachen bedeutet nach *Grünwald* die Unzulässigkeit der Wahrunterstellung entlastender Tatsachen (a.a.O., S. 65 f.). Diese Auffassung ist zwar konsequenter als die h.M., die einerseits die Wahrunterstellung von Indizien nach einem Beweisantrag als zulässig erachtet und andererseits die Anwendung des Zweifelssatzes bei Indizien generell ablehnt, sie stellt jedoch auf die unrichtige Prämisse ab, dass der Grundsatz in dubio pro reo innerhalb der Beweiswürdigung nicht gilt.

[51] Vgl. *Herdegen* (Fn. 45), S. 341.

[52] *Beulke/Swoboda* (Fn. 40), Rn. 447; *Herdegen* (Fn. 45), S. 341 m.w.H.

[53] *Beulke/Swoboda* (Fn. 40), Rn. 447; *Schmitt* (Fn. 41), § 261 Rn. 25 ff.; BGH StV 2007, 512 f.

[54] Vgl. *Volk* (Fn. 41), S. 424.

[55] So auch *Volk* (Fn. 41), S. 424, der allerdings aus der fehlenden Unterscheidung den Gegenschluss zieht. Der in dubio pro reo-Grundsatz sei generell auf Indizien nicht anwendbar, weder auf belastende noch auf entlastende.

[56] *Lüderssen/Jahn*, in: Erb/Esser/Franke/Graalmann-Scheerer/Hilger/Ignor (Hrsg.), Löwe/Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Bd. 1, 26. Aufl. 2007, Einl. Abschn. M Rn. 59.

gelegt wird.[57] Aber dies ist nicht die einzige Funktion des Grundsatzes, die hier impliziert wird, auch seine Rolle als Beweiswürdigungsregel kommt zum Ausdruck. Die Festlegung des Sachverhalts als Voraussetzung einer Entscheidung findet innerhalb der Beweiswürdigung statt und stellt ihr Ergebnis dar. Als Zwischenschritte zur Festlegung des Sachverhalts müssen die einzelnen Indizien bewertet werden und als einzelne *Teilsachverhalte* des gesamten Falles behandelt werden. Die richtige Anwendung des Zweifelsgrundsatzes auf das gesamte Ergebnis setzt dann die Anwendung des Prinzips auf die Teile des Gesamten, also auf die Zwischenschritte, voraus. Bleibt das Indiz ungewiss, greift schon an dieser Stelle der Zweifelsgrundsatz ein, damit der für den Beschuldigten günstigste *Teilsachverhalt* bestimmt wird, der wiederum in das gesamte Ergebnis einfließt. Was das hier verwendete Beispiel der Anzahl der Nutzer betrifft, sollte man bei Ungewissheit davon ausgehen, dass mehrere Nutzer Zugang zum Rechner hatten oder haben. Die Anwendung des in dubio reo-Grundsatzes beschränkt sich hier nur auf die Indiztatsache selbst und erfasst nicht die aus dem Indiz nur als Möglichkeit und auf keinen Fall zwingend abgeleitete Schlussfolgerung der fehlenden Täterschaft.[58] Die als wahr unterstellte Tatsache, dass der Beschuldigte nicht der einzige Nutzer des betreffenden Rechners ist, besagt noch nicht zwingend, dass seine Täterschaft ausgeschlossen ist. Die Anwendung des in dubio pro reo-Grundsatzes auf den Indizienbeweis als Teil des gesamten Beweiswürdigungsprozesses bedeutet nicht die Vorwegnahme seines Ergebnisses, sondern die konsequente Berücksichtigung des Rechtstaatsprinzips bezüglich aller Zwischenschritte auf dem Weg zur Urteilsfindung.[59]

Wie verhält es sich aber mit Indizien, aus denen sich ein zwingender Schluss auf eine unmittelbar entscheidungserhebliche Tatsache ergeben würde, wenn sie als wahr unterstellt würden? Der wegen Verstoßes gegen § 176 Abs. 4 Nr. 3 StGB Beschuldigte behauptet, dass ihm bei der Online-Kommunikation nicht bewusst war, dass es sich bei seinem Kommunikationspartner um ein reales Kind handelte. Er sei davon ausgegangen, dass er mit einem realitätsnah abgebildeten Avatar kommuniziert habe, also mit einer durch Algorithmen graphisch erzeugten künstlichen Figur.[60] Stimmte die Behauptung, wäre hier zwingend ein Tatbestandsirrtum anzunehmen, so dass auch eine Anwendung des Zweifelsgrundsatzes in diesem Fall gleich zum Vorsatzausschluss führen würde. Die Anwendung des Zweifelsgrundsatzes auf das Indiz für einen Tatbestandsirrtum (darauf bezieht sich die Behauptung des Angeklagten)[61] hätte hier eine unmittelbare Wirkung auf das Ergebnis der Gesamtwürdigung.

Hierin sieht die herrschende Meinung ein Voreingreifen in das Endergebnis der Beweiswürdigung.[62] Bedenkt man allerdings, dass die Beweiswürdigung des jeweiligen Indizes unter Berücksichtigung des gesamten Beweisstoffs erfolgt,[63] verliert der Vorwurf des Voreingreifens in der Gesamtwürdigung an Berechtigung. Wegen der „wechselseitigen Abhängigkeit der einzelnen Indiztatsachen“[64] nehmen Zweifel hinsichtlich Indizien, die eine zwingende Schlussfolgerung über entscheidungserhebliche Tatsachen zulassen, das Ergebnis eine Gesamtwürdigung nicht vorweg. Dies wäre nur der Fall, wenn die Gesamtwürdigung noch nicht stattgefunden hätte,[65] diese findet jedoch stets zugleich mit der Würdigung des einzelnen Indizes statt. Die Glaubwürdigkeit der Irrtumsbehauptung des Beschuldigten wird an der Gesamtheit des Beweismaterials gemessen.[66] Wird die Irrtumsbehauptung dann nicht widerlegt, ist das Gericht, nicht anders als nach der Gesamtwürdigung von Haupttatsachen, gezwungen, den in dubio pro reo-Grundsatz anzuwenden.[67]

Daher entfaltet die Unterscheidung von Zwischenergebnissen und Endergebnis der Beweiswürdigung ihren Sinn nur bei den Indizien, die nur einen möglichen Schluss zulassen, wie bei dem oben erwähnten Beispiel der Nutzerzahl.[68] Die Anwendung des Zweifelsgrundsatzes bei diesen Indizien soll dafür sorgen, dass in das Endergebnis kein aus rechtsstaatli-

[57] Vgl. *Volk* (Fn. 41), S. 423, der allerdings nur eine Sicherung der Rechtsentscheidung sieht ohne Festlegung des günstigsten Sachverhalts. Die tatsächliche Ungewissheit bleibe, eine Beweiswürdigungsregel enthalte der Grundsatz nicht: „sie gebietet nicht bei Zweifeln die günstige(re) Variante als sicher festzustellen“. Einzuwenden ist hierbei Folgendes: „In dubio pro reo“, so auch *Volk*, ist eine Fiktion. Die Rede von Wahrunterstellung entspricht genau dieser Funktion des Grundsatzes als Fiktion. Eine Wahrunterstellung ist eben keine Feststellung. Gegen eine Wahrunterstellung innerhalb der Beweiswürdigung ist aus logischem Gesichtspunkt nichts einzuwenden. Die Entscheidung, die Wahrunterstellung aus dem Bereich der Beweiswürdigung auszuschließen, ist eine normative Entscheidung, worauf *Volk* an anderer Stelle selber hinweist (S. 423), die von der Befürchtung motiviert wird, dass die freie richterliche Beweiswürdigung durch den Zweifelsgrundsatz bei den Zwischenschritten auf dem Weg zur Urteilsfindung stark einbüßen wird. Diese Sorge ist allerdings nicht gerechtfertigt, wenn man die „wechselseitige Abhängigkeit“ der Beweismittel (*Tenckhoff* [Fn. 45], S. 349) im Auge behält, die dazu führt, dass Glaubwürdigkeit der Irrtumsbehauptung des Beschuldigten an der Gesamtheit des Beweismaterials gemessen wird (dazu an späterer Stelle). Wenn die Beweiswürdigung mittels Wahrunterstellung ermöglicht wird, wird infolgedessen außerdem auch die Rechtsentscheidung gesichert, so dass eine klare Trennung zwischen Entscheidungs- und Beweiswürdigungsregel und eine klare Zuordnung des Grundsatzes gekünstelt wirken.

[58] *Tenckhoff* (Fn. 45), S. 349; *ders*. (Fn. 45), S. 150 ff.

[59] Zur Ableitung des in dubio pro reo-Grundsatzes aus dem Rechtsstaatsprinzip siehe *Schwabenbauer* (Fn. 41), S. 48.

[60] *Wittmer/Steinebach*, MMR 2019, 650 (651 f.).

[61] Ähnliches Beispiel bei *Walter* (Fn. 41), S. 347.

[62] *Volk* (Fn. 41), S. 424.

[63] *Tenckhoff* (Fn. 45), S. 349; *Herdegen* (Fn. 45), S. 341.

[64] *Tenckhoff* (Fn. 45), S. 349.

[65] Von einer nicht stattgefundenen Gesamtwürdigung geht *Volk* aus bei seiner Argumentation gegen die Anwendung des Grundsatzes auf Indizien, *Volk* (Fn. 41), S. 424.

[66] Vgl. *Tenckhoff* (Fn. 45), S. 349.

[67] *Tenckhoff* (Fn. 45), S. 349.

[68] Vgl. *Tenckhoff* (Fn. 45), S. 349.

cher Sicht bedenklicher Zwischenschluss einfließt. Jeder Teilaspekt des Sachverhalts soll bei Zweifeln in seiner für den Beschuldigten günstigsten Form bei der Festlegung des gesamten Sachverhalts berücksichtigt werden. Die Geltung des Zweifelsgrundsatzes für die Indiztatsache versagt dem Gericht, worauf bereits *Jörg Tenckhoff* hingewiesen hat, aus nicht widerlegten Tatsachen Folgerungen zum Nachteil des Angeklagten zu ziehen, die nicht erwiesen wurden.[69] Vor allem wird dadurch das Herunterspielen von Zweifeln bei der richterlichen Überzeugungsbildung erschwert. Ferner wird die Aufgabe des prozessualen Tatnachweises als Kompensation für tiefgehende staatliche Ermittlungsmethoden für die staatlichen Stellen erschwert.

3. Der in dubio pro reo-Grundsatz bezüglich unerreichbarer Beweismittel und Verfahrensfehler

Die Anwendung des in dubio pro reo-Grundsatzes bei Indiztatsachen stellt allerdings nicht die einzige Möglichkeit dar, um die Stellung des Grundsatzes innerhalb des Verfahrensrechts zu verstärken. Wie schon erwähnt, kommen noch weitere Möglichkeiten in Betracht, die allerdings hier nur angedeutet werden sollen. Entgegen der herrschenden Meinung sollte die Anwendung des Grundsatzes bei unerreichbaren Beweismitteln in Erwägung gezogen werden. Bleibt ein Beweismittel unerreichbar und ist dafür der Staat verantwortlich, weil er z.B. den Inhalt einer Akte geheim hält,[70] sollte man die Beweisbehauptung, wenn sie vom Beschuldigten stammt, zu seinen Gunsten als wahr unterstellen,[71] vor allem, wie *Klaus Lüderssen* angemerkt hat, wenn das Beweismittel das einzige ist, das die Behauptung erweisen könnte.[72] Auch bei Verfahrensfehlern der Ermittlungsbehörden sollte der Zweifelsgrundsatz gelten. Die h.M., wonach der volle Nachweis durch den Beschuldigten erbracht werden muss, ist zu überdenken.[73] Verfahrensfehler sind schwer nachweisbar.[74] Eine mittlerweile zunehmend verbreitete Gegenansicht verlangt zu Recht die Unverwertbarkeit des Beweismittels, wenn der Beschuldigte Umstände nachweist, die Anlass geben, an der Rechtmäßigkeit der Ermittlungsmethode zu zweifeln.[75]

III. Fazit

Zusammenfassend kann Folgendes festgehalten werden: Die Digitalisierung erfordert bestimmte Anpassungsleistungen des Strafrechts sowohl in materieller als auch in prozessualer Hinsicht. Im Mittelpunkt der grundlegenden Neujustierungen sollte jener Vorgang stehen, der in der heutigen Netzgesellschaft als konstitutives Moment sozialer Prozesse von zentraler Bedeutung ist: die Kommunikation. Dies würde für das materielle Strafrecht die Ausarbeitung eines strafrechtlichen Kommunikationsbegriffs bedeuten, der als Bindeglied zwischen Delikten fungieren könnte, die bisher durch die Begriffe „Computer- Internet- oder Informationsstrafrecht“[76] erfasst wurden und der sich auf die Anpassung herkömmlicher Zurechnungsstrukturen vereinheitlichend und systematisierend auswirken könnte.

In prozessualer Hinsicht ergibt sich unter anderem das Erfordernis einer Neujustierung des klassischen Grundsatzes „in dubio pro reo“. Undurchschaubare und unberechenbare digitale Kommunikation bedeutet Beweisambivalenzen, die sich zu Lasten des Beschuldigten auswirken können. Das Problem der „Unbekanntheit der Quelle“[77] digitaler Kommunikation hat bisher allerdings lediglich als Legitimation für die Erweiterung von Ermittlungsbefugnissen Berücksichtigung gefunden. Die Anpassung des Strafprozessrechts an die Eigenheiten digitaler Kommunikation verlief vor allem über eine Anpassung an die verdeckten und technischen Methoden der digitalen Kriminalität. Die Intransparenz der „entfesselten Kommunikation“[78] soll mit der Intransparenz der Ermittlungs- und Eingriffsmaßnahmen bekämpft werden. Eine Kompensation für den dadurch entstehenden staatlichen „Informationsvorsprung“[79] kann durch eine Verstärkung der Geltung des Zweifelsgrundsatzes im Prozessrecht hergestellt werden. Die Unbestimmtheit der Quelle liefert nicht einseitig den Grund für die Effektivierung der Ermittlungsinstrumente, sondern macht es erforderlich, auch den Bereich des prozessualen Tatnachweises noch stärker durch eine Inpflichtnahme des Staates im Sinne einer Zurückhaltung bei der Annahme von Wahrheiten auszugestalten.

[69] *Tenckhoff* (Fn. 45), S. 349; *ders.* (Fn. 45), S. 150.
[70] Zur Konstellation *Walter* (Fn. 41), S. 349.
[71] *Michael* (Fn. 44), S. 7; *Lüderssen* (Fn. 44), S. 538; vgl. auch *Müller* (Fn. 44), S. 80.
[72] *Lüderssen* (Fn. 44), S. 538; zur Auffassung von *Lüderssen* s. *Müller* (Fn. 44), S. 77 ff.
[73] *Jahn* (Fn. 44), 108 f.; *Ambos* (Fn. 44), 151; *Beulke/Swoboda* (Fn. 40), Rn. 143.
[74] *Jahn* (Fn. 44), 109; *Beulke/Swoboda* (Fn. 40), Rn. 143.
[75] *Jahn* (Fn. 44), 109; *Beulke/Swoboda* (Fn. 40), Rn. 143.
[76] *Eisele* (Fn. 26); *Hilgendorf/Valerius* (Fn. 26).
[77] *Luhmann* (Fn. 31), S. 309.
[78] *Schuldt* (Fn. 5), S. 102.
[79] *Beulke/Swoboda* (Fn. 40), Rn. 232.

Strafzumessung durch Algorithmen?

Von **Hannah Ofterdinger**, Hamburg*

I. Einleitung

In der heutigen Welt sind wir ständig mit Algorithmen[1] konfrontiert, die anhand über uns gesammelter Daten Präferenzen, Interessen oder Bewertungen errechnen. Dies reicht von vorgeschlagenen Suchergebnissen bei Google über Verkaufsangebote bei Amazon bis hin zu unserer Kreditwürdigkeit nach der Schufa.[2] Trotzdem wird dem justiziellen Einsatz von Computerprogrammen sowohl vonseiten der Praxis als auch vonseiten der Wissenschaft mit tiefer Skepsis begegnet. Hier wird vor allem auf Sicherheitsrisiken bei Computereinsätzen, Intransparenz der Rechenprozesse und mögliche Datenschutzverstöße hingewiesen.[3] Zudem wurde in der Vergangenheit eine Schematisierung und Mathematisierung der Strafzumessung immer wieder durch die Revisionsgerichte abgelehnt.[4] Dennoch zeigt sich wiederholt, dass sich Richterinnen und Richter an „Regelfallempfehlungen" oder „Strafmaßtabellen" orientieren.[5] Auch wird in empirischen Studien immer wieder deutlich, dass häufig unterschiedlich hohe Strafen bei Delikten mit gleichem Strafrahmen und vergleichbaren Tatumständen verhängt werden.[6] Würde es also nicht sinnvoll sein, solche „Bewertungen" von Fällen durch einen bundeseinheitlichen Algorithmus zu berechnen? Und könnte ein Algorithmus hier nicht eine legitime Hilfestellung anbieten? Dieser Beitrag soll Möglichkeiten und Grenzen des Einsatzes von Algorithmen in der Justiz beleuchten. Dabei sollen auch Fragen aufgeworfen werden, die sich bei der Programmierung und dem Einsatz eines Algorithmus im Strafprozess im Zusammenhang mit der Strafzumessung stellen können. Schließlich soll auch hinterfragt werden, ob die durchaus anzutreffende Skepsis und Kritik in Bezug auf bestimmte Aspekte gerechtfertigt ist.

Ein praktischer Anwendungsfall eines Algorithmus in der Justiz zeigt sich bei einem Blick über den Atlantik. In den USA werden bereits Algorithmen im Strafverfahren eingesetzt. Seit fast zwei Jahrzehnten nutzen Richterinnen und Richter Computerprogramme zur Bewertung der Rückfallwahrscheinlichkeit von Straftäterinnen und Straftätern.[7] In vielen US-Bundesstaaten werden diese Computerprogramme bei der Entscheidung über die Freilassung einer oder eines Untersuchungsgefangenen auf Kaution oder die vorzeitige Haftentlassung genutzt. In neun verschiedenen Bundesstaaten werden diese Computerprogramme auch während des Gerichtsverfahrens verwendet.[8] Die dabei eingesetzten Algorithmen zur Risikobewertung sind so programmiert, dass sie große Datenmengen über die kriminelle Vergangenheit und die Biografie sowie psychologische Informationen einer Straftäterin oder eines Straftäters verarbeiten und daraus einen Risikowert errechnen.[9] Je nach Einsatzbereich des Computerprogramms wird dieser Wert genutzt, um eine Entscheidung über die bedingte Haftentlassung, Rehabilitierungsmaßnahmen oder sogar die Bestrafung zu treffen.[10]

Die Verwendung solcher Computerprogramme stößt jedoch unter anderem deswegen auf Ablehnung, weil deren Funktion und Arbeitsweise oft nicht richtig bekannt sind oder durch Medienberichte nicht richtig dargestellt werden. So erschien auf der Website der Frankfurter Allgemeinen Zeitung erst letztes Jahr ein Artikel, in dem es hieß: „Sechs Jahre Haft für unerlaubtes Benutzen eines fremden Autos und mangelnde Kooperation mit der Polizei: Diese Strafe hatte Eric Loomis einem Algorithmus zu verdanken."[11] Ferner hieß es in der Überschrift „Algorithmen sprechen Recht".[12] Allerdings gab dieser Artikel weder die wirkliche Arbeitsweise des Algorith-

* Die *Verfasserin* ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Strafrecht und Strafprozessrecht einschließlich ihrer internationalen und historischen Bezüge der Universität Hamburg (Prof. *Dr. Dr. Milan Kuhli*).

[1] Die Verwendung der Begriffe „Algorithmen" oder „Computerprogramme" meint im Folgenden Software, die aus einer Reihe von Eingabewerten einen einzigen Wert berechnet, siehe *Zweig/Krafft*, in: Mohabbat Kar/Resa/Thapa/Basanta E.P./Parycek/Peter (Hrsg.), (Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, S. 204 (208).

[2] Vgl. zu weiteren Beispielen *Mohabbat Kar/Parycek*, in: Mohabbat Kar/Resa/Thapa/Basanta E.P./Parycek/Peter (Fn. 1), S. 7 f.

[3] Darstellung von Kritik und gute Lösungsvorschläge bei *Martini*, JZ 2017, 1017.

[4] Vgl. etwa nur BGH NJW 1987, 3014 (3015); BGH StV 2010, 480.

[5] *Eschelbach*, in: Satzger/Schluckebier/Widmaier (Hrsg.), Kommentar zum Strafgesetzbuch, 4. Aufl. 2018, § 46 Rn. 4.

[6] Siehe *Kudlich/Koch*, NJW 2018, 2762 (2763), mit Verweis auf *Kaspar*, Sentencing Guidelines vs. freies tatrichterliches Ermessen – Brauchen wir ein neues Strafzumessungsrecht?, Gutachten C zum 72. DJT, 2018, C 16 ff.

[7] New York State begann die Nutzung des COMPAS-Programms im Jahre 2001, vgl. *Angwin/Larson/Mattu/Kirchner*, Pro Publica, Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks, 2016, abrufbar unter https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (29.8.2020).

[8] *Angwin/Larson/Mattu/Kirchner* (Fn. 7).

[9] Siehe unter II.

[10] *Freeman*, Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis, North Carolina Journal of Law & Technology 18 (December 2016), 75.

[11] Frankfurter Allgemeine Zeitung Rhein-Main v. 11.6.2019, abrufbar unter https://www.faz.net/aktuell/rhein-main/algorithmen-werden-in-amerika-bei-gerichtsprozessen-genutzt-16230589.html (29.8.2020).

[12] Frankfurter Allgemeine Zeitung Rhein-Main v. 11.6.2019 (Fn. 11).

mus wieder noch stimmte die Aussage, der Algorithmus würde Recht sprechen.

Der Schwerpunkt dieses Beitrags liegt in der Diskussion der Frage, ob ausgewählte Strafzumessungsumstände des deutschen Rechts durch einen Algorithmus beurteilt werden könnten (III.). Zuvor soll jedoch ein Blick in die USA und auf das dort eingesetzte Programm geworfen werden (II.). Diese Betrachtung soll vor allem dazu dienen, die Programmierung und Arbeitsweise eines Algorithmus in der Strafjustiz zu skizzieren. Zuletzt sollen die eventuell zu bewältigenden Probleme im Rahmen der Programmierung und Anwendung eines Computerprogramms in Deutschland herausgearbeitet werden (IV.).

II. Die Berechnung der Rückfallwahrscheinlichkeit eines Straftäters – ein Blick in die USA

Bei der Bewertung der Rückfallwahrscheinlichkeit einer Straftäterin oder eines Straftäters kann unter anderem mit klinischen oder statistischen Methoden gearbeitet werden.[13] Während einem Menschen beide Methoden offenstehen, dürften die derzeit verwendeten Algorithmen prinzipiell nach der statistischen Methode arbeiten.[14] Bei der Erstellung eines Computerprogramms zur Bewertung der Rückfallwahrscheinlichkeit einer Straftäterin oder eines Straftäters wird auf zwei unterschiedlichen Stufen gearbeitet: Auf der ersten Stufe müssen eine Datenbasis geschaffen, Rückfallrisiken definiert und die Rückfallrisiken in ihrer Datenbasis identifiziert werden. Mithilfe dieser Informationen wird sodann ein Algorithmus kreiert, der Angaben zur Wahrscheinlichkeit eines Rückfalls liefern soll. Auf der zweiten Stufe muss dann eine Entscheidung darüber getroffen werden, wie die Ergebnisse des Algorithmus für den tatsächlichen Gebrauch in der Justiz wiedergegeben werden sollen.[15] Hier muss also bestimmt werden, wie die Daten und die Auswertung für den bewerteten Einzelfall für die jeweiligen Anwender dargestellt werden sollen.

Das in den USA eingesetzte Programm nennt sich „Correctional Offender Management Profiling for Alternative Sanctions“ oder kurz: COMPAS. Es wurde von der Firma Equivant (ehem. Northpointe) entwickelt, einem privatwirtschaftlichen Unternehmen, das nach eigenen Angaben „Werkzeuge“ für die Nutzung im Justizsystem anbietet.[16] Auch wenn die Firma nicht alle Informationen die Programmierung betreffend offengelegt hat, so sind doch einige grundlegende Informationen bekannt. Die Datenbasis oder Normgruppe bei COMPAS bildeten 7.381 Straftäterinnen und Straftäter. Entweder waren sie inhaftiert oder die Strafe bzw. der Strafrest waren zur Bewährung ausgesetzt.[17] Anhand dieser Normgruppe wurden verschiedene Kategorien identifiziert und in insgesamt 43 Skalenwerte eingeteilt.[18] Dabei wurden zum einen Risikofaktoren, zum anderen Hilfsbedarfe herausgearbeitet. Die jeweils möglichen Ergebnisse einer analysierten Person werden von COMPAS im konkreten Fall in 43 Balkendiagrammen dargestellt.[19] Die 43 Skalenwerte werden schließlich in eine Skala mit Werten von 1–10 übersetzt, wobei ein Wert von 1–4 als niedrig, 5–7 als mittel und 8–10 als hoch im Vergleich zu der Normgruppe eingestuft wird.[20] Die Werte geben also an, welchem Zehntel der Normgruppe die konkret bewertete Person ähnelt, also einer Personengruppe mit niedrigem, mittlerem oder hohem Rückfallrisiko, und fassen die ermittelten Skalenwerte zusammen. Dabei wurde nicht offengelegt, welches Gewicht den einzelnen Skalenwerten bei der Übersetzung in die Skala von 1–10 beigemessen wird. So ist nicht öffentlich bekannt, ob bestimmten Faktoren ein höheres Gewicht bei der Beurteilung des Rückfallrisikos gegeben wurde als anderen.[21]

Liegt der Richterin oder dem Richter die Prognoseentscheidung des Computerprogramms vor, muss sie oder er diese interpretieren und entscheiden, ob und wie diese in das konkrete Urteil einbezogen werden soll.[22] In ihrem Practitioners Guide weist Equivant darauf hin, dass das für die konkrete Person ermittelte Risiko relativ und immer im Vergleich zu der Normgruppe interpretiert werden muss.[23] Ferner stellt der Hersteller klar, dass die Fähigkeit zur zutreffenden Interpretation der Skalen erlernt werden muss und die verschiedenen Skalen auch in ihren wechselseitigen Beziehungen zueinander gesehen werden müssen.[24] Die von dem COMPAS-Programm ausgegebenen Risikowerte für die einzelnen Skalen werden aus der Biografie der oder des Beschuldigten und den Antworten auf 137 Fragen abgeleitet. Zusammengestellt werden die Angaben zum einen aus Polizeiakten und zum anderen aus Fragebögen, die von der oder dem Beschuldigten selbst ausgefüllt wurden.[25] Dabei wird ebenfalls getestet, ob die Antworten des Straftäters oder der Straftäterin der Wahrheit entsprechen können oder ob diese suspekt erscheinen.[26]

---

[13] *Sohn*, Angloamerikanische Untersuchungen zur Rückfälligkeit gewalttätiger Sexualstraftäter: Zwischenresultate einer Sekundäranalyse, Wiesbaden: Kriminologische Zentralstelle, 3. Aufl. 2007, S. 46 f.

[14] *John Howard Society of Alberta*, Offender Risk Assessment, 2000, S. 1 f., abrufbar unter https://www.johnhoward.ab.ca/document/offender-risk-assessment-2000/ (29.8.2020).

[15] *Eaglin*, Constructing Recidivism Risk, Emory Law Journal 67 (2017), 59 (64).

[16] Das Unternehmen selbst bezeichnet die entwickelten Programme als „tools“ vgl. „Über uns“ Website, abrufbar unter https://www.equivant.com/about-us/ (29.8.2020).

[17] *Equivant*, Practitioners Guide to Compas Core, 2019, S. 11, abrufbar unter https://www.equivant.com/practitioners-guide-to-compas-core/ (29.8.2020).

[18] *Equivant* (Fn. 17), S. 2.

[19] *Equivant* (Fn. 17), S. 3.

[20] *Equivant* (Fn. 17), S. 8.

[21] *Lischka/Klingel*, Wenn Maschinen Menschen bewerten, Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung – Arbeitspapier –, 2017, S. 9.

[22] *Lischka/Klingel* (Fn. 21), S. 9.

[23] *Equivant* (Fn. 17), S. 11.

[24] *Equivant* (Fn. 17), S. 4.

[25] *Lischka/Klingel* (Fn. 21), S. 9.

[26] Siehe zum Testverfahren *Freeman* (Fn. 10), S. 79 f.

Nicht grundlos wird der Einsatz von COMPAS und anderer Computerprogramme zur Bestimmung der Rückfallwahrscheinlichkeit in den USA kritisiert.[27] Eine Untersuchung von ProPublica, einer unabhängigen US-Nachrichtenorganisation, kam zu der Wertung, dass COMPAS zum einen unzuverlässig bei der Vorhersage zukünftiger Straftatbegehung sei und zum anderen Rassenunterschiede in seinen Ergebnissen aufweise.[28] Nach dieser Untersuchung wurden 61 % derjenigen Straftäterinnen und Straftäter, denen ein hohes Rückfallrisiko prognostiziert wurde, innerhalb von zwei Jahren nach der ersten Einstufung festgenommen – ein Wert, den die Autoren mit der Zuverlässigkeit eines Münzwurfs vergleichen.[29] Des Weiteren wies der Algorithmus in seiner damaligen Programmierung eine Tendenz auf, Schwarzen Straftäterinnen und Straftätern öfter fälschlicherweise ein hohes Rückfallrisiko zu prognostizieren als weißen. Nach den Autoren der Untersuchung wurden Schwarze Straftäterinnen und Straftäter fast doppelt so oft mit einem hohen Rückfallrisiko bewertet wie weiße.[30]

Auch wenn Equivant in seiner Antwort auf die Untersuchung deren Ergebnisse heftig bestritt,[31] so deutet die Untersuchung zumindest an, dass bestimmte Faktoren mittelbar die Einstufung des Rückfallrisikos beeinflussen können. Dies beginnt bereits bei der Bildung der Normgruppe. Hier bestand diese aus einem Personenkreis, der durch ein Gericht wegen einer Straftat verurteilt wurde. Dabei kann nicht ausgeschlossen werden, dass die jeweilige Richterin oder der jeweilige Richter bei ihrer oder seiner Urteilsfindung bestimmten Vorurteilen unterlegen ist. Auch wenn es sich nicht um offensichtliche rassistische oder sexistische Einstellungen handeln muss, so können doch genau solche Faktoren Richterinnen und Richter unterschwellig beeinflussen.

Ein weiteres Problem besteht in der Verzerrung der Falsifikation.[32] Diese tritt dann auf, wenn Richterinnen und Richter aufgrund der Risikoprognose des Computerprogramms eher zur Verhängung von Haftstrafen tendieren. Durch einen Gefängnisaufenthalt kann die Gefahr eines Rückfalles erheblich steigen, da Häftlinge in neue kriminelle Kontexte integriert und nach ihrer Entlassung auch häufig rückfällig werden.[33] Das eingesetzte Computerprogramm wird damit schließlich in seiner Einschätzung bestätigt, da die betreffende Person tatsächlich rückfällig geworden ist. Hier haben fälschlicherweise mit hohem Risiko bewertete Straftäterinnen und Straftäter kaum eine Möglichkeit zu beweisen, dass sie ohne die Verhängung einer Gefängnisstrafe nicht rückfällig geworden wären.[34]

Dieser Verzerrung kann nur dann entgegengewirkt werden, wenn zunächst eindeutig festgelegt wird, ob das Computerprogramm eher falsch-negative (fälschlicherweise mit niedrigem Risiko bewertete) oder falsch-positive (fälschlicherweise mit hohem Risiko bewertete) Ergebnisse liefern soll. Bereits bei der Programmierung muss also entschieden werden, ob es der Gesellschaft eher zuzumuten ist, dass Verurteilte während ihrer Bewährungszeit erneut Straftaten begehen, oder ob zum Schutze der Allgemeinheit jegliches Rückfallrisiko durch Haftstrafen minimiert werden soll.[35]

III. Ausgewählte Strafzumessungsumstände und deren Algorithmisierung

Die Strafzumessung ist bekanntlich die Bestimmung der Rechtsfolgen der Tat durch die Richterin oder den Richter.[36] § 46 StGB ist die zentrale Norm für die Strafzumessung durch das Gericht.[37] Sie benennt zunächst die Schuld als Grundlage der Strafzumessung (§ 46 Abs. 1 S. 1 StGB). Zudem sind die Umstände, die für und gegen die Täterin oder den Täter sprechen, durch das Gericht gegeneinander abzuwägen (§ 46 Abs. 2 S. 1, 2 StGB). Dabei bleibt das Gesetz jedoch unbestimmt, da es weder den Schuldbegriff noch die Art und Weise der Abwägung genauer definiert.[38] An dieser Stelle soll weder auf den Sinn und Zweck der Strafe bzw. auf den Begriff der Schuld eingegangen werden, noch kann im Einzelnen auf die durch das Gericht vorzunehmende Abwägung Bezug genommen werden. Hier bleibt nur grundsätzlich festzuhalten, dass die Regelung des § 46 StGB einen weiten Spielraum eröffnet, innerhalb dessen das Tatgericht im jeweiligen Einzelfall eine konkrete Strafe zu bestimmen hat.[39] Dieser Spielraum ist im Rahmen der Rechtsmittel auch nur eingeschränkt überprüfbar.[40]

---

[27] Insbesondere *Angwin/Larson/Mattu/Kirchner* (Fn. 7); *Israni*, The New York Times v. 26.10.2017, abrufbar unter https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html (29.8.2020), aber auch *Eaglin*, Emory Law Journal 67 (2017), 121.

[28] *Angwin/Larson/Mattu/Kirchner* (Fn. 7).

[29] *Angwin/Larson/Mattu/Kirchner* (Fn. 7).

[30] *Angwin/Larson/Mattu/Kirchner* (Fn. 7).

[31] Stellungnahme abrufbar unter https://www.equivant.com/response-to-propublica-demonstrating-accuracy-equity-and-predictive-parity/ (29.8.2020).

[32] Siehe auch *Lischka/Klingel* (Fn. 21), S. 10.

[33] *Lischka/Klingel* (Fn. 21), S. 9.

[34] *Lischka/Klingel* (Fn. 21), S. 9.

[35] Vgl. auch *Spielkamp*, Inspecting Algorithms for Bias, MIT Technology Review, 2017.

[36] *Horn/Wolters*, in: Wolters (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, Bd. 2, 9. Aufl. 2016, § 46 Rn. 2; *v. Heintschel-Heinegg*, in: v. Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar, Strafgesetzbuch, Stand: 1.2.2020, § 46 Rn. 1.

[37] *Eschelbach* (Fn. 5), § 46 Rn. 1; *Miebach/Maier*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 2, 3. Aufl. 2016, § 46 Rn. 1.

[38] *Streng*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 1, 5. Aufl. 2017, § 46 Rn. 19; *Eschelbach* (Fn. 5), § 46 Rn. 13, 189.

[39] *Kinzig*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 46 Rn. 68; *Miebach/Maier* (Fn. 37), § 46 Rn. 3.

[40] BGH NStZ-RR 2006, 340 (341) m.w.N.; *Eschelbach* (Fn. 5), § 46 Rn. 3, 12; *Miebach/Maier* (Fn. 37), § 46 Rn. 3; *Wenske*, in: Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2016, § 267 Rn. 387.

Insbesondere subjektive Komponenten sind unter Umständen wesentlich für die Entscheidungsfindung.[41] So kann etwa die subjektive Wahrnehmung der Richterin oder des Richters von der oder dem Angeklagten einen Einfluss auf die Entscheidungsfindung haben. Auch kann das äußere Erscheinungsbild, die Sprache oder das Verhalten der oder des Angeklagten die Entscheidung prägen.[42]

Zur Ermittlung des Maßes des konkreten Tatunrechts sowie der Höhe der Tatschuld zählt § 46 Abs. 2 S. 2 StGB beispielhaft Umstände auf, die je nach Lage des Falles zugunsten oder zulasten der oder des Angeklagten ins Gewicht fallen können. Bei den ersten vier handelt es sich um tatbezogene, während bei den letzten das Vorleben und Verhalten der Täterin oder des Täters die Bezugspunkte darstellen.[43] Im Folgenden soll anhand dreier beispielhaft gewählter Umstände untersucht werden, ob eine Bewertung dieser Aspekte möglicherweise auch mittels eines Algorithmus vollzogen werden könnte. Zudem wird kurz dargestellt, ob eine Bewertung des jeweiligen Umstandes durch einen Algorithmus überhaupt einen Vorteil erbringen würde. Die ausgewählten Umstände sind zunächst die wirtschaftlichen Verhältnisse der Täterin oder des Täters, die verschuldeten Auswirkungen der Tat sowie die Gesinnung, die aus der Tat spricht.

1. Wirtschaftliche Verhältnisse

Unter den wirtschaftlichen Verhältnissen der Täterin oder des Täters versteht man die finanziellen Verhältnisse der oder des Angeklagten zum Zeitpunkt der Verurteilung.[44] Dabei sind grundsätzlich Einkommen und Vermögen zu berücksichtigen, es können aber auch Schulden oder persönliche Verpflichtungen (z.B. gegenüber Angehörigen) bei der Ermittlung der wirtschaftlichen Verhältnisse berücksichtigt werden.[45] Die wirtschaftlichen Verhältnisse der oder des Angeklagten sind oft bei der Bemessung einer Geldstrafe von Bedeutung.[46] Dies gilt insbesondere bei Vermögens- und Steuerdelikten.[47] Darüber hinaus können die wirtschaftlichen Verhältnisse auch das Tatmotiv kennzeichnen, so dass auch die wirtschaftliche Lage zur Tatzeit Bedeutung erlangen kann. Besteht eine innere Beziehung zwischen der Tat und den wirtschaftlichen Verhältnissen, etwa weil eine Begehung aus wirtschaftlicher „Not“ erfolgte, können sie im Rahmen der Schuld relevant sein.[48] Die wirtschaftlichen Verhältnisse werden hier aber ambivalent beurteilt. So soll eine ungünstige wirtschaftliche Lage strafmildernd ins Gewicht fallen können.[49] Ob dagegen eine gute wirtschaftliche Lage, etwa bei der Begehung eines Vermögensdelikts, strafschärfend wirken kann, soll aber nach dem Einzelfall beurteilt werden.[50]

Ein Algorithmus kann hier durchaus die Rolle der Richterin oder des Richters übernehmen: eine schlicht mathematische Berechnung von Einkommen abzüglich aller Verpflichtungen. Im Rahmen der Familiengerichtsbarkeit werden bereits ähnliche Programme zur Berechnung des Versorgungsausgleichs eingesetzt.[51] Neben einer reinen Berechnungsaufgabe kann man einen Algorithmus aber auch mit weiteren Informationen „füttern“, wodurch er das Ergebnis der Berechnung in einen Kontext setzen kann. So wäre es etwa möglich abzubilden, ob das Einkommen der oder des Angeklagten über der Armutsgrenze liegt oder wie es sich im Verhältnis des Durchschnittseinkommens darstellt. Zudem könnte spezifischer ermittelt werden, ob das Einkommen am konkreten Wohnort zur adäquaten Lebensführung hinreichend ist. So können die errechneten wirtschaftlichen Verhältnisse konkret mit den durchschnittlichen Lebenshaltungskosten am Lebens- und Wohnort der oder des Angeklagten verglichen werden.

Sofern der Algorithmus aber neben einer schlicht mathematischen Berechnung zusätzlich eine Klassifikation und Bewertung der Daten vornehmen soll, stellt sich zwangsläufig die Frage, wer die dafür zu berücksichtigenden Kriterien festlegen darf. Zudem betont der BGH ausdrücklich eine fallbezogene Beurteilung der materiellen Lage der Täterin oder des Täters.[52] Eine fallbezogene Bewertung wird durch den Einsatz eines Algorithmus jedoch nicht per se ausgeschlossen. Hier ist hervorzuheben, dass der Algorithmus in keinem Fall die gesamte Beurteilung der Richterin oder des Richters ersetzen darf. Es sollen lediglich einheitliche Maßstäbe und Grundwertungen geschaffen werden. Ein Algorithmus kann unvoreingenommen und auch emotionslos schlicht Zahlen bewerten und diese in einen Kontext setzen. Für die Richterinnen und Richter kann auf diese Weise ein Hilfsmittel geschaffen werden, um die Angaben der oder des Angeklagten besser einordnen und besser bewerten zu können. Auf die Frage, wer die für einen Algorithmus zu berücksichtigenden Kriterien festlegen soll oder darf, soll am Schluss dieses Beitrages zurückgekommen werden.

2. Verschuldete Auswirkungen der Tat

Die verschuldeten Auswirkungen der Tat sind von zentraler Bedeutung für die Praxis der Strafzumessung bei Erfolgsdelikten.[53] Dabei können alle Arten von Folgen, wie materielle,

[41] *Eschelbach* (Fn. 5), § 46 Rn. 4; *Miebach/Maier* (Fn. 37), § 46 Rn. 4.
[42] *Miebach/Maier* (Fn. 37), § 46 Rn. 4.
[43] *Kühl*, in: Lackner/Kühl, Strafgesetzbuch, Kommentar, 29. Aufl. 2018, § 46 Rn. 33, 36.
[44] *Miebach/Maier* (Fn. 37), § 46 Rn. 245.
[45] *Streng* (Fn. 38), § 46 Rn. 73.
[46] *Kinzig* (Fn. 39), § 46 Rn. 37; *Streng* (Fn. 38), § 46 Rn. 73.
[47] *Kinzig* (Fn. 39), § 46 Rn. 38; a.A. *Horn/Wolters* (Fn. 36), § 46 Rn. 141.
[48] *Kühl* (Fn. 43), § 46 Rn. 39; *Horn/Wolters* (Fn. 36), § 46 Rn. 141; *Streng* (Fn. 38), § 46 Rn. 73.
[49] *Eschelbach* (Fn. 5), § 46 Rn. 159; *Kinzig* (Fn. 39), § 46 Rn. 38.
[50] *Kinzig* (Fn. 39), § 46 Rn. 38; a.A. *Horn/Wolters* (Fn. 36), § 46 Rn. 141, wonach das Unrecht in allen Fällen gleich zu werten sein soll.
[51] Hierzu krit. *Vogel*, FPR 2004, 242.
[52] BGH NStZ 1987, 450.
[53] *Streng* (Fn. 38), § 46 Rn. 57 m.w.N.

körperliche, seelische oder ideelle erheblich sein.[54] Dabei ist lediglich zu beachten, dass sie der Täterin oder dem Täter nur dann zur Last gelegt werden können, wenn sie zweifellos von ihr oder ihm verschuldet sind.[55] Ob nur diejenigen Tatfolgen, die ausdrücklich im jeweiligen Tatbestand genannt sind, oder darüber hinaus auch nicht ausdrücklich erfasste mögliche Folgen als verschuldet anzusehen sind, ist umstritten.[56] Dieser Streit soll hier jedoch weder diskutiert noch entschieden werden. Wenn im Folgenden von Auswirkungen oder Tatfolgen gesprochen wird, so meint dies zumindest die ausdrücklich vom jeweiligen gesetzlichen Tatbestand benannten Folgen.

Auf den ersten Blick erscheint die Annahme befremdlich, man könne die verschuldeten Auswirkungen der Tat durch einen Algorithmus auswerten lassen. Blicken wir jedoch in das Zivilrecht, so sehen wir, dass dort Tabellen zur Bestimmung von Schmerzensgeldsummen genutzt werden.[57] Dort wird aufgelistet, wie viel Schmerzensgeld in der Vergangenheit bei einer bestimmten Verletzung von einem Gericht zugesprochen wurde. Die Summen in der Tabelle sind also Ausdruck dessen, welche Gravität einer Verletzung und ihren Folgen in der Vergangenheit beigemessen wurde. Es erscheint also nicht fernliegend, das Ausmaß der Tat durch einen Algorithmus bestimmen zu lassen. So könnte ein Algorithmus beispielsweise in einer Weise programmiert werden, in der er Verletzungen als gering, mittel oder schwer einstuft. Auch kann der Algorithmus die gesamten Verletzungen der betroffenen Person im Zusammenhang bewerten, um eine vollständige Einschätzung zum Ausdruck zu bringen. Dabei könnten als Datenbasis sowohl vergangene Gerichtsentscheidungen als auch ärztliche Einstufungen oder Gutachten dienen.

An dieser Stelle ist hervorzuheben, dass es den Vorgaben des Gesetzgebers oder der Idee des Schuldstrafrechts widersprechen würde, wenn die Schadenshöhe die Strafzumessung streng determinieren würde.[58] Allerdings weist der BGH (insbesondere im Steuerstrafrecht) immer wieder darauf hin, dass ab einer gewissen Schadenssumme eine Geldstrafe nur noch in Ausnahmefällen in Betracht komme.[59] So bestehen also durchaus gewisse Bewertungsmaßstäbe, die Einfluss auf die Strafzumessung nehmen. Diese Bewertungsmaßstäbe in einen Algorithmus zu übersetzen, ist somit nur eine Frage der Datenbasis.

Auch hier bleibt jedoch anzumerken, dass ein Algorithmus die richterliche Bewertung nicht ersetzen kann und soll. Zum einen wird dies schon deswegen nicht möglich sein, weil die Auswirkungen immer im Kontext der jeweiligen Tat zu betrachten sind, zum anderen aber auch, weil das Ausmaß der Verletzungen oder die Schadenssumme eben nicht alleiniges Strafzumessungskriterium sein können. Algorithmen können hier aber eine relative Gleichheit schaffen. So verhält sich der Algorithmus indifferent zu der Frage, ob das Opfer in der Gerichtsverhandlung weint oder nicht, wenn es von seiner Schürfwunde am Knie erzählt. Denn eine Schürfwunde bleibt eben nur eine solche und ist auf einer Bewertungsskala geringer einzustufen als ein gebrochenes Bein. Ob und inwieweit emotionale Belastungen für die betroffenen Personen auch durch den Algorithmus einbezogen werden sollen, ist wiederum eine Frage der bei der Programmierung genutzten Datenbasis. Werden hier vergangene Gerichtsentscheidungen oder Gutachten genutzt, so werden zwangsläufig auch emotionale Belastungen in die Programmierung einfließen. Denn sowohl Richterinnen und Richter als auch Gutachterinnen und Gutachter werden bei der Bemessung von Verletzungen in der Regel von der (emotionalen) Schilderung der betroffenen Person beeinflusst sein.

3. Aus der Tat sprechende Gesinnung

Die Gesinnung, die aus der Tat spricht, ist losgelöst von der allgemeinen Gesinnung der Täterin oder des Täters zu betrachten.[60] Allerdings kann zu ihrer Feststellung auf die Persönlichkeit der Täterin oder des Täters zurückgegriffen werden.[61] Bei der Beurteilung ist eine klare Abgrenzung zu den Beweggründen und Zielen der Täterin oder des Täters kaum möglich.[62] So liefern die Beweggründe und Ziele in der Regel Kriterien für die Beurteilung der Gesinnung.[63] Die psychischen Hintergründe der Tat können sich auch bei der konkreten Ausführung zeigen, diese beeinflussen und insofern auch bei der Suche nach der Gesinnung heranzuziehen sein.[64] Dabei besteht jedoch auch schnell die Gefahr, dass moralisierende Erwägungen herangezogen werden, welche den Bestand des Urteils gefährden können.[65]

Die Frage, ob ein Algorithmus die Gesinnung einer Täterin oder eines Täters beurteilen oder bewerten könnte, führt zunächst zu der Frage, wie (Tat-)Gesinnung genau zu definieren ist. Im Duden wird sie als geistige und sittliche Grundeinstellung eines Menschen umschrieben.[66] Die Synonyme umfassen Anschauung, Ansicht, Auffassung, Einstellung, Geisteshaltung, Überzeugung, Vorstellung, Weltbild, Ethos und

[54] *Kinzig* (Fn. 39), § 46 Rn. 26; *Miebach/Maier* (Fn. 37), § 46 Rn. 214; *Schäfer/Sander/van Gemmeren*, Praxis der Strafzumessung, 6. Aufl. 2017, Rn. 584.
[55] *Kinzig* (Fn. 39), § 46 Rn. 26; *Miebach/Maier* (Fn. 37), § 46 Rn. 213.
[56] *Kinzig* (Fn. 39), § 46 Rn. 26ff.; *Kühl* (Fn. 43), § 46 Rn. 34; *Miebach/Maier* (Fn. 37), § 46 Rn. 214 f.
[57] Z.B. *Slizyk*, Schmerzensgeld 2020, Handbuch und Tabellen, 16. Aufl. 2020.
[58] *Streng* (Fn. 38), § 46 Rn. 57.
[59] BGH NJW 2009, 528 (531 f.); BGH NJW 2012, 5599 f.; BGH NStZ 2012, 634 (636).
[60] BGH NJW 1979, 1835; *Kinzig* (Fn. 39), § 46 Rn. 16; *Miebach/Maier* (Fn. 37), § 46 Rn. 193; *Schäfer/Sander/van Gemmeren* (Fn. 54), Rn. 615.
[61] *v. Heintschel-Heinegg* (Fn. 36), § 46 Rn. 33; *Schäfer/Sander/van Gemmeren* (Fn. 54), Rn. 615.
[62] *Kinzig* (Fn. 39), § 46 Rn. 16; Streng (Fn. 38), § 46 Rn. 53.
[63] *Kinzig* (Fn. 39), § 46 Rn. 16.
[64] *Streng* (Fn. 38), § 46 Rn. 52.
[65] *Miebach/Maier* (Fn. 37), § 46 Rn. 193; *Schäfer/Sander/van Gemmeren* (Fn. 54), Rn. 614.
[66] Abrufbar unter https://www.duden.de/rechtschreibung/Gesinnung (29.8.2020).

viele weitere.[67] In der höchstrichterlichen Rechtsprechung finden sich fast ebenso viele Umschreibungen dessen, was unter der aus der Tat sprechenden Gesinnung zu verstehen ist. So wird auf die sich in der Handlung äußernde innere Einstellung,[68] das Beruhen der Tat auf einer verwerflichen Gesinnung[69] oder die besondere innere Einstellung zu der Tat[70] bezogen. Wenn die Gesinnung alle Werte, Haltungen und die Weltanschauung einer Person umfasst, führt diese Erkenntnis sodann jedoch zu der Folgefrage, ob Werte und Weltanschauungen überhaupt zu bewerten sind. Daran schließt sich sodann die Frage an, wann eine Gesinnung, welche in der Tat Ausdruck gefunden hat, strafschärfend und wann strafmildernd zu berücksichtigen ist.

Nach *Kühl* soll die Gesinnung schwerpunktmäßig nach rechtlichen, unterstützend jedoch auch nach ethischen Gesichtspunkten beurteilt werden.[71] Dies führt jedoch unweigerlich zu der normativen Frage, welche ethischen Gesichtspunkte maßgeblich sein sollen. Diese Frage kann hier nicht beantwortet werden. Und vielleicht sollte sie auch gar nicht beantwortet werden. Dies gilt zumindest dann, wenn man von der Erwartung abrückt, dass sämtliche zum jetzigen Zeitpunkt von Richterinnen und Richtern anzustellenden Erwägungen algorithmisiert werden sollten. Es könnte also durchaus ausreichen, einige Kriterien einer algorithmenbasierten Bewertung zu unterwerfen, andere dabei aber bewusst auszulassen.

IV. Programmierung, Kriterien-Bestimmung und Verwendung

Zuletzt bleiben noch die Fragen, wer einen Algorithmus für die Strafzumessung programmieren könnte oder wer dies tun sollte. Zudem ist zu fragen, wer die Bewertungskriterien des Algorithmus festlegen darf und wie dessen Ergebnisse für Richterinnen und Richter dargestellt und von ihnen verwendet werden können. Dabei gilt es zunächst festzustellen, welche Funktion ein Algorithmus im Strafverfahren einnimmt. Einerseits sprechen Gründe dafür, den Algorithmus als konkretisierendes Instrument bestehender Gesetze zu verstehen. Ist es nämlich die Aufgabe des Algorithmus, die unbestimmten Strafzumessungsumstände des § 46 Abs. 2 S. 2 StGB genau zu definieren, so stellt er gesetzliche Regelungen auf. Andererseits könnte der Algorithmus auch als „Organ der Rechtsprechung“ verstanden werden. Dies ist dann der Fall, wenn es die Aufgabe des Algorithmus ist, bereits zuvor konkretisierte Strafzumessungsumstände im Einzelfall zu subsumieren. Hier würde der Algorithmus allein Aufgaben wahrnehmen, die bisher Richterinnen und Richtern vorbehalten sind.

Versteht man den Algorithmus als „gesetzliches Instrument“, so bedarf die Programmierung und Ingebrauchnahme einer parlamentarischen Legitimation. Die Zuständigkeit und das Verfahren der Kriterien-Bestimmung und deren Übersetzung in einen Algorithmus müssen denselben Regelungen folgen wie eine Gesetzesänderung desjenigen Gesetzes, welches der Algorithmus konkretisiert. Sieht man den Algorithmus dagegen als „Organ der Rechtsprechung“ so bedürfte es zunächst keiner parlamentarischen Legitimation. Hier führt jedoch das eingangs angeführte Beispiel aus den USA zu der Frage, ob es mit unserem Verständnis von Rechtsprechung vereinbar ist, wenn Programmiererinnen und Programmierer den rechtsprechenden Organen eine „Richtung“ bei der Urteilsfindung vorgeben. Dieses Problem ist jedoch bei weitem nicht unbekannt. So stellt sich diese Frage auch, wenn Richterinnen und Richter zur Beurteilung eines Sachverhalts und somit letztendlich auch zur Urteilsfindung ein Sachverständigengutachten anfordern. In diesem Fall beurteilt auch eine nicht juristisch ausgebildete Person einen Sachverhalt und die Richterin oder der Richter muss sich mangels Sachkunde auf dessen Urteil verlassen.

Es kann nicht von Juristinnen und Juristen erwartet werden, dass sie in der Lage sind, Algorithmen zu programmieren, aber gleichermaßen kann nicht von Programmiererinnen und Programmierern erwartet werden, dass sie juristisch fundierte Einschätzungen abgeben können. Eine Kooperation zwischen diesen beiden Berufsgruppen wird hier der einzig gangbare Weg sein, um zufriedenstellende Lösungen zu entwickeln. Ebenso kann bei der Beurteilung der Kriterien nur eine Kooperation zwischen Praxis und Wissenschaft zu Ergebnissen führen, welche allgemein vertretbar erscheinen. Die in den USA gewählte Methode, sich bei der Programmierung auf vergangene Urteile und Fälle zu beziehen, ist ein möglicher Weg, die Datenbasis eines Algorithmus zu speisen. Allerdings muss auch hier eine Vielzahl an Faktoren berücksichtigt werden. In Deutschland führt dies etwa zu den Fragen, ob die Urteile proportional zur Anzahl der Gerichte in den einzelnen Bundesländern ausgewählt werden und ob die jeweils als solche bezeichneten „Regelfälle“ überhaupt vergleichbar sind. Darüber hinaus berühren die festzulegenden Kriterien aber auch noch viel grundlegendere juristische und gesellschaftliche Problematiken. Denn fragen wir nach der Nutzung algorithmischer Entscheidungssysteme, so müssen wir uns zugleich auch mit Fragen der Gerechtigkeit der Bewertung von Menschen beschäftigen. Zudem müssen wir fragen, ob sich Menschen überhaupt von Algorithmen bewerten lassen wollen und ob es darauf ankommen kann.

Ein wesentliches Merkmal eines zu entwickelnden Algorithmus muss die Offenlegung der von diesem genutzten Kriterien und deren Gewichtung sein. Richterinnen und Richter können sich nur dann sinnvoll auf Ergebnisse einer algorithmischen Berechnung beziehen, wenn sie zumindest im Ansatz erkennen, was überhaupt berechnet wurde. Auch kann es nicht Sinn und Zweck des Algorithmus sein, weitere undurchschaubare Beurteilungsspielräume zu schaffen. Dient ein Algorithmus nämlich dazu, Kriterien zu veranschaulichen und einheitliche Wertungsmaßstäbe zu schaffen, dann kann dies nur erfolgen, wenn die Kriterien und Maßstäbe offen und einsehbar dargelegt werden. Zudem sollte der Einsatz eines Algorithmus nicht dazu führen, dass sich Richterinnen und Richter in der Entscheidungsfindung eingeengt fühlen. So muss immer die Möglichkeit bleiben, bewusst von dem Er-

[67] Siehe Fn. 66.
[68] BGH NStZ 1995, 128 (129).
[69] BGH NStZ 2018, 533 (534).
[70] BGH NStZ 2019, 657.
[71] *Kühl* (Fn. 43), § 46 Rn. 33.

gebnis der Berechnung abzuweichen, wie es auch im Rahmen von gutachterlichen Einschätzungen möglich ist.

V. Fazit

Die aufgezeigten Erwägungen zeigen, dass im Bereich der Digitalisierung und des damit verbundenen Einsatzes von Computerprogrammen im Strafverfahren große Herausforderungen bestehen. Neben den Risiken kann der Einsatz von Algorithmen jedoch auch Potential bieten. So könnten Abweichungen in „Regelfällen“ oder „Strafmaßtabellen“ vielleicht vermieden oder zumindest verringert werden. Dennoch sollte zum jetzigen Zeitpunkt ein gewisses Maß an richterlicher Autonomie in der Entscheidungsfindung verbleiben. So erscheint es nötig, trotz aller Undurchsichtigkeit des Beurteilungsspielraumes, auf persönliche Erfahrungen und menschliche Empathie der Richterinnen und Richter bei der Urteilsfindung zurückzugreifen. Erfahrungsgemäß werden zwei Fälle, wie ähnlich gelagert sie auch sein mögen, niemals identisch sein. Nach dem jetzigen Stand der Technik kann nicht davon ausgegangen werden, dass es einem Algorithmus gelingen wird, jede noch so kleine Differenz auszugleichen. Ein solcher Ausgleich und die von der Rechtsprechung immer wieder betonte Beurteilung des Einzelfalles muss jedoch weiterhin gewährleistet bleiben.

Das Zeitalter des digitalen Extremismus?

Einige Befunde zu politisch extremer Kommunikation in Social Media

Von Prof. Dr. **Stefan Harrendorf**, **Pia Müller**, M.A., **Antonia Mischler**, M.A., Greifswald*

I. Einleitung

Wir leben in einem Zeitalter des Digitalen. Dies zeigt sich in vielerlei Hinsicht und immer deutlicher, sei es beim Einkaufen, Arbeiten, Musikhören, Filmeschauen etc. Schlagworte wie künstliche Intelligenz,[1] Internet der Dinge, autonomes Fahren oder virtuelle Realität sind ebenfalls Ausdruck zunehmender Digitalisierung in allen Lebensbereichen. Auch Kommunikationsprozesse verlagern sich immer mehr in den Cyberspace.[2] Zwar ist die Utopie einer vollständig von der Realwelt abgekoppelten virtuellen (Parallel-)Realität[3] weiterhin nicht eingetreten; eher überlagern sich die virtuellen mit den realen Räumen und erweitern diese zu einer Art Hybrid-Realität.[4] Diese Entwicklung hat sich im Zuge der aktuellen Corona-Krise, gerade auch mit Blick auf Kommunikationsprozesse, nochmals verstärkt – in Zeiten des Social Distancing sind eben digitale Kommunikationsalternativen besonders gefragt.[5] Doch hat diese Krise auch noch einmal die augenfälligen Problembereiche digitaler, computervermittelter Kommunikation (cvK) wie unter dem Vergrößerungsglas sichtbar gemacht:

Das Internet ermöglicht die weltweite Vernetzung mit Personen, die die eigenen Auffassungen, Ansichten und Überzeugungen teilen, selbst dann, wenn diese weit abseits des gesellschaftlichen Mainstreams liegen.[6] Dies ist in vielen Bereichen positiv, führt es doch zum Empowerment sozial und politisch marginalisierter Gruppen[7] und damit dazu, dass diese Gruppen ggf. ihre Positionen durch soziale Kreativität und sozialen Wettstreit[8] verbessern können. Indessen sind diese Vernetzungsmöglichkeiten gleichermaßen für Gruppen gegeben, die gefährliche, z.B. menschenfeindliche und antidemokratische, Positionen teilen oder Verschwörungsideologien verinnerlicht haben. Dabei können, wie im Folgenden noch näher erläutert werden wird, gerade die speziellen Rahmenbedingungen der cvK Gruppenbildungs- und Polarisierungsprozesse noch verschärfen.[9] Auch hierzu hat die Corona-Krise reiches Anschauungsmaterial geliefert,[10] zeigt sie doch (wieder), wie schnell manche normal intelligenten, psychisch gesunden[11] Menschen, befeuert durch Gruppenkommunikation online und offline, bereit sind, selbst den absurdesten Verschwörungsideologien trotz evidenter wissenschaftlicher Unhaltbarkeit Glauben zu schenken.

Doch es bedurfte nicht erst der Corona-Krise, um diese Problematik sichtbar zu machen. Auch die Jahre davor waren bereits von einer anscheinend durch cvK befeuerten Radikalisierung der Kommunikation und des Handelns von Teilen der Gesellschaften weltweit geprägt. Besonders offenkundig wurde dies z.B. im Zuge der teils blitzschnellen rechtsextremen Radikalisierung von Teilen der Bevölkerung im Zuge der sog. Flüchtlingskrise insbesondere der Jahre 2015/2016.[12] Auch die rechtsextremen Terroranschläge der letzten Jahre sind ohne cvK jedenfalls in ihrer konkreten Gestalt nicht denkbar, sei es als Radikalisierungsmedium, als Plattform zur Verbreitung der Manifeste der Täter, zum Bezug von Bauanleitungen für Waffen aus dem 3D-Drucker oder von Waffen aus dem Darknet sowie zum Life-Streaming ausgeführter Anschläge.[13] Doch auch im salafistischen Jihadismus, wie er

* Prof. *Dr. Stefan Harrendorf* ist Inhaber des Lehrstuhls für Kriminologie, Strafrecht, Strafprozessrecht und vergleichende Strafrechtswissenschaften an der Universität Greifwald. *Pia Müller*, M.A., und *Antonia Mischler*, M.A., waren im dortigen RadigZ-Projekt bis zu dessen Abschluss wissenschaftliche Mitarbeiterinnen. *Pia Müller* bearbeitet mittlerweile am selben Lehrstuhl das Projekt InKoPrep, *Antonia Mischler* ist an der Kriminologischen Zentralstelle e.V. in Wiesbaden im Projekt MOTRA tätig. Soweit im Beitrag das generische Maskulinum verwendet wird, sind damit alle Geschlechter gemeint.

[1] Zur (gegenwärtigen und künftigen) Bedeutung künstlicher Intelligenz für den Bereich der Strafzumessung siehe auch *Kaspar/Höffler/Harrendorf*, Neue Kriminalpolitik 2020, 35.

[2] Der Begriff wurde maßgeblich geprägt von *William Gibson*, zuerst in der Kurzgeschichte „Burning Chrome" aus dem Jahr 1982, dann – bekannter – im Roman „Neuromancer", erschienen 1984.

[3] Dazu u.a. die Beispiele in Fn. 2.

[4] „Augmented Reality", vgl. *Lupton*, Digital Sociology, 2015, S. 168 ff.

[5] Siehe nur *Engels/Mertens/Scheufen*, Corona: Neuerungen in der beruflichen Kommunikation, 2020.

[6] *Bock/Harrendorf*, ZStW 126 (2014), 337.

[7] *Döring*, in: Schweiger/Beck (Hrsg.), Handbuch Online-Kommunikation, Wiesbaden 2018, S. 20 f.

[8] Dazu die Social Identity Theory: *Tajfel/Turner*, in: Worchel/Austin (Hrsg.), The Psychology of Intergroup Relations, 2. Aufl. 1986, S. 7 ff.

[9] Siehe auch bereits *Harrendorf/Mischler/Müller*, in: Petzsche/Heger/Metzler (Hrsg.), Terrorismusbekämpfung in Europa im Spannungsfeld zwischen Freiheit und Sicherheit, 2019, S. 273 (280 ff.); *Bock/Harrendorf*, ZStW 126 (2014), 337.

[10] Gründlichere wissenschaftliche Einordnungen sind noch selten, vgl. aber z.B. *Hacker/Pisiou/Hager*, Terrorismusszenarien und -trends: Inklusive der Auswirkung von COVID-19, 2020; *Allington et al.*, Psychological Medicine 2020, 1; siehe auch BT-Drs. 19/19785.

[11] Bei allerdings im Einzelfall fließenden Übergängen, dazu *Kröber*, Forensische Psychiatrie, Psychologie, Kriminologie 2020, S. 366 ff.

[12] Vgl. *Harrendorf/Mischler/Müller* (Fn. 9), S. 274 f.

[13] Zu denken ist zunächst an die Anschläge von Anders Behring Breivik in Oslo und auf der Insel Utøya am 22. Juli 2011, die 77 Todesopfer forderten (dazu näher *Seierstad*, Einer von uns: Die Geschichte eines Massenmörders, 2016), sodann u.a. an die sich teils unmittelbar auf diese Taten Breiviks und auf das von diesem veröffentlichte Manifest beziehenden, im Übrigen zumindest erstaunliche Parallelen aufweisenden Anschläge von München (22.7.2016, neun

von Organisationen wie Al Qaida und später insbesondere dem sog. Islamischen Staat (IS) vertreten wurde und wird, spielt cvK eine Rolle für den Radikalisierungsprozess der Täter sowie generell als Propagandainstrument. So hatte der US-amerikanische Psychologe *Sageman* schon 2008 darauf hingewiesen, dass sich die Kommunikation terroristischer Gruppen bereits ab 2004 zunehmend in die Chatrooms des Internet verlagert hatte.[14] Der IS hatte zu seiner Hochphase die Nutzung von Internetpropaganda geradezu perfektioniert und verbreitete bis 2017 gestalterisch gut gemachte, extremistische Journale, insbesondere Dabiq (bis 2016) und später Rumiyah, und war auf verschiedene Weise in Social Media aktiv. Auch hier finden sich zudem immer wieder Hinweise auf eine Radikalisierung der Täter auch über cvK oder doch zumindest auf die Nutzung von cvK als Medium zur Tatplanung und zur Verbreitung von Propagandamaterial erfolgreicher Anschläge.[15]

Vor diesem Hintergrund will der Beitrag der Frage nachgehen, ob wir in einem „Zeitalter des digitalen Extremismus" leben. Dabei spielt der Beitragstitel auf das vom Bundesministerium für Bildung und Forschung geförderte Verbundprojekt „Radikalisierung im digitalen Zeitalter" (RadigZ) an, das von Februar 2017 bis (für die meisten Teilvorhaben) August 2020 lief. Die Verfasserinnen und der Verfasser haben im Rahmen des Projekts das Teilvorhaben III („Qualitative und quantitative Analyse internetbasierter Propaganda") bearbeitet. Im Folgenden werden einige (qualitative) Untersuchungsergebnisse dieses Teilvorhabens präsentiert.

II. Das RadigZ-Verbundprojekt

Das RadigZ-Verbundprojekt im Ganzen wurde an anderer Stelle bereits genauer vorgestellt;[16] daher soll es hier mit einigen kurzen Anmerkungen zur Projektstruktur sein Bewenden haben. Grob betrachtet, gliederte sich das Gesamtvorhaben in acht Teilprojekte, von denen drei eine eher individuenbezogene, drei eine medienbezogene und zwei eine präventionsbezogene Ausrichtung aufwiesen. Die individuenbezogenen Vorhaben widmeten sich Biografie- und Netzwerkanalysen zu (De-)Radikalisierungsverläufen, Prognoseinstrumenten und Experteninterviews mit professionellen Beobachtern sowie der Ermittlung des Gefahrenpotentials und der Identifikation vulnerabler Gruppen; sie wurden an den Universitäten Köln und Göttingen sowie beim Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) durchgeführt. Die medienbezogenen Projekte analysierten neben der hier im Fokus stehenden, von uns in den Blick genommenen internetbasierten Propaganda als solcher auch konkret Aufrufe zu extremistischen Gewalthandlungen und Straftaten (Deutsche Hochschule der Polizei, Münster) und untersuchten experimentell die Wirksamkeit radikalisierender Hinweisreize (Universität Greifswald, Institut für Psychologie). Schließlich ging es bei den präventionsbezogenen Studien um die Bestandsaufnahme und Analyse bestehender Präventionsprojekte sowie die Erarbeitung entwicklungsorientierter Präventionsmaßnahmen, bearbeitet an den Universitäten Hannover bzw. Jena.

Den Teilvorhaben entsprechend, waren die Ziele des Gesamtprojekts, Vulnerabilitätsfaktoren und Risikogruppen mit Blick auf Radikalisierungsverläufe und eine Empfänglichkeit für Internetpropaganda zu untersuchen und das Ausmaß der insofern bestehenden Gefährdung zu bestimmen. Szenarien der Radikalisierung und Deradikalisierung wurden analysiert. Zudem wurde internetbasierte Propaganda untersucht und bezüglich ihrer Wirkung beurteilt. Weiterhin wurden systematische Forschungsbilanzen über bestehende Arbeiten zur Radikalisierung erstellt, eine Bestandsaufnahme und kritische Analyse bereits bestehender Präventionsbemühungen erarbeitet sowie neue Präventionsmaßnahmen entwickelt. Schließlich wurden auch universelle sowie zielgruppenspezifische Präventionsansätze und Handlungsempfehlungen für Praxis und Politik erarbeitet. Eine Kurzfassung dieser Handlungsempfehlungen wurde bereits veröffentlicht,[17] eine Langfassung ist aktuell in Vorbereitung. Zudem wird noch ein Special Issue des European Journal on Criminal Policy and Research publiziert, in dem die verschiedenen Teilvorhaben ihre jeweiligen Ergebnisse näher vorstellen. Hier ist mit einem sukzessiven Erscheinen der Online-First-Versionen der Beiträge, einen erfolgreichen Abschluss des Peer-Review-Prozesses unterstellt, im Laufe des Jahres 2021 zu rechnen.

III. Social Media und extremistische Propaganda

In einem Vorhaben, das sich „Radikalisierung im digitalen Zeitalter" nennt, war es natürlich auch nötig, sich eingangs auf einen gemeinsamen Begriff von Radikalisierung und Extremismus zu einigen. Eine Ausarbeitung dieses Begriffsverständnisses hat *Beelmann* auf der Basis der gemeinsamen Überlegungen in den Verbundtreffen vorgelegt.[18] Hiernach wird der Begriff der Radikalisierung prozesshaft verstanden als Entwicklung zum Extremismus. Der dabei verwendete

Todesopfer), Christchurch (15.3.2019, 51 Todesopfer), Halle (9.10.2019, wegen weitgehenden Fehlschlags des Tatplans „nur" zwei Todesopfer) und Hanau (19.2.2020, zehn Todesopfer).

[14] *Sageman,* Leaderless Jihad: Terror Networks in the Twenty-First Century, S. 109 ff.

[15] Zu denken ist z.B. an den Anschlag in Nizza am 14.7.2016 (86 Todesopfer), den Anschlag von Orlando am 12.6.2016 (49 Todesopfer), aber auch das Attentat am Frankfurter Flughafen am 2.3.2011 (zwei Todesopfer) oder dasjenige auf den Boston-Marathon am 15.4.2013 („nur" drei Todesopfer, aber 264 Verletzte).

[16] Initial bereits in *Kudlacek et al.*, Forum Kriminalprävention 3/2017, 23; siehe zudem *Schröder/Goede/Lehmann*, Perspektiven von Studierenden, 2020, S. 2 ff. Eine detaillierte Vorstellung aller Teilvorhaben aus der Zeit des Projektbeginns findet sich in den Beiträgen in NK Heft 4/2017.

[17] *Beelmann/Lehmann*, Radikalisierung im digitalen Zeitalter: Handlungsempfehlungen an Politik, Praxis und Gesellschaft – Kurzfassung, 2020.

[18] *Beelmann*, in: Heinzelmann/Marks (Hrsg.), Prävention & Demokratieförderung, 2019, S. 181 (183 ff.); teils abweichende begriffliche Überlegungen finden sich aber auch bei *Bibbert/Mischler/Geng/Harrendorf*, NK 2017, S. 388 ff.

Extremismusbegriff stellt – anders als andere Verständnisse[19] – nicht allein auf die feststellbare, bedeutsame Abweichung von bestehenden gesellschaftlichen und rechtlichen Wert- und Normsystemen sowie das Bestreben, diese Systeme zumindest teilweise abzuschaffen bzw. durch andere Systeme zu ersetzen, ab. Ein solcher, rein positivistischer Begriff müsste auch den legitimen Freiheitskampf gegen eine mörderische Diktatur als Extremismus einstufen.[20] Vielmehr wird nur die Ablehnung bestimmter Wert- und Normsysteme in den Blick genommen, konkret die Ablehnung der freiheitlich demokratischen Grundordnung (Menschenwürde, Demokratieprinzip, Rechtsstaatsprinzip, staatliches Gewaltmonopol)[21] sowie der universellen Geltung unveräußerlicher Menschenrechte.[22] Andererseits ist das Begriffsverständnis aber insofern ein weites, als bereits entsprechende Einstellungen als solche als extremistisch gewertet werden, es kommt also nicht auf die zur Zielerreichung verwendeten Mittel oder bestimmte Handlungsergebnisse an (so ist z.B. physische Gewalt nicht konstituierendes Element eines so verstandenen Extremismus).[23] Dies ist natürlich gerade für die medienbezogenen Analysen auch fast zwingend, weil dort von vornherein nur der kommunikative Aspekt von Radikalisierung und Extremismus in den Blick genommen werden kann. Ob die dort mitgeteilten (nicht notwendig immer auch wahrheitsgemäß berichteten) Einstellungen letztlich handlungswirksam werden, muss jedenfalls bei einer rein auf cvK bezogenen Betrachtung zwangsläufig außen vor bleiben.

Social Media fungieren als „Intermediäre“: Die Plattformen selbst produzieren keinen Inhalt. Dies übernehmen ihre User, indem sie Beiträge verfassen, „liken“ und teilen.[24] Eine mediale Gate-Keeper-Funktion, die sonst von Redaktionen bzw. professionell Medienschaffenden ausgeübt wird, entfällt.[25] Social-Media-Diskurse sind demnach frei im Zugang, die Teilnahme erfordert nur einen geringen Aufwand und potenziell können viele Menschen gleichzeitig erreicht werden. Aus diesem Grund sind Social Media auch zentrale Kommunikationskanäle extremistischer Gruppen. Sie ermöglichen ihnen, dem Nischendiskurs zu entkommen, sich in einem breiteren Mainstream zu positionieren[26] und ihre bisherige „mediale Isolation“[27] zu durchbrechen.

Die Gefährlichkeit von Internetpropaganda ergibt sich zunächst aus ihrer grundsätzlich jederzeitigen weltweiten Verfügbarkeit. Dabei kann der Prozess der Radikalisierung über das Internet als Folge einer Interaktion Einzelner mit ihren spezifischen Interessen, Einstellungen und Eigenschaften mit den situativen Rahmenbedingungen des Kommunikationsmediums Internet verstanden werden.[28] Insofern begünstigt das Medium Prozesse der Selbstselektion[29] seiner Nutzer in Foren gleich oder ähnlich denkender Individuen, die heutzutage durch die inhaltliche Filterfunktion sozialer Netzwerke wie Facebook (die sog. „Filterblase“)[30] noch einmal verstärkt werden.

Ausgehend von Annahmen des sog. Social Identity Approach[31] unterstützt cvK zudem in besonderer Weise die Herausbildung stabiler, salienter (= bewusster) sozialer Identitäten[32] und fördert dadurch die Depersonalisierung der Kommunizierenden.[33] Die Salienz einer sozialen Identität ist dabei abhängig von der kognitiven Zugänglichkeit einer bestimmten Ingroup-Outgroup-Kategorisierung und der Passung der in einer Situation verfügbaren, auf die Kategorie verweisenden sozialen Hinweisreize.[34] CvK in extremistischen oder sich radikalisierenden Gruppenkontexten beeinflusst nun diese Salienz auf zweierlei Weise: Einerseits durch das Kommunikationsmedium, andererseits durch den Kommunikationsinhalt. Inhaltsbezogen gilt, dass Ideologien über die Bereitstellung von Gruppen-Stereotypen den idealen Hintergrund für Ingroup-Outgroup-Kategorisierungen bieten.[35] Medienbezogen ist zu beachten, dass cvK mit extremistischen, möglicherweise selbst bereits strafrechtlich relevanten Inhalten häufig unter dem Schutz der Pseudonymität stattfindet. Diese erschwert nun nicht nur die Identifikation und strafrechtliche Verfolgung der Kommunizierenden, sondern hat auch weitere Effekte:[36] So bietet pseudonyme cvK günstige Bedingungen, um Dinge zu äußern, die in Face-to-face-Situationen nicht geäußert würden. Nach dem Social Identity Model of Deindividuation Effects (SIDE)[37] bewirkt Pseudo-

[19] Siehe dazu die Nachweise bei *Beelmann* (Fn. 18), S. 183 ff.
[20] *Beelmann* (Fn. 18), S. 183.
[21] Zu diesem Begriffsinhalt in Art. 21 Abs. 2 GG siehe nur BVerfGE 144, 20 (21).
[22] *Beelmann* (Fn. 18), S. 187.
[23] *Beelmann* (Fn. 18), S. 188; *Bibbert/Mischler/Geng/Harrendorf* (Fn. 18), S. 394.
[24] *Struck/Müller/Mischler/Wagner*, Kriminologie – Das Online-Journal 2 (2020), 310 (314).
[25] *Khosravinik*, Insight Turkey 19 (2017), 53 (62 f.).
[26] *Harrendorf/Mischler/Müller* (Fn. 9), S. 277.
[27] *Freter/Zimpelmann*, in: Beck/Meier/Momsen (Hrsg.), Cybercrime und Cyberinvestigations: Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie, 2015, S. 119.
[28] So bereits *Bock/Harrendorf*, ZStW 126 (2014), 337 (346); *Mischler/Müller/Geng/Harrendorf,* RW 2019, 481 (502).
[29] Vgl. *Haslam/Reicher*, Personality and Social Psychology Bulletin 33 (2007), 615.
[30] Dazu *Pariser,* Filter Bubble: Wie wir im Internet entmündigt werden, 2012.
[31] *Tajfel/Turner* (Fn. 8), *Turner*, Rediscovering the Social Group: A Self-Categorization Theory, 1987.
[32] Die soziale Identität ist der Teil der individuellen Identität, der sich aus der von einem Individuum wahrgenommenen Zugehörigkeit zu einer bestimmten Gruppe ableitet, vgl. *Tajfel/Turner* (Fn. 8), S. 16.
[33] Ausführlich bereits *Harrendorf/Mischler/Müller* (Fn. 9), S. 280 ff.
[34] *Turner* (Fn. 31), S. 54 ff.
[35] Näher noch unter V. Siehe auch *Staub*, in: Ashmore/Jussim/Wilder (Hrsg.), Social Identity, Intergroup Conflict, and Conflict Reduction, 2001, S. 159.
[36] *Bock/Harrendorf*, ZStW 126 (2014), S. 337; *Rackow/Bock/Harrendorf*, StV 2012, 687.
[37] Dazu *Spears/Lea*, Communication Research 21 (1994), 427; *Spears/Postmes*, in: Sundar (Hrsg.), The Handbook of

nymität zudem bei salienter Gruppenidentität eine weitere Verstärkung der Depersonalisierung durch Verringerung des Fokus auf die persönliche Identität, begünstigt also noch zusätzlich die Anpassung an Gruppen- bzw. Kontextnormen unabhängig von deren gesellschaftlicher Bewertung. Zudem spielen Effekte der Gruppenpolarisation eine Rolle, die dazu führen, dass bei Gruppen, deren Auffassungen zu einem Thema bereits in eine bestimmte Richtung tendierten, diese sich nach gemeinsamer Diskussion noch stärker in die Richtung des entsprechenden Extrems entwickeln.[38]

IV. Methodik der eigenen Untersuchung

Im Rahmen des RadigZ-Teilvorhabens III wurden Kommunikationsverläufe aus den Bereichen Rechtsextremismus und salafistischer Jihadismus analysiert. Es handelt sich dabei jeweils um Ideologien, die besonders zur Eskalation in Gewalt gegen Mitglieder von Outgroups tendieren[39] und bei denen sich in relevantem Umfang Radikalisierungen gerade über das Internet ereignen (können).[40] Zudem erfüllen beide Ideologien den oben eingangs unter III. näher dargestellten Extremismusbegriff.

Die cvK-bezogenen Analysen fokussierten sich insbesondere auf die folgenden Fragen:

- Welche sozialen Identitäten werden konstruiert? Auf welche Weise geschieht dies?
- Inwiefern lassen sich (szene-)typische Denk- und Argumentationsfiguren identifizieren?
- Wie gestalten sich kommunikative Radikalisierungsverläufe?

Es wurden qualitative und quantitative Inhalts-, Diskurs- und Netzwerkanalysen durchgeführt und Radikalisierungsverläufe als Kommunikationsprozesse auf drei verschiedenen Ebenen verfolgt:

- auf einem Einstiegslevel, auf dem interessierte Nutzer typischerweise erstmals mit radikalisierenden Gruppenprozessen, Diskursen und Materialien in Kontakt kommen,
- auf einem mittleren Level, der offene Gruppen für bereits Radikalisierte erfasst, sowie
- auf einem oberen Level sehr radikaler, geschlossener Gruppen, deren Nutzer teils bereits an der Schwelle zu einer Umsetzung radikaler Entwürfe in Handlungen stehen dürften (oder diese schon überschritten haben).[41]

Während der Zugang zum dritten Radikalisierungslevel retrospektiv über für Strafverfahren gesicherte Beweismittel, u.a. aus Terrorismusverfahren, erfolgen musste, basieren die Daten für die ersten beiden Levels auf unmittelbaren eigenen Erhebungen in Social Media, insbesondere unter Verwendung von Fake-Profilen auf Facebook und anderen Social-Media-Plattformen (z.B. ВКонтакте bzw. VKontakte). Genutzt wurden jeweils männliche und weibliche Profile, die den Eindruck erwecken, dass deren Inhaber der rechtsextremen Szene bzw. dem salafistisch-jihadistischen Milieu nahestehen. Die Profile enthielten sich aus forschungsethischen, strafrechtlichen und methodischen Gründen jeglicher inhaltlicher Kommunikation, äußerten sich also insbesondere nie selbst extremistisch, sondern beschränkten sich darauf, Freundschafts- und Beitrittsanfragen an Personen bzw. Gruppen zu versenden, die durch ihr Auftreten, ihre spezifischen Profilbeschreibungen und/oder ihre Inhalte der rechtsextremen Szene bzw. dem salafistisch-jihadistischen Milieu zuzuordnen sind.

Die in Gruppen der ersten beiden Radikalisierungslevels Kommunizierenden verfügen häufig (noch) nicht über ein geschlossenes rechtsextremes bzw. salafistisch-jihadistisches Weltbild. Auch kann über die eigentlichen Intentionen der sich in Social Media Äußernden letztlich ohne Kenntnis der hinter den Äußerungen stehenden Individuen nur spekuliert werden. Die Analysen erfolgten daher rein kommunikationsbezogen mit einem Fokus auf Deutungsmuster bzw. Narrative extremistischer Ideologien. Die extremistische Weltsicht hat auch Konsequenzen für die Sprache und die Sinnkonstruktion durch Sprache. Zwar kann anhand eines einzelnen Beitrags nicht festgestellt werden, ob die kommentierende Person einem geschlossen salafistisch-jihadistischen oder extrem rechten Weltbild anhängt. Doch lässt sich sehr wohl analysieren, inwiefern Kommentierende Deutungsmuster dieser Ideologien reproduzieren.[42]

Um die Analysen in zeitlicher und inhaltlicher Hinsicht zu strukturieren, erfolgte die Datenerhebung im offenen Material (Level 1 und 2) insbesondere nach Beobachtungszeitpunkten. Unter einem Beobachtungszeitpunkt wird dabei ein spezifisches Geschehen innerhalb der Gesellschaft verstanden, welches für beide Extremismen inhaltliche bzw. symbolische Relevanz hat, die z.B. darin liegen kann, dass das Ereignis die eigene Argumentation gegen Outgroups unterstützen kann, aus der eigenen Perspektive als eine Art Beweis dient, dass das Zusammenleben mit anderen Kulturen, Religionszugehörigkeiten und vor allem Individuen, die scheinbar anders und anderswertig sind, nicht als positiv angesehen

---

the Psychology of Communication Technology, 2015, S. 23 ff.

[38] Vgl. z.B. *Myers*, in: Levine/Hogg (Hrsg.), Encyclopedia of Group Processes and Intergroup Relations, 2010, S. 361.

[39] Nach *Alvarez*, in: Haveman/Smeulers (Hrsg.), Towards a Criminology of International Crimes, 2008, S. 213, neigen insbesondere solche Ideologien dazu, Gewalt der Ingroup gegen Outgroups zu legitimieren, die eines oder mehrere der folgenden Elemente enthalten: Nationalismus, Verherrlichung und Mythologisierung vergangener Opferwerdung, Dehumanisierung, „Scapegoating" (Definition einer bestimmten Outgroup als Sündenbock), absolutistische Weltsicht, Utopismus.

[40] Siehe auch bereits *Harrendorf/Mischler/Müller* (Fn. 9), S. 278 ff.

[41] *Mischler/Müller/Geng/Harrendorf*, RW 2019, 481 (504).

[42] Für eine detaillierte Auseinandersetzung mit salafistisch-jihadistischen sowie extrem rechten Deutungsmustern im Vergleich siehe *Harrendorf/Mischler/Müller* (Fn. 9); vgl. zudem *Mischler/Müller/Geng/Harrendorf*, RW 2019, 481.

werden kann und/oder konkrete Konfliktlinien zwischen beiden Extremismen markiert. Daten wurden dabei zu insgesamt elf verschiedenen Beobachtungszeitpunkten erhoben.[43] Eine vergleichbare Vorgehensweise bot sich hingegen für das geschlossene Material (drittes Radikalisierungslevel) nicht an. Dessen innere Struktur ergab sich eher aus den unterschiedlichen Verfahrensanlässen, zu denen u.a. einzelne terroristische Akte, Vorbereitungshandlungen im Vorfeld dazu, aber auch Delikte im Zusammenhang mit dem Betreiben extremistischer Webseiten sowie Äußerungsdelikte, namentlich nach § 130 StGB, zählten.

Die qualitative Analyse der Kommunikationsverläufe, die über einen Zeitraum von bis zu einem Jahr innerhalb der sozialen Medien wie Facebook und VKontakte erhoben wurden, erfolgte über ein mehrstufiges Verfahren. Dabei wurden mittels sequenzieller Textanalyse diskursanalytische Elemente mit der dokumentarischen Methode kombiniert, um nicht nur Wissen über den Inhalt der Kommunikation und die Formen kommunikativer Verbreitung zu erlangen, sondern zusätzlich auch Aussagen über Argumentationsstrategien und Interaktionsverhältnisse treffen zu können. Einige Ergebnisse der qualitativen Analysen wurden bereits andernorts veröffentlicht.[44] Diese werden hier unter V. nochmals knapp zusammengefasst. Zudem widmet sich der Beitrag unter VI. einer etwas spezifischeren Analyse, nämlich der Auswertung von Text-Bild-Kompositionen im Rahmen sog. Memes.[45] Diese spielen in der rechtsextremen Kommunikation eine besondere Rolle, sodass insofern in diesem Aufsatz nur dieser Phänomenbereich in den Blick genommen wird.

Als quantitative Analysemethoden durchgeführt wurden semantische und personenbezogene Netzwerkanalysen sowie korpuslinguistische Analysen. Die semantische Netzwerkanalyse dient dabei dazu, aus komplexen semantischen Systemen (Texten) Informationen über Wortrelationen zu extrahieren und diese graphisch dazustellen.[46] Dabei wurde im Projekt nicht die Wortebene der Texte, sondern die qualitative Kodierung dieser Texte (mit Deutungsmustern, Argumentations- und Wortergreifungsstrategien sowie Interaktionen) mit dieser Methode quantitativ mit Blick auf Kookkurrenzen (parallel auftretende Codes) und Sequenzen (nacheinander auftretende Codes) ausgewertet. Ergänzend wurden personenbezogene Netzwerkanalysen durchgeführt. Hier ging es vor allem darum, besonders aktive und einflussreiche Akteure zu identifizieren. Zudem war es so möglich, die personenbezogene mit der semantischen Ebene inhaltlich zu verknüpfen.

Durchgeführt wurden zudem quantitative korpuslinguistische Analysen. Ziele derartiger Methoden sind die Identifikation quantitativer Beziehungen zwischen einzelnen lexikalischen Elementen und die Erkennung auftretender Regelmäßigkeiten, zudem das Herausstellen sprachlicher Charakteristika eines spezifischen Korpus auch in Referenz zu anderen Korpora.[47] Im Projekt wurden aus den erhobenen Social-Media-Daten verschiedene Textkorpora gebildet, die sodann im Verhältnis zu einem umfangreichen deutschen Webkorpus referenziert wurden. Hierbei sollten Schlüsselbegriffe, Soziolekte sowie sprachliche Radikalisierungsniveaus identifiziert werden.

Erste Ergebnisse dieser quantitativen Analysen wurden auf der RadigZ-Abschlusskonferenz am 23. Juli 2020 vorgetragen; eine nähere Darstellung muss hier aufgrund der Kürze des Beitrags unterbleiben und ist dem oben erwähnten Special Issue vorbehalten.

V. Ergebnisse qualitativer Analysen

Um Argumentationsstrategien und Denkmuster in radikalen Social-Media-Gruppen zu identifizieren, zu ergründen, worauf die kommunikative Herstellung radikaler Identitäten aufbaut und woran gegebenenfalls unterschiedliche Radikalisierungsniveaus festzumachen sind, müssen die Ideologien und ihre Bedeutung innerhalb einer Gruppe in den Fokus genommen werden. Ideologien („systems of shared beliefs, ideas, and symbols that help us make sense of the world around us“[48]) stellen Individuen sinnstiftende Angebote bereit und bieten Orientierung in Form von Interpretationsschemata an.[49] Extremistische Ideologien wie der Rechtsextremismus und der salafistische Jihadismus erlauben dabei die Bewertung nach einer simplifizierenden, dichotomen Logik: „Wir“ gegen „die“, Ingroup versus Outgroup. Sie schreiben Individuen – gruppenbezogen – eine elementare Ungleichwertigkeit zu.[50] Sie begünstigen die Herausbildung einer positiven sozialen Identität auch dann, wenn die eigenen Lebensumstände im Übrigen eher ungünstig sind;[51] sie sind insofern ein Vehikel sozialer Kreativität im Sinne der Social Identity Theory[52] (d.h. der Umdeutung der relevanten Vergleichskategorien zwischen Gruppen) und begünstigen zugleich den sozialen Wettstreit mit anderen Gruppen.

Im Bereich des salafistischen Jihadismus wird der Wert des Menschen anhand seiner religiösen Überzeugung festge-

[43] In *Mischler/Müller/Geng/Harrendorf*, RW 2019, 481 (508 ff.), wurden die Ergebnisse einer vergleichenden Analyse der Deutungsmuster in der cvK zu drei verschiedenen Beobachtungszeitpunkten (Attentat am Breitscheidplatz 2016, Bundestagswahl 2017, Solidaritätskundgebung „Berlin trägt Kippa“ 2018) bereits veröffentlicht.

[44] *Harrendorf/Mischler/Müller* (Fn. 9); *Mischler/Müller/Geng/Harrendorf*, RW 2019, 481.

[45] Dazu auch *Müller/Mischler*, in: Grafl et al. (Hrsg.), „Sag, wie hast Du’s mit der Kriminologie?“ – Die Kriminologie im Gespräch mit ihren Nachbardisziplinen, 2020 (im Erscheinen).

[46] *Lietz,* Mit neuen Methoden zu neuen Aussagen: Semantische Netzwerkanalyse am Beispiel der Europäischen Verfassung, abrufbar unter http://www.haikolietz.de/docs/verfassung.pdf (2.9.2020).

[47] *Dzudzek/Glasze/Mattissek/Schirmel*, in: Glasze/Mattissek (Hrsg.), Handbuch Diskurs und Raum, 2009, S. 233.

[48] *Alvarez* (Fn. 39), S. 216.

[49] *Hall*, Ideologie, Kultur, Rassismus, 1989.

[50] Vgl. *Bozay*, in: Bozay/Borstel (Hrsg.), Ungleichwertigkeitideologien in der Einwanderungsgesellschaft, 2017, S. 125.

[51] Vgl. erneut *Staub* (Fn. 35).

[52] *Tajfel/Turner* (Fn. 8).

legt,[53] eine darauf gründende Hierarchie wird als gottgegeben angesehen. Der soziale Wert- und Achtungsanspruch von Individuen wird auf diese Weise negiert.[54] Im Rechtsextremismus bilden Sozialdarwinismus sowie Rassismen die Grundlage für eine vermeintlich „natürliche" Hierarchie. Anhand der Annahme, es bestünde „eine natürliche Ungleichwertigkeit zwischen Menschen und Völkern",[55] werden Diskriminierung und soziale Ungleichheit als naturgegebene Ordnung konstruiert. Dieser Vorgang wird von Rechtsextremismusforschenden als „Biologisierung des gesellschaftlichen Geschehens"[56] bzw. als „biologistische Umdeutung des Sozialen"[57] gefasst. Teils wird mittlerweile auch mehr auf eine vermeintliche kulturelle Überlegenheit statt die „klassische" biologische Argumentation abgestellt. Auf diese Merkmale einer konstruierten Ungleichwertigkeit werden in beiden Phänomenbereichen vermeintlich „natürliche" Hierarchien gegründet, die als Basis der jeweiligen Ideologien angesehen werden können.

Für salafistisch-jihadistische wie auch für rechtsextreme Ideologien kann festgehalten werden, dass beide Gruppen in ihrer Feindschaft gegen eine aufgeklärte, liberale, pluralistische und demokratische Gesellschaft, die die Menschenrechte achtet und vertritt, vereint sind. In ihrem inneren Kern gleichen sich diese beiden Ideologien daher teilweise und werten mit ähnlichen bis gleichen Argumentationsstrategien und Deutungsmustern die Outgroups ab, während sie sich selbst aufwerten und als überlegen darstellen. Dies wird auch in *Abbildung 1* (siehe unten S. 419) deutlich: Dort werden Gemeinsamkeiten und Unterschiede der Deutungsmuster zusammenfassend und schlagwortartig dargestellt; die doch recht großen ideologischen Gemeinsamkeiten werden gut sichtbar.

Schaut man sich dann allerdings einzelne Diskussionen zu verschiedenen Beobachtungszeitpunkten genauer an, wird doch erkennbar, dass die geführten Diskurse trotz teils ähnlicher ideologischer Deutungen durchaus verschieden sind. So dominieren beispielweise bei der Diskussion des Attentats am Breitscheidplatz vom 19. Dezember 2016 in den offenen rechten bis rechtsextremen Gruppen insbesondere die Deutungsmuster „der Staat als Helfer des Feindes", „Anti-Establishment" und verschwörungstheoretische Annahmen in wechselseitiger Verknüpfung. Es wird dort davon ausgegangen, dass die Regierung die „Wahrheit" gegenüber den Bürgern verschweige, diese absichtlich mit Fehlinformationen versorge.[58] Hingegen dominiert zwar auch in den zum salafistischen Jihadismus hin orientierten offenen Gruppen (wohlgemerkt hier wie dort nur der ersten beiden Radikalisierungslevels) das Narrativ der Verschwörungstheorie, allerdings in ganz anders gewendeter Form: Das Attentat wird in diesen – nicht hoch radikalisierten – Gruppen nicht etwa gefeiert, sondern zwar abgelehnt, aber als staatliche Verschwörung gegen die Muslime gedeutet, denen der Anschlag in die Schuhe geschoben werden solle, um sie zu diskreditieren und härtere Maßnahmen gegen sie zu begründen. So taugt dann das Attentat doch mittelbar dazu, die Ingroup zu solidarisieren.[59]

VI. Memes in (rechts-)extremistischer Internetkommunikation

Memes können in Online-Kontexten definiert werden als „(a) a group of digital items sharing common characteristics of content, form and/or stance; (b) that were created with awareness of each other, and (c) were circulated, imitated, and/or transformed via the Internet by many users".[60] Sie weisen eine inhaltliche Dimension auf, die auch ideologische Komponenten mit umfasst, zeigen aber auch eine kollektive Dynamik, mittels derer eine Vielzahl von individuellen Beiträgen in wechselseitiger Referenz produziert und reproduziert wird. Bei der hier interessierenden Erscheinungsform als Text-Bild-Kompositionen werden zudem erst durch die wechselseitige Verknüpfung von textlichen und bildlichen Elementen die jeweiligen Kompositionen bedeutungskonstituierend.[61]

Im Folgenden werden wir uns für das Thema Memes[62] auf rechte und rechtsextreme Online-Kommunikation fokussieren und auch ein Beispiel aus diesem Bereich darstellen, da dort die Nutzung solcher Bild-Text-Kompositionen sehr verbreitet ist. Innerhalb der salafistisch-jihadistischen Kommunikationsverläufe lassen sich spürbar weniger Memes auffinden.[63]

Memes werden als relevantes Kommunikationsmittel erachtet, wenn es um die Vermittlung extrem rechter Ideo-

[53] Vgl. Innenministerkonferenz, Lagebild zur Verfassungsfeindlichkeit salafistischer Bestrebungen, abrufbar unter https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/11-06-22/anlage14.pdf?__blob=publicationFile&v=2 (2.9.2020).

[54] Siehe Fn. 53.

[55] *Decker/Kiess/Eggers/Brähler*, Die „Mitte"-Studie 2016: Methode, Ergebnisse und Langzeitverlauf, in: Decker/Kiess/Brähler (Hrsg.), Die enthemmte Mitte, Autoritäre und rechtsextreme Einstellungen in Deutschland, 2016, S. 23 (36).

[56] *Decker/Brähler*, Vom Rand zur Mitte, Rechtsextreme Einstellungen und ihre Einflussfaktoren in Deutschland, 2006, S. 40.

[57] *Häusler*, Themen der Rechten, in: Virchow/Langebach/Häusler (Hrsg.), Handbuch Rechtsextremismus, 2016, S. 135 (147).

[58] Vgl. zu derartigen Deutungen auch *Küpper/Häusler/Zick*, in: Zick/Küpper/Krause (Hrsg.), Gespaltene Mitte – Feindselige Zustände, Rechtsextreme Einstellungen in Deutschland 2016, 2016, S. 143 (152).

[59] Näher hierzu *Mischler/Müller/Geng/Harrendorf*, RW 2019, 481 (509 ff.)

[60] *Shifman*, Memes in Digital Culture, 2013, S. 7 f.

[61] Vgl. *Stöckl*, in: Diekmannshenke/Klemm/Stöckl (Hrsg.), Bildlinguistik: Theorien – Methoden – Fallbeispiele, 2011, S. 45.

[62] Dazu auch *Müller/Mischler* (Fn. 45).

[63] Ein Analysebeispiel findet sich aber z.B. bei *Müller/Mischler* (Fn. 45).

logeme (Deutungsmuster) geht.[64] In den letzten Jahren bildete sich eine Art (extrem) rechter Internetkultur heraus, die soziale Medien als den Austragungsort ihrer politischen Kämpfe verstehen und nutzen. Anhand von Memes, Shitposting, Trolling und Doxing sollen jene, die entweder außerhalb ihrer weißen Gemeinschaft verortet werden und/oder entgegen ihres Weltbildes handeln, mundtot gemacht werden.[65] Prominentes Beispiel für die Aneignung eines vorher harmlosen Internetphänomens ist der Frosch Pepe, der durch die US-amerikanische Alt-Right gekapert und insbesondere im US-Wahlkampf eingesetzt wurde. Bilder von Pepe in SS-Uniform oder als Donald Trump wurden und werden unzählige Male geteilt und verbreitet.[66]

Die Attentate von Christchurch, Poway, El Paso oder Halle verdeutlichten auf schockierende Weise die Rolle, die (extrem) rechte Kommunikation und Kommunikationskanäle online spielen. Es lässt sich eine rasantere Internationalisierung des rechten Terrorismus, welche über das Internet vorangetrieben wird, beobachten,[67] bei der die Attentäter sich explizit aufeinander beziehen.[68] In Diskussionsforen und auf Imageboards kündigten sie ihre Taten an. Neben der klaren ideologischen Positionierung inszenierten sie die Anschläge und die dazu veröffentlichten Dokumente dabei in Anlehnung an Videospiele. Die Attentäter aus Christchurch und Halle stellten sogar Livestreams ihrer Taten online, sodass Menschen auf Facebook oder Twitch ihre Morde wie in einem Ego-Shooter-Videospiel, bei dem es Punkte für möglichst viele Opfer gibt, miterleben konnten. Diese Entwicklungen werden auch als „Gamification" des Terrors bezeichnet.[69] Als Vorbild diente ihnen dabei der Doppelanschlag Anders Breiviks in Norwegen im Jahr 2011.[70]

Die Attentäter werden von der Community verehrt[71] und sie folgten allesamt dem Prinzip einer „leaderless resistance", eines führungslosen Widerstands, der inspiriert und motiviert durch die vorherigen Taten, jedoch nicht im Namen einer Organisation durchgeführt wird.[72] Die Taten sind in gesellschaftlichen Zusammenhängen zu lesen, sowohl in herkömmlichen als auch in digitalen Sozialräumen. Anders als zuvor muss Propaganda nicht zentral von (extrem) rechten Akteuren betrieben werden. Die Individuen manipulieren sich selbst, indem sie fake news oder anderweitig ideologische Fragmente unzählige Male teilen. Dabei bleiben die Strukturen rechter Online-Akteure jedoch diffus, die Grenzen zwischen organisierten Aktivisten und individuellen Supportern sind fließend:[73] Auf der einen Seite lassen sich strategisch durchgeführte Kampagnen nachverfolgen, bei denen Memes eingesetzt werden, um raus aus einem Nischendiskurs, weiter in den gesamtgesellschaftlichen Diskurs vorzudringen, z.B. im Kontext des Netzwerkes Reconquista Germanica, welches es sich zum Ziel gesetzt hatte, das Internet „zurückzuerobern".[74] Auf der anderen Seite treten rechtsgerichtete menschenverachtende Ideologien nicht nur in geplanten Kampagnen organisiert in Social Media auf, sondern entladen sich z.B. in Echokammern, innerhalb derer sich Kommunizierende gegenseitig ihrer menschenverachtenden Weltsicht bestätigen.[75] Gleichzeitig bemühen sich organisierte extrem rechte Akteure, auch jenen „Hass" zu kanalisieren und die ihn Äußernden zu führen. Dies würde wiederum bedeuten, dass manche Individuen sich gegebenenfalls nicht darüber im Klaren sind, Teil faschistischer Dynamiken zu sein und geleitet zu werden,[76] also beispielsweise Memes zu teilen, ohne sich deren wahrer Bedeutung oder möglicher Auswirkungen bewusst zu sein.

Karikaturen und Memes können dabei helfen, Deutungsmuster bzw. Ideologeme, also einzelne Bestandteile solcher Ungleichwertigkeitsideologien, zu verbreiten und zu verankern.[77] Das Agieren mit und um Memes kann demnach als soziale Praktik verstanden werden, die die eigene ideologische Positionierung klarstellt. Dies kann entweder unterschwellig geschehen oder sehr explizit. *Bogerts* und *Fielitz* stellen dazu fest: „Although, at first sight, memes seem to be humorous, sometimes silly and absurd – but in any case, harmless – everyday expressions of online cultural creativity, they can still convey hate messages, attract new supporters and give rise to bigotry."[78]

Das hier dargestellte Meme (*Abbildung 2*, siehe unten S. 420) stammt aus einer offenen Facebook-Gruppe, in der vorwiegend cvK stattfand, die rechtsextreme Deutungsmuster reproduzierte. Das Meme selbst tut dies auf den ersten Blick eher unterschwellig, wirkt durch die popkulturelle Anlehnung

[64] *Albrecht/Fielitz/Thurston*, in: Fielitz/Thurston (Hrsg.), Post-Digital Cultures of the Far-Right: Online Actions and Offline Consequences in Europe and the US, 2019, S. 7.
[65] *Albrecht/Fielitz*, in: Institut für Demokratie und Zivilgesellschaft (Hrsg.), Schriftenreihe des Instituts für Demokratie und Zivilgesellschaft. Schwerpunkt: Rechtsterrorismus, 2019, S. 176 (180).
[66] *Miller-Idriss*, in: Fielitz/Thurston (Fn. 64), S. 123 f.
[67] *Albrecht/Fielitz* (Fn. 65), S. 178 f.
[68] *Sieber*, Der rechte Rand 118, 2019, abrufbar unter https://www.der-rechte-rand.de/archive/5454/halle-anschlag-ego-shooter/ (2.9.2020); *Ayyadi*, Antisemitische Tat in Halle: Die „Gamification" des Terrors – Wenn der Hass zu einem Spiel verkommt, 2019, abrufbar unter https://www.belltower.news/antisemitische-tat-in-halle-die-gamification-desterrors-wenn-hass-zu-einem-spiel-verkommt-91927/ (2.9.2020).
[69] *Sieber* (Fn. 68); *Ayyadi* (Fn. 68).
[70] Siehe auch Fn. 13.
[71] *Sieber* (Fn. 68); *Ayyadi* (Fn. 68).
[72] *Fielitz/Marcks*, Digital Fascism. Challenges for the Open Society in Times of Social Media, 2019, S. 7.
[73] *Fielitz/Marcks* (Fn. 72), S. 7 f.
[74] Siehe auch *Bogerts/Fielitz*, in: Fielitz/Thurston (Fn. 64), S. 137; *Book*, in: Speit (Hrsg.), Das Netzwerk der Identitären: Ideologie und Aktionen der Neuen Rechten, 2018, S. 93.
[75] *Montag*, in: Baldauf/Ebner/Guhl (Hrsg.), Hassrede und Radikalisierung im Netz, 2018, S. 31.
[76] *Fielitz/Marcks* (Fn. 72), S. 7 f.
[77] *Hofmann/Ipsen*, Jugend Medien Schutz-Report 41 (3/2018), 2.
[78] *Bogerts/Fielitz* (Fn. 74), S. 138.

an das bekannte Plakat des Films „Der Herr der Ringe – die Gefährten“ zunächst ironisierend und humoristisch, ist aber eindeutig mit entsprechenden extremistischen Narrativen aufgeladen.

Im Zentrum zu sehen ist Angela Merkel als „Herrin der Flüchtlinge“ „gedreht mit einem Milliardenbudget der EU“. Einer ihrer „Gefährten“ ist der türkische Präsident Recep Tayyip Erdoğan. Zwischen beiden steht Ahmed al-Assir, ein radikaler salafistischer Prediger, der 2017 im Libanon zum Tode verurteilt wurde. Die Person auf der linken Seite konnte von uns nicht identifiziert werden, es ist aber davon auszugehen, dass es sich um einen Kämpfer des IS handelt. Zudem sind Szenen einer Erschießung zu sehen. Unten im Bild erkennbar werden Geflüchtete dargestellt bzw. symbolisiert. Auf dem echten Filmplakat sind an dieser Stelle die Nazgûl abgebildet – die neun Ringgeister Saurons, dem Hauptantagonisten der Saga.

Der Kontext des Posts ist eine Amokfahrt in Münster am 7. April 2018, bei der nach Ermittlungen ein politischer oder extremistischer Hintergrund ausgeschlossen wurde. Neben verschwörungstheoretischen Annahmen, das Ereignis sei gar nicht geschehen, finden sich in der Diskussion Schuldzuweisungen an Angela Merkel. Sie selbst und Geflüchtete werden für die Amokfahrt und für die „deutschen Zustände“ im Allgemeinen verantwortlich gemacht.

Bedient werden die Deutungsmuster eines zum Opfer werdenden „deutschen Volkes“ durch „die da oben“, im Speziellen Angela Merkel. Sie selbst wird anhand ihrer Asylpolitik für einen angeblich bevorstehenden Untergang Deutschlands verantwortlich gemacht. Asylsuchende werden dabei in der zugehörigen Diskussion wie auch im Meme selbst generalisiert abgewertet – die Deutungsmuster des antimuslimischen Rassismus und des Ethnosexismus sind hiermit eng verknüpft. Im Meme werden Geflüchtete gar als Armee oder dienstbare Geister Merkels dargestellt, die in Analogie zum „Herrn der Ringe“, aber auch in Abweichung zur Bildkomposition des Originalplakates (im Zentrum steht dort der Hobbit Frodo, nicht Sauron, mit dem Merkel hier, bildlich und durch die Titelgebung, gleichgesetzt wird) ihren Willen umsetzen.

Die das Meme postende Person selbst ist im Diskussionsverlauf der Auffassung, der Amoklauf sei von einer psychisch labilen Person ausgeführt worden und widerspricht insofern den verschwörungstheoretischen Annahmen seiner Vorredner. Der Amoklauf wird aber damit entschuldigt, dass es kein Wunder sei, dass die Leute durchdrehten. Es wird ein dystopisches Bild gezeichnet: „Was hat man heute in Deutschland noch für eine Zukunft, vor allem, wenn man Familie hat, keine.“[79] Im Anschluss postet die Person das Meme. Die von der Person empfundene, angebliche „Deutschenfeindlichkeit“ wird durch das Meme nochmals betont, denn Angela Merkel ist hier die „Herrin der Flüchtlinge“ und nicht mehr der Deutschen.

Zusammenfassend lässt sich festhalten, dass hier niedrigschwellig humorisierend in eine mit rechtsextremen Deutungsmustern aufgeladene Gedankenwelt eingeladen wird, die sich manchen erst bei genauerem Hinsehen offenbart.

In stärker radikalisierten Gruppen finden sich teils auch erheblich explizitere, viel offener rechtsextreme Memes. Von einer Reproduktion solcher Memes soll hier jedoch bewusst abgesehen werden.

VII. Fazit

Die Befunde des Teilvorhabens III („Qualitative und quantitative Analyse internetbasierter Propaganda“) des Verbundprojektes „Radikalisierung im digitalen Zeitalter“ deuten durchaus darauf hin, dass das digitale Zeitalter auch eines der entgrenzten Kommunikation und damit des digitalen Extremismus ist. Extremistische Ideologien wie der Rechtsextremismus und der salafistische Jihadismus finden im Internet, z.B. in Social-Media-Gruppen, durchaus reproduktionsförderliche Umweltbedingungen vor. Dies lässt sich auch theoretisch auf der Basis des Social Identity Approach und der SIDE-Theorie gut begründen.

Mit Blick auf das hier exemplarisch fokussierte Phänomen der Memes kann zudem festgehalten werden, dass derartige Bild-Text-Kompositionen Sinn konstituieren und verbreiten. In Kommunikationskontexten, in denen ohnehin extremistische Deutungsmuster reproduziert werden, enthalten auch Memes, wenig verwunderlich, abwertende Inhalte. Diese werden aber häufig, wie im hier gewählten Beispiel, über Ironisierung bzw. Humorisierung auf den ersten Blick abgemildert. Dadurch werden die Verbreitungschancen der Memes und damit auch der mittransportierten ideologisierten, menschenfeindlichen Deutungsmuster erhöht. Dabei werden derartige Weltbilder ersichtlich auch in öffentlichen, leicht zugänglichen Gruppen auf Facebook oder VKontakte propagiert.

Die Zielsetzung (extrem) rechter Memes liegt dabei auf dem scheinbaren „Aufdecken“ von „Missständen“, auf einer Selbststilisierung als Opfer oder, konträr dazu, als überlegen. Als Feindbilder dominieren vor allem Geflüchtete, Angela Merkel sowie generell politische Gegner. Die Explizität der Memes variiert je nach Radikalisierungsgrad der Zielgruppe.

[79] Wörtliches Zitat aus dem Post.

Abbildung 1: Narrative extrem rechter und salafistisch-jihadistischer Onlinekommunikation

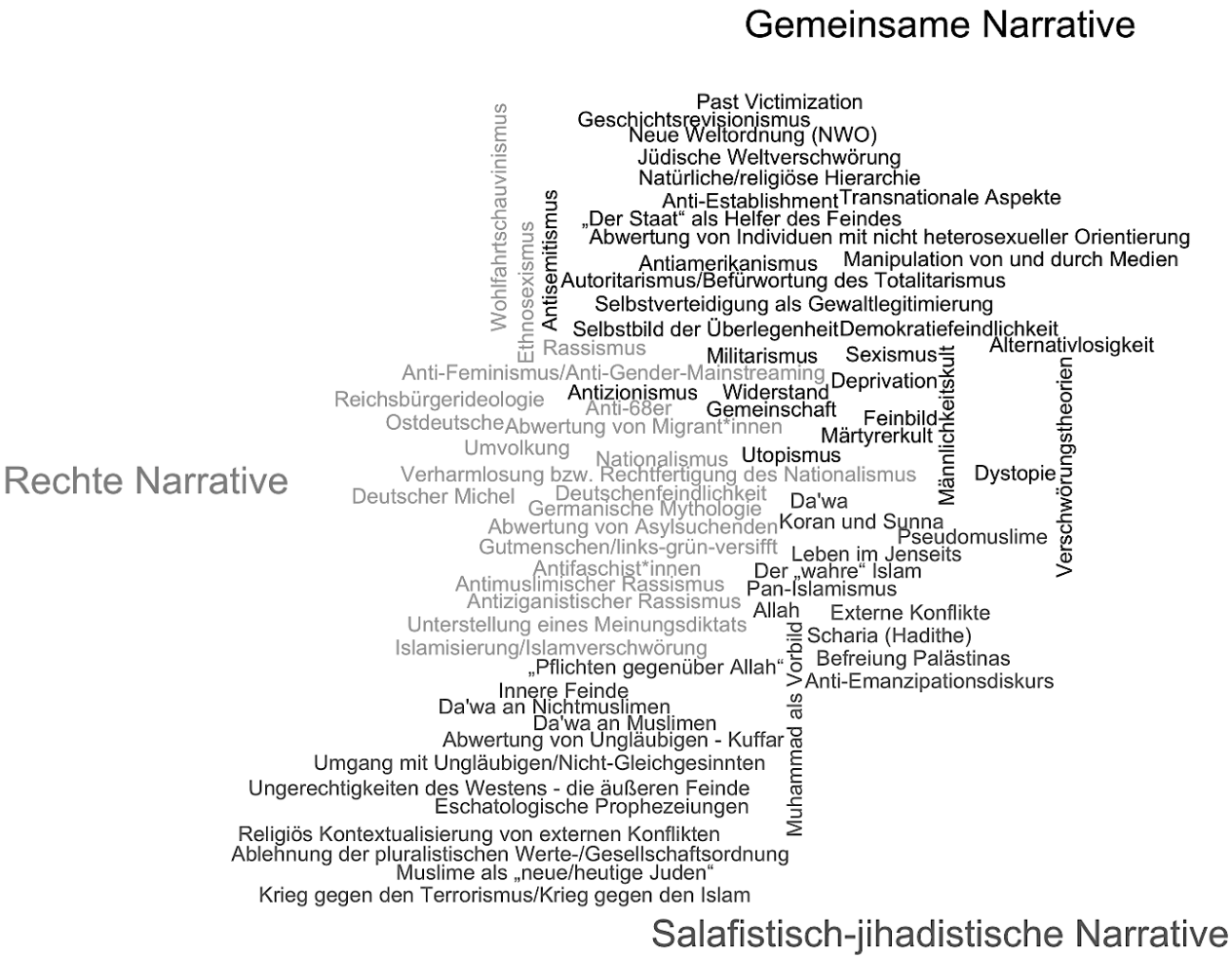
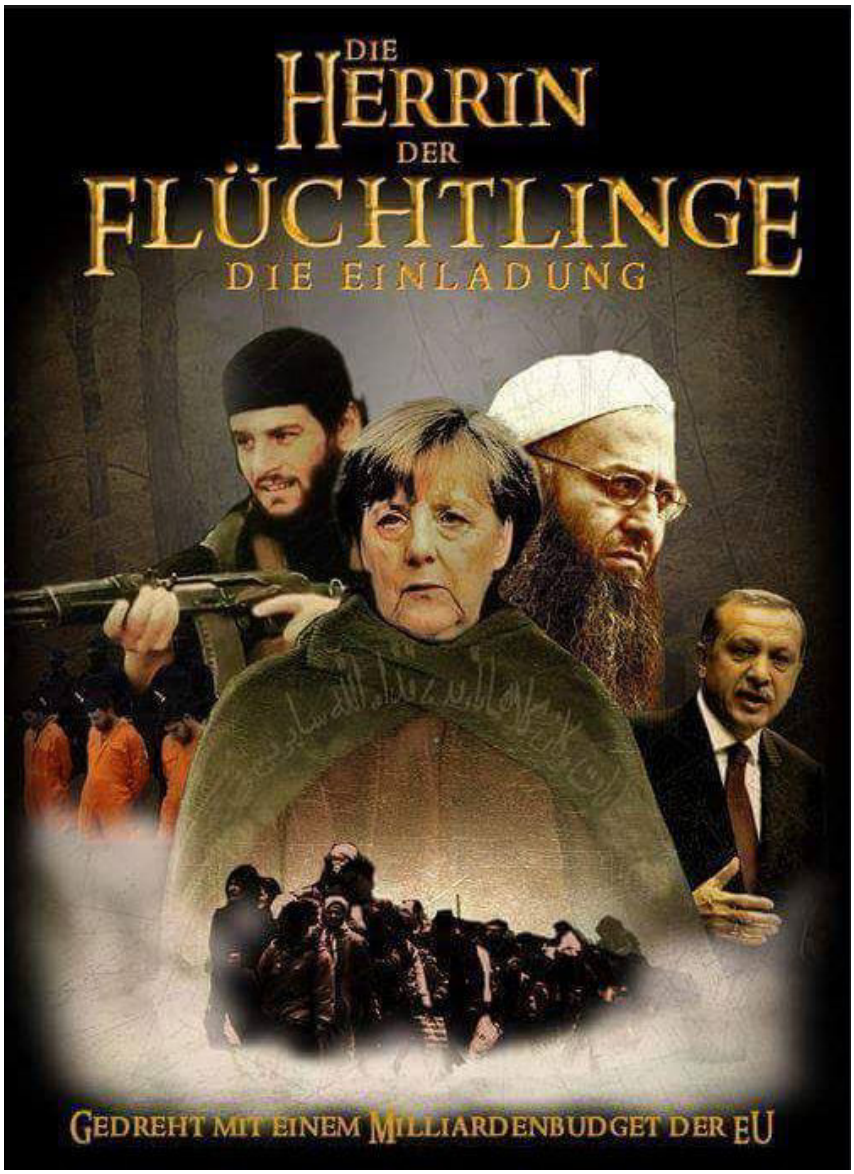


Abbildung 2: Meme aus einer rechtsextreme Deutungsmuster reproduzierenden Facebook-Gruppe



Surfen im Internet und Cloud Computing zwischen Telekommunikationsüberwachung und Online-Durchsuchung

Von Prof. Dr. **Manfred Heinrich**, Kiel

I. Neben den höchst zahlreich in der StPO geregelten Ermächtigungen zu „offenen" Eingriffen, wie insbesondere zu vorläufiger Festnahme (§§ 127 ff. StPO) und Untersuchungshaft (§§ 112 ff. StPO),[1] aber auch zu nicht freiheitsentziehenden Maßnahmen wie körperliche Untersuchung (§ 81a StPO), Durchsuchung (§§ 102 ff. StPO) und Beschlagnahme (§§ 94 ff. StPO),[2] steht den Strafverfolgungsbehörden mittlerweile auch ein ganzes Arsenal von Möglichkeiten zur Verfügung, „verdeckt" zu ermitteln:[3] von der Rasterfahndung (§ 98a StPO) bis zum Einsatz Verdeckter Ermittler (§ 110a StPO), von der Postbeschlagnahme (§ 99 StPO) bis zur Telekommunikationsüberwachung (§ 100a StPO), von der längerfristigen Observation (§ 163 f. StPO) über die Ausschreibung zur Beobachtung bei polizeilichen Kontrollen (§ 163e StPO) bis hin zur akustischen Wohnraumüberwachung (§ 100c StPO).

Gerade im Bereich des mittlerweile immer stärker in den Fokus auch der Ermittlungsbehörden gelangten Internetgeschehens hat der Gesetzgeber in den letzten Jahren zahlreiche spezifische Eingriffsnormen geschaffen, mit deren Hilfe es möglich ist, auf nahezu jedem nur erdenklichen Weg auch in der digitalen Welt effizient zu ermitteln. Die passgenauen Regeln etwa zur Bestandsdatenauskunft (§ 100j StPO), zur Erhebung von Verkehrsdaten (§ 100g StPO), zur Lokalisierung von Mobilfunkendgeräten (§ 100i StPO) und letztens auch zur Quellen-TKÜ (§ 100a Abs. 1 S. 2, 3 StPO) sowie zur Online-Durchsuchung (§ 100b StPO) scheinen kaum mehr nennenswerte Lücken im einschlägigen Regelungskonzept unserer StPO zu belassen.

Bei genauerem Hinsehen ist dem jedoch keineswegs so, und zwar gerade auch im Hinblick auf ganz grundlegende Verhaltensweisen des heutigen Internetnutzers. So ist es noch längst nicht ausdiskutiert, ob bzw. inwieweit und unter Heranziehung welcher Eingriffsnormen man auf das wohl als Regelverhalten aller Internet-Nutzer anzusprechende „Surfen im Internet" strafverfolgerischen Zugriff nehmen darf;[4] und nichts anderes gilt auch für das zwar noch nicht ubiquitär anzutreffende, aber doch in immer weiter zunehmendem Maße genutzte sog. Cloud Computing[5] – was letztlich nichts anderes meint, als die Möglichkeit, sowohl Daten wie auch ganze Datenverarbeitungsprozesse auf im Netz für diese Zwecke verfügbar gestellte fremde Server auszulagern.[6]

Nun ist es durchaus nachvollziehbar, dass die Strafverfolgungsbehörden ein gehobenes Interesse daran haben, im Rahmen ihrer Ermittlungstätigkeit ggf. auch in diesen soeben benannten Richtungen hin tätig zu werden.[7] Dabei ist aus dem Instrumentarium der StPO heraus an eben die beiden im Titel dieses Beitrags erwähnten Eingriffsermächtigungen zu denken: zum einen die Telekommunikationsüberwachung des § 100a StPO (TKÜ)[8] und zum anderen die Online-Durchsuchung des § 100b StPO[9]. Ihrem Wesen nach unterscheiden sich die beiden Maßnahmen ganz grundlegend darin, dass die TKÜ sich mit dem Auslesen bzw. Ausleiten der Inhalte aktuellen Kommunikationsgeschehens beschäftigt,[10] die Online-Durchsuchung hingegen Zugriff zu nehmen gestattet auf die gesamten im betreffenden Informationsverarbeitungssystem anzutreffenden Inhalte, gleichgültig, ob diese sich schon lange auf den Speichermedien des Systems befinden oder gerade „frisch hereingekommen" sind.[11]

---

[1] Näher hierzu *Heinrich*, in: Krey/Heinrich, Deutsches Strafverfahrensrecht, 2. Aufl. 2019, Rn. 718 ff., 773 ff.

[2] Eingehend auch zu diesen *Heinrich* (Fn. 1), Rn. 798 ff.

[3] Vgl. *Heinrich* (Fn. 1), Rn. 856 ff. mit Überblick in Rn. 857 f.

[4] Für eine Anwendbarkeit des § 100a StPO bspw. *Bruns*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, § 100a Rn. 4; dagegen u.a. *Wolter/Greco*, in: Wolter (Hrsg.), Systematischer Kommentar zur Strafprozessordnung, Bd. 2, 5. Aufl. 2016, § 100a Rn. 31a m.w.N.; für eine Anwendbarkeit des § 100b StPO etwa *Eschelbach*, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafprozessordnung, 3. Aufl. 2018, § 100a Rn. 5.

[5] Wie Fn. 4; siehe auch *Hauck*, in: Becker/Erb/Esser/Graalmann-Scheerer/Hilger/Ignor, Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 3/1, 27. Aufl. 2019, § 100a Rn. 85.

[6] Ausführlich zum Begriff „Cloud Computing" *Hiéramente/Fenina*, StraFo 2015, 365 (366 f.); näher noch unten, IV. 1.

[7] Vgl. speziell zum Cloud Computing *Gähler*, HRRS 2016, 340 (341): „Ein Zugriff auf all diese Daten ist aus Perspektive der Ermittlungsbehörden selbstredend von großem Interesse."; siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (367): „Grundsätzlich haben die Ermittlungsbehörden aus ermittlungstaktischen Gründen ein Interesse, weitgehenden und zeitnahen Zugriff auf die Daten zu erlangen."

[8] Ausführlich hierzu *Heinrich* (Fn. 1), Rn. 871 ff.

[9] Ausführlich hierzu *Heinrich* (Fn. 1), Rn. 914 ff.

[10] Vgl. nur *Bruns* (Fn. 4), § 100a Rn. 5: „regelt § 100a nur den Eingriff in den technischen Vorgang der Nachrichtenübermittlung, also vom Absenden der Signale bis zu deren Empfang beim Adressaten"; siehe auch *Eschelbach* (Fn. 4), § 100a Rn. 2: „Überwachung und Aufzeichnung von laufender Kommunikation".

[11] Vgl. wiederum *Bruns* (Fn. 4), § 100a Rn. 6, insoweit klar von laufenden Übertragungsvorgängen abgrenzend: Es seien „die auf der Festplatte […] gespeicherten empfangenen Daten […] nicht von § 100a erfasst", der Zugriff auf die „angekommenen" Daten erfolge vielmehr „unter den besonderen Voraussetzungen der Online-Durchsuchung nach § 100b"; in diesem Sinne auch *Knierim/Oehmichen*, in: Knierim/Oehmichen/Beck/Geisler, Gesamtes Strafrecht aktuell, 2018, Kap. 20 Rn. 27; siehe auch *Eschelbach* (Fn. 4), § 100b Rn. 1: Auslesen von „Informationen, die auf dem informationstechnischen System *gespeichert* sind" (*Hervorhebung* auch im Original).

II. Beginnen wir mit der TKÜ: Diese in § 100a StPO sehr detailliert geregelte Maßnahme[12] erlaubt unter vergleichsweise strengen Voraussetzungen[13] die Überwachung und Aufzeichnung von „Telekommunikation". Und damit stellt sich bereits die erste in unserem Zusammenhang kernrelevante Frage: Erfasst der in § 100a StPO zugrunde zu legende „Telekommunikations"-Begriff überhaupt auch den *einseitigen Datenabruf*, wie er namentlich beim bloßen Surfen im Internet, im Falle der Internetrecherche oder auch beim Cloud Computing zu verzeichnen ist? Hier scheiden sich die Geister, sind doch mindestens drei verschiedene Ausdehnungen für diesen Begriff (und damit den Anwendungsbereich der TKÜ) im Gespräch:

Der weiteste Begriff von Telekommunikation ist derjenige des § 3 Nr. 22 Telekommunikationsgesetz (TKG), in welchem er definiert wird als „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen".[14] Danach wären auch die Übertragungsvorgänge beim Internetsurfen und dem Cloud Computing ohne Weiteres „Telekommunikation".[15]

Nun besteht aber weitestgehend Einigkeit darüber, dass diese einzig am technischen Aspekt des Telekommunikationsgeschehens ausgerichtete Sicht dem Schutzzweck des § 100a StPO nicht gerecht wird,[16] nachdem dieser doch die Grenzen zulässigen Eingriffs in das Fernmeldegeheimnis des Art. 10 GG festlegen will.[17] Mit der seinerzeit[18] erfolgten Umformulierung der ehemaligen „Überwachung des Fernmeldeverkehrs" in die heutige „Telekommunikationsüberwachung" sollte zwar der technischen Entwicklung Rechnung getragen werden.[19] Nicht aber ging es darum, den an Art. 10 GG ausgerichteten Schutzbereich der Eingriffsnorm zu verändern:[20] Nach wie vor sollteEreignisraum der ggf. über. § 100a StPO zu rechtfertigenden Eingriffe der Bereich menschlichen Kommunizierens sein,[21] nicht aber auch den – vom technikorientierten § 3 Nr. 22 TKG ebenfalls erfassten – „‚blinden' Austausch von Informationen zwischen Maschinen"[22] umgreifen.[23] Nach allgemeiner Auffassung fallen daher aufgrund ihrer automatischen Generierung – und als damit von vornherein außerhalb des Schutzbereichs des Art. 10 GG stehend – weder die Positionsmeldungen eines Mobilfunkendgerätes unter „Telekommunikation" i.S.d. § 100a StPO,[24] noch die im Zuge der Mauterfassung auf deutschen Autobahnen erhobenen und weitergeleiteten Daten.[25]

Angesichts dessen stellt sich nun die Frage, ob denn nicht auch die hier zu behandelnden Formen des einseitigen Datenabrufs diesem Verdikt unterfallen. Dies wird im Schrifttum vielfach angenommen,[26] weil es sich bei der im Internetsur-

[12] Ausführlich zu ihr *Heinrich* (Fn. 1), Rn. 871 ff.

[13] Vgl. im Einzelnen *Heinrich* (Fn. 1), Rn. 880 ff.

[14] Wobei gemäß § 3 Nr. 23 TKG unter „Telekommunikationsanlagen" zu verstehen sind: „Technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können".

[15] So denn etwa auch *Bruns* (Fn. 4), § 100a Rn. 4; siehe auch *Hauck* (Fn. 5), § 100a Rn. 31.

[16] Vgl. nur *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, 63. Aufl. 2020, § 100a Rn. 6, sowie BVerfG NJW 2016, 3508 (3509), Rn. 32: „Die nähere Auslegung des Begriffs ‚Telekommunikation' im Rahmen des § 100a StPO muss sich […] insbesondere auch an dem grundrechtlichen Schutz des Betroffenen durch Art. 10 GG orientieren […]. Dabei ist […] zu berücksichtigen, dass Art. 10 I GG nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes folgt."; siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a: „Der Telekommunikationsbegriff von Art. 10 GG deckt sich nicht mit dem entsprechenden Begriff aus dem Telekommunikationsgesetz."

[17] BVerfG NJW 2016, 3508 (3509), Rn. 32: „denn das Fernmeldegeheimnis ist der verfassungsrechtliche Maßstab für die heimliche Überwachung flüchtiger Daten".

[18] Durch Art. 2 Abs. 9 Nr. 2 des Gesetzes v. 17.12.1997, BGBl. I 1997, S. 3108.

[19] So ist es denn dank ebendieser technischen Entwicklungsoffenheit des § 100a StPO mittlerweile auch „selbstverständlich und weitestgehend unstreitig, dass SMS, E-Mails, Chatnachrichten, Internettelefonie mittels einer Telekommunikationsüberwachung überwacht werden dürfen." (*Hiéramente/Fenina*, StraFo 2015, 365 [370]).

[20] *Hiéramente/Fenina*, StraFo 2015, 365 (370): „Der Wechsel des Kommunikationsmediums führt zwar zu technischem Anpassungsbedarf, ändert aber die Zielrichtung des § 100a StPO nicht wesentlich."

[21] In diesem Sinne zu Recht auch BGH NStZ 2018, 611 (612); siehe auch *Köhler* (Fn. 16), § 100a Rn. 6: „geht es bei § 100a um die Erfassung kommunikativen Sozialverhaltens"; *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl. 2017, § 36 Rn. 4: „Telekommunikation setzt das Vorhandensein eines menschlichen Kommunikationspartners voraus."

[22] So die Formulierung bei *Wolter/Greco* (Fn. 4), § 100a Rn. 14; siehe auch BGH NStZ 2018, 611 (612): „lediglich ein Datenaustausch zwischen technischen Geräten".

[23] BVerfG NJW 2007, 351 (353 f.); BGH NStZ 2018, 611 (612); *Wolter/Greco* (Fn. 4), § 100a Rn. 14; *Köhler* (Fn. 16), § 100a Rn. 6; siehe auch *Roxin/Schünemann* (Fn. 21), § 36 Rn. 4: „Werden Informationen von Anlage zu Anlage automatisch übermittelt, geht es noch nicht um Kommunikation."; *Hauck* (Fn. 5), § 100a Rn. 29 verlangt, „dass eine Person mittels dieser Technik Kommunikation betreibt".

[24] Vgl. BVerfG NJW 2007, 351 (353 f., zum Einsatz eines „IMSI-Catchers"), sowie BGH NStZ 2018, 611 (612, zum Versenden sog. „stiller SMS"); ebenso *Roxin/Schünemann* (Fn. 21), § 36 Rn. 4; *Wolter/Greco* (Fn. 4), § 100a Rn. 21; *Köhler* (Fn. 16), § 100a Rn. 6a; *Hauck* (Fn. 5), § 100a Rn. 68 (näher zur Technik a.a.O., Rn. 65).

[25] *Niehaus*, NZV 2004, 502 f.; *Köhler* (Fn. 16), § 100g Rn. 10; siehe auch *Knierim/Oehmichen* (Rn. 11), Kap. 20 Rn. 22; a.A. LG Magdeburg NJW 2006, 1073 (1074).

[26] Vgl. nur *Eschelbach* (Fn. 4), § 100a Rn. 5; *Köhler* (Fn. 16), § 100a Rn. 6, 14f.; *Roxin/Schünemann* (Fn. 21), § 36 Rn. 5; *Wolter/Greco* (Fn. 4), § 100a Rn. 31a m.w.N;

fen und beim Cloud Computing vonstattengehenden „einseitigen Nutzung informationstechnischer Systeme ohne sozialen Informationsaustausch“ um „keine vertrauliche ‚Kommunikation‘“ im Sinne des § 100a StPO handele.[27] Dem möchte ich hier gerne beipflichten.

Was gerade das Surfen im Internet anlangt, ist es doch tatsächlich so, dass im Internet Informationen lediglich für eine unbestimmte Zahl noch unbekannter Empfänger bereitgestellt werden, welche von diesen dann aus eigener Initiative heraus abgerufen werden können;[28] *wer* das dann aber im Zuge seiner Internetnutzung *wann* und *wo* und *in welchem Umfang* tut, ist nicht vorauszusehen.[29] Dieses letztlich *ungezielte* Ineinandergreifen von Informationsangebot und Informationsinanspruchnahme durch zwei in keiner Weise miteinander auch nur im Entferntesten verbundene Personen als individualisierte Kommunikation in einem sich in § 100a StPO widerspiegelnden materiellen Sinne aufzufassen,[30] will mir nicht so recht gelingen.[31]

Dies gilt insbesondere auch mit Blick darauf, dass bei der ehemaligen Überwachung des Fernmeldeverkehrs (landläufig: der früheren *Telefon*überwachung) angesichts damals noch begrenzter technischer Möglichkeiten gerade und nur an den kommunikativen Austausch zwischen zwei Personen gedacht worden war (eben den Beteiligten an einem Telefonat) und die Ausgestaltung des § 100a StPO sich an gerade dieser Grundkonstellation orientierte[32] – unter Abwägung der aus ihr erwachsenden gegenläufigen Interessen zwischen Persönlichkeitsschutz und Strafverfolgungsinteressen.[33] Gerade darauf hin, jene klassische zweiseitige Kommunikation angemessen zu erfassen, war § 100a StPO a.F. bei seiner Schaffung ausgelegt worden.[34]

Und auch beim Umbau der Vorschrift anlässlich des Wechsels von der Telefon- hin zur Telekommunikationsüberwachung[35] sollte an dieser Grundjustierung nicht gerüttelt werden,[36] wurden jedenfalls keine gesetzgeberischen Gedanken darauf verwendet, neben der altbekannten zweiseitigen Kommunikation nunmehr auch etwaige Formen einseitiger Kommunikation mit ins Boot zu nehmen, sprich: einen in diesem Sinne erweiterten Anwendungsbereich in die Neugestaltung des § 100a StPO mit einfließen zu lassen.[37] Anders gesagt: Es haben sich zwar neue Formen im weiteren Sinne kommunikativen Geschehens entwickelt, § 100a StPO ist aber bis heute (mangels entsprechend ausgerichteter Umgestaltung) von seinem Regelungspotential noch immer allein auf die herkömmliche zweiseitige Kommunikation hin ausgerichtet.[38] Angesichts des niemals vorgenommenen entsprechenden Umbaus ist er auch gar nicht in der Lage, in einer den Besonderheiten einseitiger Kommunikation gerecht werdenden Weise über den tradierten Anwendungsbereich hinaus sachgerechte Ergebnisse zu liefern.[39]

Dem hält das BVerfG allerdings entgegen:[40] „Bei der Nutzung des Internets durch eine natürliche Person kommunizieren […] nicht ausschließlich technische Geräte miteinander […]. Vielmehr ist das für die Auslösung des Art. 10 GG notwendige spezifische Gefährdungspotenzial für die

siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (370): „Der Telekommunikationsbegriff der StPO setzt eine soziale Dimension voraus.“ – Dagegen jedoch *Bär*, in: v. Heintschel-Heinegg/Stöckel (Hrsg.), KMR, Kommentar zur Strafprozeßordnung, 70. Lfg., Stand: November 2013, § 100a Rn. 11a: „Der Telekommunikationsbegriff ist nicht auf eine Kommunikation zwischen Personen begrenzt.“; in diesem Sinne auch *Bruns* (Fn. 4), § 100a Rn. 4; *Hauck* (Fn. 5), § 100a Rn. 31.

[27] So speziell zum Internetsurfen *Wolter/Greco* (Fn. 4), § 100a Rn. 31a m.w.N.: „Bei § 100a müssen Sender und Empfänger natürliche Personen sein.“; entsprechend *Hiéramente/Fenina*, StraFo 2015, 365 (372) zum Cloud Computing: „Wer eine virtuelle Festplatte nutzt, Rechenleistung in der Cloud abruft oder dort Programme/Apps zur Datenverarbeitung verwendet, kommuniziert nicht im Sinne des § 100a StPO.“; siehe auch *Köhler* (Fn. 16), § 100a Rn. 6: Es gehe „bei § 100a um die Erfassung kommunikativen Sozialverhaltens“.

[28] So ganz richtig *Eidam*, NJW 2016, 3511 (3512).

[29] *Eidam*, NJW 2016, 3511 (3512).

[30] Explizit dagegen zu Recht *Eidam*, NJW 2016, 3511 (3512).

[31] In diesem Sinne auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a m.w.N.: „Bei der Lektüre einer Online-Zeitung oder dem Betrachten eines Livestreams oder gar von Internetfernsehen kann schwerlich von Telekommunikation die Rede sein“.

[32] Ganz richtig *Hiéramente/Fenina*, StraFo 2015, 365 (370): „Hinsichtlich der Intention des Gesetzgebers der Ursprungsfassung des § 100a StPO kann aufgrund der limitierten Fähigkeiten des analogen Telefonanschlusses […] mit hinreichender Wahrscheinlichkeit angenommen werden, dass ein sozialer Kommunikationsbegriff zugrunde gelegt wurde. Das heutige Multifunktionsgerät war schließlich nicht einmal in Sichtweite.“

[33] Näher und treffend hierzu *Hiéramente/Fenina*, StraFo 2015, 365 (369 f.).

[34] Vgl. *Hiéramente/Fenina*, StraFo 2015, 365 (369): „Einleuchten dürfte, dass die ursprüngliche Intention des § 100a StPO das Abhören von ‚Ganovengesprächen‘ gewesen ist.“

[35] Vgl. bereits oben bei und in Fn. 18.

[36] So denn auch BVerfG NJW 2016, 3508 (3509): „Der Begriff ‚Telekommunikation‘ […] setzt das ‚Fernmeldewesen‘ fort und wird nach wie vor in Anlehnung an die Definition dieses verfassungsterminologischen Vorläufers bestimmt“.

[37] Vgl. nur die einschlägige Gesetzesbegründung in BR-Drucksache 369/97, S. 27 ff., 45 f.

[38] So entspricht es denn auch durchaus der immer wieder erwähnten „technischen Entwicklungsoffenheit“ des § 100a StPO und ist es von daher „selbstverständlich und weitgehend unstreitig, dass SMS, E-Mails, Chatnachrichten, Internettelefonie mittels einer Telekommunikationsüberwachung überwacht werden dürfen“ (*Hiéramente/Fenina*, StraFo 2015, 365 [370]).

[39] Nach (zutreffender) Auffassung von *Hiéramente*, HRRS 2016, 448 (452), ist „die Überwachung der Internetnutzung […] ein Grundrechtseingriff eigener Art“, der „aufgrund der gesteigerten Eingriffsintensität eine eigenständige strafprozessuale Grundlage“ erfordert.

[40] BVerfG NJW 2016, 3508 (3510); explizit dagegen *Eschelbach* (Fn. 4), § 100a Rn. 5 m.w.N.

Privatheit der Kommunikation vorhanden, da […] willensgesteuert auf konkrete Kommunikationsinhalte zugegriffen wird. Auch das ‚Surfen' im Internet ist unter das Fernmeldegeheimnis zu subsumieren."

Nun ist dies freilich nur auf den ersten Blick ein Plädoyer für einen entsprechend weiten Anwendungsbereich des § 100a StPO.[41] Denn es mag ja sein und es soll hier auch gar nicht bestritten werden,[42] dass auch die „einseitige Nutzung informationstechnischer Systeme ohne sozialen Informationsaustausch"[43] in den Schutzbereich des Art. 10 GG fällt[44] – doch mehr hat das BVerfG auch gar nicht gesagt.[45] Insbesondere hat es aus seiner Aussage *nicht* den Schluss gezogen, aufgrund der Subsumierbarkeit unter das Fernmeldegeheimnis sei auch bereits per se und ohne Weiteres der Anwendungsbereich des – wie ich meine: dazu weder gedachten, noch geeigneten – § 100a StPO eröffnet.[46] Letztlich ging es dem Gericht vielmehr darum herauszuarbeiten, dass ein extensives Verständnis des § 100a StPO immerhin insofern verfassungskonform sei, als es mit dem in Art. 10 GG ausgelobten Schutz des Fernmeldegeheimnisses im Einklang stehe.[47] Wo also das Auslesen der Positionsmeldungen eines Mobiltelefons schon mangels überhaupt eines Bezugs zum Fernmeldegeheimnis aus der Anwendbarkeit des § 100a StPO herausfalle,[48] lasse sich dies im Hinblick auf Vorgänge des einseitigen Datenabrufs aufgrund ihrer Grundrechtsrelevanz nicht behaupten.[49]

Das war es dann aber auch, mehr Bindendes zur Anwendbarkeit des § 100a StPO ist aus den Ausführungen des BVerfG nicht herauszulesen.[50] So hebt denn auch das Gericht selbst ausdrücklich noch einmal den eingeschränkten verfassungsrechtlichen Prüfungsmaßstab hervor:[51] „Ein etwaiger Fehler der Fachgerichte muss gerade in der Nichtbeachtung von Grundrechten liegen. […] Nach diesem Maßstab ist die angegriffene Entscheidung des Landgerichts Ellwangen von Verfassungs wegen nicht zu beanstanden."[52] Nicht mehr und nicht weniger ist also mit der Feststellung des BVerfG im Hinblick auf die vom Landgericht Ellwangen befürwortete Erstreckung des § 100a StPO auch auf bloßes Surfen im Internet zum Ausdruck gebracht.[53] Ob nun aber § 100a StPO in eben dieser weiten Form nicht nur – aus verfassungsrechtlicher Sicht – angewendet werden dürfe, sondern vielleicht ja (aus welchen Gründen auch immer) sogar müsse, sei – so zu Recht das BVerfG[54] – eine Frage, die allein die Fachgerichte zu entscheiden hätten.

III. Somit ist die Frage der Erstreckbarkeit des § 100a StPO auch auf Internetsurfen und Cloud Computing letztlich aus einer wertenden Betrachtung des dem § 100a StPO einfachgesetzlich innewohnenden Regelungszwecks heraus zu beantworten – im Bewusstsein dessen, dass zwar die Eingriffsregelung des § 100a StPO sich im Rahmen des durch Art. 10 GG eröffneten Schutzbereichs bewegen muss, nicht aber angesichts jenes Schutzbereichs jede innerhalb seiner Umgrenzung stattfindende Ermittlungsmaßnahme auch von der Ermächtigungsnorm des § 100a StPO erfasst zu sein braucht.[55] Vielleicht, so der Gedanke, handelt es sich ja bei der strafverfolgerischen Überwachung des Internetsurfens oder Cloud Computings um Maßnahmen, die zwar in das

[41] In jenem (missverstandenen) Sinne etwa *Beulke/Swoboda*, Strafprozessrecht, 14. Aufl. 2018, Rn. 253a: „Auch das Surfverhalten […] unterfällt bei einer weiten Auslegung des Begriffs der Telekommunikation, wie sie vom BVerfG bestätigt wurde, dem Anwendungsbereich des § 100a StPO."

[42] Anders jedoch *Eschelbach* (Fn. 4), § 100a Rn. 5.

[43] So die Formulierung bei *Eschelbach* (Fn. 4), § 100a Rn. 5.

[44] Insofern durchaus überzeugend *Gähler*, HRRS 2016, 340 (343), speziell zum Cloud Computing.

[45] In diesem Sinne auch *Hiéramente*, HRRS 2016, 448 (449): „Eine umfassende Antwort haben die Karlsruher Richter vermieden."

[46] So aber (freilich noch vor der Entscheidung des BVerfG) *Bär* (Fn. 26), § 100a Rn. 11a; dies kritisierend sprechen *Hiéramente/Fenina*, StraFo 2015, 365 (371), ganz richtig von dem „fragwürdige[n] Umkehrschluss von der Interpretation des Art. 10 GG auf die Interpretation des § 100a StPO"; und auch *Wolter/Greco* (Fn. 4), § 100a Rn. 13, betonen, dass „der häufig anzutreffende Schluss von der Betroffenheit des Schutzbereichs von Art. 10 I GG auf die Anwendung von § 100a nicht richtig ist."; siehe auch unten, Fn. 55.

[47] In diesem Sinne auch *Hiéramente*, HRRS 2016, 448 (449).

[48] Hierzu BVerfG NJW 2007, 351 (353 f.), zum Einsatz eines „IMSI-Catchers".

[49] Vgl. BVerfG NJW 2016, 3508 (3510): „Bei der Nutzung des Internets durch eine natürliche Person kommunizieren […] nicht ausschließlich technische Geräte miteinander".

[50] Ganz richtig *Hiéramente*, HRRS 2016, 448 (449): „Auch wenn eine gewisse Tendenz für eine extensive Interpretation der staatsanwaltschaftlichen Ermittlungsbefugnisse zu erkennen ist, zieht sich der 2. Senat des Gerichts auf die grundlegende Feststellung zurück, dass die Entscheidung des Landgerichts Ellwangen aus verfassungsrechtlichen Gründen nicht in Zweifel zu ziehen sei."

[51] So auch der Hinweis bei *Hiéramente*, HRRS 2016, 448 (449).

[52] BVerfG NJW 2016, 3508.

[53] BVerfG NJW 2016, 3508 (3510): „Somit steht auch der Bedeutungsgehalt des Art. 10 I GG der vom LG vorgenommenen Auslegung des § 100a StPO nicht entgegen".

[54] Vgl. BVerfG NJW 2016, 3508: Es sei zu beachten, „dass die Auslegung und Anwendung von Strafprozessrecht Sache der dafür allgemein zuständigen Gerichte und einer Nachprüfung durch das BVerfG grundsätzlich entzogen ist, soweit bei der zu treffenden Entscheidung nicht Willkür vorliegt oder spezifisches Verfassungsrecht verletzt wird".

[55] So konstatiert denn auch *Gähler*, HRRS 2016, 340 (343), zu Recht, es sei „anerkannt, dass allein von der Eröffnung des Schutzbereichs des Art. 10 Abs. 1 Var. 3 GG nicht auf Vorliegen einer ‚Telekommunikation' i.S.d. §§ 100a ff. StPO geschlossen werden kann."; vgl. nur *Wolter/Greco* (Fn. 4), § 100a Rn. 13 m.w.N; siehe auch BVerfG NJW 2009, 2431 (2433), sowie bereits oben, Fn. 46.

Grundrecht aus Art. 10 GG eingreifen, nicht aber durch § 100a StPO legitimiert sind.[56]

Dass diese Möglichkeit besteht,[57] wird gerade auch in den literarischen Stellungnahmen zur Problematik zumeist nicht beachtet. Stattdessen wird zum Ausdruck gebracht, dass doch auch die einseitige Datennutzung im Internet dem Schutzbereich des Art. 10 GG unterfalle (was ja durchaus zutreffen mag) und deswegen gerade aus Schutzzwecküberlegungen heraus § 100a StPO anwendbar sein müsse,[58] um derartige Ermittlungsmaßnahmen den (wie schon erwähnt) doch vergleichsweise strengen Voraussetzungen dieser Eingriffsnorm zu unterwerfen.[59]

Was dabei freilich übersehen wird, ist, dass mit einer dergestalt motivierten – vermeintlichen – Ausweitung des grundrechtlichen Schutzes man eben diesem einen Bärendienst erweist:[60] Erfasst man nämlich die einseitige Internetnutzung über § 100a StPO, ist damit nicht nur eine Anbindung an die (nochmals: vergleichsweise strengen) Eingriffsvoraussetzungen der TKÜ verbunden,[61] sondern wird damit eine legale Zugriffsmöglichkeit überhaupt erst geschaffen:[62] Denn wie jeder andere Grundrechtseingriff auch, bedarf auch der Zugriff auf die Formen einseitiger Internetnutzung einer gesetzlichen Eingriffsgrundlage, die erst über die Anwendung des § 100a StPO auf diese Fälle verfügbar wird, die hingegen bei Ablehnung einer solchen Anwendbarkeit schlicht nicht vorhanden wäre: Eine analoge Anwendung des § 100a StPO stünde, da mittels Analogie begründete Eingriffsermächtigungen im Strafverfahrensrecht per se nicht zulässig sind,[63] ebenso wenig zur Debatte, wie die Möglichkeit, entsprechende Zugriffe auf die Ermittlungsgeneralklauseln der § 161 Abs. 1 S. 1 StPO und § 163 Abs. 1 S. 2 StPO zu stützen.[64] Denn diese können nach allgemeiner – und richtiger – Auffassung nur herangezogen werden für Ermittlungsmaßnahmen, die entweder *nicht* in Grundrechte eingreifen oder bei denen allenfalls von einem geringfügigen, weniger intensiven Eingriff gesprochen werden kann[65] – wovon bei der Überwachung von Internetsurfen und Cloud Computing bei Weitem nicht die Rede sein kann.[66] Zurückzuweisen ist dabei der Gedanke, es könne „die offene Informationspreisgabe im Internet eine Einwilligung darstellen, sodass der polizeiliche Zugriff auf solche Informationen schon keinen Eingriff in das Fernmeldegeheimnis darstellt“[67] und deswegen „der polizeiliche Ermittlungszugriff schon über die Generalklausel des § 161 Abs. 1 S. 1, § 163 Abs. 1 S. 2 StPO gedeckt“ wäre.[68] Denn ebenso gut könnte man sonst die (ob ihrer Eingriffsintensität zu Recht) in §§ 100f, 100h und 163f StPO eigens geregelten Ermittlungsmaßnahmen schlicht auf die polizeiliche Eingriffsgeneralklausel stützen mit der Begründung, wer

[56] Ganz in diesem Sinne *Hiéramente/Fenina*, StraFo 2015, 365 (371): „Nur weil das Verhalten des Bürgers im Internet im Lichte des Art. 10 GG besonders schutzwürdig ist, muss es noch nicht § 100a StPO unterfallen.“; siehe auch *Hiéramente*, HRRS 2016, 448 (450): „Aus der grundgesetzlichen Schutzbedürftigkeit folgt nicht die Notwendigkeit der extensiven Interpretation der Eingriffsmaßnahme.“

[57] Ganz richtig heißt es bei *Hiéramente/Fenina*, StraFo 2015, 365 (371): „Ein Gleichlauf der Definitionen ist keineswegs zwingend.“, und, mit Blick auf u.a. BVerfG NJW 2009, 2431 (2433), es habe das BVerfG „bereits betont, dass der Rückschluss vom Grundrecht auf die Ermächtigungsgrundlage nicht zwangsläufig ist.“; siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 13: „Der Befugnisbereich von § 100a ist […] *nicht* mit dem Schutzzweck des Telekommunikationsgeheimnisses deckungsgleich.“ (*Hervorhebung* auch im Original).

[58] Vgl. *Gähler*, HRRS 2016, 340 (344): „Eine Zuordnung [zu § 100a StPO] muss auch unter Berücksichtigung des Aspektes erfolgen, ob der Betroffene aufgrund der Verdecktheit des Eingriffs in erhöhtem Maße schutzbedürftig ist.“

[59] So denn auf „die hohe Schutzbedürftigkeit des Cloud-Nutzers“ verweisend *Gähler*, HRRS 2016, 340 (344): „Durch die Subsumtion als Telekommunikation wird der Cloud-Nutzer […] privilegiert.“

[60] Ganz zu Recht spricht *Roggan*, StV 2017, 821 (823), hier von „*vermeintlich* grundrechtsfreundlicher Interpretation“ (*Hervorhebung* von *mir*).

[61] So aber *Hauck* (Fn. 5), § 100a Rn. 31, 81; siehe auch *Gähler*, HRRS 2016, 340 (344): „Der Eingriff darf erst unter den vergleichsweise strengen Voraussetzungen des § 100a StPO erfolgen und nicht schon nach den weiter gefassten Eingriffsvoraussetzungen anderer strafprozessualer Ermittlungsmaßnahmen.“; welche anderen (legalen) Maßnahmen dies sein sollen, lässt *Gähler* freilich offen.

[62] Ganz richtig *Hiéramente/Fenina*, StraFo 2015, 365 (371): „Schließt man Verhalten, wie etwa die Internetrecherche, aus dem Anwendungsbereich des § 100a StPO aus, ist […] die Überwachung […] dann mangels Eingriffsgrundlage in der StPO schlichtweg untersagt.“; ebenso die Einschätzung bei *Roggan*, StV 2017, 821 (823): Mittels Einbeziehung des Cloud-Computing in den Bereich der Telekommunikation „könnte […] die Zulässigkeit der Überwachung des Cloud-Computing auf Grundlage des § 100a Abs. 1 S. 2 StPO gefolgert werden“.

[63] Vgl. nur BVerfGE 29, 183 (195–197, für Eingriffe mit Freiheitsentzug), wo vom „Analogieverbot aus Art. 104 I GG, vergleichbar dem strafrechtlichen Analogieverbot aus Art. 103 II GG“ die Rede ist; siehe auch BVerfG NStZ 1996, 615; *Amelung*, NStZ 1982, 38 (40, zu § 136a StPO); *Konzak*, NVwZ 1997, 872 f.; *Krey*, ZStW 101 (1989), 838 (854 ff.); näher *Heinrich* (Fn. 1), Rn. 7 f., 701 m.w.N.

[64] So explizit *Wolter/Greco* (Fn. 4), § 100a Rn. 31a; ebenso hält LG Ellwangen ZD 2014, 33 (36), das Bemessen an dieser Vorschrift für „eher fatal“; anders jedoch *Hauck* (Fn. 5), § 100a Rn. 31, 81.

[65] Vgl. BGHSt 51, 211 (218, „lediglich geringfügig“); siehe auch *Köhler* (Fn. 16), § 161 Rn. 1 („weniger intensiv“); i.d.S. auch *Hilger*, NStZ 2000, 561 (564); *Griesbaum*, in: Hannich (Fn. 4), § 161 Rn. 1; näher *Heinrich* (Fn. 1), Rn. 703 ff. m.w.N.

[66] So betonen auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a, dass „die Ermittlungsgeneralklausel […] der Schwere des Eingriffs nicht gerecht zu werden vermag“.

[67] So aber *Hauck* (Fn. 5), § 100a Rn. 81.

[68] *Hauck* (Fn. 5), § 100a Rn. 81.

sich frei in der Öffentlichkeit bewege, willige damit konkludent in seine akustische bzw. visuelle Überwachung ein.

Kurzum: „Schließt man Verhalten, wie etwa die Internetrecherche, aus dem Anwendungsbereich des § 100a StPO aus, ist solch ein Verhalten nicht schutzlos gestellt. Im Gegenteil: Die Überwachung ist dann mangels Eingriffsgrundlage schlichtweg untersagt."[69]

IV. Lehnt man mithin, wie hier vertreten, da es sich bei der einseitigen Internetnutzung um keinen „sozialen Informationsaustausch", um „keine vertrauliche ‚Kommunikation' zwischen zwei Personen" und damit nicht um „Telekommunikation" i.S.d. § 100a StPO handelt, die Tauglichkeit eben dieser Vorschrift als Eingriffsnorm ab,[70] fragt sich, worauf sich Maßnahmen der Überwachung und Aufzeichnung von Internetsurfen, Internetrecherche, Cloud Computing etc. denn sonst stützen lassen – auf eine analoge Anwendung des § 100a StPO und eine Anwendbarkeit der Ermittlungsgeneralklauseln der § 161 Abs. 1 S. 1 StPO und § 163 Abs. 1 S. 2 StPO, wie schon erwähnt, jedenfalls nicht. Was bleibt, wäre noch die neuerdings vom Gesetzgeber in § 100b StPO zur Verfügung gestellte Online-Durchsuchung.[71]

Tatsächlich wird denn auch im Schrifttum nicht selten davon gesprochen, der hoheitliche Zugriff auf Internetsurfen, Cloud Computing etc. ähnele „ebenso im Erscheinungsbild wie beim Belastungsgewicht einer Online-Durchsuchung"[72] und sei daher „nunmehr nach § 100b StPO zu beurteilen".[73] An dieser Stelle ist es nun Zeit, zwischen Internetsurfen und Cloud Computing zu unterscheiden.

1. Wenden wir uns zunächst dem Letzteren zu. Worum also geht es der Sache nach beim sog. Cloud Computing und seiner Überwachung? „Wer eine virtuelle Festplatte nutzt, Rechenleistung in der Cloud abruft oder dort Programme/Apps zur Datenverarbeitung verwendet, kommuniziert nicht im Sinne des § 100a StPO."[74] So weit, so gut. Was aber geschieht denn eigentlich beim Cloud Computing? Um es noch einmal auf den Punkt zu bringen: Cloud Computing ist letztlich zu verstehen als „ein IT-Bereitstellungsmodell […], bei dem der Cloud-Nutzer auf die Beschaffung eigener Hard- und/oder Software verzichtet und stattdessen auf die ständig zu diesem Zweck bereitgestellten Ressourcen des Cloud-Anbieters zurückgreift".[75] „Das Spektrum dieser Dienste reicht von der Bereitstellung ‚einfacher' Datenspeicherplätze wie etwa Dropbox, Skydrive, Googledrive und der iCloud bis zur Auslagerung ganzer Benutzeroberflächen und gar Firmensystemen in die ‚Cloud'."[76]

Häufig geht es dabei im Wesentlichen oder gar ausschließlich um die Nutzung externer Speichermöglichkeiten, insbesondere um von verschiedenen Endgeräten aus oder von mehreren Personen unabhängig voneinander auf die in die Cloud gestellten Daten zugreifen zu können. Ständig wachsend ist jedoch auch die Nutzung vom Cloud-Anbieter zur Verfügung gestellter Möglichkeiten zur externen Datenverarbeitung.[77] Kurz und gut: Letztlich bedeutet mehr oder minder exzessiv praktiziertes Cloud Computing nichts anderes, als eine Verlagerung der sonst im Inneren des heimischen Computers vonstattengehenden Datenspeicherungs- bzw. Datenverarbeitungsvorgänge nach außen, im Ergebnis also eine virtuelle Erweiterung des eigenen PCs in die Cloud hinein.[78] In letzter Konsequenz „verbleibt am eigentlichen Arbeitsplatz nur noch ein Monitor und ein rudimentärer Rechner, der mehr oder weniger nur noch den Zugang zur Cloud ermöglicht."[79]

Will nun die Strafverfolgungsbehörde heimlichen Zugriff nehmen auf das in die Cloud hinein outgesourcte Datenverarbeitungsgeschehen,[80] insbesondere auf die in der Cloud auf fremden Speichermedien angelegten Datenbestände, stellt sich das im Grunde kaum anders dar, als würde sie auf das Datenverarbeitungsgeschehen am heimischen PC des Beschuldigten bzw. auf die auf dessen Festplatte abgespeicherten Daten zugreifen.[81] Dieses Bild einfach eines in die Cloud

[69] So ganz richtig *Hiéramente/Fenina*, StraFo 2015, 365 (371).

[70] Vgl. soeben Abschnitt III.

[71] Eingefügt durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens v. 17.8.2017, BGBl. 2017 I, S. 3202, in Kraft seit 24.8.2017; zur Gesetzgebungsgeschichte *Knierim*, in: Knierim/Oehmichen/Beck/Geisler (Fn. 11), Kap. 18 Rn. 1.

[72] *Eschelbach* (Fn. 4), § 100a Rn. 5 a.E.; speziell zur Überwachung des Cloud Computing siehe auch *Köhler* (Fn. 16), § 100a Rn. 14f.: Sie stehe „einer Online-Durchsuchung […] näher als einer TKÜ-Maßnahme"; *Roggan*, StV 2017, 821 (823): Sie komme „in qualitativer Hinsicht einem heimlichen Ausleiten von Datenbeständen mittels Online-Durchsuchung wesentlich näher als der Überwachung einer (Tele-)Kommunikation"; *Hiéramente/Fenina*, StraFo 2015, 365 (373): „(mindestens) dieselbe Eingriffsintensität".

[73] *Eschelbach* (Fn. 4), § 100a Rn. 5 a.E.; ebenso *Roggan*, StV 2017, 821 (825).

[74] *Hiéramente/Fenina*, StraFo 2015, 365 (372); vgl. schon oben, Abschnitt III.

[75] So zusammenfassend *Mavany*, ZIS 2018, 86, in seiner Rezension von *Wicker*, Cloud Computing und staatlicher Strafanspruch, 2016; siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (366): „ein Dienstleistungskonzept […], welches dem Nutzer Zugriff auf Soft- und/oder Hardware ermöglicht".

[76] *Gähler*, HRRS 2016, 340.

[77] Näher zu diesen *Hiéramente/Fenina*, StraFo 2015, 365 (367).

[78] Vgl. *Hiéramente/Fenina*, StraFo 2015, 365 (367): „stellt die Cloud eine externe Fortsetzung des Geräts des Cloudnutzers dar", und a.a.O., 372: „Die lokale Festplatte wird schrittweise durch die Speicherung in der Cloud ersetzt."

[79] *Gähler*, HRRS 2016, 340; siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (366): „Mehr und mehr werden Computer […] zum reinen Zugangsinstrument für den Abruf dezentral gelagerter Daten."

[80] Zur Möglichkeit des *offenen*, *nicht verdeckten* Zugriffs auf die in der Cloud gespeicherten Datenbestände über §§ 94 ff. StPO bzw. §§ 102, 110 Abs. 3 StPO vgl. nachfolgend Fn. 81.

[81] Was es, wie *Hiéramente/Fenina*, StraFo 2015, 367, ganz richtig dartun, den Strafverfolgungsbehörden denn auch ermöglicht, im Rahmen einer gem. § 102 StPO erfolgenden *offenen* Durchsuchung beim Verdächtigen über § 110 Abs. 3

hinein erweiterten, aber funktionell in sich geschlossenen „informationstechnischen Systems“ des Beschuldigten i.S.d. § 100b Abs. 1 StPO macht unschwer vorstellbar, dass zumindest diejenigen Autoren, die eine Anwendbarkeit des § 100a StPO ablehnen und von daher vor Einfügung des § 100b in die StPO davon überzeugt waren, es gebe somit de lege lata keine legale Möglichkeit der heimlichen Überwachung des Cloud Computing,[82] nunmehr geradezu aufatmend davon ausgehen mögen, dass jetzt in der Regelung der Online-Durchsuchung eine hinreichende Ermächtigungsgrundlage für entsprechende Eingriffe zu erblicken ist.

So nimmt man – zu Recht – an, dass § 100b StPO jetzt eben auch den heimlichen Zugriff nicht nur auf den heimischen PC des Beschuldigten ermögliche, sondern auch denjenigen auf den Server des Cloud-Anbieters, soweit es das Cloud Computing des Beschuldigten betrifft;[83] § 100b Abs. 3 S. 2 StPO stellt diese Möglichkeit des Eingriffs in informationstechnische Systeme anderer Personen (hier: des Cloud-Anbieters) ja auch ausdrücklich zur Verfügung.[84] Das mit dieser Lösung einhergehende Manko, dass damit freilich der Zugriff auf die (nicht als Telekommunikation im Sinne der TKÜ zu begreifenden) Übertragungsvorgänge in die Cloud hinein und aus der Cloud heraus mangels Anwendbarkeit des § 100a StPO noch immer nicht statthaft ist, verblasst angesichts der mit § 100b StPO eröffneten Möglichkeit, nunmehr auf die als Ergebnis der Übertragungsvorgänge in der Cloud gespeicherten Daten heimlichen Zugriff nehmen zu können.

2. Ist somit das Problem des Cloud Computing in der beschriebenen Weise mit Hilfe des § 100b StPO wohl hinreichend befriedigend in den Griff zu bekommen, lässt sich diese Lösung nicht einfach eins zu eins auch auf das Surfen im Internet übertragen. Denn so, wie sich die TKÜ und die Online-Durchsuchung ganz wesentlich dadurch voneinander unterscheiden, dass Erstere den Zugriff auf die laufende Kommunikation regelt, Letztere hingegen den Zugriff auf den vorhandenen Datenbestand,[85] unterscheiden sich auch die nach § 100b StPO zulässigen Überwachungsmaßnahmen beim Cloud Computing auf der einen und die beim Internetsurfen in den Blick zu nehmenden auf der anderen Seite: Gelangt man beim Überwachen des Cloud Computings mittels Online-Durchsuchungs-basiertem Auslesen des Cloud-Servers ans gewünschte Ermittlungsziel,[86] geht es beim Überwachen des Surfverhaltens gerade um den strafverfolgerischen Zugriff auf das laufende Internet-Geschehen, womit man sich im Grunde in der Domäne der Telekommunikationsüberwachung bewegt – wenn auch mit dem entscheidenden Schönheitsfehler, dass eben (wie in Abschnitt III. dargestellt) die Regelung des § 100a StPO zur TKÜ mangels zweiseitig erfolgender Kommunikation, nicht anwendbar ist. Was also tun?

Nun ist kaum bestreitbar, dass das Überwachen des Internetsurfens einen besonders schwerwiegenden Eingriff in die Persönlichkeitsrechte des Beschuldigten darstellt.[87] Immerhin geht es ja nicht um das eher punktuelle Abhören bzw. Mitverfolgen einzelner Surfvorgänge, sondern letztlich um eine flächendeckende Erfassung des gesamten Surfverhaltens.[88] Übertragen auf die analoge Welt wäre dies vergleichbar mit dem Einsatz einer Drohne, die tagein tagaus unsichtbar über dem zu Überwachenden schwebt und ihn ununterbrochen auf Schritt und Tritt begleitet. Dies ist ersichtlich um Einiges eingriffsintensiver als eine auf die Überwachung einzelner Telekommunikationsvorgänge beschränkte TKÜ. Wenn nun das BVerfG dem im Grunde auch durchaus zustimmt,[89] dann aber doch behauptet, durch die bei der Überwachung des Internetsurfens geschehende „Ausleitung der aufgerufenen HTML-Seiten“ ergebe sich zwar „ein quantitatives Mehr an überwachter Kommunikation als bei der Telefonüberwachung“, dieser Umstand rechtfertige aber „keine andere Bewertung“,[90] so vermag dies nicht zu überzeugen.

StPO vom durchsuchten Computer aus auch auf die Daten zuzugreifen, die in der (als bloße Erweiterung des sich körperlich beim Beschuldigten befindlichen PCs zu begreifenden) Cloud gespeichert sind. Nur wird die offene Durchsuchung vielfach nicht das Mittel der Wahl sein, wenn es (etwa im Zuge längerfristiger Ermittlungen) darum geht, den Verdächtigen auszuforschen, ohne ihn in u.U. ermittlungsgefährdender Weise in Kenntnis von den Ermittlungen zu setzen (auch hierzu a.a.O., 367 f.). Dazu, dass schließlich auch die (offene) Beschlagnahme gem. §§ 94 ff. StPO unmittelbar beim Cloudanbieter „nur bedingt für längerfristige Ermittlungen geeignet“ ist, ebenfalls a.a.O., 368). – Zum offenen Zugriff auf Cloud-Inhalte auch *Wolter/Greco* (Fn. 4), § 100a Rn. 41; *Wohlers/Greco*, in: Wolter (Fn. 4), § 94 Rn. 26.

[82] Vgl. nur (im Jahr 2016) *Wolter/Greco* (Fn. 4), § 100a Rn. 41: „Für den heimlichen Zugriff auf Cloud-Inhalte gibt es nach geltendem Recht keine Rechtsgrundlage.“; siehe *Hiéramente/Fenina*, StraFo 2015, 365 ff.: Es sei § 100a StPO „für die Überwachung des Internetdatenstroms […] schlichtweg ungeeignet“ (a.a.O., 373), bei Wegfall des § 100a StPO dann aber „die Überwachung […] mangels Eingriffsgrundlage in der StPO schlichtweg untersagt“ (a.a.O., 371).

[83] Vgl. nur *Köhler* (Fn. 16), § 100b Rn. 1, 10; insoweit ebenso *Roggan*, StV 2017, 821 (825); s.a. *Knierim/Oehmichen* (Fn. 11), Kap. 20 Rn. 32, 65.

[84] Explizit auf § 100b Abs. 3 StPO rekurrierend *Köhler* (Fn. 16), § 100b Rn. 10; *Roggan*, StV 2017, 821 (826); siehe auch *Bruns* (Fn. 4), § 100b Rn. 13.

[85] Vgl. hierzu bereits oben im Text bei Fn. 10 und 11.

[86] Vgl. oben Abschnitt 1., letzter Absatz.

[87] Näher und überzeugend hierzu *Hiéramente*, HRRS 2016, 448 (451 f.); siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a: „Die Maßnahme ist in ihrer Eingriffsintensität mit der Online-Durchsuchung vergleichbar, möglicherweise sogar mit dem Zugriff auf Selbstgespräche.“

[88] Vgl. *Hiéramente*, HRRS 2016, 448 (451): „Bei der […] Internetüberwachung werden massenhaft Daten generiert, die bei einer längeren Überwachung die Erstellung eines umfassenden Persönlichkeitsprofils erlauben“.

[89] BVerfG NJW 2016, 3508 (3511) konzediert (immerhin) „ein quantitatives Mehr an überwachter Kommunikation als bei der Telefonüberwachung“.

[90] BVerfG NJW 2016, 3508 (3511).

Nicht schlagend ist gerade das Hauptargument des BVerfG, das da lautet:[91] „Denn der Masse an aufgerufenen Webseiten und eingegebenen Suchbegriffen steht ein fragmentarischer Inhalt des einzelnen Abrufs bzw. der einzelnen Informationsrecherche gegenüber. Es werden lediglich Einzelakte einer häufig nur sehr kurzen bzw. wie gerade beim ‚Surfen' lediglich oberflächlichen Kommunikation zur Kenntnis genommen."

Dem ist entschieden zu widersprechen: „Der Betroffene offenbart im Rahmen eines Telefonats, einer Email oder im Chat bewusst und freiwillig Wissen gegenüber einem Dritten. Er begibt sich damit freiwillig, wenn auch graduell des Schutzes der Privatsphäre."[92] Demgegenüber erfordert „die Nutzung des Internets zum Zwecke der reinen Informationsgewinnung (‚Googlen', ‚Surfen', Nutzung von Navigationssystemen, etc.) beziehungsweise Unterhaltung (Fernsehen, Spiele, Apps) […] keine Interaktion mit Dritten",[93] kein diesen gegenüber bewusstes Freigeben von Informationen und ist damit „seiner Natur nach […] privater",[94] weniger nach außen gerichtet. Sie ist damit „dem Selbstgespräch und Tagebucheintrag näher als der sozialen Interaktion mit Freunden und Bekannten".[95] Demgemäß ist – gerade im Hinblick auf ihr Gefährdungspotential – „die Überwachung des Surfverhaltens […] von der ‚klassischen' Telekommunikation wesensverschieden".[96] Nicht also geht es um ein bloßes quantitatives Mehr gegenüber der TKÜ, die Überwachung des Surfverhaltens stellt vielmehr ein dieser gegenüber deutliches qualitatives Plus dar.[97] Letztlich handelt es sich bei der Überwachung des Internetverkehrs um eine Form digitaler Totalüberwachung.[98]

Insoweit erscheint es – von den geschilderten Wertungsgesichtspunkten aus – durchaus naheliegend, dann eben die gegenüber den Anwendungsvoraussetzungen des § 100a StPO noch ein gutes Stück strenger ausgestaltete Online-Durchsuchung nach § 100b StPO als sedes materiae zu betrachten und demgemäß für deren Anwendbarkeit zu plädieren.[99]

Nun ist jedoch leider zu konstatieren, dass es beim Überwachen des Surf-Verhaltens um einen Eingriff in das aktuelle Nutzerverhalten geht, die Online-Durchsuchung aber den Zugriff auf den im Informationsverarbeitungssystem vorhandenen Datenbestand im Auge hat. Das passt nicht zusammen.

Möglich mag es ja sein, dass die Ermittlungsbehörden mit Hilfe der Online-Durchsuchung nach auf der Festplatte des Nutzers ggf. perpetuierten Restspuren vorherigen Surfens suchen, nur wird das bloße Surfen im Internet in aller Regel keine solchen bleibenden, mittels der Online-Durchsuchung abgreifbaren Surfspuren hinterlassen, so dass den Ermittlern bestenfalls unzusammenhängende Schnipsel des betreffenden Surfgeschehens sichtbar werden, was vermutlich nicht allzu viel Nutzen bringt.

Eine der TKÜ ähnliche *durchgehende* Überwachung des Surfverhaltens aber ist mittels § 100b StPO nicht zu rechtfertigen.[100] Und eine – ob der ja vielleicht vergleichbaren Eingriffsschwere angemessen erscheinende – analoge Heranziehung des § 100b StPO ist aufgrund des bereits erwähnten Analogieverbots bei Eingriffsnormen keine legitime Möglichkeit der Problembewältigung.[101]

V. So ist denn am Ende dieser Überlegungen zu konstatieren, dass zwar die strafverfolgerische Auswertung des Cloud Computing (im Hinblick auf die in der Cloud gespeicherten Daten) de lege lata über § 100b StPO legitimierbar ist,[102] nicht aber die Überwachung des bloßen Internetsurfens: Weder die Ermächtigungsnormen zur Telekommunikationsüberwachung noch diejenigen zur Online-Durchsuchung und schon gar nicht die allgemeinen Eingriffsgeneralklauseln der §§ 161 und 163 StPO vermögen eine solche Maßnahme zu gestatten.[103] Im Ergebnis ist also festzuhalten, dass die unmittelbare Überwachung und Auswertung des aktuellen Surfverhaltens nach unserer heutigen Gesetzeslage schlicht unzulässig ist und somit im Kanon der polizeilichen Ermittlungsmöglichkeiten jedenfalls derzeit keinen Platz findet.

De lege ferenda freilich ist durchaus die Schaffung einer eigenen Eingriffsnorm vorstellbar[104] und ein entsprechendes Tätigwerden des Gesetzgebers höchst wünschenswert, denn es lässt sich ja schwerlich bestreiten, dass in vielen Fällen ein legitimes Interesse der Strafverfolgungsbehörden daran besteht, eine Überwachung des Surfverhaltens eines Beschuldigten vorzunehmen, um auf diese Weise anders nicht zu

[91] BVerfG NJW 2016, 3508 (3511).
[92] *Hiéramente*, HRRS 2016, 448 (451).
[93] *Hiéramente*, HRRS 2016, 448 (451).
[94] *Hiéramente*, HRRS 2016, 448 (451).
[95] *Hiéramente*, HRRS 2016, 448 (451); auch *Roxin/Schünemann* (Fn. 21), § 36 Rn. 5 betonen „die Nähe zum Selbstgespräch".
[96] *Hiéramente*, HRRS 2016, 448 (451).
[97] Ausführlich und überzeugend hierzu *Hiéramente*, HRRS 2016, 448 (450 ff.).
[98] Ganz richtig *Hiéramente*, HRRS 2016, 448 (452): „[…] eignet sich die Überwachung des Internets besonders zur Erstellung umfassender Persönlichkeitsprofile".
[99] So denn auch *Eschelbach* (Fn. 4), § 100a Rn. 5: „Der hoheitliche Zugriff auf die Informationsbeschaffung der Zielperson im Internet […] ist nunmehr nach § 100b zu beurteilen."
[100] Insoweit zumindest missverständlich aber *Roggan*, StV 2017, 821 ff., wenn er zwar (ganz richtig) die „Beschränkung auf eine passive Kenntnisnahme von Datenbeständen, die sich bereits in dem System befinden", konstatiert (a.a.O., 826), dann aber (insoweit wertungswidersprüchlich) behauptet, es sei „möglich […] auch ein ‚Live-Zugriff', also der ‚heimliche Blick über die Schulter' des Betroffenen" (a.a.O., 825).
[101] Vgl. bereits im Text oben bei Fn. 63 mit Nachweisen in Fn. 63.
[102] Vgl. oben, Abschnitt IV. 1.
[103] Vgl. oben, Abschnitt IV. 2.
[104] In diesem Sinne offenbar auch *Hiéramente*, HRRS 2016, 448 (452): „Die Überwachung der Internetnutzung ist ein Grundrechtseingriff eigener Art und erfordert insbesondere aufgrund der gesteigerten Eingriffsintensität eine eigenständige strafprozessuale Grundlage."

erlangende Erkenntnisse zu gewinnen.[105] Dabei wäre aber unter Überwindung überkommener Regelungskonzepte zu berücksichtigen, dass die einseitige Internetnutzung „dem Selbstgespräch und Tagebucheintrag näher [ist] als der sozialen Interaktion mit Freunden und Bekannten“,[106] mithin „die Nutzung des Internet zu nicht sozial-kommunikativen Zwecken […] ein, von Art. 10 GG geschütztes, menschliches Verhalten eigener Art“ darstellt[107] und man deswegen „die Erhebung von Daten, die nicht sozial-kommunikativer Natur sind, als eigenständigen, typusprägenden Grundrechtseingriff anzusehen“ hat.[108] Nicht von ungefähr spiegelt sich dieser qualitative Unterschied denn auch in der Zielrichtung der Behörden wider, die eine entsprechende Maßnahme ergreifen: „Während das Abhören des Telefons und der Emailkommunikation primär dem Einblick in den Meinungs- und Wissensaustausch zwischen Beschuldigten dient, dient eine Internetüberwachung regelmäßig der Ermittlung der persönlichen Hintergründe und Vorlieben des Beschuldigten.“[109] Dem müsste in einer sachgerechten Neuregelung Rechnung getragen werden.

Auf dieser Grundlage wäre dann schließlich noch eine weitere, letztlich entscheidende Frage zu beantworten: Wie streng müsste eine solche surfspezifische Regelung ausgestaltet sein? So streng wie die ja schon eingangs als „vergleichsweise streng“ bezeichnete Regelung der TKÜ? Noch ein wenig strenger, nämlich so streng, wie die tatsächlich nur unter *noch* engeren Voraussetzungen anwendbare Online-Durchsuchung? Ohne dies hier nun aus Umfangsgründen in extenso ausbreiten zu können: Weder das eine, noch das andere.

Eine etwa zu schaffende Neuregelung müsste vielmehr in ihren Anwendungsvoraussetzungen jedenfalls strenger sein als die TKÜ,[110] aber sogar strenger auch als die Online-Durchsuchung.[111] Sie müsste (zumindest!) den gegenüber §§ 100a und 100b StPO noch einmal enger gehaltenen Anwendungsbedingungen der akustischen Wohnraumüberwachung des § 100c StPO unterworfen werden. Man denke insoweit nicht nur an den bei § 100b i.V.m. § 100d Abs. 3 StPO gegenüber § 100c i.V.m. § 100d Abs. 4 StPO weniger stark ausgeprägten Kernbereichsschutz,[112] sondern auch an das in § 100b Abs. 1 StPO fehlende Äquivalent zu der bei Lauschangriffen in § 100c Abs. 1 Nr. 3 verlangten „auf Grund tatsächlicher Anhaltspunkte“ – und nicht bloß auf Grund kriminalistischer Erfahrungswerte[113] – *konkret* bestehenden Erwartbarkeit, ermittlungsrelevante Beschuldigtenäußerungen zu erfassen:[114] „Eine solche ‚Erfolgsprognose‘ im Sinne einer Wahrscheinlichkeit des Ausleitens verfahrensrelevanter Informationen haben die Ermittler bei Online-Durchsuchungen […] nicht zu erstellen.“[115]

Denn nur so ist dem Umstand hinreichend Rechnung zu tragen, dass der beim Surfen lückenlos Überwachte mehr noch als der von einer Online-Durchsuchung[116] Betroffene für die Ermittlungsbehörden quasi zum „gläsernen Menschen“ wird, in völliger Transparenz im Hinblick auf seine Vorlieben, Neigungen und Interessen. Gerade das vermeintlich unbeobachtete Herumstöbern auf mitunter auch eher fragwürdigen Internetseiten vermag in der Summe so viel über den Einzelnen zu verraten, wie es vielleicht noch nicht einmal ein Blick in sein Tagebuch zu offenbaren vermöchte.[117]

Dem Rechnung zu tragen, wäre zwar eine klare Absage an die vom BVerfG geäußerte Auffassung, das Surfen im Internet sei nur ein quantitative*s* Mehr gegenüber der zweiseitigen Kommunikation via Telefonat, SMS oder E-Mail.[118] In der Sache aber wäre damit im Gesamtsystem der digitalen

---

[105] Deutlich strenger insofern *Roxin/Schünemann* (Fn. 21), § 36 Rn. 5: „legt die Nähe zum Selbstgespräch und sogar zum Denken selbst eher nahe, dass man auf ‚solipsistische‘ Inhalte keinen Zugriff erlaubt“.

[106] So ganz richtig *Hiéramente*, HRRS 2016, 448 (451), dies wie folgt erläuternd: „Die Nutzung des Internets zum Zwecke der reinen Informationsgewinnung (‚Googlen‘, ‚Surfen‘, Nutzung von Navigationssystemen, etc.) beziehungsweise Unterhaltung (Fernsehen, Spiele, Apps) erfordert […] keine Interaktion mit Dritten und ist [gegenüber der ‚klassischen‘ Telekommunikation] seiner Natur nach […] privater“.

[107] *Hiéramente*, HRRS 2016, 448 (451); sie stelle „eine logisch abgrenzbare und verfassungsrechtlich besonders schützenswerte Persönlichkeitsentfaltung dar“.

[108] *Hiéramente*, HRRS 2016, 448 (451).

[109] *Hiéramente*, HRRS 2016, 448 (451); ebenso *Roggan*, StV 2017, 821 (823).

[110] Vgl. *Roggan*, StV 2017, 821 (823): Es hätten „für entsprechende Maßnahmen angesichts ihrer evident erheblich gesteigerten Eingriffsintensität (zumindest!) die tatbestandlichen Schwellen von § 100b StPO zu gelten“, kämen sie doch „in qualitativer Hinsicht einem heimlichen Ausleiten von Datenbeständen mittels Online-Durchsuchung wesentlich näher als der Überwachung einer (Tele-)Kommunikation“.

[111] Siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a: Die Überwachung des Surfverhaltens sei in ihrer Eingriffsintensität (nicht nur) „mit der Online-Durchsuchung vergleichbar“, (sondern) „möglicherweise sogar mit dem Zugriff auf Selbstgespräche“.

[112] Näher hierzu *Roggan*, StV 2017, 821 (828).

[113] Diese dezidiert nicht ausreichen lassend *Wolter*, in: Wolter (Fn. 4), § 100c Rn. 46.

[114] So der mehrfache Hinweis bei *Roggan*, StV 2017, 821 (825 und 827).

[115] *Roggan*, StV 2017, 821 (825); siehe auch a.a.O. 827: Es enthalte „§ 100b Abs. 1 StPO nicht einmal einen Ansatz eines Äquivalents zur (selbst dort schwachen) ‚Lauscherfolgs-Wahrscheinlichkeit‘ in § 100c Abs. 1 Nr. 3 StPO“.

[116] Wobei bereits bei dieser Maßnahme zu Recht zu monieren ist, dass sie „potenziell die heimliche Erstellung umfassender Persönlichkeitsprofile […] ermöglicht“ (so *Singelnstein/Derin*, NJW 2017, 2646 [2647]).

[117] Ganz richtig *Hiéramente*, HRRS 2016, 448 (452): „Selbst aus für sich genommen fragmentarischen Informationen kann ein Mosaik konstruiert werden, das Aufschluss über Gewohnheiten und Vorlieben aus allen Lebenslagen zu geben vermag.“

[118] BVerfG NJW 2016, 3508 (3511); vgl. bereits oben, Abschnitt IV. 2., bei Fn. 90.

Ermittlungsmöglichkeiten der dem Wesen und dem Gefährdungspotential einschlägiger Überwachung entsprechende, zutreffende Platz zugewiesen.

Der Einsatz von Lügendetektorsoftware im Strafprozess – aufgrund des technischen Fortschritts in Zukunft doch rechtmäßig?

Von Prof. Dr. **Sönke Florian Gerhold**, Bremen

I. Einleitung

Nina Nestler hat es sehr schön formuliert: „‚Als Zeuge ist der Mensch eine Fehlkonstruktion.' Er irrt sich – und er lügt."[1] Dies entspricht der allgemeinen Einschätzung, nach der Zeugen als sehr unzuverlässige Beweismittel gelten. Dennoch kommt kaum ein Strafverfahren ohne sie aus. In Aussage-gegen-Aussage-Situationen hängt häufig sogar der gesamte Prozessausgang von ihnen ab.[2] Für die Einlassung des Angeklagten gilt nichts anderes.

Die Frage, ob eine Bekundung tatsächlich Erlebtes zum Gegenstand hat oder der Fantasie des Angeklagten oder Zeugen entsprungen ist, beschäftigt die Gerichte daher schon seit Jahrhunderten.

Die Versuche, den Wahrheitsgehalt einer Einlassung oder Aussage zu ergründen, reichen dabei selbst im historischen deutschen Strafprozess von der Narkoanalyse[3], umgangssprachlich auch als Geständnisspritze oder Verabreichung eines Wahrheitsserums bezeichnet,[4] über den Einsatz forensischer Hypnotherapeuten[5] bis zur Gestattung der Folter[6] als prozessual anerkanntem Instrument der Wahrheitsfindung. Die meisten dieser Ansätze sind – zum Glück – bereits seit 1950[7] explizit durch § 136a StPO verboten.

Bezogen auf die Zulässigkeit des Einsatzes von Hypnose als erinnerungsunterstützendes Verfahren, mit der die Willensfreiheit nicht beeinträchtigt, sondern durch das Lösen posthypnotischer sowie posttraumatischer Hemmungen oder Blockaden gerade umgekehrt wiederhergestellt werden soll, ist die wissenschaftliche Diskussion derzeit in vollem Gange.[8] In Bayern soll das Staatsministerium für Justiz und Verbraucherschutz im Jahr 2009 sogar eine leider nicht im Original einsehbare Dienstanweisung mit detaillierten Regelungen für die Einbindung von Hypnotherapeuten in polizeiliche Ermittlungen erlassen haben.[9] Nach dieser sollen die Polizeibeamten der Vernehmung etwa nicht selbst beiwohnen dürfen, sondern die Vernehmung durch den Hypnotherapeuten muss aufgezeichnet werden und der Vernommene im Anschluss an diese frei entscheiden, ob die Aufzeichnung von den Ermittlungsbeamten eingesehen werden darf oder ob er in einer neuen Vernehmung weitere Erkenntnisse preisgeben möchte.

Im vorliegenden Beitrag steht jedoch eine andere moderne Möglichkeit der Wahrheitsermittlung im Mittelpunkt der Betrachtung und zwar der Einsatz KI-gestützter Lügendetektoren. In einem ersten Schritt (II.) wird dargestellt, welche Entwicklungen sich auf dem Feld der Lügendetektion in den letzten Jahren verzeichnen lassen. In einem zweiten Schritt (III.) wird geklärt, ob sich die bislang in der Rechtsprechung vorgebrachten Argumente, mit denen die Unzulässigkeit des Einsatzes von Polygraphen begründet worden ist, auf moderne Lügendetektoren übertragen lassen. Abschließend (IV.) gilt es die Frage zu beantworten, ob der Einsatz eines Lügendetektors einer Ermächtigungsgrundlage bedarf.

II. Die neueren Entwicklungen im Bereich der Lügendetektion

1. Die erhofften Trefferquoten eines modernen Lügendetektors im Vergleich mit denjenigen anderer Methoden der Wahrheitsermittlung

Der technische Fortschritt und insbesondere der Einsatz künstlicher Intelligenz im Rahmen von Befragungen lässt in nicht allzu ferner Zukunft auf eine Trefferquote bei der Erkennung bewusster Lügen von deutlich über 90 % hoffen.[10] Bereits jetzt wird die Trefferquote etwa der Software EyeDetect mit 85 bis 90 % angegeben,[11] diejenige der Software DARE mit 88 %.[12]

Beauftragt das Gericht demgegenüber einen Sachverständigen mit einem Glaubhaftigkeitsgutachten, liegt dessen Trefferquote selbst bei Einhaltung aller Regeln der Kunst – einmal alle methodischen Probleme entsprechender Untersu-

---

[1] *Nestler*, JA 2017, 10, unter Berufung auf *Hussel*, Kriminalistik 2011, 114.

[2] *Nestler*, JA 2017, 10 (11); *Schmuck/Brügge-Niemann*, NJOZ 2014, 601 (602).

[3] Vgl. *Kranz*, Die Narkoanalyse als diagnostisches und kriminalistisches Verfahren, 1950.

[4] Vgl. *Bohne*, ZStW 65 (1953), 267 (280).

[5] Vgl. *Beetz/Delhaes*, Hypnose-ZHH 2011, 165 (167).

[6] Vgl. *Vormbaum*, Einführung in die moderne Strafrechtsgeschichte, 4. Aufl. 2019, S. 86.

[7] Gesetz zur Wiederherstellung der Rechtseinheit auf dem Gebiet der Gerichtsverfassung, der bürgerlichen Rechtspflege, des Strafverfahrens und des Kostenrechts vom 12.9.1950, BGBl. 1950 I, S. 455, 484 f.

[8] Vgl. zum Streit um die Zulässigkeit von Hypnose zur Wiederherstellung der Erinnerungsfähigkeit *Beetz/Delhaes*, Hypnose-ZHH 2011, 165 (168 f.); *Deckers*, in: Bayerischer Anwaltsverband (Hrsg.), Neue Vernehmungsmethoden – Hypnose, Hirnforschung, Polygraph, 2012, S. 148, beide m.w.N.

[9] *Beetz/Delhaes*, Hypnose-ZHH 2011, 165 (169 f.); *Deckers* (Fn. 8), S. 148.

[10] Vgl. etwa die Prognose von *Mickelsen*, zitiert nach *Heller*, FAZ v. 12.10.2019, abrufbar unter https://www.faz.net/aktuell/wissen/kuenstliche-intelligenz-soll-luegendetektoren-endlich-praktikabel-machen-16408179-p2.html (1.9.2020); oder *Elgan*, Computerwoche v. 31.1.2018, abrufbar unter https://www.computerwoche.de/a/killer-app-luegendetektor,3544177 (1.9.2020). Kritisch demgegenüber *Dahle/Lehmann*, in: Bayerischer Anwaltsverband (Fn. 8), S. 48 (74).

[11] *Heller* (Fn. 10); IT Boltwise v. 15.10.2019, abrufbar unter https://www.it-boltwise.de/augenanalyse-kuenstliche-intelligenz-soll-schwaechen-von-polygraphen-luegendetektoren-ausgleichen.html (1.9.2020).

[12] https://doubaibai.github.io/DARE/ (1.9.2020).

chungen ausgeklammert – im Durchschnitt wohl nur bei leicht über 70 %.[13] Die Trefferquote eines nicht sachverständig beratenen Richters oder Spruchkörpers dürfte daher naheliegender Weise noch geringer ausfallen.[14] Ein nicht geschulter Laie kommt lediglich auf eine Trefferquote von 50 %.[15]

Besonders bedenklich sind die bislang zu erzielenden Trefferwahrscheinlichkeiten vor allem deshalb, weil ein Glaubhaftigkeitsgutachten faktisch nur in Zweifelsfällen eingeholt wird und das Gericht dem Gutachter schlussendlich in mehr als 95 % der Fälle folgt.[16] Dass verschiedene Studien in mindestens einem Drittel, nach anderen Schätzungen sogar in mehr als der Hälfte der Fälle methodische Fehler der Gutachten belegen,[17] sodass die Ergebnisse entweder relativiert werden müssen oder im Einzelfall sogar jeder Aussagekraft entbehren,[18] wird neben der schon unter Optimalbedingungen eher geringen Trefferwahrscheinlichkeit von den Gerichten offensichtlich ebenfalls ausgeblendet.

2. Derzeitige Pilotprojekte und Laborstudien

Der Gedanke, die beschriebenen Unsicherheiten durch den Einsatz moderner Technik auszugleichen, liegt daher nicht fern. Im Grunde genommen macht eine moderne Lügendetektorsoftware trotz der höheren Trefferquote auch nichts anderes als ein Mensch, der isoliert über eine Aussage zu urteilen hat. Sie wertet die ihr über Kamera und Mikrofon zugänglichen Informationen wie Mimik, Gestik, Sprachduktus oder die Häufigkeit bestimmter Begriffe und Formulierungen aus und gleicht diese mit ihrem Erfahrungswissen ab.[19] Im Ergebnis kombiniert die KI also insbesondere Ansätze der sog. Voice-Stress-Analyse mit denen der sog. Gesichts-Scan-Analyse.[20]

Im Gegensatz zum Menschen kann sie dabei jedoch auf ihre Kernkompetenz, das Erkennen von Mustern, und im Optimalfall einen schier unendlichen Datenpool zurückgreifen.[21]

a) Das Projekt der University of Michigan

Erste Experimente in diese Richtung führte die University of Michigan bereits in den Jahren 2015 und 2016 durch.[22] Wissenschaftler trainierten eine künstliche Intelligenz mit zunächst nur 120 Videos amerikanischer Gerichtsprozesse, in denen als wahr und als unwahr bekannte Aussagen enthalten waren. Die künstliche Intelligenz erkannte sodann unter anderem Zusammenhänge im Hinblick auf „die Häufigkeit bestimmter Gesten, die Zahl der verwendeten Füllwörter und Gesprächspausen, die Häufigkeit von Blickkontakten sowie Besonderheiten in der Intonation beim Ausdrücken von Gedanken oder Erinnerungen“.[23] Im direkten Vergleich mit Studierenden übertraf die künstliche Intelligenz diese bereits nach diesem kurzen Training und der relativ geringen Anzahl eingespeister Videos im Hinblick auf die Treffergenauigkeit um 25 %.[24] Der Vorteil einer künstlichen Intelligenz gegenüber einem Menschen, so die Projektleiterin, sei nämlich neben dem potentiell größeren Datenpool, auf den diese zurückgreifen könne, insbesondere ihre Fähigkeit sämtliche nonverbalen und verbalen Signale, die auf potenzielle Unstimmigkeiten hindeuten würden, gleichzeitig und gleichberechtigt auszuwerten, wohingegen sich die Aufmerksamkeit des Menschen stets auf einzelne Punkte konzentriere und er seine Bewertung auf das von ihm wahrgenommene Gesamtbild stütze.[25]

Die Datenbasis der künstlichen Intelligenz ließe sich für weitere Untersuchungen zudem unproblematisch erhöhen und

[13] *Vrij*, Psychology, Public Policy and Law 2005, 3 (32 f.). Vgl. auch *Köhnken*, in: v. Granhag/Strömwall (Hrsg.), The detection of deception in forensic contexts, 2004, S. 41 (60).

[14] Vertiefend hierzu *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (639 f.).

[15] Vgl. *Coelius*, The Michigan Engineer News Center v. 14.4.2016, abrufbar unter https://news.engin.umich.edu/2016/04/lie-detecting-software/ (1.9.2020).

[16] Vertiefend *Jordan/Gresser*, Der Sachverständige 2014, 71 (75); *Fegert/Schnoor/König/Schläfke*, Psychiatrische Begutachtung in Sexualstrafverfahren – Eine empirische Untersuchung von Gutachten zur Schuldfähigkeit bei jugendlichen, heranwachsenden und erwachsenen Beschuldigten in Mecklenburg-Vorpommern, 2006, S. 100.

[17] Vertiefend *Passow*, Zur Qualität forensisch-psychiatrischer Sachverständigengutachten bei Sexualstraftätern mit angeordneter Sicherungsverwahrung, 2010, S. 8 ff.; *Pfäfflin*, in: v. Fegert/Häßler (Hrsg.), Qualität forensischer Begutachtung, insbesondere bei Jugenddelinquenz und Sexualstraftaten, 2000, S. 45 (54 ff.); *Salewski/Stürmer*, Qualitätsmerkmale in der familienrechtspsychologischen Begutachtung – Untersuchungsbericht I, 2014, S. 2.

[18] Vertiefend *Salewski/Stürmer* (Fn. 17), S. 6 f.; vgl. auch *Eisenberg*, Beweisrecht der StPO, 9. Aufl. 2015, Rn. 1605.

[19] Vgl. *Dahle/Lehmann* (Fn. 10), S. 48 (53 f.).

[20] Vgl. *Dahle/Lehmann* (Fn. 10), S. 48 (74).

[21] Vgl. *Daum*, Das Filter v. 26.3.2018, abrufbar unter http://dasfilter.com/gesellschaft/kuenstliche-intelligenz-der-neue-luegendetektor-understanding-digital-capitalism-iii-teil-9 (1.9.2020).

[22] Vgl. *Coelius* (Fn. 15); Deutschlandfunk Nova v. 18.12.2015, abrufbar unter https://www.deutschlandfunknova.de/beitrag/luegendetektor-software-soll-luegner-entlarven (1.9.2020). Vgl. zu weiteren Projekten zur Lügendetektion unter Einsatz von KI über die in Fn. 11 und 12 Genannten hinaus bspw. das Projekt „Silent Talker“ (https://www.silent-talker.com/ [1.9.2020]) oder das Projekt „AVATAR“ (https://www.discernscience.com/avatar/ [1.9.2020]).

[23] *Arbor*, pressetext.com v. 15.12.2015, abrufbar unter https://eilert-akademie.de/presse_referenzen/Luegendetektor_Software_15_12_2015.pdf (1.9.2020).

[24] *Arbor* (Fn. 23).

[25] *Mihalcea*, zitiert nach *Arbor* (Fn. 23). Vgl. zur nur selektiven Wahrnehmung von Menschen *Nestler*, JA 2017, 10 (11).

auch der Vorwurf, dass die Daten einem Modellversuch entnommen seien, ließe sich bei einem Training mit Originalbefragungen nicht erheben. Ein körperlicher Kontakt zwischen Mensch und Maschine wird künftig ebenfalls nicht mehr vorausgesetzt.[26] Erforderlich für einen Einsatz der neuen Technik ist nicht mehr als eine Kamera, ein Mikrofon und ein ausreichend leistungsstarker Computer. Der Einsatz einer Wärmebildkamera oder entsprechender bildgebender Verfahren könnte die Treffergenauigkeit ggf. noch weiter erhöhen, ist aber gar nicht erforderlich, damit die künstliche Intelligenz Menschen und Sachverständige bei unterstellter Validität der bisherigen Untersuchungsergebnisse übertrifft.[27] Durch eine geeignete Befragungsmethode soll der KI ihre Arbeit zudem noch weiter erleichtert werden können.[28] Gängig sind diesbezüglich die Kontrollfragentechnik, kurz KFT, und die Tatwissenstechnik, kurz TWT, die beide das Ziel verfolgen, Reaktionen durch die Verwendung starker und schwacher Stimuli möglichst aussagekräftig ausfallen zu lassen.[29]

b) Die ersten Tests von modernen Lügendetektoren in der Praxis

Außerhalb des Strafrechts wird von diesen neuen technischen Möglichkeiten daher bereits tatsächlicher Gebrauch gemacht. So hat die EU-Grenzschutzorganisation Frontex etwa ein von der EU-Kommission mit 4,5 Millionen Euro gefördertes Pilotprojekt Namens „iBorderCtrl“ an vier Grenzübergängen in Griechenland, Lettland und Ungarn durchgeführt, in dessen Rahmen von November 2018 bis August 2019 Einreisende von einer künstlichen Intelligenz befragt worden sind.[30] Wer als „unbedrohlich“ eingestuft wurde, konnte anschließend ohne weiteren Kontakt zu Grenzbeamten einreisen. In allen anderen Fällen erfolgt eine Überprüfung durch die Beamten. Auch dieses Programm arbeitet im Wesentlichen mit der Erkennung von Mikroimpressionen ohne körperlichen Kontakt.[31] Nach einem kurzen Training unter Laborbedingungen erreichte die Software auch hier eine Trefferquote von 76 %, die sich nach der Hoffnung der leitenden Wissenschaftler durch den Feldversuch unter Realbedingungen bereits auf 85 % erhöhen und dann nach Möglichkeiten noch weiter gesteigert werden soll.[32]

Es fragt sich daher, ob der Einsatz eines solchen Systems auch im Strafprozess vorstellbar wäre oder ob ihm rechtliche Gründe entgegenstehen.

Zur Beantwortung dieser Frage soll im Folgenden untersucht werden, welche Einwände insbesondere in der Rechtsprechung[33] gegen den Einsatz klassischer Polygraphen erhoben worden sind und ob diese Bedenken auch dann noch tragen, wenn die neuartige Technik hält, was ihre Entwickler versprechen.

Eine Auseinandersetzung mit den grundsätzlichen Problemen des Einsatzes von Algorithmen im Recht soll vorliegend nicht erfolgen.

III. Überblick über die bisherige Argumentation der Rechtsprechung

1. Der behauptete Verstoß gegen die Menschenwürde bzw. das allgemeine Persönlichkeitsrecht

a) Die Argumentation der Gerichte

Der BGH bejahte in seiner ersten Entscheidung zur (Un-)Zulässigkeit einer polygraphischen Untersuchung im Strafverfahren eine Verletzung der Menschenwürde und damit zugleich des § 136a StPO.[34] Die rechtliche Bewertung hänge daher nicht von der Brauchbarkeit des Polygraphen zur Aufklärung von Straftaten ab und auch nicht von der Richtigkeit und Verlässlichkeit der wissenschaftlichen Erwägungen, auf denen er beruhe.[35]

Den Menschenwürdeverstoß begründete der BGH damit, dass der Beschuldigte durch die polygraphische Untersuchung zum Verfahrensgegenstand gemacht werde, da er nicht mehr frei entscheiden könne, ob und wie er eine Frage beantworte, wenn unbewusste Äußerungen seiner Persönlichkeit dabei anders wahrnehmbar hervorträten als auch sonst im Umgang mit ihm.[36] Der Polygraph aber bezwecke gerade mehr und andere Aussagen als sie beim üblichen Verhör zu erlangen seien, darunter gerade auch solche, die der Beschuldigte unwillkürlich mache und die ohne das Gerät gar nicht wahrnehmbar wären. Ein solcher Einblick in die Seele des Beschuldigten und seine unbewussten Regungen verletze die

[26] Vgl. *Dahle/Lehmann* (Fn. 10), S. 48 (74).
[27] Bereits für den klassischen Polygraphentest stellte *Undeutsch*, Psychologische Rundschau 2003, 115, fest, dieser schneide im Vergleich zu den sonstigen persönlichen und sachlichen Beweismitteln sehr gut ab. Entsprechend auch *Putzke*, ZJS 2011, 557 (559 f.), m.w.N.
[28] Vgl. *Dahle/Lehmann* (Fn. 10), S. 48 (53 f. und 74), die dem Einsatz von Polygraphen allerdings skeptisch gegenüberstehen.
[29] Vgl. *Dahle/Lehmann* (Fn. 10), S. 48 (55 ff. und 74). Umfassend zu den Fragetechniken *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (612 ff.).
[30] *Kolb*, SZ v. 5.11.2018, abrufbar unter https://www.sueddeutsche.de/digital/grenze-kuenstliche-intelligenz-software-iborderctrl-1.4196243 (1.9.2020); Spiegel v. 26.7.2019, abrufbar unter https://www.spiegel.de/netzwelt/web/iborderctrl-luegendetektor-im-eu-grenzschutzprojekt-getestet-a-1279230.html (1.9.2020); euronews v. 21.10.2018, abrufbar unter https://de.euronews.com/2018/10/21/check-in-mit-lugendetektor-iborderctrl (1.9.2020).
[31] *Kolb* (Fn. 30).
[32] *Kolb* (Fn. 30).
[33] Eine umfassende und überzeugende Auseinandersetzung mit jedenfalls der überwiegenden Zahl aller gegen den Polygraphentest erhobenen normativen Einwände findet sich bei *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (628 ff.).
[34] BGHSt 5, 332 (333); OLG Karlsruhe NStZ-RR 1998, 368 (369).
[35] BGHSt 5, 332 (333).
[36] BGHSt 5, 332 (334 f.).

Freiheit der Willensentschließung und -betätigung und sei im Strafverfahren unzulässig.[37]

Ausdrücklich stellt der BGH allerdings klar, dass bewusste und unbewusste Ausdrucksvorgänge beim Angeklagten bei der Beweiswürdigung berücksichtigt werden dürften, wenn sie in der Hauptverhandlung in üblicher Weise hervorträten.[38] Diesen stünden solchen, die durch Messung unbewusster und verborgener Körpervorgänge gewonnen und dann zur seelenkundlichen Deutung benutzt würden, nicht gleich.

Ganz ähnlich argumentierte auch das BVerfG, das allerdings keine Menschenwürdeverletzung, sondern eine Verletzung des allgemeinen Persönlichkeitsrechts bejahte.[39] Es heißt in der Entscheidung zusammengefasst, das Ziel, mittels einer Apparatur sonst nicht wahrnehmbare, unwillkürliche körperliche Reaktionen zu registrieren, um daraus Schlüsse auf die subjektive Richtigkeit des Ausgesagten zu ziehen, lasse den Untersuchten zu einem bloßen Anhängsel des Apparates werden und führe zu einer unzulässigen Durchleuchtung der Person, welche die Aussage als deren ureigenste Leistung entwerte.[40] Selbst wenn man einen Eingriff in den Kernbereich des Persönlichkeitsrechts verneinen wollte, ließen sich keine überwiegenden Interessen der Allgemeinheit oder des Beschuldigten anführen, um einen solchen Eingriff zu rechtfertigen.[41] Sogar bei einer Treffsicherheit von unterstellten 90 % komme dem Untersuchungsergebnis nämlich nur eine Indizwirkung zu, die im Hinblick auf die Schwere des erforderlichen Eingriffs in das allgemeine Persönlichkeitsrecht außer Verhältnis stehe.[42]

b) Die Bewertung der Argumentation

Beide Entscheidungen stellen den Gedanken der Ausforschung für einen Richter unsichtbarer Körperreaktionen in den Mittelpunkt der Betrachtung, aus denen Rückschlüsse auf Vorgänge gewonnen werden sollen, die die untersuchte Person nicht preisgeben möchte. Der BGH sieht in einem solchen Vorgehen einen Versuch, „einen Einblick in die Seele“[43] des Probanden zu erlangen, und daher einen Menschenwürdeverstoß. Das BVerfG sieht einen nicht zu rechtfertigenden Eingriff in das allgemeine Persönlichkeitsrecht. Neben dem Versuch, Unsichtbares sichtbar zu machen, wog für das BVerfG zudem schwer, dass die jeweilige Person zum Zwecke der Wahrheitsfindung an eine Maschine angeschlossen wurde.

Zu einem anderen Ergebnis kann bzw. muss man daher im Umkehrschluss gelangen, wenn Hilfsmittel zur Bewertung von Körpervorgängen eingesetzt werden, die der Richter auch mit seinen eigenen Sinnen wahrnehmen könnte, und wenn der Proband nicht mehr an eine Maschine angeschlossen werden müsste. In diesen Fällen wäre entweder kein Menschenwürdeverstoß gegeben oder das Gewicht des Grundrechtseingriffs müsste als weniger schwer beurteilt werden.

Tatsächlich treffen beide Gesichtspunkte auf die neue Generation von Lügendetektoren zu. Selbst bei alleiniger Auswertung nach außen tretender Körperreaktionen scheinen die Künstlichen Intelligenzen hohe Trefferquoten zu erzielen, weshalb ein körperlicher Kontakt zur untersuchten Person nicht mehr erforderlich ist.

Zudem kann auch nicht davon ausgegangen werden, dass bereits der Versuch, eine Lüge zu erkennen, zu einer Ausforschung des Seelenzustandes einer Person und damit zu einem nicht zu rechtfertigenden Eingriff in die Menschenwürde oder den Kern des allgemeinen Persönlichkeitsrechts führt, da anderenfalls beispielsweise auch Glaubhaftigkeitsgutachten ausgeschlossen wären.[44] Ein Recht auf unerkannte und unhinterfragte Lügen existiert nämlich nicht.

Es ist insofern zwischen einer unzulässigen Ausforschung des Unterbewussten sowie einer zulässigen und zugleich zuverlässigen Bewertung äußerlich erkennbarer Umstände zu differenzieren. Auf Letzteres ist die moderne Lügendetektion ausgerichtet. Es handelt sich bei einem modernen Lügendetektor um nicht mehr als um eine Interpretationshilfe offen erkennbarer sprachlicher oder mimisch-gestischer Besonderheiten, weshalb die Verhältnismäßigkeitsprüfung entscheidend wird.

Die Bewertung der Verhältnismäßigkeit durch das BVerfG war dabei bereits 1982 ein zentraler Kritikpunkt an der Entscheidung, da es sich im damaligen Fall um einen Indizienprozess gehandelt hat.[45] Im Rahmen der vorzunehmenden Gesamtwürdigung der Indizien durch das Gericht hätte aber eine zu 90 % als zutreffend anzusehende Einlassung durchaus begründete Zweifel an der Schuld des Angeklagten bei den Richtern hervorrufen können.[46] Zudem hätte der drohende Grundrechtseingriff, im konkreten Fall eine lebenslange Freiheitsstrafe, mit dem gewählten Grundrechtseingriff, einem allenfalls wenige Stunden andauernden Eingriff in das allgemeine Persönlichkeitsrecht abgewogen werden müssen, weshalb unklar sei, aus welchem Grund das

[37] BGHSt 5, 332 (335).

[38] BGHSt 5, 332 (335 f.). So auch BGHSt 44, 308 (316), wo es heißt, von dem Gericht dürften „auch sonst vom Willen nicht steuerbare Ausdrucksvorgänge eines Beschuldigten, die es ohne technische Hilfsmittel wahrnehmen kann (z.B. starke Schweißbildung, Erröten, Sprechstörungen oder andere Orientierungs-, Anstrengungs- oder Verlegenheitsreaktionen), verwertet werden“. Entsprechend *Matz*, ZaöRV 1999, 1107 (1109), die zudem hervorhebt, dass die Möglichkeit zur Bewertung dieser äußerlich in Erscheinung tretenden unwillkürlichen Äußerungen nicht bestritten werde.

[39] BVerfG NJW 1982, 375; vgl. auch BVerfG NJW 1998, 1938 (1939).

[40] BVerfG NJW 1982, 375. Ähnlich auch *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Kommentar, 90. Lfg., Stand: Februar 2020, Art. 2 Abs. 1 GG Rn. 155: „Der Aussagende wird quasi technisch durchleuchtet und mit seiner Aussage als eigener Persönlichkeitsdarstellung mechanisch (nicht sozial) relativiert, er wird insoweit zu einem bloßen Anhängsel eines Apparates.“

[41] BVerfG NJW 1982, 375.

[42] BVerfG NJW 1982, 375.

[43] BGHSt 5, 332 (335).

[44] Vgl. dazu BGHSt 44, 308 (316 f.).

[45] *Amelung*, NStZ 1982, 38.

[46] Vertiefend *Schwabe*, NJW 1982, 367 f.

BVerfG den vom Beschuldigten herbeigesehnten Grundrechtseingriff für offensichtlich unverhältnismäßig gehalten habe.[47]

Schwabe spitzte diese fehlende Nachvollziehbarkeit der Verhältnismäßigkeitsprüfung durch das BVerfG dabei wie folgt zu: „Bei der Alternative ‚Lebenslang' trotz denkbarer Unschuld oder – angeblich – menschenunwürdiger Erhebung eines Unschuldsindizes beim Einwilligenden entscheidet man sich für die Lösung ‚Lebenslang'. Absurder geht es kaum noch. Man stelle sich eine Rechtsordnung vor, die bestimmte entlastende Zeugenaussagen vom Prozess ausschließt mit dem Argument, die Zeugen würden zwangsläufig Einzelheiten aus dem Intimbereich des Angeklagten berühren, was man zu seinem Schutz verhindern müsse. Hiervon sind wir gar nicht sehr weit entfernt."[48]

Abhängig von der konkreten Gewichtung des Grundrechtseingriffs durch einen Lügendetektortest und den ohne dessen Indizwirkung drohenden Konsequenzen lassen sich daher unproblematisch Fälle bilden, in denen das Recht auf Freiheit der Person den Eingriff in das allgemeine Persönlichkeitsrecht überwiegt. Der Sachverhalt, der der Entscheidung des BVerfG zugrunde lag, dürfte ein klassisches Beispiel hierfür darstellen.

Sofern im Einzelfall, bspw. im Zusammenhang mit Bagatelldelikten oder Ordnungswidrigkeiten, das allgemeine Persönlichkeitsrecht überwiegt, stellt sich die Frage, ob in den ansonsten nicht gerechtfertigten Grundrechtseingriff eingewilligt werden kann.

2. Die Annahme einer Einwilligungssperre

a) Die Argumentation der Gerichte

Für den BGH kam die Zulassung einer Einwilligung 1954 bereits deshalb nicht in Betracht, weil er einen Eingriff in die Menschenwürde bejaht hat. Das BVerfG, das lediglich einen Eingriff in das allgemeine Persönlichkeitsrecht bejahte, musste sich demgegenüber mit der Einwilligungsfähigkeit des Beschuldigten, der einen Lügendetektortest verlangt hatte, auseinandersetzen. Es kam zu dem Ergebnis, dass eine Einwilligung in den Grundrechtseingriff mangels Freiwilligkeit ausscheide, da der von einer empfindlichen Freiheitsstrafe bedrohte Angeklagte nicht ohne äußeren Zwang habe wählen können, ob er sich der Untersuchung unterziehe oder nicht, sondern diese für ihn Chancen eröffnende Möglichkeit nicht ausschlagen könne.[49] Die im konkreten Fall erteilte Einwilligung vermochte den Grundrechtseingriff vor diesem Hintergrund nicht zu rechtfertigen.

b) Die Bewertung der Argumentation

Richtig an den Ausführungen des BVerfG ist zunächst, dass der Angeklagte tatsächlich vor der Wahl steht, einen Eingriff in sein allgemeines Persönlichkeitsrecht zu dulden, oder mit einer gewissen Wahrscheinlichkeit einen solchen in sein Recht auf Freiheit aus Art. 2 Abs. 2 S. 2 GG[50] oder bei einer Geldstrafe in sein Eigentumsrecht aus Art. 14 GG hinzunehmen.

Hieraus eine Einwilligungssperre für das allgemeine Persönlichkeitsrecht abzuleiten, wäre dennoch verfehlt, da dem Angeklagten auf diese Weise neue Handlungsoptionen eröffnet werden und sein Selbstbestimmungsrecht gestärkt wird. Man spricht insofern von einer eingriffsmildernden Einwilligung, deren Anerkennung *Amelung* aus dem Verhältnismäßigkeitsgrundsatz ableitet.[51] Der Betroffene müsse vor dem Hintergrund legitimen staatlichen Zwanges die Möglichkeit haben, einen bestimmten Grundrechtseingriff zu mildern bzw. zu verhindern, also ein Rechtsgut preiszugeben, um ein anderes vor staatlichem Zugriff zu retten, das ihm wertvoller erscheine als das aufgeopferte.[52]

Diese verfassungsrechtliche Sichtweise entspricht auch der strafrechtlichen Einwilligungsdogmatik, die eine Einwilligung nicht in jeder Drucksituation ausschließt, sondern nur in einer rechtswidrigen und vom Einwilligungsempfänger, meist dem Täter, zu verantwortenden.

Eine Einwilligung in eine Operation ist daher auch bei einer schweren Krebserkrankung möglich, die ohne Behandlung zeitnah zum Tode führt, und ein Erpressungsopfer kann sich für die Geldübergabe der Hilfe eines Boten bedienen, ohne dass dieser sich wegen Beihilfe strafbar macht.[53] Die Zwangslage schränkt die Handlungsspielräume des Betroffenen nämlich nur ein, hebt sie aber nicht auf. Die noch verbleibenden Handlungsspielräume muss der Betroffene im Hinblick auf sein allgemeines Persönlichkeitsrecht selbstbestimmt nutzen können, weshalb *Rönnau* von einer Freiheit in der Unfreiheit spricht.[54] Diese gilt es zu respektieren.

Auch einfachgesetzlich ist die Einwilligungsmöglichkeit trotz ansonsten drohender gravierender prozessualer Nachteile in den verschiedensten Normen wie bspw. in § 56c Abs. 3 StGB, der Erteilung der Weisung, sich einer Entziehungskur zu unterziehen, um eine Strafaussetzung zu erhalten, in § 81a StPO, der körperlichen Untersuchung zur eigenen Entlastung, in § 148 Abs. 2 StPO, der Einwilligung in die Kontrolle des Schriftverkehrs mit dem Verteidiger, oder in § 257c StPO, der Verständigung, anerkannt.[55] Als besonders markantes Beispiel verweist *Amelung* zudem auf § 3 KastrG, in dessen Abs. 2 ausdrücklich festgeschrieben ist, dass die Einwilligung des Betroffenen nicht deshalb unwirksam wird, weil er zur Zeit der Einwilligung auf richterlicher Anordnung in einer Anstalt verwahrt wird.[56] Dabei ist der Grund der Einwilligung natürlich im Regelfall der, der weiteren Voll-

[47] *Amelung*, NStZ 1982, 38 (39).
[48] *Schwabe*, NJW 1982, 367. Ähnlich *Meyer-Mews*, NJW 2000, 916 (917); *Putzke*, ZJS 2011, 557 (558). Umfassend zum Nichtvorliegen einer Verletzung der Menschenwürde oder des allgemeinen Persönlichkeitsrechts *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (629 ff.).
[49] BVerfG NJW 1982, 375.
[50] Vgl. *Amelung*, NStZ 1982, 38.
[51] *Amelung*, NStZ 1982, 38 (39).
[52] *Amelung*, NStZ 1982, 38 (39).
[53] Vertiefend *Rönnau*, JuS 2005, 481 (485).
[54] *Rönnau*, JuS 2005, 481 (485).
[55] Vgl. *Amelung*, NStZ 1982, 38; *Schwabe*, NJW 1982, 367.
[56] *Amelung*, NStZ 1982, 38 (39). Vertiefend *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 2009, 607 (631 f.).

streckung der Freiheitsstrafe oder Maßregel zu entgehen.[57] Man kann daher allgemein festhalten, dass kein rechtlicher Grundsatz existiert, nach dem „bei der Beschaffung von Entlastungsbeweisen […] ausnahmslos Unfreiheit besteh[t]“.[58]

Zu Recht ist der BGH der Ansicht des BVerfG daher in späteren Entscheidungen auch nicht gefolgt.[59] Auch das BVerfG selbst hat seine Erwägungen in jüngeren Entscheidungen, soweit ersichtlich, nicht wiederholt. Eine Einwilligung in einen Lügendetektortest ist mithin nicht aus verfassungsrechtlichen Gründen ausgeschlossen.

3. Der Lügendetektor als vollkommen ungeeignetes Beweismittel

a) Die Argumentation der Gerichte

Bereits seit Ende der 1990er Jahre argumentiert der BGH konsequent nicht mehr mit einem Verstoß gegen die Menschenwürde oder der Unbeachtlichkeit einer erteilten Einwilligung, sondern er stellt fest, eine polygraphische Untersuchung sei ein vollkommen ungeeignetes Beweismittel i.S.d. § 244 Abs. 3 S. 3 Nr. 4 StPO und aus diesem Grund unzulässig.[60]

Die Begründung lautet im Wesentlichen wie folgt: Ein Polygraph alter Bauart ermögliche keinen Einblick in die Seele des Untersuchten, da kein eindeutiger Zusammenhang zwischen bestimmten kognitiven oder emotionalen Zuständen und hierfür spezifischen Reaktionsmustern im vegetativen Nervensystem zu erkennen sei.[61] Im Ergebnis könne daher nicht gemessen werden, ob der Untersuchte die Wahrheit sage.[62] Dies gelte jedenfalls für die bislang verwendeten Testverfahren, also den Einsatz des Polygraphen in Verbindung mit dem Kontrollfragen- oder dem Tatwissenstest.

Der Kontrollfragentest sei deshalb als ungeeignet zu bewerten, da die erzielten Ergebnisse nicht valide seien.[63] Das Untersuchungsergebnis habe keinerlei Beweiswert.[64] Zwar erscheine es auf den ersten Blick plausibel, dass ein Täter auf die direkt die Tatbegehung betreffenden Fragen aus Furcht vor Bestrafung mit stärkerer Erregung reagieren soll als auf die Kontrollfragen, während sich dies beim Nichttäter umgekehrt verhalte.[65] Dabei werde allerdings verkannt, dass der zu Unrecht Beschuldigte in gleichem oder noch stärkerem Maße befürchten könne, das gegen ihn geführte Verfahren werde strafrechtliche oder sonstige Folgen nach sich ziehen.[66]

Da das Kontrollverfahren somit konzeptionell nicht abgesichert und seine Funktionsweise nicht belegbar sei, käme unter seiner Verwendung gewonnenen Ergebnissen grundsätzlich keine Beweisbedeutung zu.[67] Einen gewissen indiziellen Beweiswert könnte das Verfahren nur dann haben, „wenn eine hinreichend breite Datenbasis belegen würde, dass – warum auch immer – bestimmte gemessene Körperreaktionen mit einem Verhalten (hier: wahre oder unwahre Äußerungen) in hohem Maße zusammenhängen. Diese Voraussetzung ist beim Kontrollfragentest jedoch nicht erfüllt.“[68] Die im damaligen Verfahren mitgeteilten Trefferquoten von 70 bis 90 % unterlägen im Hinblick auf die erheblichen Zweifel an der Kontrollfragenmethode tiefgreifenden Bedenken.[69] Diese würden dadurch gestützt, dass es sich überwiegend um Analogstudien gehandelt habe, die keine Gewähr für eine Vergleichbarkeit des Modellversuchs und dessen Aussagekraft in der Praxis böten. Bei den Studien, denen echte Kriminalfälle zugrunde lägen, seien statistische Verzerrungen festzustellen und es fehle ein tauglicher Prüfungsmaßstab für die Validitätsuntersuchungen.[70] Das Urteil, das Geständnis oder die panel-Entscheidung, anhand derer die Frage beantwortet worden wäre, ob die polygraphische Untersuchung richtig gewesen sei, sei nämlich in den Studien mit hoher Wahrscheinlichkeit selbst durch das polygraphische Untersuchungsergebnis determiniert gewesen.[71] Die weder vom Untersucher noch vom Gericht überprüfbaren Wechselwirkungen von Prüfungsgegenstand und Prüfungsmaßstab nähmen den vorliegenden Feldstudien jegliche Aussagekraft und machten sie statistisch wertlos.

Der Tatwissenstest funktioniere demgegenüber nur unter der Voraussetzung, dass dem Befragten keine Details über den Tatablauf und die Tatdetails bekannt geworden seien. Sobald der Beschuldigte also Akteneinsicht hatte, handelt es sich auch bei dieser Befragungsmethode um eine ungeeignete.[72]

b) Die Bewertung der Argumentation

Für die modernen Lügendetektoren ist zunächst festzustellen, dass sie, jedenfalls wenn man der bisherigen Berichterstattung vertraut, auch unabhängig von der Befragung des Probanden durch einen an bestimmte Befragungsregeln gebundenen Sachverständigen überzeugende Ergebnisse liefern.[73] Auf die fehlende Eignung des Tatwissenstests oder des Kontrollfragentests käme es dann gar nicht an.

Zudem ist darauf hinzuweisen, dass dem BGH wiederholt vorgeworfen wurde, neue Studien zur Validität in den Folgeentscheidungen nicht berücksichtigt zu haben, sondern sich nach wie vor nur auf den Stand der Forschung im Jahr 1998

[57] *Amelung*, NStZ 1982, 38 (39).
[58] *Schwabe*, NJW 1982, 367.
[59] BGHSt 44, 308 (312).
[60] BGHSt 44, 308 (312 f.); BGH HRRS 2011, Nr. 220 Rn. 8; vgl. auch BGH NJW 1999, 662 (663).
[61] BGHSt 44, 308 (315).
[62] BGHSt 44, 308 (316).
[63] BGHSt 44, 308 (319).
[64] BGHSt 44, 308 (319).
[65] BGHSt 44, 308 (320).
[66] BGHSt 44, 308 (320).
[67] BGHSt 44, 308 (322).
[68] BGHSt 44, 308 (322).
[69] BGHSt 44, 308 (323).
[70] BGHSt 44, 308 (323).
[71] BGHSt 44, 308 (324).
[72] vgl. BGHSt 44, 308 (327).
[73] Anders die These von *Dahle/Lehmann* (Fn. 10), S. 48 (55 ff. und 74).

zu beziehen.[74] Neuere Studien sollen demgegenüber die hohe Treffsicherheit der polygraphischen Untersuchungen belegen, ohne an den vom BGH ausgemachten methodischen Fehlern zu leiden.[75] *Putzke* stellt daher richtigerweise klar, dass die Annahme des BGH, es sei nach einhelliger wissenschaftlicher Auffassung nicht möglich, eindeutige Zusammenhänge zwischen bestimmten kognitiven oder emotionalen Zuständen und hierfür spezifischen Reaktionsmustern im vegetativen Nervensystem zu erkennen, heutzutage nicht mehr zutreffe.[76] Der *1. Strafsenat* habe in der bislang letzten Polygraphenentscheidung darüber geirrt, dass die 1998 gewonnenen Erkenntnisse noch Gültigkeit beanspruchen würden.

Für die neuen KI-gestützten Lügendetektoren kann derzeit zwar noch nicht beurteilt werden, ob künftig belastbare Studien über deren Treffergenauigkeit vorgelegt werden können. Unterstellen wir dies jedoch zunächst, wäre allein aus diesem Grund die Eignung des Beweismittels belegt. Die Bedenken, die der BGH gegen die frühen zum Kontrollfragentest durchgeführten Untersuchungen ins Feld geführt hat, ließen sich leicht vermeiden. Da die KI mit Videos aus Gerichtsverfahren trainiert worden ist und ebenso an Videos aus Gerichtsverfahren getestet werden kann, würde es sich nicht lediglich um Laborversuche ohne Aussagekraft handeln. Da die KI auch nicht selbst dazu beigetragen hat, dass die jeweilige Aussage im Verfahren und anschließend von den Versuchsleitern als glaubhaft oder nicht glaubhaft bewertet wird, wird auch der gerügte Zirkelschluss vermieden.

Anzumerken ist zudem, dass es gar nicht erforderlich ist, dem polygraphischen Ergebnis eine Trefferwahrscheinlichkeit nahe 100 % zu bescheinigen, um dessen Eignung als Beweismittel zu bejahen.[77] Es genügt zur Vermeidung von den Angeklagten belastenden Fehlurteilen bereits, dass vernünftige Zweifel an dessen Schuld begründet werden.[78] Bedenkt man, dass gerade im Bereich der Sexualdelikte von einer hohen Anzahl falscher Anzeigen und Aussagen ausgegangen werden muss, könnte ein entlastendes Testergebnis selbst bei einer Fehlerquote von noch 10 bis 15 % zu solchen Zweifeln führen. Dies gilt erst recht, wenn die Lügendetektorsoftware lediglich zur Absicherung bestimmter Ergebnisse eingesetzt wird und in Kombination mit anderen Beweismitteln oder Indizien genutzt wird.

Hinzu kommt, dass sich Wahrscheinlichkeitsurteile unter der Prämisse, dass sie unabhängig voneinander zustande gekommen sind, auch mit einer einfachen mathematischen Formel kumulieren lassen.[79] Nehmen wir beispielsweise an, ein Glaubhaftigkeitsgutachter und ein KI-gestützter Lügendetektor bescheinigen einer Aussage einmal mit siebzigprozentiger und einmal mit fünfundachtzigprozentiger Wahrscheinlichkeit, dass sie wahres Erleben zum Gegenstand hat, beträgt die Gesamtwahrscheinlichkeit für die Wahrheit der Aussage bereits 93 %. Dass eine kriteriengestützte Aussageanalyse, die sich maßgeblich auf den Inhalt der Aussage stützt – der sog. inhaltsbasierte Ansatz –, und ein KI-gestützter Lügendetektor, der maßgeblich mit Mikroimpressionen arbeitet – der sog. verhaltensbasierte Ansatz –, ihre Ergebnisse auf unterschiedlichem Wege erzielen, scheint dabei als Grundannahme jedenfalls plausibel.[80]

Entsprechend betrüge die Wahrscheinlichkeit dafür, dass der Angeklagte die Wahrheit sagt, ein Belastungszeuge aber lügt, 96 %, wenn der Wahrheitsgehalt beider Aussagen durch die Künstliche Intelligenz mit fünfundachtzigprozentiger Wahrscheinlichkeit prognostiziert würde.

Bei höheren Ausgangswahrscheinlichkeiten oder einer größeren Anzahl die Aussage stützender Wahrscheinlichkeiten erhöht sich die Gesamtwahrscheinlichkeit weiter spürbar.

Zumindest begründete Zweifel im Falle einer falschen Verdächtigung wird ein KI-gestützter Lügendetektortest daher schüren können.

Konsequent hat insofern bereits das AG Bautzen dem BGH in mehreren Entscheidungen die Gefolgschaft versagt und den Einsatz eines klassischen Polygraphen in verschiedenen Verfahren zugelassen.[81] In seiner ersten diesbezüglichen Entscheidung hatte die Sachverständige sowohl den Beschuldigten als auch das mutmaßliche Vergewaltigungsopfer mittels eines Polygraphen untersucht.[82] Wie bereits erwähnt, erhöht sich die Trefferwahrscheinlichkeit des Tests durch eine solche Doppelabsicherung noch einmal beträchtlich, da zufällig beide Testergebnisse fehlerhaft sein müssten, wenn in einem Fall eine Lüge und in dem anderen Fall eine wahre Aussage bestätigt wird und es sich tatsächlich andersherum verhalten sollte.

Im Rahmen der Beweiswürdigung hob das AG zur Rechtfertigung des Polygrapheneinsatzes sodann zutreffend hervor, dass der BGH einen Sachverständigen nicht schon dann als völlig ungeeignetes Beweismittel bewerte, wenn dieser absehbar aus den Anknüpfungstatsachen keine sicheren und eindeutigen Schlüsse zu ziehen vermöge, sondern umgekehrt bereits dann von einer Eignung als Beweismittel ausgehe, wenn die sachverständigen Schlussfolgerungen die unter Beweis gestellte Behauptung als mehr oder weniger wahrscheinlich erscheinen lasse und hierdurch unter Berücksichtigung des sonstigen Beweisergebnisses Einfluss auf die Über-

[74] AG Bautzen BeckRS 2013, 8655; *Putzke*, ZJS 2011, 557 (559 f.); *Undeutsch*, Psychologische Rundschau 2003, 115 (117 f.).

[75] AG Bautzen BeckRS 2013, 8655; *Putzke*, ZJS 2011, 557 (559 f.); *ders./Scheinfeld*, StraFo 2010, 58; *ders./Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (621 ff.).

[76] *Putzke*, ZJS 2011, 557 (559 f.).

[77] *Amelung*, NStZ 1982, 38 (39).

[78] *Amelung*, NStZ 1982, 38 (39).

[79] Die Gesamtwahrscheinlichkeit der Wahrscheinlichkeiten W1 und W2 errechnet sich wie folgt: 1/(1+[{1 – W1} x {1 – W2}/W1 x W2]). Weitere Wahrscheinlichkeiten können nach demselben Muster in der Formel ergänzt werden.

[80] Vgl. *Nestler*, JA 2017, 10 (13).

[81] AG Bautzen BeckRS 2013, 8655; AG Bautzen BeckRS 2017, 138202; AG Bautzen BeckRS 2018, 42301. Entsprechendes gilt für familiengerichtliche Verfahren u.a. auch für das OLG Bamberg NJW 1995, 1684; OLG Dresden BeckRS 2013, 16540.

[82] AG Bautzen BeckRS 2013, 8655.

zeugungsbildung des Gerichts erlangen könne.[83] Da eine neuere Untersuchung unter Feldbedingungen eine Treffsicherheit des Kontrollfragenverfahrens von 98,5 % ergeben habe, ohne an den vom BGH aufgezeigten methodischen Mängeln zu leiden, sei diese Voraussetzung erfüllt. Jedenfalls sei das physiopsychologische Verfahren anderen Methoden der forensischen Aussageuntersuchung jedoch überlegen.[84] Frei zusammengefasst, müsste man daher entweder auch auf aussagepsychologische Begutachtungen verzichten, da diese nicht besser abgesichert seien als physiopsychologische Untersuchungen, oder eben beide zulassen.[85] Dies hat das AG sodann konsequent getan.

Da der Einsatz der KI-gestützten Lügendetektoren mangels Erhebung sonst nicht wahrnehmbarer Daten und mangels des Erfordernisses, den Probanden an eine Maschine anzuschließen, einen geringeren Grundrechtseingriff darstellt als das frühere Vorgehen, müsste man daher auch den modernen Lügendetektor als dem Grunde nach zulässiges Beweismittel ansehen.

Es bleibt daher nur noch eine letzte Frage zu beantworten und zwar die, ob der Einsatz eines Polygraphen einer gesetzlichen Ermächtigungsgrundlage bedarf.

IV. Das Erfordernis einer Ermächtigungsgrundlage

Das Ergebnis einer klassischen polygraphischen Untersuchung ist bislang im Wege des Sachverständigenbeweises in das Strafverfahren eingeführt worden.[86] Die Aufzeichnungen des Mehrkanalschreibers bedurften der Interpretation im Hinblick auf das zugrunde liegende Testverfahren.

Die Ergebnisse eines KI-gestützten Lügendetektortests ließen sich daher ebenfalls im Wege des Sachverständigenbeweises einführen, wenn entweder das Testverfahren besonderer Sachkunde bedarf oder die Ergebnisse zu interpretieren sind.

Es ist jedoch auch vorstellbar, dass die Ergebnisse künftig im Wege des Augenscheins- oder Urkundenbeweises in das Verfahren eingeführt werden können, etwa wenn eine wahrscheinlich unwahre Aussage durch das Aufblinken einer roten Lampe symbolisiert wird oder ein Computerausdruck Aufschluss darüber gibt, welche Antworten wahrscheinlich erlebnisbasiert beantwortet worden sind und welche Antworten wahrscheinlich der Fantasie entsprungen sind.

Fraglich ist daher, ob § 244 StPO jede vom Sachverständigen angewandte Untersuchungsmethode mitlegitimiert[87] und dem Gericht ggf. auch erlaubt, die Urkunde oder den Augenschein erst zu erzeugen.

Nach allgemeinen Grundsätzen hängt dies von der Schwere des Grundrechtseingriffs ab, was sich auch den §§ 72 ff. StPO implizit entnehmen lässt. Nicht explizit geregelte Untersuchungsmethoden wie die Befragung des Untersuchten durch einen Psychologen zur Durchführung einer kriteriengestützten Aussageanalyse stellen entweder keine oder nur geringfügige Grundrechtseingriffe dar. Die benannten Untersuchungsmethoden rechtfertigen demgegenüber deutliche Grundrechtseingriffe und sind deshalb ausdrücklich gestattet.

Insofern ist nach altem Recht zutreffend zwischen Maßnahmen gegen den Willen und solchen mit Einwilligung unterschieden worden.[88] Die polygraphische Untersuchung des Beschuldigten mit Einwilligung ist insofern von den Befürwortern dieses Verfahrens ohne weitere Ermächtigungsgrundlage zugelassen worden,[89] eine entsprechende Untersuchung ohne Einwilligung sollte aus verschiedenen Gründen undurchführbar sein.[90]

Für Beschuldigte bleibt es auch künftig dabei, dass der Einsatz eines Lügendetektors gegen ihren Willen im Hinblick auf den nemo-tenetur-Grundsatz auszuscheiden hat. Bei Zeugen könnte die neue Generation der Lügendetektoren aus technischer Sicht ggf. auch gegen ihren Willen eingesetzt werden und zu aussagekräftigen Ergebnissen führen. In diesem Fall müsste der Eingriff in das allgemeine Persönlichkeitsrecht wohl als erheblich genug angesehen werden, um den Gesetzesvorbehalt auszulösen.

Ob für den Einsatz KI-gestützter Lügendetektoren mit Einwilligung nach wie vor auf eine Ermächtigungsgrundlage verzichtet werden kann, ist seit Inkrafttreten der Richtlinie (EU) 2016/680[91] und ihrer Umsetzung im neuen BDSG fraglich.

Dass im Falle der Einwilligung kein Grundrechtseingriff vorliegt, steht dabei nach wie vor fest.[92] Allerdings könnte sich das Erfordernis einer Ermächtigungsgrundlage trotz Einwilligung aus der bereits genannten Richtlinie und § 51 BDSG ergeben.

Die Richtlinie (EU) 2016/680 regelt nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 u.a. die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten durch die jeweils zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung und ist insofern anwendbar.[93] Für die

[83] So das AG Bautzen BeckRS 2013, 8655, unter zutreffender Berufung auf BGH, NStZ 2012, 345; ebenso AG Bautzen BeckRS 2018, 42301 Rn. 37.

[84] Vertiefend AG Bautzen BeckRS 2013, 8655 m.w.N.

[85] AG Bautzen BeckRS 2013, 8655; ähnlich auch *Putzke*, ZJS 2011, 557 (561 f.).

[86] *Putzke/Scheinfeld*, StraFo 2010, 58 (62).

[87] So wohl *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (638).

[88] Vgl. zu dieser Unterscheidung im Hinblick auf das neue Datenschutzrecht *El-Ghazi*, ZIS 2019, 110 f.

[89] AG Bautzen BeckRS 2013, 8655; AG Bautzen BeckRS 2017, 138202; AG Bautzen BeckRS 2018, 42301; *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (638).

[90] *Putzke/Scheinfeld/Klein/Undeutsch*, ZStW 121 (2009), 607 (628 f.).

[91] Richtlinie 2016/680/EU 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, ABl. EU 2016 Nr. L 119/89, S. 89 ff.

[92] Vertiefend *El-Ghazi*, ZIS 2019, 110 f.

[93] Vertiefend zur Anwendbarkeit *El-Ghazi*, ZIS 2019, 110 (111 f.).

genannten Zwecke legt Art. 8 Abs. 1 der Richtlinie fest, dass die Mitgliedstaaten regeln müssen, dass die Verarbeitung nur dann rechtmäßig ist, wenn und soweit die Verarbeitung für die Aufgabenerfüllung erforderlich ist und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt. In Erwägungsgrund 35 heißt es zunächst, dass die Einwilligung im Falle der Aufforderung zur Mitwirkung an einer Maßnahme nicht per se rechtfertigende Wirkung entfalten solle, da keine echte Wahlfreiheit bestehe. Dies solle die Mitgliedstaaten jedoch nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person einwilligen könne, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung.

In Erwägungsgrund 37 heißt es für die Verarbeitung besonders sensibler Daten, ihre Verarbeitung sollte durch Rechtsvorschriften erlaubt sein, wenn die betroffene Person der Datenverarbeitung, die besonders stark in ihre Privatsphäre eingreift, ausdrücklich zugestimmt hat. Die Einwilligung der betroffenen Person allein sollte jedoch noch keine rechtliche Grundlage für die Datenverarbeitung liefern.

Ob hieraus folgt, dass nach den unionsrechtlichen Vorgaben stets eine Ermächtigungsgrundlage erforderlich sei, die explizit eine Einwilligung vorsehen müsse, ist umstritten.[94] Die besseren Gründe, etwa die konsequente Unterscheidung der Richtlinie zwischen den Formulierungen „Recht der Mitgliedstaaten" und „Rechtsgrundlagen" (in den Mitgliedstaaten), sprechen dagegen.[95] Ein weiteres tragendes Argument ist die Formulierung von Erwägungsgrund 35, in dem es ebenfalls heißt: „Wenn in dieser Richtlinie auf Recht der Mitgliedstaaten, eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt, wobei Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats unberührt bleiben."[96] Die deutsche Verfassung erfordert nun aber gerade keine spezielle Ermächtigungsgrundlage, wenn eine Einwilligung vorliegt.

Für die derzeit in Deutschland geltende Rechtslage kommt es auf diesen Streit im Ergebnis allerdings auch gar nicht weiter an, da der deutsche Gesetzgeber sich in § 51 Abs. 1 BDSG i.S.d. Ermächtigungslösung festgelegt hat.[97] Es heißt: „Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können."

Im Vergleich dazu heißt es in Art. 7 Abs. 1 DSGVO: „Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat." Dies ist ein klarer Beleg dafür, dass das BDSG eine Ermächtigungsgrundlage auch für den Fall der Einwilligung fordert.

Bekanntermaßen sieht die StPO bislang keine Möglichkeit vor, in einen Lügendetektortest einzuwilligen.

Da jedoch bei sachgemäßer Ausgestaltung des Verfahrens kein höherrangiges Recht entgegensteht[98] und auch die Frage der Validität heute anders zu beantworten ist als noch 1998, steht der Zulassung des Lügendetektortests gerade auch in Form eines KI-gestützten Verfahrens, das den Grundrechtseingriff deutlich abschwächt, nichts entgegen.

Dies gilt jedenfalls, wenn der Test lediglich zu Gunsten des Beschuldigten eingesetzt wird und zudem bei einem bestimmten Katalog schwerer Delikte, insbesondere beim Vorwurf einer Vergewaltigung. Falsch positive Ergebnisse, beispielsweise ausgelöst durch eine unreflektierte Orientierung der Richter an dem Untersuchungsergebnis, könnten so nicht zustande kommen und die Rechte des Beschuldigten auf Eigentum und persönliche Freiheit würden bereits unabhängig von der Einwilligungsproblematik ein erhebliches rechtfertigendes Gewicht entfalten.

Weiteren vorgebrachten Bedenken gegen den Einsatz von Lügendetektorsoftware ließe sich dadurch begegnen, dass lediglich der freiwillige Lügendetektortest zugelassen wird,[99] der von vornherein nicht zu einem Grundrechtseingriff führt, nach dem Wortlaut des § 51 Abs. 1 BDSG aber dennoch einer Ermächtigungsgrundlage bedarf.

In der einzuführenden Erlaubnisnorm können sodann weitere Vorgaben für das einzuhaltende Verfahren und dessen Standards gemacht werden. Ein Hinweis auf die Selbstverständlichkeit, dass die fehlende Einwilligung in einen Lügendetektortest nicht zulasten des Beschuldigten verwertet werden darf, ließe sich klarstellend einfügen. Eine entsprechende Regelung in die StPO aufzunehmen, dürfte sich nach alledem künftig empfehlen, sofern die derzeitigen Pilotprojekte den Erwartungen und Prognosen standhalten. Bis zur Einführung einer solch speziellen Einwilligungsnorm ist zudem zu erwägen, jedenfalls bei erheblichen Tatvorwürfen eine verfassungskonforme Reduktion des § 51 Abs. 1 BDSG im Hinblick auf polygraphische Untersuchungen des Beschuldigten mit dem Ziel der Selbstentlastung vorzunehmen. Das Recht auf ein faires Verfahren, die bei Verurteilung drohenden Grundrechtsverletzungen sowie das Allgemeine Persönlichkeitsrecht könnten es gebieten, dem Beschuldigten diese Möglichkeit zur Selbstentlastung trotz des entgegenstehenden Wortlauts des § 51 Abs. 1 BDSG zu gewähren. Eine genaue Grenzziehung, was aus verfassungsrechtlichen Gründen entgegen § 51 Abs. 1 BDSG auch ohne Ermächtigungsgrundlage gestattet werden muss, kann vorliegend jedoch nicht geleistet werden.

[94] Gegen die These der im Unionsrecht verankerten Ermächtigungsgrundlage *El-Ghazi*, ZIS 2019, 110 (113 ff.); dafür *Stief*, StV 2017, 470 (474); *Schwichtenberg*, DuD 2016, 605 (606).

[95] Vertiefend *El-Ghazi*, ZIS 2019, 110 (114 f.).

[96] So bereits *El-Ghazi*, ZIS 2019, 110 (115).

[97] *Stemmer/Wolff*, in: Wolff/Brink, BeckOK Datenschutzrecht, 33. Lfg., Stand: August 2020, § 51 Rn. 13 m.w.N.

[98] So „unter dem Vorbehalt hoher Verlässlichkeit der Ergebnisse" im Hinblick auf eine erteilte Einwilligung auch *Herdegen*, in: Maunz/Dürig (Fn. 40), Art. 1 Abs. 1 GG Rn. 85.

[99] Vgl. zum unfreiwilligen Lügendetektortest auch die kritische Bewertung von *Di Fabio* (Fn. 40), Art. 2 Abs. 1 GG Rn. 162; *Herdegen* (Fn. 97), Art. 1 Abs. 1 GG Rn. 85.

Das „Reformpaket zur Bekämpfung sexualisierter Gewalt gegen Kinder“

Von Prof. Dr. **Tatjana Hörnle**, Berlin*

I. Empörung über gravierende Sexualdelikte gegen Kinder

Manche Ermittlungsverfahren wegen sexuellen Missbrauchs von Kindern finden sehr große öffentliche Aufmerksamkeit, nämlich dann, wenn mehrere Personen beschuldigt werden, vielfache schwere Sexualdelikte an Kindern begangen und Filmaufnahmen davon in Umlauf gebracht zu haben. Presse und Fernsehen berichteten im Juni 2020 ausführlich über das laufende Verfahren gegen einen Hauptverdächtigen aus Münster und (derzeit) 20 weitere Personen,[1] wie auch schon zuvor über den Fall in Lügde. Politikerinnen und Politiker wurden befragt, welche Maßnahmen sie gegen solche Delikte zu ergreifen gedächten. Wesentlicher Bestandteil der Antworten war die Forderung nach Strafschärfungen.[2] Auch in der Öffentlichkeit wird nach härteren Strafen verlangt.[3] Zwar sind die einschlägigen Straftatbestände seit den neunziger Jahren mit insgesamt sechs Gesetzesänderungen wie bei keiner anderen Deliktskategorie kontinuierlich ausgeweitet und verschärft worden.[4] Doch ist dies nur wenigen bekannt, und ein nüchterner Hinweis darauf, dass selbst ein lückenloses Strafrecht Delikte nie ganz unterbinden kann, würde in öffentlichen Diskursen als Zeichen emotionaler Kälte gedeutet und negativ bewertet.

Am 1. Juli 2020 hat das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) ein „Reformpaket zur Bekämpfung sexualisierter Gewalt gegen Kinder“ vorgestellt.[5] Die Bundesjustizministerin Christine Lambrecht hatte auf den Ruf nach härteren Strafen zunächst zurückhaltend reagiert. Das trug ihr den Vorwurf von Kinderschutzverbänden ein, in einem „Elfenbeinturm“ zu leben und unfähig zu sein, „auch nur einen Hauch von Empathie für die Betroffenen zu entwickeln“.[6] Das nunmehr vorgelegte Reformpaket lässt einen weitgehenden Meinungsumschwung erkennen. Darin wird vorgeschlagen, die Strafrahmen für mehrere Tatbestände in den §§ 176, 176a und § 184b StGB deutlich anzuheben (dazu unten III. 1., 3.). Zudem soll die Tatbestandsüberschrift „Sexueller Missbrauch von Kindern“ durch „Sexualisierte Gewalt gegen Kinder“ ersetzt werden (dazu unten III. 2.).

II. Zur Funktion von gesetzlichen Strafrahmen und Tatbestandsüberschriften

Zeitdruck beim Verfassen von Reformvorschlägen und eine starke Emotionalisierung der Debatten geben Anlass zu der Annahme, dass eine Änderung des Strafrechts keine Verbesserung sein könnte. Allerdings sind rechtspolitische Ideen in solchen Kontexten nicht *per se*, d.h. *nur* wegen einer solchen Vorgeschichte kritikwürdig. Ein Blick auf erfolgte Änderungen kann auch zu der Erkenntnis führen, dass das geltende Recht defizitär war und selbst mit hastig beschlossenen Gesetzen (jedenfalls teilweise) eine Verbesserung erreicht werden konnte.[7] Entscheidend für die Beurteilung ist Klarheit über die normativen Kriterien, die anzulegen sind, damit geltendes Recht als defizitär und eine entsprechende Änderung als gelungen bezeichnet werden kann. Auch für eine

* Die *Verfasserin* ist Geschäftsführende Direktorin und Leiterin der Abteilung Strafrecht am Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht sowie Honorarprofessorin an der Humboldt-Universität zu Berlin.

[1] Stand Ende Juni; siehe Zeit Online, v. 30.6.2020, abrufbar unter https://www.zeit.de/gesellschaft/zeitgeschehen/2020-06/sexueller-missbrauch-muenster-kindesmissbrauch-tatverdaechtigte-herbert-reul-cdu (7.9.2020).

[2] Siehe z.B. Spiegel Online v. 8.6.2020, abrufbar unter https://www.spiegel.de/politik/deutschland/kindesmissbrauch-in-muenster-herbert-reul-wir-werden-garantiert-nie-alle-erwischen-a-02e52d17-b2f6-4637-8720-533e79fa985b (7.9.2020); Der Tagesspiegel v. 18.6.2020, abrufbar unter https://www.tagesspiegel.de/politik/sexueller-missbrauch-von-kindern-giffey-fordert-mehr-aufklaerung-und-haertere-strafen/25929534.html (7.9.2020).

[3] Siehe *Seidel*, Deutschlandfunk v. 4.7.2020, abrufbar unter https://www.deutschlandfunk.de/haertere-strafen-bei-kindesmissbrauch-ein-laengst.720.de.html?dram:article_id=479901 (7.9.2020); außerdem die Petition auf https://www.openpetition.de/petition/argumente/haertere-strafen-fuer-kinderschaender (7.9.2020).

[4] Siehe für einen Überblick über die Gesetzesänderungen *Renzikowski*, in: Erb/Schäfer (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 4. Aufl. (im Druck), Vor § 174 Rn. 89 ff.

[5] Zu finden auf der Homepage des BMJV unter https://www.bmjv.de/SharedDocs/Artikel/DE/2020/070120_Bekaempfung_sexualisierte_Gewalt_Kinder.html (7.9.2020).

[6] Siehe Deutsches Verbände Forum (online), Pressemitteilung v. 10.06.2020, abrufbar unter https://www.verbaende.com/news.php/Ministerin-Lambrecht-Kindesmissbrauch-ist-Vergehen-Deutsche-Kinderhilfe-e-V-Sie-ist-nicht-mehr-tragbar?m=135433 (7.9.2020).

[7] Entgegen verbreiteter Kritik (siehe *Hoven*/Weigend, JZ 2017, 182; *Lamping*, JR 2017, 347; *Fischer*, StGB, 67. Aufl. 2020, § 177 Rn. 4; *Wolters/Noltenius*, in: Wolter [Hrsg.], Systematischer Kommentar zum Strafgesetzbuch, Bd. 4, 9. Aufl. 2017, § 177 Rn. 5) würde ich diese Diagnose für die Reform des § 177 StGB im Jahr 2016 stellen. Zwar wäre eine bedachtere Reform wünschenswert gewesen. So ist die Aufblähung des jetzigen § 177 StGB zu kritisieren: Eine klarere Struktur von Grundtatbeständen und Qualifikationen wäre vorzugswürdig, und es wurde nicht bedacht, dass die Änderungen in § 177 Abs. 5 (Wegfall des Verbs „nötigen“ und Abschaffung des Finalzusammenhangs) nicht mehr zu der Überschrift „sexuelle Nötigung“ passen. Alles in allem ist es aber gelungen, in Absatz 1 und Absatz 2 Tatbestände einzuführen, welche sexuelle Selbstbestimmung besser schützen als das alte Recht.

Bewertung des Reformpakets sollte der erste Schritt darin bestehen, sich über *allgemeine* normative Anforderungen an Strafgesetze zu vergewissern. Gesetzliche Strafrahmen und die dort festgelegten Ober- und Untergrenzen haben Funktionen für die richterliche Strafzumessung zu erfüllen (unten 2.) und sie haben expressive Bedeutung (unten 1.). Überschriften von Tatbeständen sollten eine inhaltlich passende, systematisch stimmige und sprachlich funktionierende Kurzbeschreibung ergeben (unten 3.).

1. Die expressive Funktion von Strafrahmen

Ein Verweis auf die expressive Bedeutung von Strafgesetzen und Strafrahmen bedarf der Erklärung. Er kann deskriptiv gemeint sein und mündet dann meist in kriminalpolitische Kritik an symbolischen Gesetzen.[8] Im Folgenden gehe ich von einer normativen Prämisse aus: Nicht nur die Verhaltensnorm, sondern auch der damit verbundene Strafrahmen sollen etwas kommunizieren, und zwar nicht nur gegenüber potentiellen Tätern, sondern an die gesamte Bevölkerung gerichtet. Das Strafniveau, das durch Unter- und Obergrenzen definiert wird, vermittelt, in welchem Ausmaß das beschriebene Verhalten als strafwürdiges Unrecht zu gelten hat. Dafür kommt es entscheidend auf die Beeinträchtigung von Opferrechten an. Anders als im Schrifttum gelegentlich angenommen, ist nicht die Opferorientierung als solche zu kritisieren,[9] sondern das Anlegen falscher Maßstäbe bei Aussagen zum Unrechtsausmaß. Das Kernproblem des Reformvorhabens liegt darin, dass Begründungen an mehreren Stellen nicht über die Ebene intuitiver Moralurteile („besonders verwerflich“) hinausreichen.

Aussagen zum Ausmaß des Unrechts sollten in sachlich-abwägender Weise die Verletzung individueller Rechte von Opfern bewerten. Nicht nur bei der Strafzumessung im Einzelfall, sondern bereits für die Festsetzung der gesetzlichen Strafrahmen kommt es auf die Analyse der unrechtsrelevanten Faktoren an. In erster Linie ist darauf abzustellen, wie intensiv verbotene Handlungen Rechte der kindlichen Opfer verletzen. Das Ausmaß der Missachtung sexueller Selbstbestimmung und damit die Intensität und Häufigkeit der abzuurteilenden sexuellen Handlungen sind von zentraler Bedeutung.[10] Außerdem ist die Verletzung weiterer Rechte (vor allem des Rechts auf körperliche Integrität) maßgeblich sowie das Ausmaß der psychischen Belastungen und Gefahren für Kinder bei und wegen der Tat.[11] Zu diesen Gefahren gehören auch mögliche Langzeitfolgen für ihre psychische und soziale Entwicklung. Neben solchen das Erfolgsunrecht prägenden Umständen hängt die Unrechtsbemessung von Faktoren ab, die das Handlungsunrecht prägen; dazu gehört neben Wissen und Wollen der Täter ggf. auch der Missbrauch von Vertrauensverhältnissen.[12] Zur Festsetzung der Höhe und Spannbreite gesetzlicher Strafrahmen ist zu überlegen, welche Rechte der kindlichen Opfer durch das tatbestandliche Verhalten immer, typischerweise, manchmal, oder beim konkreten Deliktstypus nie beeinträchtigt werden (z.B. verletzen Handlungen ohne Körperkontakt nicht das Recht auf körperliche Integrität und gehören deshalb in eine niedrigere Unrechtskategorie). Von Bedeutung ist außerdem, ob das tatbestandliche Verhalten die Rechte von Kindern verletzt, oder aber nur dazu dient, späteren Missbrauch vorzubereiten, also Kinder (wenn überhaupt) gefährdet, aber nicht verletzt.

An diesem Punkt ist es unvermeidbar, auf Unterschiede zwischen der rechtlichen Bewertung von Unrecht und der Perspektive von Nicht-Juristen zu verweisen. Wer nie damit befasst war, systematisch Erfolgsunrecht und Handlungsunrecht zu analysieren und zwischen Verletzungen und Gefährdungen zu unterscheiden, wird zwangsläufig auf vage und holistische Bewertungen wie „besonders verwerflich“ zurückgreifen. Befremdlich ist, wenn in einem Dokument aus einem Justizministerium diese moralisch-holistische Sichtweise dominiert. Rationale Rechtsgestaltung sollte auf den Fundus der Rechtswissenschaft zurückgreifen. Ein verantwortungsvoller Umgang mit der expressiven Funktion des Strafrechts erfordert eine Unrechtsbewertung, die sich präzise an den möglichen Verletzungen und Gefährdungen der Rechte potentieller Opfer orientiert.

2. Strafrahmen sollen für das gesamte Spektrum tatbestandlicher Handlungen unrechtsangemessene Strafen ermöglichen

Eine weitere wichtige Vorgabe für die Festsetzung von Strafrahmen ist, dass für *jede vorstellbare Variante* an Handlungen und Begleitumständen, die unter den Tatbestand zu subsumieren sind, eine dem Unrecht angemessene Strafe möglich ist. Die Untergrenze des gesetzlichen Strafrahmens ist dabei mit Blick auf die leichtesten möglichen Sachverhalte zu prüfen.[13] Die Testfrage bei Entscheidungen des Gesetzgebers sollte sein, ob Gerichte über Fallgestaltungen zu entscheiden hatten oder ob Sachverhalte vorstellbar sind, für welche die

[8] Siehe dazu unten Text bei Fn. 48.

[9] Kritisch zur Opferorientierung *Greco*, GA 2020, 258.

[10] *Schäfer/Sander/van Gemmeren*, Praxis der Strafzumessung, 6. Aufl. 2017, S. 648.

[11] *Schäfer/Sander/van Gemmeren* (Fn. 10), S. 649.

[12] *Schäfer/Sander/van Gemmeren* (Fn. 10), S. 226 (zum Thema sexuelle Nötigung; dasselbe gilt aber auch für andere Sexualdelikte).

[13] Siehe zur Bedeutung der Ober- und Untergrenzen *Dreher*, in: Frisch/Schmid (Hrsg.), Festschrift für Hans-Jürgen Bruns zum 70. Geburtstag, 1978, S. 141 (149); *Schöch*, in: Frisch (Hrsg.), Grundfragen des Strafzumessungsrechts aus deutscher und japanischer Sicht, 2011, S. 163 (166 f.); *Schneider*, in: Cirener/Radtke/Rissing-van Saan/Rönnau/Schluckebier (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 4, 13. Aufl. 2020, § 46 Rn. 298; *Meier*, Strafrechtliche Sanktionen, 5. Aufl. 2019, S. 238 f. Die Staffelung dazwischen, d.h. die Frage, ob das arithmetische Mittel des Strafrahmens einem abstrakt-theoretisch zu bildenden Durchschnittsfall oder einem statistisch ermittelbaren Regelfall entspricht (dazu *Dreher*, a.a.O., S. 150; *Meier*, a.a.O., S. 239 f.), ist für den Gesetzgeber weniger wichtig als für die Tatgerichte. Siehe für weiterführende Überlegungen dazu *Giannoulis*, Studien zur Strafzumessung, 2014, S. 281 ff.

gesetzliche Mindeststrafe als disproportional streng angesehen werden müsste. Mit Blick auf die allerschwersten Fälle, bei denen sämtliche möglichen unrechtserhöhenden Umstände kumulativ vorliegen, ist dagegen zu fragen, ob für ein solches Maximalunrecht die gesetzliche Höchststrafe ausreichend wäre. Beide Fragen kann nur beantworten, wer die Struktur des Tatbestandes sowie die Auslegung von Tatbestandsmerkmalen kennt und auf dieser Basis beurteilen kann, wie Fälle aussehen könnten, für die die Untergrenze bzw. die Obergrenze angemessen wäre.

Dies ist deshalb zu betonen, weil Personen ohne strafrechtliche Ausbildung die Ratio von Unter- und Obergrenzen und die Vielfalt an Lebenssachverhalten in der Regel nicht kennen, sondern davon ausgehen, was sie als „typischen Fall" wahrnehmen. Diese Wahrnehmungen beruhen auf Medienberichten und fiktionalen Darstellungen in Filmen und Kriminalromanen. Dies ergibt zwangsläufig eine starke Verzerrung: Sowohl Medienberichte über Ermittlungs- und Gerichtsverfahren als auch Plots im Krimi-Genre konzentrieren sich auf sehr schwere Fälle. Bürgerinnen und Bürger verbinden mit den Stichworten „Kindesmissbrauch und Kinderpornographie" Sachverhalte, wie sie bei den Tatserien in Münster und Lüdge vorlagen. Ihre Straferwartungen orientieren sich an solchen Taten, bei denen sehr viele unrechtserhöhende Umstände zusammentrafen: schwere Formen sexueller Handlungen (Eindringen in den Körper des Kindes); viele betroffene Opfer; massive körperliche und seelische Verletzungen und Gefahren für die zukünftige psycho-sexuelle Entwicklung der Kinder; mehrere Täter und Bandenstrukturen; viele Taten zulasten eines Opfers; Missbrauch von Vertrauensverhältnissen, da Kinder aus dem Familienkreis angegriffen werden; Anfertigung von Foto- und Filmaufnahmen; Personen, die sich in Internetforen wechselseitig bestärkt und zu Taten überredet haben. Wer nur solche Tatkomplexe vor Augen hat, muss zwangsläufig zu sehr viel höher angesetzten Strafrahmen kommen als Juristen, die zwischen unrechtskonstituierenden und mannigfaltigen unrechtserhöhenden Faktoren differenzieren.

Ein weiteres Problem für die Rechtsgestaltung liegt bei den sozialpsychologischen Effekten, die starke moralische Normen in zeitgenössischen Diskursen haben. Der aus juristischer Sicht zwingende Hinweis, dass es neben den jetzt bekannt gewordenen Tatserien auch Sachverhalte gibt, in denen alle unrechtsrelevanten Merkmale viel schwächer ausgeprägt sind, wäre in einer Talkshow und bei ähnlichen Anlässen eine riskante Äußerung: Zu erwarten wäre der Vorwurf, dass Kindesmissbrauch verharmlost und pädophile Handlungen (erneut) bagatellisiert würden. Auch an dieser Stelle besteht ein scharfer Kontrast zwischen einer juristisch-sachverständigen Bewertung von Unrecht und der Laienperspektive. Für die juristische Bewertung gilt ein Differenzierungs*gebot*: Strafgerichte müssen in vergleichender Weise Unterschiede des Tatunrechts genau erfassen, ohne damit die Täterperspektive einzunehmen oder gar leichtere Fälle zu entschuldigen. Manche Nicht-Juristen, vor allem aus Betroffenenverbänden, neigen dagegen in die Richtung eines Differenzierungs*verbots*.

3. Anforderungen an die Tatbestandsüberschriften

Eine Herausforderung für die Rechtsgestaltung liegt darin, die richtigen Begriffe auszuwählen, um das verbotene Verhalten präzise zu beschreiben. Dazu gehören auch die Überschriften für die Tatbestände im StGB, die den Delikten Namen geben. Diese Namen haben wie die Strafrahmen expressive Funktionen und sollten deshalb das jeweilige Unrecht treffend charakterisieren. Auch bei der Vergabe von Überschriften ist auf die Systematik des StGB und auf Konsistenz zu achten. „Sexualdelikte" ist ein Sammelbegriff für Deliktsuntergruppen. Sexuelle Selbstbestimmung kann auf sehr unterschiedliche Weise angegriffen werden,[14] und verwandte Angriffstypen sind in Gruppen zusammenzufassen,[15] wobei im unübersichtlichen 13. Abschnitt des StGB strukturverwandte Tatbestände nicht immer in unmittelbarer Nähe zueinander stehen.[16] Das Verständnis für im Unrecht vergleichbare Tatbestandscluster trägt dazu bei, dem Gesamtsystem mehr Rationalität zu verleihen. Umgekehrt steigert es Inkonsistenz, wenn bei der Neugestaltung von Überschriften und Strafrahmen sachlich verwandte Tatbestände nicht gesehen werden – auch hier liegt ein Manko des vorliegenden Reformvorhabens, das § 176 StGB mit „sexualisierte Gewalt" betiteln will (siehe unten III. 2.).

III. Bewertung des Reformpakets

1. Vorschläge für die Strafrahmen in den §§ 176, 176a StGB

a) Erhöhung der Obergrenze in § 176 Abs. 1 StGB

Das Reformpaket sieht vor, beim Grundtatbestand des einfachen sexuellen Missbrauchs (§ 176 StGB) die Obergrenze von bisher zehn Jahren auf 15 Jahre hochzusetzen. Für den Qualifikationstatbestand des schweren sexuellen Missbrauchs (§ 176a StGB) liegt die Höchststrafe bereits bei 15 Jahren. Die Testfrage zur Überprüfung der Notwendigkeit dieser Änderung ist, ob die schwersten vorstellbaren Sachverhalte des einfachen sexuellen Missbrauchs nach geltendem Recht nicht angemessen bestraft werden können. Da § 176a StGB eine Vielzahl an erschwerenden Umständen anführt (u.a. vorbestrafte Täter; Eindringen in den Körper – dazu gehört auch Oralverkehr[17] –; die Gefahr einer schweren Gesundheitsschädigung oder einer erheblichen Schädigung der körperlichen oder seelischen Entwicklung; Absicht der Produk-

[14] Dazu *Sick/Renzikowski*, in: Hoyer/Müller/Pawlik/Wolter (Hrsg.), Festschrift für Friedrich-Christian Schroeder zum 70. Geburtstag, 2006, S. 603 (607 ff.); *Hörnle*, ZStW 127 (2015), 851 (860 ff.); *Green*, Criminalizing Sex. A Unified Liberal Theory, 2020.

[15] Siehe dazu auch *Renzikowski* (Fn. 4), Vor § 174 Rn. 12 ff.; *Hörnle*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 6, 12. Aufl. 2010, Vor § 174 Rn. 50 ff.; *Laubenthal*, Handbuch Sexualstraftaten, 2012, S. 55 ff.

[16] Siehe zu einem Vorschlag, wie die unsystematisch über diesen Abschnitt verstreuten Normen sinnvoll neugeordnet werden könnten, *Laubenthal*, in: Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 1144 ff.

[17] BGHSt 45, 131.

tion von Kinderpornographie), werden öffentlich diskutierte, Abscheu erregende Tatserien in der Regel von § 176a StGB erfasst. Was bleibt an schwersten Sachverhalten, die nur unter § 176 Abs. 1 StGB fallen? Zu denken wäre an Tatserien, in denen ein Familienangehöriger oder eine andere Person aus dem sozialen Nahraum Kinder über Jahre hinweg durch sexuelle Berührungen unterhalb der Schwelle des § 176a Abs. 2 Nr. 1 StGB (keine Penetration) drangsaliert hat. Allerdings besteht unter solchen Umständen meist die Gefahr einer erheblichen Schädigung der seelischen Entwicklung, sodass § 176a StGB Abs. 2 Nr. 3 anwendbar ist. Wenn man sich vergegenwärtigt, dass alle Tatumstände, die eine massive Verletzung oder Gefährdung von Opfern bedeuten, unter § 176a StGB fallen, wird klar, dass für die schwersten vorstellbaren Fälle eines einfachen sexuellen Missbrauchs die Obergrenze von zehn Jahren ausreichend ist. Besonders hohe Freiheitsstrafen aus dem Strafrahmensegment zwischen zehn und 15 Jahren sollten Fällen vorbehalten bleiben, in denen kumulativ und ausgeprägt mehrere unrechtserschwerende Gründe vorlagen, wie sie in § 176a StGB angeführt werden.

b) Höhere Mindeststrafe für Handlungen nach § 176 Abs. 1 StGB

Für den Grundtatbestand des einfachen sexuellen Missbrauchs greift die Justizministerin (SPD) einen Vorschlag auf, der in den letzten Jahrzehnten mehrfach aus den Reihen der CDU/CSU kam:[18] Die Mindeststrafe soll bei Delikten mit Körperkontakt (§ 176 Abs. 1 StGB) ein Jahr Freiheitsstrafe betragen. Welche Argumente könnten dafür angeführt werden? Nicht passend ist es, auf die Tatserien in Münster und Lügde zu verweisen: Diese Täter (und Teilnehmer) sind wegen schweren sexuellen Missbrauchs (§ 176a StGB) aus Strafrahmen mit sehr viel höheren Mindeststrafen zu verurteilen. In der politischen Diskussion schlägt sich die oben skizzierte Sichtweise von Nicht-Juristen nieder, die den Unterschied zwischen dem Grundtatbestand und dem Qualifikationstatbestand nicht kennen und unterschiedliche Sachverhalte zu einem unscharfen Bild von „sexueller Gewalt gegen Kinder“ verschmelzen. Eine rational begründete Erhöhung des gesetzlichen Mindestmaßes würde voraussetzen, dass auch die leichtesten möglichen Fälle ein Unrechtsausmaß erreichen, das nur mit einem Jahr Freiheitsstrafe angemessen geahndet werden könnte.

Wie sehen die leichtesten möglichen Fälle eines einfachen sexuellen Missbrauchs aus? Es gibt vor allem zwei Gruppen von Sachverhalten, die im Gesamtspektrum des Tatunrechts unten angesiedelt sind. Zum einen sind dies Konstellationen, in denen die Altersgrenze von 14 Jahren im Einzelfall nicht gut passt, zum anderen Berührungen, die die Grenze zur sexuellen Handlung nur knapp überschreiten. Die starre Altersgrenze, d.h. das absolute Verbot von sexuellen Handlungen (darunter fällt nach der Rechtsprechung auch ein Zungenkuss[19]), hat den Vorteil der Rechtssicherheit. Sie passt in der Lebensrealität aber nicht immer. Erfahrungen mit Küssen hat heute die Mehrheit der 14-Jährigen bereits gemacht und auch weitergehende Körperkontakte kommen in diesem Alter vor.[20] Aus normativer Sicht ist die entscheidende Frage, ob 12- und 13-Jährige in ausreichendem Maß urteilsfähig sind, um über erste Intimkontakte zu entscheiden. Dies ist möglich: Im Einzelnen kommt es auf die konkrete Art der Interaktion und die fehlende Überlegenheit des Partners/der Partnerin an, insbesondere auch den Altersunterschied. Nach geltendem deutschen Recht gibt es jedoch keinen Anknüpfungspunkt,[21] um bei 12- und 13-Jährigen die Strafbarkeit von geringfügig älteren Partnern zu verneinen. Die Reformkommission Sexualstrafrecht empfiehlt eine strafbarkeitsausschließende Regelung, wenn der Altersunterschied gering ist.[22] Erfreulicherweise wird dieser Punkt im Reformpaket des BMJV aufgegriffen. Allerdings wird es auch dann Grenzfälle geben, wenn eine Ausnahmeklausel eingeführt wird.

In anderen Konstellationen kann die Art der sexuellen Handlung den Einwand begründen, dass ein Jahr Freiheitsstrafe in Relation zu anderen Taten zu streng wäre, etwa wenn es sich um eine einmalige Berührung über der Kleidung handelte, welche die Grenze zur Erheblichkeit (§ 184h Nr. 1 StGB) nur knapp überschreitet. Für solche Fälle bedarf es flexibler Strafrahmen, damit Tatgerichte nach Aufklärung der Umstände des Einzelfalls die passende Strafe festsetzen können. Zu betonen ist nochmals, dass die Erwähnung solcher Sachverhalte nicht bedeutet, andere Fälle zu verharmlosen – rationale Rechtsgestaltung muss differenzieren.

c) Die Strafrahmen für Handlungen ohne Körperkontakt

Ein offensichtlich problematischer Teil des Reformpakets schlägt vor, Taten nach § 176 Abs. 5 StGB (Anbieten oder Nachweisen eines Kindes) statt wie bisher mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren mit Freiheitsstrafe von einem Jahr bis zu 15 Jahren zu bestrafen. Die erstaunlich schlichte Begründung lautet lediglich: „Denn eine solche Tat ist besonders verwerflich. Vor diesem Hintergrund erscheint es sachgerecht, denselben Strafrahmen vorzusehen wie für die sexualisierte Gewalt selbst.“ Das basiert nicht auf einer ernsthaften Auseinandersetzung mit dem Tatunrecht. Es besteht ein erheblicher Unterschied zwischen Handlungen, die sexuelle Selbstbestimmung verletzen, und Handlungen, die allenfalls (wenn überhaupt) Vorbereitung für eine spätere Tat sind. Schon bei der Einführung von § 176 Abs. 5 StGB im Jahr 2003 wurde Kritik laut.[23] Verurteilungen nach dieser Norm können nicht durchgängig damit begründet werden, dass Kinder gefährdet wurden: § 176 Abs. 5 StGB wird selbst

[18] BT-Drs. 13/8587, S. 58; BT-Drs. 14/6709, S. 3; BT-Drs. 15/29, S. 5.

[19] BGHSt 56, 223.

[20] Bundeszentrale für gesundheitliche Aufklärung, Jugendsexualität. Die Perspektive der 14–25-Jährigen, 2015, S. 97 ff.

[21] Die Strafgesetze in Österreich und in der Schweiz sind einen Schritt weiter: Sie schließen bei geringem Altersunterschied die Strafbarkeit aus (§ 207 Abs. 4 öStGB; Art. 187 Abs. 2 schwStGB).

[22] Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 316.

[23] Eingeführt mit dem SexualÄndG vom 27.12.2003, BGBl. I 2003, S. 3007; krit. *Duttge/Hörnle/Renzikowski*, NJW 2004, 1065 (1068); *Wolters*, in: Wolter (Fn. 7), § 176 Rn. 47.

dann angewendet, wenn der Beschuldigte nur geprahlt oder Phantasien entwickelt hat, also sein Anbieten oder Versprechen nicht ernst meinte.[24] Hierin liegt keine Gefährdung eines konkreten Kindes und keine Vorbereitung späteren Missbrauchs. Selbst bei einer Reduktion auf ernst gemeinte Angebote, Versprechen oder Verabredungen wäre es für die Strafzumessung nicht vertretbar, den erheblichen Unterschied zwischen der tatsächlichen Begehung einer Tat und den ersten Schritten zur Vorbereitung einer solchen einzuebnen, wie es das Reformpaket anstrebt. Auch § 30 StGB sieht bei Kommunikation über ein schweres Verbrechen, z.B. einen Mord, eine deutliche Rahmenmilderung (§ 49 Abs. 1 StGB) vor. Ein Strafrahmen für das Reden über Kindesmissbrauch, der höher ausfällt als für gefährliche Körperverletzung (§ 224 StGB) oder reales Quälen von Schutzbefohlenen (§ 225 StGB), wäre deutlich zu hoch angesiedelt.

Nicht gut durchdacht ist schließlich die vorgeschlagene Ausweitung der Versuchsstrafbarkeit für Fälle, wenn Täter pornographische Inhalte zeigen (§ 176 Abs. 4 Nr. 4 StGB) und irrtümlich meinen, dies gegenüber einem Kind zu tun, während sie tatsächlich mit einem Erwachsenen kommunizieren. Beim sog. Cybergrooming (§ 176 Abs. 4 Nr. 3 StGB) wurden im März 2020 derartige untaugliche Versuche der Kontaktaufnahme mit einem Kind unter Strafe gestellt,[25] siehe § 176 Abs. 6 S. 2 StGB. Die Verfasser des Reformpakets gehen davon aus, dass es sich um vergleichbare Konstellationen handle, mit der Formulierung: „Denn auch diese Fälle sind strafwürdig." Damit wird jedoch ein wesentlicher Unterschied zwischen dem nicht zweckgebundenen Vorzeigen von Pornographie nach § 176 Abs. 4 Nr. 4 StGB und dem zielgerichteten Einwirken gemäß § 176 Abs. 4 Nr. 3 StGB verkannt. Das Verbot, Kindern pornographische Inhalte zu zeigen, ist anders begründet als das Verbot des Cybergrooming.[26] Die Ratio ist nicht, späteren sexuellen Missbrauch zu verhindern, sondern es geht um Jugendschutzanliegen, die auch mit § 184 StGB verfolgt werden: Kinder sollen davor bewahrt werden, durch explizite Bilder sexueller Handlungen verstört, verunsichert oder fehlinformiert zu werden.[27] Cybergrooming ist die gefährlichere Variante. Bei den nunmehr strafbaren Versuchen nach § 176 Abs. 6 S. 2 StGB ist zwar die Einzelhandlung ungefährlich, aber die Ermittlungen durch Polizeibeamte, die sich als Kinder ausgeben, können gerechtfertigt werden, weil die Täter gefährliche Folgetaten vorbereiten.[28] Dieser Bezug zu zukünftigen Sexualdelikten fehlt bei Taten nach § 176 Abs. 4 Nr. 4 StGB. Dass die Begründung des Reformvorhabens trotzdem von „vergleichbaren Regelungen" ausgeht, zeigt eine eigentümliche Fokussierung auf moralische Bewertungen.

d) Entfallen des minder schweren Falls in § 176a Abs. 4 StGB

Das Reformpaket schlägt außerdem vor, bei den Delikten des schweren sexuellen Missbrauchs die Strafzumessungsnorm in § 176a Abs. 4 StGB zu streichen, die für minder schwere Taten nach § 176a Abs. 1 und Abs. 2 eine niedrigere Mindeststrafe zulässt. Eliminiert würde damit immerhin eine Unstimmigkeit bei vorbestraften Tätern: Wenn (z.B. bei einer die Erheblichkeitsschwelle nur knapp überschreitenden sexuellen Handlung) ein minder schwerer Fall zugestanden wird, gilt für einen vorbestraften Täter (§ 176a Abs. 1 StGB) ein niedrigerer Strafrahmen (beginnend bei drei Monaten Freiheitsstrafe) als für einen nicht vorbestraften Täter (Mindeststrafe sechs Monate Freiheitsstrafe, da es in § 176 StGB schon nach geltendem Recht keinen minder schweren Fall mehr gibt).[29] Im Übrigen ist jedoch ähnliche Kritik vorzubringen wie an der geplanten Heraufsetzung der Mindeststrafe in § 176 Abs. 1 StGB: Es fehlt das Verständnis für die Heterogenität der Fälle und für Grenzfälle, in denen, vor allem bei einvernehmlichen Handlungen nach § 176a Abs. 2 Nr. 1 StGB von 13-Jährigen mit unwesentlich älteren Partnern, eine nicht zur Bewährung aussetzbare Freiheitsstrafe zu hoch wäre.

2. „Sexualisierte Gewalt" statt „sexuellem Missbrauch"

Der Vorschlag, statt von „sexuellem Missbrauch" von „sexualisierter Gewalt" zu sprechen, greift ein verschiedentlich vertretenes Anliegen auf.[30] Die kurzen Ausführungen im Reformpaket des BMJV übernehmen die Einschätzung, dass das Wort „Missbrauch" impliziere, es gebe auch einen lega-

[24] BT-Drs. 15/380, S. 18; BGH NStZ 2013, 224: Erforderlich ist nur, dass das Angebot für die anderen Kommunikationsteilnehmer als ernst gemeint erscheinen kann und der Täter insoweit bedingten Vorsatz hatte. Für eine engere Auslegung *Bezjak*, Grundlagen und Probleme des Straftatbestandes des sexuellen Missbrauchs von Kindern gemäß § 176 StGB, 2015, S. 292 ff.; *Wolters* (Fn. 23), § 176 Rn. 47.

[25] 57. StrÄndG v. 3.3.2020, BGBl. I 2020, S. 431.

[26] § 176 Abs. 4 Nr. 4 StGB beschreibt zwar ebenfalls, wie Nr. 3, die Tathandlung mit dem Verb „einwirken". Das Einwirken beim Cybergrooming muss jedoch zielgerichtet auf weitere, nachfolgende Ereignisse (sexuelle Handlungen) ausgerichtet sein, während dasselbe Verb beim Pornographieverbot nur die Funktion hat, Fälle auszuschließen, in denen das Kind lediglich einen flüchtigen Eindruck vom pornographischen Inhalt erhalten hat, siehe BGH NStZ 1991, 485; *Hörnle* (Fn. 15), § 176 Rn. 99.

[27] Siehe zu der Diskussion, inwieweit bei Jugendlichen solche Anliegen kritikwürdiger Paternalismus sind, *Lenz*, Die Jugendschutztatbestände im Sexualstrafrecht, 2017, S. 300 ff. Bei Kindern liegt aber eine andere Beurteilung nahe.

[28] Dies ist bereits umstritten; siehe für Kritik an der Einführung der Versuchsstrafbarkeit *A. Schneider*, KriPoZ 2020, 137.

[29] Dazu *Hörnle* (Fn. 15), § 176a Rn. 18.

[30] Siehe z.B. den Sprachgebrauch im Familienministerium: BMFSFJ (online), Kinder und Jugendschutz. Gesamtkonzept gegen sexualisierte Gewalt, Hintergrundmeldung v. 9.8.2018, abrufbar unter https://www.bmfsfj.de/bmfsfj/themen/kinder-und-jugend/kinder-und-jugendschutz/schutz-vor-sexualisierter-gewalt/gesamtkonzept/gesamtkonzept-gegen-sexualisierte-gewalt/127336 (7.9.2020).

len „sexuellen Gebrauch“ von Kindern.[31] Dabei wird zum einen nicht gewürdigt, dass das Wort „Missbrauch“ bereits auf der alltagssprachlichen Ebene eine komplexere Begriffsgeschichte hat[32] und dass auch im heutigen Sprachgebrauch zwei Bedeutungen voneinander unterschieden werden, nämlich „in unerlaubter Weise benutzen/gebrauchen“ und „sich vergehen“.[33] Zum anderen ist im strafrechtlichen Kontext die Bezeichnung „sexueller Missbrauch“ als die Zusammenfassung einer etwas längeren Aussage zu verstehen. Die vollständige Aussage ist: Missbraucht wird ein Abhängigkeitsverhältnis, um Sexualkontakte zu ermöglichen. Hier liegt der Kern aller Missbrauchsdelikte, von denen es mehrere im 13. Abschnitt des StGB gibt. In den §§ 174, 174a bis 174c StGB wird eine Reihe von Abhängigkeitsverhältnissen beschrieben. Ausnutzung von Abhängigkeit findet nicht nur bei Kindern statt, sondern u.a. auch bei Personen, die als Strafgefangene vom Vollzugspersonal abhängig sind (§ 174a Abs. 1 StGB), als Beschuldigte von Polizeibeamten verhört werden (§ 174b StGB) oder als Psychotherapiepatienten in einem besonderen Verhältnis zu Therapeuten stehen (§ 174c Abs. 2 StGB). Die Überschriften für alle diese Tatbestände lauten „sexueller Missbrauch“. Der Reformvorschlag geht nicht darauf ein, ob sämtliche Delikte dieses Typus nunmehr als „sexualisierte Gewalt“ bezeichnet werden sollen. Dies läge nahe, da die Logik der Begründung nicht exklusiv auf Kinder zugeschnitten ist: Auch bei Strafgefangenen und Patienten gibt es keinen legalen „sexuellen Gebrauch“ in der Haft- oder Krankenanstalt. Von einer extensiven Verwendung des Begriffs „Gewalt“ ist aber abzuraten.

Ein Sexualstrafrecht, das unterschiedliche Varianten der Missachtung sexueller Selbstbestimmung erfassen soll, benötigt Deliktsnamen, die unterschiedliche Angriffsformen erfassen. Sexuelle Übergriffe (nachdem Personen ihren entgegenstehenden Willen ausgedrückt haben bzw. unfähig waren, dies zu tun, § 177 Abs. 1, 2 StGB) sind von den erschwerten Formen einer Nötigung oder Gewaltanwendung (§ 177 Abs. 5 StGB) und von der Ausnutzung von Abhängigkeit zu unterscheiden. Missbrauch von Abhängigkeitsverhältnissen tangiert in anderer Weise sexuelle Selbstbestimmung. Unter solchen Umständen kommt es nicht darauf an, ob die Opfer zustimmen (oder sogar den Sexualkontakt initiieren)[34], da eine solche Zustimmung wegen des bestehenden Abhängigkeitsverhältnisses nicht als Ausdruck von Selbstbestimmung gilt. Wenn jedwede Form der Verletzung sexueller Selbstbestimmung gleichermaßen als „sexualisierte Gewalt“ bezeichnet wird, geht das Vokabular verloren, das wir brauchen, um das Unrecht konkreter Taten genau zu bestimmen. Es ist Unrecht, die Abhängigkeit von Kindern auszunutzen, indem man sie zu sexuellen Handlungen überredet. Noch größer ist aber das Unrecht, wenn das Vertrauen von Kindern und ihre Schutzlosigkeit zu körperlicher Gewalt *und* sexuellen Handlungen ausgenutzt werden, etwa wenn Täter Kinder festhalten oder betäuben. Auch an dieser Stelle führt das Differenzierungsverbot in die Irre, von dem viele Nicht-Juristen ausgehen, weil sie eine abgestufte Bewertung von Unrecht als Verharmlosung und fehlende Anerkennung des Leidens der Opfer interpretieren und Begriffe wie „sexualisierte Gewalt“ bevorzugen, die Unrechtsunterschiede verschleifen. Das BMJV wirbt für eine solche Verschleifung kurioserweise mit den Worten: „Wir wollen künftig klare Begriffe verwenden“.

Zu erwägen wäre allenfalls, ob es einen Ersatz für den Begriff „Missbrauch“ geben könne, der nicht zu einer Verschleifung mit tatsächlich gewaltsamem Vorgehen führt, sondern ohne Begriffsextension lediglich eine andere Bezeichnung einführen würde. Auch wenn die Aversion gegen das Wort „Missbrauch“ bei einem nüchternen Blick auf Begriffsgeschichte und strafrechtliche Funktion nicht begründet ist, könnte das Anliegen einer höheren Normakzeptanz für eine Begriffsauswechslung sprechen. Eine solche müsste jedoch alle Missbrauchsdelikte einschließen, nicht nur die §§ 176, 176a StGB. Die Herausforderung wäre, einen Begriff zu finden, der einerseits die relevanten Hintergründe der Missachtung sexueller Selbstbestimmung skizziert, andererseits knapp genug ist, um als Schlagwort in Kommunikationen (über Normen, für die Zwecke der Strafverfolgung etc.) zu funktionieren. Zu erwägen wäre vielleicht „Sexuelle Handlungen mit … (Schutzbefohlenen, Kindern, Gefangenen etc.)“ – aber dies bedürfte einer ausführlicheren Diskussion als hier möglich. „Sexualisierte Gewalt“ ist jedenfalls nicht der richtige Ansatz.

3. Vorschläge für die Strafrahmen in § 184b StGB

Das Reformpaket beinhaltet mehrere Verschärfungen bei den Strafen für Kinderpornographie (§ 184b StGB). Für diesen Tatbestand wird keine Änderung der Überschrift vorgeschlagen, obwohl dies bei § 184b StGB näher läge als bei § 176 StGB.[35] In der internationalen Diskussion wird gefordert,

[31] Siehe *Fischer* (Fn. 7), Vor § 174 Rn. 8.

[32] Das Deutsche Wörterbuch von Jakob und Wilhelm Grimm (dtv-Ausgabe, Band 12, S. 2279) unterscheidet mehrere Formen des „miszbrauchens“; davon ist für unser Thema die Variante „umhüllend für schänden“ relevanter als die Variante „verkehrten Gebrauch von etwas machen“.

[33] Duden, Synonymwörterbuch, 5. Aufl. 2010, Missbrauch.

[34] Siehe dazu die Berichte über ein Strafverfahren vor dem LG Erfurt im Juli 2020 gegen zwei Polizeibeamte, das mit einer Verurteilung wegen sexuellen Missbrauchs unter Ausnutzung einer Amtsstellung und Vorteilsannahme endete, so z.B. in der FAZ v. 13.7.2020, abrufbar unter https://www.faz.net/aktuell/gesellschaft/kriminalitaet/thueringen-zwei-polizisten-wegen-sexuellen-missbrauchs-verurteilt-16859629.html (7.9.2020).

[35] Über die passenden Begriffe hat eine Interagency Working Group mit Mitgliedern aus den Vereinten Nationen, der EU und NGOs beraten und 2016 „Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse“ veröffentlicht, abrufbar unter https://www.unicef.org/protection/files/Terminology_guidelines_396922-E.pdf (7.9.2020). Zu „child sexual abuse“ wird dort auf S. 18 festgestellt: „This term appears to have a generally agreed meaning and/or can be used without stigmatising and/or otherwise harming the child.“ Von der Verwendung des Begriffs „child pornography“ wird dagegen abgeraten, a.a.O., S. 40.

statt „child pornography“ die Bezeichnungen „child sexual abuse images“ oder „child sexual abuse material“ zu verwenden.[36] Neuere EU-Dokumente enthalten den Begriff der child pornography bereits nicht mehr.[37] Der Begriff „Kinderpornographie“ ordnet die entsprechenden Inhalte als Unterkategorie von Pornographie ein und lässt dabei einen fundamentalen Unterschied außer Acht. Pornographie herzustellen und zu vertreiben ist nicht per se illegal: Es wird lediglich mit § 184 StGB die Art und Weise des Vertriebs reguliert, weil der Konsum auf Erwachsene beschränkt werden soll. Abbildungen des sexuellen Missbrauchs von Kindern sind dagegen absolut verboten, sie sind deshalb nicht nur eine Unterkategorie mit spezielleren pornographischen Inhalten, wie z.B. „gay pornography“. Allerdings zeigt sich auch beim Nachdenken über die passendste Überschrift für § 184b StGB, dass es vor allem in der deutschen Sprache nicht einfach ist, eine gelungene Balance von sachlicher Präzision einerseits, Prägnanz und Kürze andererseits zu finden. Die Tatobjekte korrekt als „Abbildungen des sexuellen Missbrauchs von Kindern“ zu beschreiben, würde zu umständlichen Verbotsnormen führen.

Das Reformpaket konzentriert sich auf die Erhöhung von Strafrahmen. Sowohl für das Verbreiten von kinderpornographischem Material als auch für Besitz- und Besitzverschaffungsdelikte sollen die Mindest- und Höchststrafen deutlich erhöht werden: jeweils auf ein Jahr die Mindeststrafe, die Höchststrafe auf fünf Jahre (Besitz, Besitzverschaffung) bzw. zehn Jahre (Verbreiten). Bei gewerbsmäßigem Handeln oder Handeln als Mitglied einer Bande (§ 184b Abs. 2 StGB) sollen die Strafen ebenfalls angehoben werden, nämlich auf zwei bis 15 Jahre. Die Begründung für diese Vorschläge fällt wieder kurz und vage aus: „Denn hinter Kinderpornographie steht in der Regel sexualisierte Gewalt gegen Kinder.“

Auch an dieser Stelle müsste tiefer angesetzt werden. § 184b StGB stellt eine Vielzahl unterschiedlicher Handlungen unter Strafe, und eine unrechtsangemessene Staffelung der Strafrahmen setzt zwingend voraus, die Ratio dieser Normen zu verstehen. In der öffentlichen Diskussion sind Abscheu und moralische Verurteilung so ausgeprägt, dass Kindesmissbrauch und der Umgang mit den Abbildungen solcher Taten kurzerhand gleichgesetzt werden. Strafrechtliche Unrechtsurteile erfordern aber eine präzisere Analyse der Verantwortungsstrukturen. Ausgangspunkt muss sein, dass in dem Moment, in dem jemand Dateien hoch- oder herunterlädt, der in den gespeicherten Bildern gezeigte sexuelle Missbrauch *in der Vergangenheit* liegt.[38] Es ist ausgeschlossen, Personen in der Vergangenheit liegende Ereignisse zuzuschreiben, an denen sie nicht beteiligt waren. Der Umgang mit Missbrauchsbildern kann aber wegen der *Gefahr zukünftigen sexuellen Missbrauchs* verboten werden. Teilnehmer an einem illegalen Markt tragen kollektiv Verantwortung dafür, dass die geschaffenen Austauschstrukturen weitere Nachfrage schaffen und damit den erneuten sexuellen Missbrauch von Kindern fördern.[39] Ein weiterer Grund für Verbote liegt darin, dass die sich über Jahre erstreckende Zirkulation von Missbrauchsbildern die Persönlichkeitsrechte[40] und die Menschenwürde[41] der betroffenen Kinder verletzt. Eine Feinabstufung des Unrechts hängt daran, wie intensiv die in den §§ 184b, 184d StGB beschriebenen Handlungen jeweils das Austauschgeschehen am Laufen halten. Das Verbreiten[42] und das vielen anderen Personen Zugänglichmachen bedeuten typischerweise eine intensivere Form der Marktteilnahme als das Herunterladen für den eigenen Besitz oder das Ansehen (§ 184d Abs. 2 StGB). Natürlich gibt es Täter, die sehr große Mengen an Dateien angehäuft haben und intensiv als Nachfragende aktiv waren, was bei der Strafzumessung zu berücksichtigen ist. Unter dem Aspekt „Gefahren durch Marktgeschehen“ kommt es jedoch auch auf die Erweiterung des Kreises der Marktteilnehmer an. Insbesondere tragen diejenigen ein gesteigertes Maß an Verantwortung, die im Netz Plattformen zum Austausch von Fotos und Filmen organisieren und betreiben (§ 184d Abs. 1 i.V.m. § 184b Abs. 1 Nr. 2 StGB). Es beruht auf einer konsistenten Bewertung von Unrecht, dass das geltende Recht das Verbreiten und das Zugänglichmachen mit etwas höheren Strafen bedroht als Besitzdelikte. Der Vorschlag im Reformpaket, für den Besit-

[36] Siehe z.B. die Kampagne der Internet Watch Foundation gegen den Begriff „child pornography“, IWF, There’s #NoSuchThing as child pornography, It’s child sexual abuse, abrufbar unter https://www.iwf.org.uk/nosuchthing (7.9.2020); ebenso den folgenden Beschluss des Europäischen Parlaments von 2015: European Parliament resolution of 11 March 2015 on child sexual abuse online (2015/2564(RSP)), abrufbar unter https://www.europarl.europa.eu/doceo/document/TA-8-2015-0070_EN.html (7.9.2020); außerdem die nachfolgende Fn.

[37] Siehe das Dokument der Kommission „EU Strategy for a More Effective Fight against Child Sexual Abuse“ v. 24.7.2020, KOM (2020) 607 endg.

[38] Wenn Personen live, etwa mittels einer Webkamera, beim Missbrauchsgeschehen dabei sind, werden sie wegen Teilnahme am sexuellen Missbrauch oder nach § 184d Abs. 2 StGB bestraft.

[39] Siehe dazu BT-Drs. 12/3001, S. 5; *Ost*, Child Pornography and Sexual Grooming, 2009, S. 113 ff.; *Harms*, NStZ 2003, 646; *Hörnle*, in: Hoyer/Müller/Pawlik/Wolter (Fn. 14), S. 477; *Krause*, ZRP 2019, 69 (70); *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 184b Rn. 2; *Hörnle*, in: Erb/Schäfer (Fn. 4), § 184b Rn. 1. Kritisch *Wolters/Greco*, in: Wolter (Fn. 7), § 184b Rn. 2.

[40] *Greco*, RW 2011, 275 (298 ff.); *Gropp*, in: Esser/Günther/Jäger/Mylonopoulos/Öztürk (Hrsg.), Festschrift für Hans-Heiner Kühne zum 70. Geburtstag, 2013, S. 679 (690 f.); *Wolters/Greco* (Fn. 39), § 184b Rn. 2; *Eisele* (Fn. 39), § 184b Rn. 2; *Hörnle* (Fn. 39 – Erb/Schäfer), § 184b Rn. 4.

[41] *Hörnle* (Fn. 39 – Hoyer et al.), S. 494 f. A.A. *Renzikowski*, in: Fahl/Müller/Satzger/Swoboda (Hrsg.), Festschrift für Werner Beulke zum 70. Geburtstag, 2015, S. 521.

[42] Die Definition setzt voraus, dass die Schrift einem größeren Personenkreis zugänglich gemacht wird, BGH NStZ-RR 2015, 39 (40); *Eisele* (Fn. 39), § 184b Rn. 20; *Fischer* (Fn. 7), § 184b Rn. 15.

zer von Missbrauchsbildern dieselbe Mindeststrafe vorzusehen wie für den Verbreiter, überzeugt dagegen nicht.[43]

In zwei Punkten würde ich dem Änderungsvorhaben nicht widersprechen. Erstens ist immerhin insofern eine differenzierende Unrechtsbewertung erkennbar, als die Strafrahmenerhöhung nicht für fiktive Kinderpornographie gelten soll. Zweitens ist eine Anhebung der Höchststrafe für Anbieter (§ 184b Abs. 1 Nr. 1, Nr. 2 i.V.m. § 184d StGB) mit Blick auf die extremsten Formen solcher Aktivitäten sinnvoll. Die Qualifikation in § 184b Abs. 2 StGB beschränkt sich auf gewerbsmäßiges Handeln und auf das Handeln als Mitglied einer Bande, womit nicht alle hochaktiven „Superspreader“ von kinderpornographischem Material zu erfassen sind. Wer Plattformen organisiert und viele andere in das Austauschgeschehen involviert, aber damit keine Gewinnerzielungsabsicht verbindet (was für Gewerbsmäßigkeit erforderlich wäre[44]), und allein oder nur zu zweit agiert,[45] wird zwar von § 184b Abs. 1 Nr. 2 StGB, nicht aber von der Qualifikation in § 184b Abs. 2 StGB erfasst.[46] Nachzudenken wäre über eine Neufassung der Qualifikation (ersatzweise, wie vom BMJV vorgeschlagen, über eine höhere Obergrenze für Verbreiter).[47]

IV. Schwächen gegenwärtiger Kriminalpolitik

Die vom BMJV unterbreiteten Vorschläge zur Änderung des materiellen Strafrechts sind nicht überzeugend. Aus den Reihen der Strafrechtswissenschaft wird das Reformpaket wahrscheinlich als symbolische Kriminalpolitik kritisiert werden; dieses Deutungsmuster hat sich in den letzten Jahrzehnten etabliert.[48] Allerdings lohnt es sich, auf die Analysen *Winfried Hassemers* zurückzugreifen, der darauf hingewiesen hat, dass bis zu einem gewissen Grad jede Strafgesetzgebung symbolische Züge aufweist und dass es einer präziseren Erfassung der kritischen Punkte bedarf.[49] Mit den folgenden Punkten würde ich die Schwachstellen des aktuellen kriminalpolitischen Vorhabens zusammenfassen: Erstens werden expressive Funktionen in einer Weise überbetont, die zulasten einer gerechten Strafe im Einzelfall gehen kann; zweitens handelt es sich um ein Ausweichmanöver (was dann besonders problematisch wird, wenn nicht einmal mehr ernsthaft versucht wird, das eigentliche Problem anzugehen); drittens ist es bedenklich, dass ausgerechnet aus dem Bundesjustizministerium Vorschläge kommen, die durch Desinteresse am Gesamtsystem des StGB gekennzeichnet sind.

1. Expressive Funktionen zulasten von Strafmaßgerechtigkeit im Einzelfall

Expressive und in diesem Sinne symbolische Funktionen des Strafrechts verdienen nicht per se Kritik.[50] Die Bewertung ändert sich aber dann, wenn das grundsätzlich berechtigte Anliegen, die Schwere bestimmter Rechtsverletzungen zu betonen, mit einer einseitig-asymmetrischen Fokussierung auf die Delikte einhergeht, die als besonders schwere Fälle zum Gegenstand intensiver Berichterstattung geworden sind. Ein wesentlicher Einwand gegen die geplanten Strafrahmenänderungen ist, wie oben dargelegt, dass sie in den leichtesten möglichen Fällen für das dann verwirklichte Unrecht zu hoch sind. Die Gefahr einer zu hohen Mindeststrafe droht für Grenzfälle: wenn eine körperliche Berührung nur knapp die Schwelle zu einer sexuellen Handlung erreicht; bei substanzlosem Phantasieren über Kindesmissbrauch; beim einmaligen Betrachten des Fotos eines Kindes, das sexualisierte Posen einnimmt (§ 184d Abs. 2 S. 1 i.V.m. § 184b Abs. 1 Nr. 1 b, Abs. 3 StGB).

2. Ausweichmanöver

Wer in der Rechtspolitik ein zweckrationales Anliegen verfolgt, d.h. die Zahl zukünftiger Missbrauchsdelikte verringern und die Effektivität der Strafverfolgung steigern will, muss zum einen die Ermittlungspraxis verbessern und Ressourcen ausweiten, zum anderen ermöglichen, beim Fund von Missbrauchsbildern die Personen zu identifizieren, die diese Bilder ins Netz gestellt haben. Ersteres ist Sache der Landespolitik[51] und eignet sich deshalb nicht als Aktionsfeld für Rechts-

[43] Siehe außerdem zu sozial und psychologisch erfassbaren Unterschieden zwischen den beiden Tätergruppen, die sich auf Gefährlichkeitsurteile auswirken (die Verbreiter sind die problematischere Gruppe), *Clevenger/Navarro/Jasinski*, Sexual Abuse 28 (2016), 555.

[44] Siehe *Sternberg-Lieben/Bosch*, in: Schönke/Schröder (Fn. 39), Vor §§ 52 ff. Rn. 95 m.w.N.

[45] Siehe zur Rechtsprechung, die drei Personen für eine Bande verlangt, BGHSt. 46, 321; *Bosch*, in: Schönke/Schröder (Fn. 39), § 244 Rn. 24.

[46] Das Abstellen auf gewerbsmäßiges Handeln zeigt die Orientierung an der Qualifikation für Hehlerei (§ 260 StGB), womit aber verkannt wurde, dass nicht auf allen illegalen Märkten Anbieter mit Gewinnerzielungsabsicht handeln.

[47] Der Vorschlag, mit einem neuen Tatbestand (§ 126a StGB) die Anbieter illegaler Produkte und Dienstleistungen im Darknet zu erfassen (BR-Drs. 33/19; dazu *Zöller*, KriPoZ 2019, 274), wäre wegen des deutlich niedrigeren Strafrahmens ohne große Bedeutung für Kinderpornographiedelikte: Plattformbetreiber machen sich, da sie zwar nicht der Öffentlichkeit, aber doch einer anderen Person kinderpornographische Inhalte zugänglich machen, nach § 184d Abs. 1 S. 1 i.V.m. 184b Abs. 1 Nr. 2 StGB strafbar.

[48] Siehe statt vieler z.B. *Prittwitz*, Strafrecht und Risiko, Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft, 1993, S. 253 ff.; *Kunz*, in: Dölling/Götting/Meier/Verrel (Hrsg.), Verbrechen – Strafe – Resozialisierung, Festschrift für Heinz Schöch zum 70. Geburtstag am 20. August 2010, 2010, S. 353 (361 f.); *B. Heinrich*, KriPoZ 2017, 4 (8); *Kreuzer*, NK 2018, 141 (146); *Wrobel*, KriPoZ 2020, 77 (80). Kritisch zur breiten Verwendung des Begriffs *Peters*, JR 2020, 414.

[49] *Hassemer*, NStZ 1989, 553 (555 ff.); so auch *Peters*, JR 2020, 414 (419 f.), die dafür plädiert, auf den Begriff zu verzichten.

[50] *Hassemer*, NStZ 1989, 553 (556).

[51] Siehe z.B. Landesregierung Nordrhein-Westfalen, Pressemitteilung v. 18.6.2019, abrufbar unter https://www.land.nrw/de/pressemitteilung/reul-reformiert-struktur-der-kinderpornografie-ermittlungen (7.9.2020).

politik auf Bundesebene. Das Nachdenken über die rechtlichen Rahmenbedingungen für Ermittlungen im Cyberspace führt zu schwierigen und konfliktbeladenen Themen: Bestandsdatenauskunft, Vorratsdatenspeicherung und Verschlüsselung von Datenübertragung. Wenn Ermittlungen zu einer IP-Adresse geführt haben, müsste im nächsten Schritt diese IP-Adresse einer Person zugeordnet werden, was nur möglich ist, wenn vorsorglich Informationen gespeichert wurden. Das Bundeskriminalamt weist darauf hin, dass allein im Jahr 2019 2.100 (aus den USA stammende) Verdachtsmeldungen, die sich auf Kinderpornographie und IP-Adressen in Deutschland bezogen, nicht weiter bearbeitet werden konnten.[52] Zwar ist aus der Zahl 2.100 nicht auf eine ähnlich hohe Zahl von gegenwärtigem, fortgesetztem Missbrauch zu schließen – viel gemeldetes Material ist wahrscheinlich schon älteren Datums.[53] Es ist jedoch realistisch, davon auszugehen, dass einige laufende Tatserien unterbrochen werden könnten, wenn zu rekonstruieren wäre, wer Bilder sexuellen Missbrauchs ins Netz eingespeist hat.[54] Die Voraussetzungen dafür zu schaffen, ist aber kaum mehr möglich. Die bestehende Regelung zur Übermittlung vorhandener Bestandsdaten (§ 113 TKG) hat der *1. Senat* des BVerfG jüngst erneut als unvereinbar mit dem Grundgesetz eingestuft.[55] Vorratsdatenspeicherung scheitert, trotz existierender gesetzlicher Grundlage,[56] am Widerstand von Telekommunikationsunternehmen und Datenschutzaktivisten, und es ist ungewiss, wie sich der EuGH zum deutschen Recht verhalten wird.[57] Neue Kommunikationswege und die zunehmende Verschlüsselung von Messenger-Diensten verschlechtern die Ermittlungsmöglichkeiten[58] – in jedem Fall wird die Abhängigkeit der Strafverfolgungsbehörden vom guten Willen der großen, international aktiven Technologiekonzerne weiter zunehmen. Weil es sich um komplexe, auf nationaler Ebene kaum mehr lösbare Probleme handelt, liegt es für deutsche Politikerinnen und Politiker nahe, Handlungsbereitschaft dort zu demonstrieren, wo dies noch möglich und einfach ist: beim national geregelten materiellen Strafrecht. Auch wenn solche Ausweichmanöver menschlich verständlich sein mögen, sind sie kritisch zu sehen. Wer es ernst meint mit dem Schutz von Kindern, müsste sich ernsthaft für Kompromisse beim Datenschutz einsetzen (und sollte sich auch mit der Grundsatzfrage befassen, ob Datenschutz wirklich als eigenständiges Grundrecht zu konzipieren ist)[59].

3. Verlust der Brückenfunktion des Bundesjustizministeriums

Dass Politikerinnen und Politiker in öffentlichen Debatten Emotionen und Meinungen aus der Bevölkerung aufgreifen und deshalb starke moralische Bewertungen dominieren, ist nicht verwunderlich. Man muss dies nicht ausschließlich als eigennützige politische Strategie interpretieren. Expressive Funktionen haben auch eine zweckrational nachvollziehbare Bedeutung. Gesellschaftstheoretisch gesehen, kann es positiv gewertet werden, wenn sich in sozial und kulturell fragmentierten Gesellschaften noch Themen finden lassen, die Einigkeit stiften. Die Bedeutung von Kinderschutz und die Solidarisierung mit kindlichen Opfern sind in der heutigen Gesellschaft so fest verankert, dass ein energischer Kampf gegen Kindesmissbrauch und Kinderpornographie über politische Gräben und soziokulturelle Unterschiede hinweg auf Zustimmung stößt.

Gleichzeitig gibt es aber aus der Perspektive des Rechtssystems Anforderungen an Rechtspolitik, die in einem offensichtlichen Spannungsverhältnis zur Herangehensweise von Nicht-Juristen stehen. Für das Ausbalancieren der unterschiedlichen Perspektiven ist das Bundesjustizministerium mit seinem in den Abteilungen gebündelten Fachwissen von großer Bedeutung. Dort muss eine Brücke vom System Politik zum System Recht geschlagen werden. Beim vorliegenden Reformpaket ist dies nicht geschehen. Die Eigenlogik des Strafrechts, ein Bemühen um Kohärenz im StGB und die feinen Differenzierungskriterien der fachlichen Perspektive spielten ersichtlich keine Rolle. Es bleibt abzuwarten, ob sich ein breiterer Trend entwickelt, der auf eine noch stärker schwindende Bedeutung von Expertenwissen in der Kriminalpolitik zuläuft. Auch wenn dieses Reformpaket wegen der besonderen symbolischen Aufladung des Themas nicht repräsentativ sein mag, handelt es sich um einen besorgniserregenden Vorgang.

[52] Siehe dazu die Mitteilung des BKA auf seiner Homepage, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Kinderpornografie/Zahlen_und_Fakten/zahlen_und_fakten_node.html (7.9.2020).

[53] *Albrecht u.a.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, 2. Aufl. 2011, S. 95.

[54] *Albrecht u.a.* (Fn. 53), untersuchten den Einfluss von Vorratsdatenspeicherung auf Aufklärungsquoten. Die Studie verwendete aggregierte Daten über längere Zeiträume bis 2010, dabei ergaben sich keine quantitativ messbaren Effekte auf die Aufklärungsquote (a.a.O., S. 78 ff.), auch nicht für Kinderpornographiefälle, S. 97 ff. Allerdings ist eine makrostatistische Untersuchung nur bedingt aussagekräftig, da eine große Zahl anderer Faktoren die Entwicklung von Aufklärungsquoten im Laufe der Zeit beeinflusst. Aggregierte Daten sind letztlich auch nicht entscheidend, wenn man bei Tatserien mit sehr großem Unrecht ansetzt, deren Aufklärung wichtig ist, auch wenn sich die Gesamtaufklärungsquote nicht messbar verändert.

[55] BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II).

[56] Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 10.12.2015, BGBl. I 2015, S. 2218.

[57] Vorlage durch das BVerwG: Beschl. v. 25.9.2019 – 6 C 12.18, 6 C 13.18; dazu *Hammer/Müllmann*, K&R 2020, 103; zur Rspr. des EuGH *Ziebarth*, ZUM 2017, 398.

[58] Siehe zum Darknet *Krause*, NJW 2019, 678 (679 ff.), und zu den Folgen der Pläne von Facebook, die Verschlüsselung auszuweiten, den Direktor des FBI *Shortell* bei CNNPolitics v. 4.10.2019, abrufbar unter https://edition.cnn.com/2019/10/04/politics/fbi-facebook-child-encryption/index.html (7.9.2020).

[59] Dazu *Poscher*, in: R. Miller (Hrsg.), Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair, 2017, S. 129.

Nachruf auf Prof. Dr. Julio Maier

Von Prof. Dr. Dr. h.c. **Kai Ambos**, Göttingen/Den Haag*

Am 13.7.2020 ist der bedeutende argentinische Strafprozessrechtswissenschaftler Julio Maier verstorben. Ich habe Julio Maier anlässlich eines Forschungsprojekts zur lateinamerikanischen Strafprozessrechtsreform, das ich Ende der 1990er Jahre als zuständiger Referent des Max-Planck-Instituts für ausländisches und internationales Strafrecht[1] geleitet habe[2], persönlich kennengelernt. Wir haben Maier damals angefragt, weil er als der vielleicht größte lebende Experte auf dem Gebiet des lateinamerikanischen Strafprozesses galt und schon seit den 1960er Jahren sehr enge Beziehungen zu Deutschland hatte (insbesondere Bonn als Stipendiat der Humboldt-Stiftung [Armin Kaufmann], Frankfurt a.M. [Winfried Hassemer], Köln [Hans Joachim Hirsch, Hilde Kaufmann], München [Reinhart Maurach, Claus Roxin, Klaus Volk] und Münster [Eberhard Struensee, Friedrich Dencker]). Maier hat also mehrere Jahre in Deutschland gelebt und studiert und die deutsche Sprache sehr gut beherrscht. Er hat eine einflussreiche Übersetzung der deutschen Strafprozessordnung (StPO) vorgelegt,[3] die vielen spanischsprachigen Wissenschaftlern und Kollegen erst den Zugang zum deutschen Strafprozessrecht ermöglicht hat. Maier hat sich aber immer die kritische Distanz zum deutschen Strafprozessrecht bewahrt, was sich u.a. an seiner Kritik an zahlreichen Strukturmerkmalen und Regeln der StPO zeigt.[4] Besonders ist mir seine – zutreffende – Kritik in Erinnerung geblieben, dass der Richter/das Gericht des Hauptverfahrens zugleich über dessen Eröffnung im Zwischenverfahren entscheidet (§ 199 Abs. 1 StPO). Die lateinamerikanischen Reformentwürfe sind dem deutschen Recht in diesem Punkt bekanntlich nicht gefolgt, vielmehr ist meist explizit vorgesehen, dass in diesen unterschiedlichen Verfahrensstadien unterschiedliche Richter/Gerichte zuständig sein sollen.[5]

Auch die Bedeutung Maiers für die lateinamerikanische Strafverfahrensreform der 1990er Jahre kann kaum überschätzt werden. Sie ergibt sich schon daraus, dass diese Reform sich ursprünglich – an dem von Maier mitverfassten – Iberoamerikanischen Modellentwurf eines Strafprozessgesetzes[6] (der wiederum vom deutschen Verfahrensrecht inspiriert war) orientiert hat.[7] Aus dem späteren Oeuvre Maiers ist insbesondere seine dreibändige Abhandlung zum Strafprozessrecht hervorzuheben.[8] Die Strafprozessrechtsreform ist dann allerdings später bekanntlich weitgehend dem angloamerikanischen adversatorischen Strafverfahrensmodell gefolgt, hat sich also von der eher deutschfreundlichen Position Maiers abgewendet. Ironischerweise ist dies letztlich auch auf seinen Einfluss zurückzuführen, weil mit Alberto Binder einer seiner Schüler – neben der chilenischen Diego-Portales-Schule – einer der Hauptprotagonisten dieser Entwicklung war und sehr für eine

* Ich danke meinem Doktoranden *Sem Sandoval Reyes* (LL.M.) für die Unterstützung bei der Recherche und meinem Freund *Daniel Pastor* für wichtige persönliche Hinweise.

[1] Das Institut hat inzwischen eine andere Ausrichtung, wie auch der neue Name erkennen lässt: „Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht".

[2] Als Projektkoordinatoren wirkten auch Eberhard Struensee, ein guter Freund Maiers, und sein Schüler Daniel Pastor sowie Jan Woischnik mit.

[3] *Maier*, La Ordenanza Procesal Penal Alemana, Bd. 1, 1978 und Bd. 2, 1982. Eine weitere (ältere Übersetzung) stammt von *Gomez Colomer*, El proceso penal alemán, introducción y normas básicas, 1985.

[4] Siehe seine Diskussion mit Jürgen Baumann aufgrund Maiers Rezension seines Buchs: *Maier*, Doctrina Penal 3 (1980), Nr. 11, 745; Replik *Baumann*, Doctrina Penal 5 (1982), Nr. 17–20, 169; Duplik *Maier*, Doctrina Penal 5 (1982), Nr. 17–20, 363.

[5] Siehe etwa Art. 52 ff., 279 f., 281 ff. Bundesstrafprozessordnung Argentinien; Art. 260 ff., 281 ff. StPO Chile; Art. 323, 351–355, 371–374 StPO Perú; Art. 603, 604, 609–614 StPO Ecuador 2014; Art. 316 ff., 342 ff. StPO Costa Rica; Art. 341, 342, 347, 349 Bundes-StPO México. Eine ähnliche Regelung enthielt schon der Iberoamerikanische Modellentwurf (sogleich Fn. 6), siehe *Maier* (Fn. 3 – Bd. 2), S. 24–26 bezugnehmend auf Art. 267–277, 282 ff. Modellentwurf. Vgl. auch *Woischnik*, Untersuchungsrichter und Beschuldigtenrechte in Argentinien: eine kritische Würdigung des neuen Bundesstrafverfahrensrechts anhand der rechtsstaatlichen Vorgaben der Menschenrechtskonventionen, 2001, S. 96–115; in spanisch: *ders.*, Juez de instrucción y derechos humanos en Argentina, 2003, S. 121–140.

[6] Vgl. zur Entstehungsgeschichte Instituto Iberoamericano de Derecho Procesal (Hrsg.), Código Procesal Penal Modelo para Iberoamérica, Editorial Hammurabi S.R.L., 1989, S. 7 ff. Der Entwurf wurde 1988 von *Jaime Bernal Cuéllar*, *Fernando de la Rúa*, *Ada Pellegrinie Grinover* und *Julio B. J. Maier* vorgelegt.

[7] Vgl. *Langer*, Revolución en el proceso penal Latinoamericano: Difusión de ideas legales desde la periferia, Centro de Estudios de la Justicia de las Américas, S. 27–31, abrufbar unter https://inecip.org/wp-content/uploads/Langer-Revolucion-en-el-proceso-penal.pdf (29.8.2020); *Vargas Viancos*, Revista Latinoamericana de Seguridad Ciudadana Nr. 3 (Januar 2008), 33, abrufbar unter https://revistas.flacsoandes.edu.ec/urvio/article/view/33-47/1645 (29.8.2020); *Binder*, La reforma de la justicia penal en América Latina como política de largo plazo, in: Niño Guarnizo, (Hrsg.), La Reforma a la justicia en América Latina: las lecciones aprendidas, 2016, S. 67–77, abrufbar unter https://library.fes.de/pdf-files/bueros/la-seguridad/12574.pdf (29.8.2020).

[8] *Maier*, Derecho Procesal Penal, Bd. 1, 2. Aufl. 1996, Bd. 2, 2003, und Bd. 3, 2011. Die Erarbeitung des vierten Bands hat Maier Daniel Pastor, Gabriel Pérez Barberá und Eugenio Sarrabayrouse überantwortet, wobei er die finale Fassung redigieren wollte, wozu es aufgrund seines Todes aber nicht mehr gekommen ist. Nach Veröffentlichung des 3. Bands hat Maier keine größeren wissenschaftlichen Werke mehr veröffentlicht, aber Anekdoten, Gedichte und ein Musikbuch. Auch dies zeigt seine enorme Kreativität.

radikale Abwendung vom überkommenen schriftlichen Inquisitionsverfahren plädiert hat. Mit dieser radikalen Abwendung war aber ein reformiert-inquisitorisch (von manchen auch instruktorisch) genanntes Modell wie das deutsche unvereinbar.[9]

Maier hat sich nie in die Niederungen lateinamerikanischer Strafrechtspolitik begeben, sondern die Dinge eher von einer distanzierten, „höheren" akademischen Warte betrachtet. Natürlich war Maier eine wichtige Referenzperson der Reformbewegung. Es gab kaum eine Person mit seiner soliden Ausbildung und seinem Überblick über das weltweite strafprozessuale Geschehen. Er hat sich aber nie in den Vordergrund gedrängt, sondern musste, ganz anders als die „jungen Wilden" dieser Zeit, einige davon seine Schüler, doch sehr um Intervention gebeten werden. Wissenschaftliche Projekte hat Maier hingegen immer mit Verve und großer Solidarität unterstützt.

Das zu Beginn dieser kleinen Erinnerung erwähnte Forschungsprojekt hat übrigens zu einem im Jahre 2000 in Argentinien veröffentlichten Buch zu den Strafprozessrechtsreformen geführt,[10] das weite Verbreitung gefunden hat und bis heute noch verfügbar ist.[11] Inwiefern dieses Forschungsprojekt auch den Reformprozess beeinflusst hat, ist schwer zu sagen, aber wohl – wie bei solchen wissenschaftlichen Projekten ja generell – eher zu bezweifeln. Denn dieser hat sich mehr und mehr, wie schon oben gesagt, am angloamerikanischen kontradiktorischen Verfahren orientiert, weil man sich nur auf diese Weise die notwendige radikale Abkehr vom überkommenden Inquisitionsprozess versprach. Allerdings wurden keineswegs alle Strukturelemente dieses Verfahrensmodells übernommen (insbesondere nicht überall die Geschworenengerichte)[12] und es ist aus heutiger Sicht – with the benefit of hindsight – auch durchaus fraglich, ob diese radikale Hinwendung zum kontradiktorischen Verfahren der richtige Weg gewesen ist.[13] Inzwischen ist ja sattsam bekannt, dass Reformen ohne die bessere Aus- und Fortbildung der strafprozessualen Akteure, insbesondere der Ermittlungsbehörden (Polizei!),[14] kaum erfolgreich sein können. Jedenfalls hat sich der Reformprozess wohl vom Código Modelo entfernt, was vielleicht auch die zunehmende Distanz Maiers zu diesem Prozess erklärte. Dem Werk und Vermächtnis von Julio Maier tut dies jedenfalls alles keinen Abbruch. Er bleibt als einer der ganz großen Strafprozessrechtswissenschaftler in Erinnerung, dessen Ableben nicht nur für Lateinamerika einen herben Verlust bedeutet.

[9] Zur Klassifizierung der Verfahrensmodelle, insbesondere der (häufig irreführenden) Verwendung des Begriffs „acusatorio" siehe *Ambos/Woischnik*, ZStW 113 (2001), 334 (348 ff.); in spanisch: *dies.*, in: Maier/Ambos/Woischnik (Hrsg.), Las reformas procesales penales en América Latina, 2000, S. 867, abrufbar unter http://www.department-ambos.uni-goettingen.de/data/documents/Forschung/Projekte/Reformas%20Procesales%20Penales/ReformasPPAL.pdf (29.8.2020); aus rechtshistorischer Sicht *Ambos*, Jura 2008, 586; in spanisch: *ders.*, in: Bachmaier Winter (Hrsg.), Proceso Penal y Siste–mas Acusatorios, 2008, S. 49; auch *Bachmaier Winter*, Revista del Instituto de Ciencias Jurídicas de Puebla A.C. Nr. 24, 2009, 172, abrufbar unter http://www.bibliotecad.info/wp-content/uploads/2018/08/Sistemas-procesales.-superar-dicotomia.pdf (29.8.2020).

[10] *Ambos/Woischnik* (Fn. 9 – Las reformas); zusammenfassend *Ambos/Woischnik*, ZStW 113 (2001), 334.

[11] Siehe die Verlagsseite unter http://www.editorialadhoc.com/busqueda/ambos# (29.8.2020).

[12] Siehe auch *Langer*, *Vargas* und *Binder* (alle Fn. 7).

[13] Für eine „gemischte Bewertung" („balance mixto") siehe *Ambos*, Revista Política Criminal, Nr. 2, 2006, abrufbar unter https://www.department-ambos.uni-goettingen.de/data/documents/Veroeffentlichungen/epapers/Breves%20comentarios%20sobre%20la%20reforma%20judicial%20en%20America%20Latina,%20Political%20Criminal%20%202006.pdf (29.8.2020); jüngst kritisch zum Zustand der lateinamerikanischen Strafjustiz *Ambos/Aboueldahab*, in: Maihold/Sangmeister/Werz (Hrsg.), Lateinamerika: Handbuch für Wissenschaft und Studium, 2019, S. 172 ff.; siehe auch die Bewertung der chilenischen Reform in: Arellano (Hrsg.), Desafíos de la Reforma Procesal Penal en Chile: Análisis retrospectivo a más de una década, 2017, 245–256, abrufbar unter https://biblioteca.cejamericas.org/bitstream/handle/2015/5595/4%20-%20Desaf%c3%ados%20de%20la%20Reforma%20Procesal%20-%20VERSI%c3%93N%20DEFINITIVA.pdf?sequence=5&isAllowed=y (29.8.2020).

[14] Zur Polizei vgl. *Ambos/Gómez-Colomer/Vogler*, La Policía en los Estados de Derecho Latinoamericanos, 2003, abrufbar unter http://cedpal.uni-goettingen.de/data/investigacion/grupales/Antiguos/PoliciaKaiAmbos.pdf (29.8.2020); zusammenfassend *Ambos/Malarino*, ZStW 116 (2004), 513; zu Chile siehe Arellano (Fn. 13), S. 250 f. (zum Verhältnis zwischen Staatsanwaltschaft und Polizei).