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

AUSGABE 2/2020
S. 39 - 83
15. Jahrgang

Inhalt

ISSN
1863-6470

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

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

Die vorliegende Sonderausgabe zu „Strafrecht und Digitalisierung in Wissenschaft und Praxis“ greift den gegenwärtigen tiefgreifenden technologischen Wandel im strafrechtlichen Kontext auf. Der Titel enthält mit dem Strafrecht, der Digitalisierung, der Wissenschaft sowie der Praxis vier Bereiche, die in vielfältigen Verhältnissen zueinander stehen. Diese Feststellung ergibt sich bereits für die ersten beiden Aspekte – das Strafrecht und die Digitalisierung. Ebenso wie es ein Strafrecht der Digitalisierung geben kann, ist auch eine Digitalisierung des Strafrechts denkbar. Während das Strafrecht der Digitalisierung etwa den Bereich der Internetkriminalität erfasst, ist der Rahmen der Digitalisierung des Strafrechts erheblich weiter gespannt. Die Digitalisierung des Strafrechts betrifft neben Fragen der Anwendung des geltenden Rechts auf die veränderte Lebenswirklichkeit auch das Problem, in welchem Umfang der geltende Rechtsrahmen mit Blick auf den technologischen Wandel angepasst und damit geändert werden muss.[1]

Die Wirkmacht der Digitalisierung erfasst die Rechtsanwendung nicht nur dadurch, dass etwa Legal Tech zum integralen Bestandteil der Tätigkeit von Anwaltskanzleien wird oder neue Sachverhalte auftreten, die in rechtlicher Hinsicht regelungsbedürftig erscheinen. Vielmehr können die digitalen Veränderungen auch dazu führen, dass grundlegende Rechtsprinzipien einen Bedeutungswandel erfahren müssen, etwa weil der Einsatz von Robotern regelmäßig zu einer zeitlichen Vorverlagerung rechtsgutsrelevanter menschlicher Entscheidungen führt.[2] Darüber hinaus muss die Rechtswissenschaft ihrem normativen Gestaltungsanspruch im Zusammenhang mit der technischen Entwicklung gerecht werden, indem der geltende Rechtsrahmen angepasst wird und neue Lösungswege angeboten werden.[3]

Diese und weitere Fragen bildeten den Gegenstand des Workshops „Strafrecht und Digitalisierung in Wissenschaft und Praxis“, der von der Initiatorin und dem Initiator dieser ZIS-Sonderausgabe veranstaltet wurde und der im Juni 2019 an der Universität Hamburg stattfand. Die Bezugnahme auf die Wissenschaft und Praxis ist dabei sowohl gegenständlich als auch personell zu verstehen. Es war eines der Ziele der Veranstaltung, ein Forum zum wechselseitigen Austausch zwischen Wissenschaftlerinnen und Wissenschaftlern sowie Praktikerinnen und Praktikern zu bieten. Dabei wurde ein weites Strafrechtsverständnis zugrunde gelegt, in dem Fragen des Strafverfahrens nicht ausgeblendet werden.

Die vorliegende Sonderausgabe beinhaltet unter anderem die schriftlichen Ergebnisse dieses Workshops. Prof. *Dr. Susanne Beck*, LL.M. (Universität Hannover), befasst sich in diesem Rahmen mit der Diffusion strafrechtlicher Verantwortlichkeit durch Digitalisierung und Lernende Systeme. Aus einer Täterperspektive seien internetgestützte Aktivitäten (wie etwa sogenannte Shitstorms) häufig dadurch gekennzeichnet, dass ein einzelner Nutzer zu einem bestimmten Ergebnis nur einen kleinen Teil beitrage.[4] Nehme man demgegenüber eine Opferperspektive ein, so sei festzustellen, dass die kommunikative Angreifbarkeit im Internet vergleichsweise einfach ist. Vor diesem Hintergrund untersucht *Beck* die Frage, zu welchen Veränderungen diese und andere Phänomene im Hinblick auf die Frage der strafrechtlichen Verantwortlichkeit führen.

Prof. *Dr. Kai Cornelius*, LL.M. (Universität Heidelberg), legt das Hauptaugenmerk seines Beitrags auf den Einsatz sogenannter Künstlicher Intelligenz.[5] Unter anderem beleuchtet *Cornelius* die Frage der Verantwortlichkeit beim Einsatz solcher KI-Systeme. Darüber hinaus diskutiert er verschiedene Ansätze einer KI-Compliance, unter anderem den präventiven Ansatz einer KI-Compliance by Design sowie den retrospektiven Ansatz einer KI-Compliance by detection. Mit Systemen Künstlicher Intelligenz befasst sich auch *Lasse Quarck* (Universität Kiel), der sich in seinem Beitrag vor allem der Frage der Strafbarkeit sogenannter e-Personen widmet und ein erweitertes, über die bisherigen Grenzen der Individualstrafrechtsdogmatik hinausgehendes Verständnis der Begriffe Handlung, Schuld und Strafe diskutiert.[6] LOStA PD *Dr. Ralf Peter Anders* (Universität Hamburg)[7] sowie Rechtsanwalt *Dr. Frédéric Schneider* (Hamburg)[8] nehmen in ihren Beiträgen einen strafprozessualen Blick auf das digitale Zeitalter ein. Gegenstand der Untersuchung von *Anders* sind die normativen und tatsächlichen Implikationen eines staatsanwaltschaftlichen Zugriffs auf personenbezogene Daten in Speichern privater Dritter. *Schneider* erörtert die Auswirkungen der Digitalisierung auf das Ermittlungsverfahren aus der Verteidigerperspektive. Vor dem Hintergrund, dass die Digitalisierung heutzutage große Datenmengen verfügbar macht, geht *Schneider* der Frage nach, welche Konsequenzen hieraus für die Voraussetzungen des Anfangsverdachts sowie für die Anforderungen an Durchsuchungen folgen.

---

[1] Vgl. allgemein zu diesen unterschiedlichen Dimensionen des Verhältnisses zwischen Recht und Digitalisierung: *Ringe/Trute*, Zentrum für Recht in der digitalen Transformation (ZeRdiT), abrufbar unter https://www.jura.uni-hamburg.de/forschung/institute-forschungsstellen-und-zentren/digitalisierung-und-recht.html (27.1.2020).

[2] Mit Unterschieden: *Hörnle/Wohlers*, GA 2018, 12 (23); *Hevelke/Nida-Rümelin*, Jahrbuch für Wissenschaft und Ethik 19 (2015), 5; vgl. zu dieser These: *Kuhli*, in: Bung u.a. (Hrsg.), Festschrift für Reinhard Merkel (erscheint demnächst).

[3] *Brüning*, in: Rotsch (Hrsg.), Criminal Compliance – Status quo und Status futurus (erscheint demnächst).

[4] *Beck*, ZIS 2020, 41.

[5] *Cornelius*, ZIS 2020, 51.

[6] *Quarck*, ZIS 2020, 65.

[7] *Anders*, ZIS 2020, 70.

[8] *Schneider*, ZIS 2020, 79.

Es ist augenscheinlich, dass das Thema „Strafrecht und Digitalisierung in Wissenschaft und Praxis“ nicht im Format eines einzelnen wissenschaftlichen Workshops erschöpfend behandelt werden kann. Die Veranstaltung sollte eher Anregungen und Denkanstöße geben, um weitere Forschungsaktivitäten zu generieren. Vor diesem Hintergrund fand im Januar 2020 an der Universität Hamburg bereits eine Nachfolgeveranstaltung („Strafverfolgung und Digitalisierung in Wissenschaft und Praxis“) statt, deren schriftliche Ergebnisse noch dieses Jahr ebenfalls als ZIS-Sonderausgabe veröffentlicht werden.

Alle, die schon einmal eine wissenschaftliche Veranstaltung organisiert haben, wissen, dass dies ohne vielfältige Unterstützung nicht zu realisieren ist. Ein großer Dank gebührt zunächst dem Verbund Norddeutscher Universitäten, der die Durchführung dieses Projektes durch eine großzügige finanzielle Zuwendung unterstützt hat. Danken möchten die Initiatorin und der Initiator auch den Teams ihrer Lehrstühle, die die Durchführung der Veranstaltung und die Publikation in dieser Ausgabe tatkräftig unterstützt haben. Darüber hinaus danken wir den Referentinnen und Referenten, die den Workshop mit ihren Beiträgen bereichert haben. Dies sind Prof. *Dr. Susanne Beck*, LL.M. (Universität Hannover), Prof. *Dr. Kai Cornelius* (Universität Heidelberg), *Lasse Quarck* (Universität Kiel), Rechtsanwalt *Dr. Frédéric Schneider* (Hamburg) und Prof. *Karoline Starkgraff* (Polizeiakademie Hamburg). Prof. *Dr. Thomas Rotsch* möchten wir herzlich für die freundliche Bereitschaft danken, die Beiträge in der vorliegenden Sonderausgabe der ZIS zu publizieren.

Wir wünschen eine anregende Lektüre!

Die Diffusion strafrechtlicher Verantwortlichkeit durch Digitalisierung und Lernende Systeme*

Von Prof. Dr. **Susanne Beck**, LL.M. (LSE), Hannover

„In times of change the greatest danger is to act with yesterday's logic."[1]

I. Einführung

Die überragende Bedeutung des Internets, von Smartphones, E-Mails, Kommunikation über WhatsApp oder Viber, die Aktivität in sozialen Netzwerken – wir leben bereits im digitalen Zeitalter: Bis 2030 sollen ca. eine halbe Billion Geräte über das Internet vernetzt sein.[2] Um die 95 % der weltweiten technologischen Informationskapazität ist digital.[3] Aktuell kommen Entwicklungen hinzu wie Industrie 4.0, KI-gestützte Diagnosesysteme in der Medizin, Pflegeroboter, selbstfahrende Kraftfahrzeuge, autonome Waffensysteme etc. In den nächsten Jahren und Jahrzehnten wird die Automatisierung, d.h. die Übertragung von Entscheidungen auf Maschinen und direkte Interaktion mit (teilweise verkörperter) Künstlicher Intelligenz (KI) unseren Alltag prägen.[4]

Digitalisierung bedeutet schnelle, weltweite Kommunikation, zeitunabhängige Information zu fast allen Lebensfragen, Vernetzung, Arbeitsteilung, Alltagserleichterung.[5] In vielen Bereichen werden nur noch Maschinen die Informationsflut bewältigen können, und nicht selten werden ihre Entscheidungen weniger Fehler aufweisen als die Entscheidungen von Menschen.

Diese technologische Entwicklung verändert zwangsläufig unsere Kommunikation und Interaktion, zwischen den Menschen, aber auch mit Maschinen und der Maschinen untereinander. Das hat natürlich Folgen für das Recht, das diese Entwicklungen steuernd begleiten muss. Auch für das Strafrecht und die ihm zugrunde liegende Konzeption von Verantwortlichkeit sind die soziale Stellung des Einzelnen im Kontext der Digitalisierung und Automatisierung, die Besonderheit vernetzter Interaktion, die Übertragung von Entscheidungen auf Maschinen und die – gesellschaftlichen und individuellen – Folgen digitalisierten Handelns und dieser Übertragungen von Bedeutung. Deshalb werden im Folgenden zunächst die technologischen Entwicklungen aus strafrechtlicher Perspektive, insbesondere aus Täter- und Opferperspektive, beleuchtet und anschließend erläutert, was das für die strafrechtliche Verantwortlichkeit bedeutet bzw. ob diese ggf. neu justiert werden muss.

II. Die Entwicklung der Digitalisierung und Lernender Systeme

Digitalisierung[6] meint zunächst die Aufbereitung von Informationen, um sie speichern und weiterverarbeiten zu können. Digitalisierung als gesellschaftliche Entwicklung schließt (neben diesen technischen Vorgängen) auch die Entstehung und das stetige Voranschreiten des Internets ein. Durch die Verlagerung der Kommunikation auf den elektronischen Weg entsteht eine große Distanz zwischen Absender und Empfänger, die Kommunikation kann anonym erfolgen und der Adressatenkreis ist theoretisch unbegrenzt und vom Absender regelmäßig nur schwer kontrollierbar. Inhalte bleiben dauerhaft gespeichert, das Netz „vergisst nicht".

Hinzu kommt die Weiterentwicklung von Sensoren und den diese verwendenden Maschinen, Computerprogrammen und Algorithmen. Teilweise sind diese Systeme in der Lage, selbst zu „lernen", das heißt sich weiterzuentwickeln, bestimmte Strukturen zu verstehen, ggf. Verhalten nach Fehlern zu verändern etc. Beim sogenannten „Deep Learning"[7] sind hierbei nicht einmal mehr die Vorgänge des Lernens nachvollziehbar, weil diese über eine Art neuronale Netze stattfinden.

Neben der unendlichen Menge an Informationen, die uns auf diese Weise zugänglich gemacht werden, eröffnet das Internet jedem Teilnehmer eine grenzenlose Kommunikationsinfrastruktur. Die zur Verarbeitung dieser Informationsflut eingesetzten Algorithmen werden derzeit stetig weiterentwickelt. So können im High-Speed-Trading nur noch Software-Agenten schnell genug entscheiden; im medizinischen Bereich können Big Data und die aktuelle Forschung kaum noch von menschlichen Ärzten ausgewertet werden – KI-gestützte Diagnosesysteme scheinen demgegenüber erhebliche Vorteile mit sich zu bringen[8]. Die Lebensbereiche, in denen solche selbstlernenden Maschinen eingesetzt werden, nehmen ständig zu, vom Aktienhandel und der Medizin bis hin zur Kreditvergabe, der Auswahl aus verschiedenen Bewerbern, Übersetzungsprogrammen etc. Zudem werden künstliche neuronale Netze und Deep Learning vermehrt in sich bewegenden Maschinen eingesetzt werden, so dass in Verbindung mit verbesserter Sensorik selbstfahrende Kraft-

* Für unersetzliche Unterstützung bei der Recherche gilt mein herzlicher Dank Frau Diplom-Juristin *Melina Tassis* und Herrn Stud. iur. *Oliver Marks*. Vgl. zum Folgenden überdies weitergehend *Beck*, in: Fischer/Hoven (Hrsg.), Schuld, 2017, S. 289.

[1] *Peter Drucker* (österreichischer Ökonom, verstorben 2005).

[2] Siehe http://www.bmwi.de/Redaktion/DE/Dossier/digitalisierung.html (4.2.2020).

[3] *Hilbert/López*, Science 332 (2011), S. 60–65; www.martinhilbert.net/WorldInfoCapacity.html (4.2.2020).

[4] *Beck*, in: Beck/Meier/Momsen (Hrsg.), Cybercrime und Cyberinvestigations, 2015, S. 9 (14 f.); *Borges*, NJW 2018, 977; *Klesen*, in: Hilgendorf/Beck (Hrsg.), Robotik und Recht, 2017, S. 13 f.

[5] *Krüger*, ZRP 2016, 190; *Uffmann*, NZA 2016, 977.

[6] Vgl. zum Folgenden auch *Beck* (Fn. *), S. 289.

[7] Durch „Deep Learning"-Techniken werden Roboter in die Lage versetzt, zu „sehen" und Software Agents Sprache zu verstehen (Beispiele sind u.a. Siri und Alexa); vgl. *Keßler*, MMR 2017, 589.

[8] *Hernandez*, WIRED v. 6.2.2014, abrufbar unter https://www.wired.com/2014/06/ai-healthcare/ (4.2.2020); http://www.openclinical.org/aiinmedicine.html (4.2.2020).

fahrzeuge und intelligente Lagersysteme Einzug in den Alltag finden.[9] Sogar bei der Beurteilung der Rückfallwahrscheinlichkeit von Straftätern wird in den USA[10] schon auf computergesteuerte Vorschläge zurückgegriffen.

III. Beispielsfälle

Die mit diesen Entwicklungen verbundenen potentiellen rechtlichen Probleme seien, bevor anschließend das Problem detailliert analysiert wird, an zwei Beispielsfällen verdeutlicht:

Fall 1: A wird auf Instagram Opfer eines Shitstorms, weil er ein angeblich „prolliges" Foto mit nacktem Oberkörper postete. Zahllose Nutzer kommentieren sein Bild, machen sich über ihn lustig, bezeichnen ihn als „Lauch" und „Vollpfosten". A nimmt dieses Ereignis psychisch sehr mit, gerade weil so viele Menschen gleichzeitig auf ihn losgehen und weil viele Nutzer sowie seine Freunde und Familie die Beschimpfungen lesen können und weil selbst nach der Löschung seines Posts immer wieder Screenshots davon auftauchen. Die Kommentierenden dagegen finden ihr Verhalten nicht schlimm, das seien doch ganz normale Kommentare, A möge sich nicht so anstellen. Außerdem hätten alle anderen doch etwas Ähnliches geschrieben.

Fall 2: Hersteller H produziert selbstfahrende Kraftfahrzeuge. Hierfür zuständig ist unter anderem Programmierer P. Ein von diesem programmiertes Kraftfahrzeug wird von der entsprechenden Zulassungsstelle geprüft, an den Halter X geliefert und anschließend vom Taxifahrer A gefahren. Bei einer Fahrt sieht sich A einen Film an, da er sich auf das Kraftfahrzeug verlässt und nicht auf den Straßenverkehr achtet. Das Kraftfahrzeug übersieht einen weißen, quer stehenden Lkw, weil die Sonne auf die Plane scheint und die Sensoren nicht reagieren. An so eine Möglichkeit hatte P nicht gedacht. Das Kraftfahrzeug kollidiert mit dem Lkw, prallt ab und verletzt den auf dem Bürgersteig laufenden Fußgänger B schwer.

IV. Digitalisierung und Automatisierung aus strafrechtlicher Perspektive

An den Beispielsfällen zeigen sich bereits einige Schwierigkeiten, die aufgrund der Digitalisierung und Automatisierung entstehen. Im Folgenden sollen die Entwicklungen der Digitalisierung und Automatisierung aus strafrechtlicher Perspektive betrachtet werden, wobei zu Beginn der Täter und anschließend das Opfer in den Fokus genommen wird.

1. Täter-Perspektive

Zunächst sei bei der Darstellung der Effekte von Digitalisierung und Automatisierung zunächst der Täter, also der Akteur, betrachtet.

Da die Interaktion im Netz und mit Maschinen regelmäßig vernetzt stattfindet, trägt ein einzelner Nutzer zu einem bestimmten Ergebnis häufig nur einen kleinen Teil bei. Als Beispiel hierfür seien DDoS-Attacken[11] angeführt: Diese sind grundsätzlich nur erfolgreich, wenn zahlreiche User zugleich auf eine Internetseite zugreifen, um sie für andere zu sperren. Ein „Shitstorm"[12] erhält seine Bedeutung auch für das Opfer gerade dadurch, dass er sich aus einer großen Anzahl beleidigender Beiträge zusammensetzt. Die Massivität der Beleidigungen und Verletzungen gründet zudem nicht zuletzt im gegenseitigen Anstacheln und dem Gefühl des Einzelnen, in der Menge unterzugehen.[13]

Nicht nur die große Anzahl an Nutzern, sondern auch die Möglichkeiten, unter Fake-Profilen aufzutreten, in Foren keine Klarnamen angeben zu müssen, sich also hinter einer Scheinidentität zu verstecken, vermitteln den Akteuren eine – mehr oder weniger vermeintliche – Anonymität.[14] Damit zusammen hängt das Phänomen der erheblichen Distanz zwischen Täter und Opfer.[15] Die zeit- und ortsunabhängige Kommunikation und die digitalisierte Vermittlung verhindert, dass der Täter die Auswirkungen beim Opfer direkt erlebt. Das erleichtert ihm die Entpersonalisierung seines Opfers, insbesondere dann, wenn er das Opfer nicht „real" kennt. Auch da die Delikte – etwa Phishing oder Hacking – oft nur geringe Schäden beim individuellen Opfer verursachen und der Täter primär von der Summe der Schädigungen profitiert, fällt ihm eine Neutralisierung der Schädigung gelegentlich leichter als in realen Konstellationen. Hinzu kommt die Besonderheit, dass der Täter im digitalen Raum agiert. Regelmäßig werden die Delikte allein vor dem Bildschirm begangen. Das verringert die Schamgrenze und das Gefühl, etwas „Falsches" zu tun. Der Täter wird weder durch das Opfer noch durch andere Mitbürger, die sein Verhalten kontrollieren und bewerten, direkt wahrgenommen. Das Umfeld des Internets suggeriert vielmehr Regellosigkeit, einen „rechtsfreien Raum"[16].

---

[9] *Eckert*, WELT v. 23.7.2016, abrufbar unter https://www.welt.de/wirtschaft/article157235743/Warum-wir-schon-bald-voellig-anders-arbeiten.html (4.2.2020); *Stockburger*, SPIEGEL v. 4.2.2017, abrufbar unter http://www.spiegel.de/auto/aktuell/kuenstliche-intelligenz-wie-autos-durch-neuronale-netze-das-fahren-lernen-a-1132759.html (4.2.2020).

[10] *Angwin/Larson/Mattu/Kirchner*, ProPublica v. 23.5.2016, abrufbar unter https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (4.2.2020).

[11] Durch einen solchen Angriff werden Webseiten so lange massenhaft mit Klicks bombardiert, bis sie zusammenbrechen und nur noch stark eingeschränkt bzw. gar nicht mehr verfügbar sind; vgl. *Lutz*, WELT v. 23.4.2017, abrufbar unter https://www.welt.de/wirtschaft/webwelt/article163934774/Problem-der-Cyberkriminalitaet-wird-immer-groesser.html (4.2.2020).

[12] Zu Deutsch: Empörungswelle, http://www.dict.cc/englisch-deutsch/shitstorm.html (4.2.2020); vgl. auch *Ebner*, socialmediafacts v. 2.12.2014, abrufbar unter http://www.socialmediafacts.net/shitstorms/shitstorm-checkliste-definition (4.2.2020).

[13] *Cornelius,* ZRP 2014, 164 (167).

[14] *Meier*, in: Beck/Meier/Momsen (Fn. 4), S. 93 (95 f.).

[15] *Meier* (Fn. 14), S. 96 f.

[16] *Hilgendorf*, ZIS 2010, 208 (210).

Weiterhin führt das Netz aufgrund der Vielzahl an Nutzungsmöglichkeiten nicht selten zu einer Art Spaltung der Persönlichkeit. Während man auf beruflichen Seiten seine Seriosität betont, präsentiert man auf sozialen Netzwerken wie etwa Facebook eher seine privaten Persönlichkeitsanteile. Das kann auch dazu führen, dass man eine dieser vielen Persönlichkeiten für rechtlich oder moralisch problematische Verhaltensweisen vorbehält, sich aber gleichzeitig von dieser distanziert, so dass für „kriminelles oder unsoziales Verhalten […] die geschaffene Cyberidentität verantwortlich gemacht“[17] wird.

Ein spezifisches, relativ neues Problem ist die Automatisierung von Systemen. Immer öfter werden Entscheidungen oder zumindest Teile davon von Maschinen übernommen oder vorbereitet. So könnte etwa ein Algorithmus über den An- oder Verkauf von Wertpapieren[18], die beste Fahrtroute oder das Rufen des Notarztes bei fehlender Reaktion einer überwachten älteren Person entscheiden. Nicht nur die Situationen der vollständigen Übertragung von Entscheidungen auf Maschinen, sondern auch die kooperativen Entscheidungen sind kaum noch mit traditionellen Entscheidungssituationen vergleichbar. Die Maschine sortiert zum einen regelmäßig vorher bestimmte Optionen aus, zum anderen führen ihre Vorschläge zu Voreingenommenheit beim menschlichen Akteur. Überdies begründen strukturelle und zeitliche Gegebenheiten nicht selten Situationen, in denen es dem menschlichen Kooperationspartner faktisch kaum möglich ist, in verantwortungsvoller Weise zu reflektieren. So haben Angestellte bei Facebook drei Sekunden, um ein Post als „Hassrede“ oder in sonstiger Weise unzulässig einzuordnen – und dafür sehen sie nur den konkreten Post, keinerlei Kontext. Fahrer eines Kraftfahrzeugs, das großteils autonom fährt und von ihnen nur noch „überwacht“ wird – wie bei einem Tesla-Fahrzeug – brauchen viel länger, um im Notfall zu übernehmen als jemand, der selbst fährt. Man geht von einer Reaktionszeit von 6 bis 26 Sekunden aus[19].

2. Die Opferperspektive

Digitalisierung und Automatisierung haben auch Auswirkungen auf (potentielle) Opfer. Die Virtualität vereinfacht faktisch die Kommunikation mit ihnen und über sie. Zudem kann über Massen-E-Mails und soziale Netzwerke eine große Anzahl an Opfern erreicht und so die Wahrscheinlichkeit erhöht werden, dass zumindest einige Adressaten wie gewünscht reagieren. Virtuelle Bedrohung wird nicht so stark empfunden wie reale Bedrohung, so dass weniger Schutzmaßnahmen ergriffen werden.[20]

Zugleich ist die Anzahl der Leser von etwa Verleumdungen im Netz theoretisch unbegrenzt und dies erhöht den Unrechtsgehalt der Tat.[21] Auch besteht die Gefahr, dass das Internet derartige Angriffe und andere strafbare Kommunikation (Volksverhetzungen, Kinderpornographie usw.) über einen langen Zeitraum zur Verfügung stellt.[22] Schließlich ist es im Netz nicht nur schwer, Gegendarstellungen denselben Raum zu verschaffen, sondern auch, den Täter zu ermitteln, ihm die Tat nachzuweisen, ihn zu bestrafen. Das Opfer wird mit seiner Verletzung vermehrt allein gelassen.[23]

V. Veränderung der strafrechtlichen Verantwortlichkeit

Digitalisierung und Automatisierung könnten die strafrechtliche Verantwortlichkeit in vielerlei Hinsicht verändern. Wir wollen uns hier auf einige Aspekte fokussieren. So kann sich die Interaktion zwischen vielen Beteiligten und die Herbeiführung von Erfolgen erst durch Kumulation der Einzelbeiträge etwa auf die Zurechenbarkeit – und natürlich auch auf die Beweisbarkeit des Einzelbeitrags – auswirken. Das gilt auch für die Übertragung von Entscheidungen (oder Teilen davon) auf Maschinen. Hinzu kommt die Relevanz der technologischen Entwicklung für die persönliche Vorwerfbarkeit – insbesondere die Digitalisierung und die besondere Situation des Nutzers im Netz, aber auch die massive Verletzung des Opfers im Internet könnten die Schuld verändern.

1. Auswirkungen der Digitalisierung auf die strafrechtliche Verantwortung

Bereits die Interaktion verschiedener Akteure im Internet, etwa die kooperative Herstellung von Produkten auf entsprechenden Plattformen, die kollektive Empörung mittels eines Shitstorms oder das kumulative Bewirken eines Website-Shut Downs können sich auf der Ebene des objektiven Tatbestands auswirken, z.B. bei der objektiven Zurechenbarkeit. Das gilt etwa für die im *Beispielsfall 1* angedeutete Problematik. Doch sind diese Probleme durchaus mit anderen Entwicklungen kollektiven Zusammenwirkens vergleichbar und sollen deshalb nicht im Fokus unserer heutigen Betrachtungen stehen. Die generelle Entwicklung der Digitalisierung könnte jedoch Auswirkungen auf die individuelle strafrechtliche Schuld haben. Die spezifische Persönlichkeitsaufspaltung, die neuen Neutralisierungsmechanismen, die Verringerung des zumindest für den Täter gefühlten Unrechts, aber auch das gesteigerte Maß der Verletzung des Opfers, wie es sich ebenfalls in *Fall 1* deutlich zeigt, könnten nicht nur die Schuldfähigkeit, sondern auch das Ausmaß der Schuld verändern und so etwa die Strafzumessung beeinflussen.

Ob die spezifische Situation, in der sich der Täter befindet, zu Schuldunfähigkeit führen könnte, hängt unter anderem damit zusammen, wie man die Schuldkonzeption konstruiert.

[17] *Bocij*, Cyberstalking: Harassment in the Internet Age and How to Protect Your Family, 2004, S. 104.
[18] *Ripatti*, wallstret online v. 10.10.2018, abrufbar unter https://www.wallstreet-online.de/nachricht/10917930-kuenstliche-intelligenz-algorithmen-aktienmarkt (4.2.2020).
[19] *Breitinger*, Zeit Online v. 2.2.2017, abrufbar unter http://www.zeit.de/mobilitaet/2017-02/autonomes-fahren-auto-fahrer-reaktionszeit (4.2.2020).
[20] *Cornelius*, ZRP 2014, 164 (166 f.).
[21] *Hilgendorf*, ZIS 2010, 208 (211).
[22] *Hilgendorf*, ZIS 2010, 208 (213).
[23] Vermehrt handelt es sich um Privatklagedelikte, deren Strafverfolgung für das Opfer umständlich und mit Kosten verbunden ist.

Wenn es mit *Jakobs*[24] um einen Verhaltensanspruch an den Täter in der konkreten Situation geht, könnte die Lockerung von Normen im Internet und die geringe Einbindung in eine soziale Kontrolle sowie die zwangsläufige Verringerung von Empathie durchaus eine Rolle für die Schuld des Einzelnen spielen. Ähnliches könnte man mit *Roxin*[25] anführen: In der digitalisierten Welt wird es erschwert, sich für normorientiertes Verhalten zu entscheiden – so argumentieren ja auch die Kommentierenden in unserem ersten Fall; in diesem Kontext sind möglicherweise alle Nutzer in gewissem Sinne „unreif". Durch die verringerte soziale Kontrolle schwindet auch das Vertrauen in die Geltung von Normen, was insofern zu schwächerer Ansprechbarkeit des Handelnden führt. Das gilt jedenfalls für die Verhaltensweisen, die im Netz Normalität erlangen und bei denen der einzelne Nutzer nur einen geringen Beitrag leistet und ihm Verletzung und Geltung der Norm nicht bewusst sind, d.h. etwa DDos-Attacken oder Shitstorms. Zugleich liefern beide Konzeptionen Anhaltspunkte dafür, dass dies nicht generell etwas am „Ob" der Schuld ändern kann. Trotz der genannten Aspekte besteht gesellschaftliche Einigkeit darüber, dass digitales Handeln an den geltenden Strafnormen zu messen ist. Trotz Abspaltung von Persönlichkeitsanteilen existiert die Vermutung einer normativen Ansprechbarkeit in der digitalisierten Welt. Und gerade aufgrund des geringen Normvertrauens scheint es durchaus auch wichtig zu betonen, dass trotz Digitalisierung die üblichen Standards gelten. Insofern ist positive Generalprävention besonders bedeutsam.

Es ist deshalb nicht möglich, auf diese Argumentation eine generalisierende Schuldunfähigkeit oder auch nur eine entsprechende Vermutung zu gründen. Vielmehr ändert die Digitalisierung alleine zunächst nichts an der grundsätzlichen Verantwortlichkeit des im Internet Agierenden.

Die Auswirkungen der Digitalisierung auf Täter und Opfer können sich jedoch beim Maß der Schuld, also der Strafzumessungsschuld, auswirken. An dieser Stelle sind nicht primär die bestehenden Kategorien, d.h. pathologische Zustände des Täters (§ 21 StGB[26]) oder spezifische Irrtümer über die rechtliche Bewertung der Tat (§ 17 StGB[27]), gemeint. Aber die Zusammenschau der Umstände der Tat und des Ausmaßes des Unrechts könnten die Strafhöhe beeinflussen. Insofern bestehen Wechselwirkungen mit der Frage, was das Unrecht der Straftat begründet. Dabei spielen sowohl handlungs- als auch folgenbezogene Aspekte eine Rolle, die zudem gegeneinander abzuwägen sind.

Mit Blick auf die Situation in der der Täter agiert, sprechen wie oben dargelegt einige Argumente dafür, von verringertem Unrecht auszugehen. Gerade das Maß des Unrechts wird auch an den Umständen bemessen; selbst wenn wir also davon ausgehen, dass man trotz der veränderten Bedingungen im Internet durchaus weitgehend im strafrechtlich relevanten Sinne verantwortlich agieren kann, bleibt es möglich, diese Bedingungen als einschränkend, strafbares Handeln erleichternd, den Einzelnen überfordernd anzusehen und strafmildernd zu berücksichtigen: Soziale Erwartungen, normative Ansprechbarkeit und das Unrechtsbewusstsein verändern sich, die Empathiefähigkeit nimmt ab etc. Demgegenüber stehen jedoch ebenfalls relevante folgenbezogene Argumente. Durch die Digitalisierung wird die Rechtsgutsverletzung erleichtert, potenziert, ist permanent und kaum korrigierbar.[28] Das erhöht in vielen Fällen – am offenkundigsten bei einer öffentlichen, nicht mehr löschbaren Beleidigung wie in unserem ersten Beispielsfall – den Grad der Rechtsgutsverletzung mit Blick auf das Opfer und damit das Unrecht der Tat.

Die handlungsbezogenen Argumente müssen mit den situationsbezogenen Aspekten in einen Ausgleich gebracht werden, sprechen doch erstgenannte für eine Erhöhung, letztere für eine Verringerung von Schuld. Insofern lässt sich auf die bewusst in Kauf genommene Inkonsistenz bzw. den bewussten Einzelfallbezug der praktischen Strafzumessung nach § 46 StGB[29] verweisen. Dies sei nur durch den kurzen Hinweis darauf ergänzt, dass auch die Gewichtung in dieser Abwägung mit der vertretenen Schuldkonzeption zusammenhängt. Eine stärker präventiv ausgerichtete Konzeption wird eher die Folgen des Handelns im Blick haben, während mit einem Fokus auf die Repression die Umstände des Handelns eine größere Rolle spielen dürften. Selbst wenn also durchaus gerade die aktuelle, häufig eskalierende Situation im Netz dagegenspricht, von einer verringerten Schuld der Nutzer auszugehen, sollte zumindest ein Bewusstsein dafür bestehen, dass es sich hierbei um eine stark folgenbezogene und wenig täterorientierte Argumentation handelt.

2. Auswirkungen des Einsatzes Lernender Systeme auf die strafrechtliche Verantwortung

Eine besondere Rolle mit Blick auf die strafrechtliche Verantwortung nehmen Maschinen ein, die einen eigenen Entscheidungsspielraum haben, durch Sensoren und Vernetzung Informationen erhalten und selbst auswerten. In diesen Fällen, wie etwa in unserem zweiten Beispielsfall, lässt sich weder im Vorhinein vorhersehen, welche Entscheidungen die Maschinen in welchen Situationen treffen werden, noch im Nachhinein feststellen, worauf die Entscheidungen beruhten. Insbesondere ob einer der Beteiligten, d.h. der Programmierer, Produzent oder der Nutzer einen Fehler gemacht hat, ist häufig nicht mehr nachweisbar.[30] Selbst wenn der Nachweis gelingt, sind die klassischen Zurechnungsstrukturen – wie wir im Folgenden sehen werden – nicht ohne Weiteres anwend-

[24] Vgl. *Jakobs*, Schuld und Prävention, 1976, S. 10, 14.

[25] Vgl. *Roxin*, Strafrecht, Allgemeiner Teil, Bd. 1, 4. Aufl. 2006, § 19 Rn. 36, 47.

[26] Vgl. *Perron/Weißer*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 21 Rn. 1 ff.

[27] Vgl. *Joecks*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 1, 3. Aufl. 2017, § 17 Rn. 1 ff.

[28] *Hilgendorf*, ZIS 2010, 208 (212).

[29] Vgl. zur Strafzumessung etwa *Miebach/Maier*, in: Joecks/Miebach (Fn. 27), § 46 Rn. 1.

[30] *Buck-Heeb/Dieckmann*, in: Oppermann/Stender-Vorwachs (Hrsg.), Autonomes Fahren, 2017, S. 60 (63); *Schuster*, DAR 2019, 6 (11).

bar.[31] Das bedeutet nicht, dass keine Konstellationen denkbar sind, in denen einer der Beteiligten nachweisbar einen Fehler gemacht hat, aber es bleibt die Ausnahme.[32]

a) Auswahl der relevanten menschlichen Handlung

Eine vor allem in der Praxis relevante Frage ist die nach dem Anknüpfungspunkt der strafrechtlichen Beurteilung; gemeint ist damit hier die Auswahl der Handlung. Grundsätzlich gilt, dass jeder, der eine strafrechtlich relevante Handlung begeht, zu sanktionieren ist und jeder entsprechende Verdacht zu verfolgen ist. Da eine Bestrafung der autonomen Systeme absehbar politisch unvorstellbar ist, kommen für eine mögliche Strafbarkeit grundsätzlich folgende Personen in Frage: der Forscher, der Programmierer, der Hersteller, der Verkäufer oder der Nutzer.[33] Meist wird bei kollektiven Geschehnissen nur auf einzelne Beteiligte abgestellt; sei es mit Blick auf die Nachweisbarkeit, Öffentlichkeitswirkung etc. Diese Auswahl ist aber ein wichtiger Schritt bezüglich der Zuschreibung strafrechtlicher Verantwortung und sollte deshalb auch in Kontexten des Zusammenwirkens mehrerer Menschen untereinander und mit Maschinen kritisch begleitet werden.

Erforderlich für die Strafbarkeit ist das Vorliegen einer menschlichen Handlung.[34] Auch wenn die Diskussion um den Handlungsbegriff in den letzten Jahrzehnten an Vehemenz verloren hat, sind die Überlegungen doch für neue Fragestellungen wie die unsere weiterhin relevant. An dieser Stelle ist nicht die Diskussion über eine Strafbarkeit von Maschinen gemeint,[35] sondern die Frage, wann die Interaktion des Menschen als Handlung angesehen werden kann – und zwar unabhängig von der Frage der Vorwerfbarkeit. Das ist nicht mehr der Fall, wenn der menschliche Anteil des Verhaltens nicht als vom Willen gesteuert oder steuerbar angesehen werden kann oder wenn die Maschine das menschliche Verhalten übersteuert.[36] Wenn also der Nutzer eines autonomen Kraftfahrzeugs in dem Fahrzeug schläft und das Kraftfahrzeug selbst alle Fahrfunktionen übernommen hat, dann „fährt" er nicht – es verbleibt natürlich ggf. bei einer Strafbarkeit wegen Unterlassens, aber nur wenn und soweit er zum Eingreifen in bestimmten Situationen verpflichtet wäre. Auch wenn das Kraftfahrzeug etwa an einer roten Ampel stehen bleibt, obwohl der Nutzer über die Kreuzung fahren möchte, das autonome System also den Rechtsbruch verhindert, wäre eine Handlung des Nutzers zu verneinen.[37]

b) Objektive Zurechenbarkeit des Erfolgs

Der konkrete Erfolg muss dem potentiellen Täter zurechenbar sein – zumindest nach der h.L.[38] Hierbei handelt es sich um einen der entscheidenden Aspekte bei der strafrechtlichen Analyse der Kollaboration von Mensch und Maschine.[39] Die Zurechnung könnte problematisch sein, weil bis zum Erfolgseintritt zahlreiche Entscheidungen verschiedener Personen bezüglich der Ausgestaltung und Nutzung der Maschine getroffen werden. Auch bei Herstellung und Programmierung der Systeme interagieren zahlreiche Personen.[40] Dieses Problem unterscheidet sich jedoch wie dargelegt kaum von den Schwierigkeiten bei der Produktion anderer Geräte bzw. sonstiger kollektiver Handlungen.[41]

Im Bereich der Robotik und KI tritt jedoch eine viel wichtigere Problematik hinzu: In die Interaktion wird nun auch eine Maschine einbezogen.[42] Das mag kein „Handeln" oder „Entscheiden" im klassischen Sinn sein;[43] durch die spezifische Technologie, d.h. Programmierung, Information, Netzwerkaktivität, Training, Lernen aus Fehlverhalten etc., wird die Maschine jedoch ein bedeutsamer Teil der „Entscheidung" des mit ihr kooperierenden Menschen. Deshalb lässt sich durchaus fragen, ob nicht allein schon dadurch der Zurechnungszusammenhang unterbrochen wird. Denn bei derart eng verwobenen und nicht ohne weiteres verteilbaren Entscheidungen ist schwer begründbar, dass sich der Erfolg als das Werk des menschlichen Akteurs darstellt.

Das kann auch in den Fällen gelten, in denen beim Einsatz von KI bzw. Assistenzsystemen die Letztentscheidung beim menschlichen Akteur verbleibt (wenn etwa der Mensch dem Vorschlag des Assistenzsystems noch zustimmen muss). Aus dieser, nicht selten normativ begründeten Einbeziehung

[31] So auch *Valerius*, in: Hilgendorf/Beck (Hrsg.), Autonome Systeme und neue Mobilität, 2016, S. 9 (12 f.).
[32] Vgl. dazu *Sander/Hollering*, NStZ 2017, 193 (193); *Beck*, in: Oppermann/Stender-Vorwachs (Fn. 30), S. 33 (50).
[33] Siehe hierzu auch den Bericht der *Ethik-Kommission*, Automatisiertes und Vernetztes Fahren, Juni 2017, S. 27, abrufbar unter https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (4.2.2020).
[34] *Roxin* (Fn. 25), § 7 Rn. 5.
[35] Vgl. hierzu *Gaede*, in: Hilgendorf/Beck (Hrsg.), Künstliche Intelligenz – Rechte und Strafen für Roboter?, 2019, S. 65.
[36] *Schuster*, DAR 2019, 6.
[37] *Rich*, in: Harvard Journal of Law and Public Policy, Forthcoming, Elon University Law Legal Studies Research Paper No. 2012-03, 2012, S. 802 f.
[38] *Heuchemer*, in: v. Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar, Strafgesetzbuch, Stand: 1.11.2019, § 13 Rn. 23; *Hoffmann-Holland*, in: Joecks/Miebach (Fn. 27), § 22 Rn. 81; *Roxin*, ZStW 74 (1962), 411 (431 ff.); *Sternberg-Lieben/Schuster*, in: Schönke/Schröder (Fn. 26), § 15 Rn. 54a.
[39] *Beck* (Fn. 6), S. 293; *Hilgendorf*, in: Beck (Hrsg.), Jenseits von Mensch und Maschine, 2012, S. 119 f.; *Beck* (Fn. 32), S. 35.
[40] *Lutz*, NJW 2015, 119 (121); *Sternberg-Lieben/Schuster* (Fn. 38), § 15 Rn. 217; *Vogt*, NZV 2003, 153 (158).
[41] *Seher*, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, 2016, S. 45 (52 f.).
[42] *Hilgendorf*, in: Hilgendorf/Hötitzsch/Lutz (Hrsg.), Rechtliche Aspekte automatisierter Fahrzeuge, 2015, S. 15 (25 f.); *Kütük-Markendorf/Essers*, MMR 2016, 22 (23 f.).
[43] *Gasser*, in: Maurer/Gerdes/Lenz/Winner (Hrsg.), Autonomes Fahren, 2015, S. 543 (552 ff.).

eines „human in the loop“[44] wird zwar zum Teil geschlussfolgert, dass die Konsequenzen der Entscheidung auch gerade diesem die Entscheidung treffenden bzw. zur Überwachung verpflichteten Menschen zuzurechnen seien. Das könnte jedoch zum einen die Idee der Entscheidungsübertragung untergraben und zum anderen auch normativ zweifelhaft sein. Die Einbeziehung einer KI erfüllt gerade den Zweck, die eigenen Defizite (zu wenig Information, zu langsame Entscheidungsfindung) auszugleichen und sich zumindest teilweise zu entlasten. Wird eine solche Nutzung gesellschaftlich akzeptiert, vielleicht auch weil die Maschine zumindest teilweise weniger fehlerbehaftet ist, rationaler und schneller beurteilen kann, dann ist wenig überzeugend, wenn der Nutzer für jede falsche Entscheidung strafrechtlich verantwortlich bliebe.[45] Denn das würde eine umfassende Prüf- und Kontrollpflicht bedeuten und keine Entlastung ermöglichen. Bei einem autonomen Kraftfahrzeug etwa würde dies bedeuten, dass der Fahrer sich weiterhin permanent konzentrieren müsste – was im Übrigen sogar faktisch schwerer wäre, wenn der Fahrer über lange Zeiträume passiv bleibt.[46] Dadurch würde die Nutzung von KI in vielen Fällen sinnlos oder zumindest in ihrer Funktionalität deutlich beeinträchtigt. Dies wäre hinzunehmen, wenn die Zuschreibung der Verantwortung normativ überzeugte. Doch das ist nicht der Fall, denn die Entscheidung ist keineswegs grundsätzlich als Werk des mitwirkenden Menschen anzusehen. Vielmehr ist in den meisten Fällen der Erfolg primär das Werk der Maschine und der menschliche Anteil kaum noch relevant.[47] Eine „meaningful control“[48] kann nur selten bejaht werden.

Diesbezüglich lässt sich generalisieren: Je größer die psychische und physische Hemmschwelle ist, sich gegen die Maschine zu entscheiden[49], desto eher ist die objektive Zurechnung zu verneinen. Das gilt umgekehrt dann nicht, wenn eine bedeutsame Kontrolle über die Maschine und damit letztlich die Entscheidung erhalten bleibt. Dann lässt sich überzeugend davon sprechen, dass der Erfolg als Werk des Menschen anzusehen ist. Sinnvoll erscheint es, verschiedene (technisch umsetzbare) Kooperationsszenarien durchzuspielen und so herauszufinden, wann die Entscheidung noch als kontrolliert angesehen werden kann und wie die verschiedenen Szenarien rechtlich einzustufen sind.

c) Sonderproblem: Fahrlässigkeit

Viele dieser Schwierigkeiten, insbesondere, aber nicht nur, der objektiven Zurechnung, stellen sich mit Blick auf die Fahrlässigkeit, weshalb einige ihrer Voraussetzungen genauer beleuchtet werden sollen.[50] Die jeweilige dogmatische Verortung bzw. der umstrittene Zusammenhang zwischen den einzelnen Aspekten der Fahrlässigkeitshaftung[51] sollen dabei jedoch nicht im Fokus stehen.

Grundsätzlich sind vorhersehbare Verletzungen Dritter zu vermeiden. Die Vorhersehbarkeit der Gefahr[52] ist also von zentraler Bedeutung. Je autonomer und gefährlicher ein System ist, desto eher ist abstrakt vorhersehbar, dass es irgendwann Menschen verletzen wird. So werden durch die Nutzung autonomer Fahrzeuge zweifellos in der Zukunft Menschen verletzt oder gar getötet;[53] durch ihre Herstellung und Nutzung wird also ein statistisches, abstraktes Risiko begründet.[54] Zugleich bleibt die Vorhersehbarkeit eben abstrakt; die spezifischen Umstände und Ereignisse werden durch die Autonomie der Systeme immer unvorhersehbarer.[55] Das liegt an der Verwendung komplexer neuronaler Netze sowie daran, dass es sich bei diesen Systemen um unbekannte Werkzeuge handelt, deren Verhalten für uns noch nicht berechenbar geworden ist. Diese Entwicklung zeigt auf, dass die Vorhersehbarkeit in Zukunft noch weiter konkretisiert werden muss,[56] d.h. es wird zu fragen sein, ob sie auf spezifische Umstände, Kausalzusammenhänge und konkrete Verletzungen gerichtet sein muss, oder ob es ausreicht, die abstrakte Möglichkeit vorherzusehen, Menschen zu verletzen.

Dabei ist insbesondere zu beachten, dass man mit Abstellen auf die bloße Vorhersehbarkeit abstrakter Risiken eine gewisse Handlungsunfähigkeit beim Einsatz derartiger Systeme herbeiführen könnte, denn dass durch sie irgendwann einmal Menschen verletzt oder getötet werden, ist sicher; das Strafbarkeitsrisiko bei ihrer Herstellung und Nutzung wäre also sehr hoch.[57] Man sollte deshalb jedenfalls dadurch entstehende erhebliche Strafbarkeitsrisiken im Blick behalten und Aspekte wie Wahrscheinlichkeit, Größe und Konkretheit des Schadens im Einzelfall berücksichtigen.

Neben der Vorhersehbarkeit ist ein Verstoß gegen die „erforderliche Sorgfalt erforderlich.[58] Dieser Standard bestimmt

[44] *Beck*, (Fn. 6), S. 293; *Sharkey*, in: Bhuta/Beck/Geiß/Hin-Yan Liu/Kreß (Hrsg.), Autonomous weapons systems, 2016, S. 23 (34 ff.).
[45] Etwa im Sinne einer Übernahmefahrlässigkeit, vgl. hierzu *Duttge*, in: Joecks/Miebach (Fn. 27), § 15 Rn. 131 ff.
[46] *May*, DVT 2015, 81 (85).
[47] *Beck* (Fn. 32), S. 49.
[48] *Beck* (Fn. 4), S. 14, 32 f.
[49] Insofern kann auch auf entsprechende empirische Erkenntnisse zurückgegriffen werden.
[50] *Beck* (Fn. 32), S. 38 ff.
[51] *Gropp*, Strafrecht, Allgemeiner Teil, 4. Aufl. 2015, § 12 Rn. 9; *Kühl*, Strafrecht, Allgemeiner Teil, 8. Aufl. 2017, § 17 Rn. 3.
[52] RGSt 65, 135 (136); *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 29. Aufl. 2018, § 15 Rn. 46; *Sternberg-Lieben/Schuster* (Fn. 38), § 15 Rn. 125; *Zieschang*, Strafrecht, Allgemeiner Teil, 5. Aufl. 2017, Rn. 429 ff.
[53] Siehe Augsburger Allgemeine v. 9.1.2012, abrufbar unter http://www.augsburger-allgemeine.de/bayern/Nach-Horrorunfall-Schlaganfall-am-Steuer-ist-nicht-selten-id18228966.html (4.2.2020).
[54] Vgl. *v. Bar*, Die Lehre vom Kausalzusammenhang, 1871, S. 14.
[55] Vgl. *Sternberg-Lieben/Schuster* (Fn. 38), § 15 Rn. 125.
[56] *Beck* (Fn. 32), S. 47 f.
[57] RGSt 33, 346 (347); bezogen auf alltägliche Handlungen, denen stets ein Risiko anhaftet: *Duttge* (Fn. 45), § 15 Rn. 135 f.
[58] *Hilgendorf* (Fn. 42), S. 25; *Kudlich*, in: v. Heintschel-Heinegg (Fn. 38), § 15 Rn. 35 ff.

sich typischerweise danach, welches Verhalten von einer vernünftigen Person aus einem bestimmten sozialen Kreis erwartet werden kann. Indikatoren sind nicht-staatliche Regeln aus dem jeweiligen Kontext, wie z.B. ISO- oder DIN-Normen.[59] Für unsere Problemstellung müssen einige Aspekte beachtet werden: So gibt es aktuell nur wenige Standards für den Umgang mit solchen Systemen;[60] es bleibt somit nur eine Orientierung an der generalisierenden Formel. Diese hilft in komplexen technischen Angelegenheiten wie der unseren jedoch kaum weiter.[61] Lernende, vernetzte Systeme sind eben noch in Entwicklung begriffen und die möglichen Risiken großteils unbekannt. Selbst wenn Standards existieren, ist zu beachten, dass die ihnen innewohnenden Wertungen nicht selten fragwürdige Interessen repräsentieren und gelegentlich aus intransparenten Regelungsverfahren stammen. Das gilt etwa für unternehmensinterne Richtlinien, die vor allem Interessen des Unternehmens beinhalten. Dies ist jedoch problematisch. Da Strafrecht nicht zuletzt das normative Bewusstsein der Gesellschaft bezüglich sozial inadäquater Handlungen stabilisieren soll,[62] ist für die Strafwürdigkeit eines Verhaltens neben seiner Gefährlichkeit auch erforderlich, dass es eine gesellschaftlich anerkannte Verhaltensregel verletzt.[63] Diese Regeln müssen allgemein akzeptiert sein. Regeln, die ein singuläres bzw. gruppenspezifisches Interesse schützen, können deshalb nicht in Strafgesetze einfließen.[64] Unabhängig von diesen spezifischen Problemen ist im Kontext von autonomen Systemen ungeklärt, wie überhaupt ein Sorgfaltsmaßstab in neuen Situationen, bei der Entwicklung neuer Technologien mit noch unbekannten Herausforderungen, gesamtgesellschaftlich zu bestimmen ist, inwieweit hier außerrechtliche Standards einfließen sollten und welche anderen Bezugnahmen denkbar und sinnvoll sind.

Aus den bisherigen Überlegungen könnte sich nun ergeben, dass aus dem bisher nicht bezifferbaren, unbekannten Risiko ein umfassendes Verbot derartiger Systeme folgen sollte bzw. nach derzeitigem Recht den Beteiligten häufig Fahrlässigkeitsstrafbarkeit droht.[65] Diese drohende Strafbarkeit könnte die Beteiligten von der weiteren Erforschung, Herstellung, dem Vertrieb und der Nutzung solcher Systeme abhalten. Angesichts der Vorteile, die autonome Systeme versprechen, kann dieses Ergebnis jedoch nicht überzeugen. Nicht nur aus diesem Grund, sondern auch aufgrund der fehlenden Zurechenbarkeit erscheint, wie dargestellt, auch eine grundsätzlich umfassende Haftung der Beteiligten (z.B. des Nutzers) für jeden künftigen Fehler des Systems angesichts der unklaren rechtlichen Vorgaben und der damit verbundenen faktischen Folgen nicht vertretbar.[66] Zweifellos darf das aber nicht zu umfassender Sorglosigkeit und zu untragbaren Risiken für Unbeteiligte führen.

Soweit die Beteiligten selbst über das Eingehen eines Risikos entscheiden, kann als Maßstab für die Erlaubtheit des Risikos das von ihnen, einem abgegrenzten Personenkreis, in Kauf genommene Risiko angesehen werden. Können jedoch Unbeteiligte verletzt werden, muss sich ein Maß für die Erlaubtheit von Risiken erst noch gesamtgesellschaftlich bilden. Soweit man den Einsatz der Systeme generell akzeptiert und dabei bestimmte Gefahren auch für Unbeteiligte hinnimmt, kann man dann vom Hersteller und Nutzer keine unverhältnismäßigen Sicherungen verlangen.[67] Für die Ermittlung des erlaubten Risikos ist letztlich eine transparente Diskussion darüber erforderlich, in welchen Bereichen die Vorteile autonomer Systeme die Nachteile überwiegen und wo die Grenzen des erlaubten Risikos liegen sollen. Folgende Faktoren sind dabei einzubeziehen: der Nutzen der Systeme bzw. die Frage, wer von ihrem Einsatz profitiert, ihre Beherrschbarkeit durch den Beteiligten und die Nutzung aller denkbaren Möglichkeiten der Risikominimierung.[68] Gefährdet das System gänzlich Unbeteiligte, ist das erlaubte Risiko niedriger als in den Fällen, in denen nur Nutzer oder Personen, die sich bewusst dafür entschieden haben, mit ihr interagieren.[69]

d) Zwischenfazit zur strafrechtlichen Verantwortung bzgl. Lernender Systeme

Unabhängig von konkreten Normen und spezifischen Kategorien der Anwendung lässt sich fragen, wie mit den Situationen umzugehen ist, in denen das lernende System die menschliche Entscheidung vorbereitet, der Mensch durch diese Vorbereitung aber einen nur noch stark verringerten Entscheidungsspielraum hat (etwa aufgrund einer besonders hohen psychischen Hemmschwelle, sich gegen die Maschine zu entscheiden, einer geringen Zeitspanne für die Reaktion oder fehlende Transparenz der maschinellen Vorschläge). Es handelt sich also um Konstellationen, in denen der oft geforderte „human in the loop" letztlich nur noch eine symbolische Funktion hat.[70] Insofern gilt – auch unter Heranziehung verschiedener Schuldtheorien[71] –, dass die Gesellschaft vom

[59] Vgl. z.B. BGH NJW 1954, 121; *Hilgendorf*, DVT 2015, 55 (67); *Jänich/Schrader/Reck*, NZV 2015, 313 (317); hierzu skeptisch *Duttge* (Fn. 45), § 15 Rn. 114 ff.

[60] Vgl. z.B.: ISO 10218-1: 2006; ISO 10218-2: 2011; ISO 13482: 2014.

[61] *Duttge* (Fn. 45), § 15 Rn. 114.

[62] *Gropp* (Fn. 51), § 1 Rn. 143 f.; *Jescheck/Weigend*, Strafrecht, Allgemeiner Teil, 5. Aufl. 1996, § 1 I. 1.

[63] Der Gesetzgeber wird auch von Lobbygruppen beeinflusst, agiert aber immer noch demokratisch kontrolliert; *Burkatzki*, ZIS 2011, 160.

[64] *Kühl*, in: Dannecker/Langer/Ranft/Schmitz/Brammsen (Hrsg.), Festschrift für Harro Otto zum 70. Geburtstag am 1. April 2007, 2007, S. 63 (64 ff.).

[65] *Beck* (Fn. 32), S. 44.

[66] *May*, 53. Deutscher Verkehrsgerichtstag 2015, 81 (101).

[67] BGH NJW 2009, 2952 (2954); *Sternberg-Lieben/Schuster* (Fn. 38), § 15 Rn. 145.

[68] *Hoyer*, ZStW 121 (2009), 860 (872 f.); *Sternberg-Lieben/Schuster* (Fn. 38), § 15 Rn. 145; *Vogt*, NZV 2003, 153 (160).

[69] *Hoyer*, ZStW 121 (2009), 860 (879); *Förster*, in: Bamberger/Roth/Hau/Poseck, Beck'scher Online-Kommentar, Bürgerliches Gesetzbuch, Stand: 1.11.2019, § 823 Rn. 687 ff.

[70] *Beck* (Fn. 6), S. 298.

[71] *Jakobs*, Strafrecht, Allgemeiner Teil, 2. Aufl. 1991, Abschn. 10 und 17: Nach dem funktionalen Schuldbegriff wird die Schuld über die Funktion der Strafe begründet und begrenzt. Entsprechend einer positiv-generalpräventiven

Individuum jedenfalls nicht mehr erwarten kann, als ihm möglich ist. Bei der Kooperation von Menschen mit Robotern und KI-gestützten Systemen ist also im Einzelfall genau zu prüfen, wie sich die Einbeziehung der Maschine auf den Entscheidungs- und Handlungsspielraum des Menschen auswirkt und ob das nach den vertretenen Schuldkonzeptionen seine Schuld ausschließt oder zumindest maßgeblich verringert.

Ruft man sich in Erinnerung, dass das Strafrecht traditionell auf die Sanktionierung einer Handlung ausgerichtet ist, die einem persönlich verantwortlichen Individuum zugerechnet werden kann, zeigt sich, dass das im Bereich von Robotik und KI kaum noch möglich ist. Eine konkret verwerfliche (etwa gegen Sorgfaltsmaßstäbe verstoßende) Handlung ist nur selten nachweisbar, die Zurechenbarkeit lässt sich in vielen Fällen bezweifeln, nicht selten ist auch die Schuld des Handelnden fraglich. In Fällen der umfassenden oder zumindest teilweisen Übertragung von Entscheidungen auf Maschinen ergeben sich somit offensichtlich Schwierigkeiten für die Konzepte von Schuld, aber auch von strafrechtlicher Verantwortung im weiteren Sinne – Vorhersehbarkeiten bei Fahrlässigkeitsdelikten, objektive Zurechnung, Nachweisbarkeit von Fehlverhalten etc.[72]

VI. Strafrechtliche Verantwortungsdiffusion und Alternativen

Die dargestellten Veränderungen mit Blick auf die strafrechtliche Verantwortlichkeit könnten zur Folge haben, dass in der digitalen Welt bzw. im Kontext Lernender Systeme kaum Strafen verhängt werden. Das kann jedoch zu Problemen führen, wenn die Gesellschaft durch die fehlende Übernahme persönlicher Verantwortung beunruhigt und die Normgeltung bezweifelt wird.

Aus diesem Grund könnten im Strafrecht Neujustierungen erforderlich werden.[73] Dabei sollte es jedoch nicht zu viel von seinen spezifischen Eigenschaften einbüßen; eine rein funktionelle Ausrichtung des Strafrechts, die auf das Element der individuellen Verantwortung verzichtet oder dieses zumindest reduziert, lässt sich mit dem deutschen Rechtssystem nur schwer vereinbaren. Die Zuschreibung individueller Verantwortung des Staates zum Bürger bzw. der Bürger untereinander ist grundlegend für unsere gegenseitige Wahrnehmung sowie unsere Selbstwahrnehmung. Dies spiegelt sich auch in der Menschenwürde nach Art. 1 Abs. 1 GG und den darauf basierenden strafrechtlichen Prinzipien. Zugleich sollte der Einzelne mit dieser Verantwortung auch nicht überfordert werden bzw. es ist genau zu prüfen, wer sinnvoller Adressat der Zuschreibung im konkreten Einzelfall ist. Das ist nicht immer der die letzte Entscheidung treffende Mensch, der ggf. durch die KI schon erheblich beeinflusst ist, vielmehr können je nach den Umständen auch Programmierer, Produzent oder auch andere Beteiligte als strafrechtlich Verantwortliche in Betracht kommen.

Möglicherweise müssen deshalb andere, nicht-strafrechtliche Lösungen gefunden werden, um so das gesellschaftliche Vertrauen in die Normgeltung wiederherzustellen bzw. die Vorteile der individuellen Verantwortlichkeit, dem Gefühl von Verantwortung für das eigene Verhalten, zu erhalten. Dies könnte auf Governance-Ebene erfolgen, ggf. auch primär im moralischen Bereich.

Aus rechtlicher Perspektive ist grundsätzlich durchaus auch vorstellbar, dass Verantwortlichkeiten systemisch bzw. bezogen auf Kollektive konzipiert werden, sowohl präventiv bezüglich der Notwendigkeit, bestimmte Bedingungen für den Einsatz von Maschinen oder Programmen einzuhalten, als auch retrospektiv mit Blick auf Haftungsaspekte, sei es durch die Bildung kollektiver Haftungsadressaten, sei es durch Versicherungssysteme. Derartige Lösungen sind jedoch in anderen Rechtsgebieten besser aufgehoben, also im öffentlichen Recht durch Vorgabe der angemessenen Bedingungen für die Entwicklung und den Einsatz moderner Technologien und im Zivilrecht durch Herbeiführung eines adäquaten Ausgleichs ggf. entstehender Schädigungen.[74]

Doch das Ausweichen auf andere Rechtsgebiete sollte nicht die einzige Lösung sein. Bei der Suche nach Alternativen und Umgestaltung des bestehenden Rechts, insbesondere des Strafrechts, sind nämlich folgende Aspekte von Bedeutung: Zum einen ist zu fragen, welche normativen Bedürfnisse die Gesellschaft hat. So kann eine erhebliche Rechtsgutsverletzung durch technologischen Fortschritt das Normvertrauen der Gesellschaft erschüttern – ein bloßer Verweis auf Entschädigungen oder bessere Regulierung für die Zukunft allein werden dieses Vertrauen nicht wiederherstellen können. Ähnliche Befunde lassen sich mit Blick auf das Opfer

Funktion enttäuscht der Täter durch die Tat das Vertrauen der Rechtsgemeinschaft in die Geltung der Norm. Durch Zuschreibung kann das Verhalten als fehlerhaft gedeutet und durch die daran anknüpfende Bestrafung das Normvertrauen wiederhergestellt werden. An die Person des Täters ist aufgrund seiner festgelegten gesellschaftlichen Rolle ein bestimmter Verhaltensanspruch zu stellen – er handelt schuldig, wenn er objektiv fixierte Standards verfehlt und den Anforderungen einer Maßstabsperson nicht gerecht wird. Diese Standards erfordern die Bereitschaft des Zuschreibenden, in der Situation, in der sich der Täter befindet, selbst Verantwortung zu akzeptieren. Für ein Schuldurteil bedarf es einer Organisationsalternative. *Roxins* Schuldkonzept (vgl. *Roxin* [Fn. 25], § 19 Rn. 36, 47) basiert maßgeblich auf der normativen Ansprechbarkeit des Täters, d.h. er muss zum Zeitpunkt der Tat in einer physischen und psychischen Verfassung sein, die ihm erlaubt, sich für ein normorientiertes Verhalten zu entscheiden – die dem zugrundeliegende Freiheitsannahme ist eine normative Setzung auf Basis des menschlichen Selbstverständnisses, freiheitlich handeln zu können, und der darauf aufbauenden bestehenden Ordnung des Soziallebens. Davon ausgehend handeln schwer gestörte oder unreife Menschen nicht schuldhaft – sie werden von Normen nicht erreicht und an sie werden keine sozialen Erwartungen zur Normeinhaltung gestellt.

[72] *Beck*, AJP/ PJA 2017, S. 183 (184).

[73] *Beck* (Fn. 4), S. 26.

[74] Zu Haftungsfragen auch *Keßler*, MMR 2017, 589 (592); *Weisser/Färber*, MMR 2015, 506 (510); *v. Bodungen/Hoffmann*, NZV 2016, 449 f.

erstellen: auch dessen Rechtsgutsverletzung wird durch eine bloß materielle Wiedergutmachung möglicherweise nicht umfassend abgegolten. Insofern ist der umfassende Verzicht auf Strafrecht nicht unproblematisch. Zudem stellen Strafnormen, aber auch die entsprechenden strafrechtlichen Verurteilungen, eben auch eine Form der normativen Kommunikation dar, ja sogar eine besonders starke und eindrückliche Form. Diese würde bei einem völligen Verzicht auf strafrechtliche Verantwortlichkeit in diesem Kontext fehlen. Dann wäre jedenfalls erforderlich, nach alternativen Formen einer solchen normativen Kommunikation zu suchen – und auch hier ist es eben nicht ausreichend, auf die anderen Rechtsgebiete zu verweisen, da diese die bestehenden gesellschaftlichen Normen und Werte nicht vergleichbar kommunizieren wie dies strafrechtliche Normen und Urteile können.[75]

Wie genau strafrechtliche Verantwortlichkeit erhalten bleiben kann, ohne dass inadäquate Inanspruchnahme der oft in kollektiven Strukturen verhafteten „human in the loops"[76] erfolgt, muss in den nächsten Jahren noch genau eruiert werden. Ggf. müssen Konzepte wie Handlung und Erfolgszurechnung überdacht werden[77] – möglicherweise gibt es Kontexte, in denen die strafrechtliche Haftung eher in der Herbeiführung von bestimmten Situationen und Entwicklungen zu sehen ist als in spezifischen Handlungen; auch könnte auf Interessen, auf Machtpositionen oder dergleichen abgestellt werden. Da hierzu jedoch eine Neukonstruktion strafrechtlicher Verantwortlichkeit erforderlich wäre, ist dies dem Gesetzgeber überlassen. Zudem ist eine grundlagenbezogene Diskussion darüber erforderlich, ob eine solche Neukonstruktion überhaupt möglich wäre und was sie ggf. für Konsequenzen für das sonstige Strafrecht hätte.[78]

VII. Aktuelle Entwicklungen

1. Neurotechnologie und KI

Digitalisierung hat viele Facetten. Eine Entwicklung, die durchaus gesellschaftlich bedeutsam sein könnte und zudem das Recht erheblich herausfordert, ist die Neurotechnologie.[79] Die Vermessung oder gar Beeinflussung des menschlichen Gehirns durch Technologie eröffnet völlig neue Dimensionen. Es handelt sich um eine neuartige, spezifische Verbindung von Mensch und Maschine, die ganz eigene Probleme mit sich bringt.[80] Durch Neurotechnologie wird es möglich sein, viele und sehr detaillierte Informationen über die Prozesse des Gehirns zu erhalten, ja vielleicht sogar – jedenfalls in einer bestimmten Art und Weise – „Gedanken lesen" zu können. Insbesondere in Verbindung mit Lernenden Systemen und Big Data werden hier zahlreiche, wichtige Informationen generiert und die Möglichkeiten, Gehirnströme zu beeinflussen, verbessert. Diese Eingriffe können invasiv, aber auch nicht-invasiv erfolgen, sie können Gefühle und Verhalten beeinflussen, sie können sogar Bewegungen induzieren. So ist es durchaus auch denkbar, dass über Gehirn-Computer-Schnittstellen Menschen gesteuert oder gar manipuliert werden; dies kann theoretisch sogar von einem anderen Gehirn ausgehen, so dass hier letztlich mehrere Gehirne gemeinsam agieren und eine Handlung aus dieser Verbindung hervorgehen könnte.[81]

Die Möglichkeiten der bildgebenden Verfahren haben bereits vor einigen Jahren eine wichtige Debatte im Strafrecht angestoßen bzw. wieder belebt: Die Debatte um die Willensfreiheit.[82] Experimente von *Libet* (u.a.) hatten in den Neurowissenschaften sowie in der Philosophie dazu geführt, dass die Prämissen und Konzeptionen zum „Freien Willen", zu menschlichen Entscheidungen und Handlungen, von nicht wenigen Stimmen hinterfragt wurden.[83] Unabhängig davon, ob die Experimente tatsächlich etwas Neues über die Willensfreiheit aussagen können,[84] war doch die aktuelle Auseinandersetzung mit den Bedingungen für eine strafrechtliche Verurteilung zweifellos fruchtbar. Die Auseinandersetzung darüber, inwieweit Willensfreiheit aus strafrechtlicher Perspektive überhaupt erforderlich ist[85], bzw. was genau Willensfreiheit aus dieser Perspektive bedeutet[86], erlaubt eine aktualisierte Bestimmung der Grundkonzeptionen unseres Strafrechts.

Doch auch die aktuellen Entwicklungen in der Neurotechnologie verändern strafrechtliche Konzeptionen. So wird zum Beispiel mit Blick auf mögliche Schuldunfähigkeit nach Anschalten eines „Hirnschrittmachers" diskutiert, ob – im

---

[75] *Beck* (Fn. 4), S. 17.
[76] Siehe https://machine-rockstars.com/lexikon/was-ist-human-in-the-loop/ (4.2.2020).
[77] So auch *Young-Whan*, in: Heinz (Hrsg.), Risiko und Prognose – Rechtliche Instrumente zur Regelung von Gefährdungen in Korea, Japan und Deutschland aus zivil-, öffentlich- und strafrechtlicher Sicht, 2006, S. 25 (26).
[78] Vgl. zur strafrechtlichen Verantwortlichkeit auch *Sander/Hollering*, NStZ 2017, 193 (195 ff.).
[79] Siehe https://www.bmjv.de/SharedDocs/Artikel/DE/2019/041219_KI__Gehirndaten_Tagung.html (4.2.2020).
[80] *Leiner*, ÄrzteZeitung v. 10.1.2018, abrufbar unter https://www.aerztezeitung.de/medizin/krankheiten/neuro-psychiatrische_krankheiten/article/955099/hirn-computer-schnittstelle-neurowissenschaftler-fordern-umfassenden-datenschutz.html (4.2.2020).
[81] mdr Wissen v. 14.9.2017, abrufbar unter https://www.mdr.de/wissen/faszination-technik/computer-gehirn-anschluss-100.html (4.2.2020);
Lenzen, Spektrum v. 12.2.2016, abrufbar unter https://www.spektrum.de/news/gehirn-computer-schnittstellen-werdenalltagstauglicher/1398145 (4.2.2020);
Griffin, Independent v. 10.7.2015, abrufbar unter https://www.independent.co.uk/life-style/gadgets-and-tech/news/brainet-scientists-could-make-an-internet-of-human-brains-10381069.html (4.2.2020).
[82] *Schiemann*, NJW 2004, 2056 (2059).
[83] *Reinelt*, NJW 2004, 2792 (2793); *Nørretranders*, Spüre die Welt, 1994, S. 311 ff.
[84] *Schiemann*, NJW 2004, 2056 (2057); *Roth*, Fühlen, Denken, Handeln, 2003, S. 521.
[85] *Reinelt*, NJW 2004, 2792.
[86] *Marlie*, ZJS 2008, 41 (44 ff.).

Sinne der actio libera in causa – die Verantwortlichkeit auch hier auf den Zeitpunkt des Anschaltens vorverlagert werden könnte. Zugleich ist in diesen Konstellationen aber zu bedenken, dass der Patient Symptome einer Krankheit bekämpfen möchte, es also gute und nachvollziehbare Gründe dafür gibt, dass er den Hirnschrittmacher trotz Kenntnis eines (potentiell) darauffolgenden kriminellen Verhaltens anschaltet. Aus diesem Grund lassen sich nicht alle Überlegungen etwa der alkoholinduzierten Schuldunfähigkeit auf diese Situation übertragen. So könnte man hier argumentieren, dass der Patient nicht für das Anschalten als solches, sondern dafür verantwortlich ist, dass er nicht gleichzeitig zumutbare Sicherungsmaßnahmen ergreift. Er wäre dann wegen Unterlassens strafbar. Diese Überlegungen sind zudem jedenfalls Anlass, die herkömmliche Zurechnungsstruktur der actio libera in causa zu überdenken.[87]

Aber auch darüber lassen sich aufgrund der dargestellten Entwicklungen Konzeptionen wie Täterschaft und Teilnahme oder die objektive Zurechnung etc. hinterfragen, denn wenn sich nicht einmal mehr klären lässt, auf wessen Gehirnströmen eine bestimmte Handlung basiert, sind die traditionellen strafrechtlichen Verantwortungsstrukturen offensichtlich nicht mehr ohne Weiteres anwendbar. Zugleich ist zu beachten, dass eine zu weitgehende Veränderung der Strukturen das Kernstrafrecht schwächen könnte. Wie auch in anderen Kontexten ist deshalb bei einer künftigen erforderlichen Veränderung des Strafrechts abzuwägen zwischen der Anpassung der strafrechtlichen Konzepte und der Erhaltung wichtiger grundlegender Prämissen.

2. Impossibility structures

Eine weitere Besonderheit der Digitalisierung, die das Recht vor ganz spezifische Herausforderungen stellen wird, ist die Entstehung sogenannter impossibility structures[88]. Hierbei handelt es sich um technische Strukturen, die aus sich heraus Rechtsverstöße verhindern sollen,[89] etwa ein Kraftfahrzeug, das das Überfahren einer roten Ampel verhindert oder ein Upload-Filter, der das Hochladen illegaler Inhalte auf Websites blockiert. Man kann durchaus bezweifeln, ob bzw. wann derartige Vorgehensweisen technisch realisierbar sein werden, ist es doch erforderlich, dass die Maschinen auch zulässige Ausnahmen anerkennen und entsprechend z.B. Güterabwägungen oder Verhältnismäßigkeitsprüfungen vornehmen. So ist es etwa durchaus zulässig, in einer Situation, in der sonst keine Kraftfahrzeuge oder andere Verkehrsteilnehmer auf der Straße sind, zur Rettung eines Schwerverletzten eine rote Ampel zu überfahren. Theoretisch ist jedoch zumindest denkbar, dass Maschinen derartige Einschätzungen vornehmen und somit die Technik die Einhaltung rechtlicher Vorschriften gewährleistet bzw. Rechtsverstöße verhindert.

Zum einen wäre hier natürlich auch zu diskutieren, wer verantwortlich ist, wenn die technischen Strukturen versagen, der Nutzer sich aber auf ihre Funktionsfähigkeit verlassen hat. Hier ergeben sich grundsätzlich im Vergleich zur Haftung bzw. Verantwortlichkeit für Lernende Systeme keine Besonderheiten[90] – aber natürlich ist es bei Strukturen, die gerade dazu dienen sollen, Rechtsverstöße zu verhindern, noch widersinniger, vom Nutzer zu verlangen, diese Strukturen zu überwachen bzw. zu kontrollieren und ihn für technische Fehlentscheidungen umfassend verantwortlich zu machen.

Eine Besonderheit, die hier jedoch zu diskutieren ist, ist die Frage, wie sich die Verantwortlichkeit generell, das Normvertrauen und die Normgeltung etc. verändern, wenn zumindest teilweise die Entscheidung über die Rechtsbefolgung auf Maschinen übertragen wird. Insofern wird von einigen Stimmen bereits jetzt hinterfragt, ob es nicht ein Recht auf Rechtsbruch geben müsste, oder anders gewendet, ein Recht darauf, sich freiwillig für die Einhaltung des Rechts zu entscheiden. Auch wenn es zunächst merkwürdig erscheint, dass das Recht selbst den Rechtsbruch zulassen sollte, ist doch zumindest nicht unplausibel, dass die Normgeltung geschwächt wird, wenn die Einhaltung des Rechts lediglich erzwungen wird und nicht auf einer eigenständigen Entscheidung beruht.[91]

VIII. Zusammenfassung

Digitalisierung und KI/Lernende Systeme wirken sich in erheblichem Maß auf die strafrechtliche Schuld aus und verändern die grundlegende Konzeption individueller Verantwortlichkeit. Unabhängig von den dogmatischen Details muss das Strafrecht sich auf diese Veränderungen einstellen, d.h. die Vorstellung individueller strafrechtlicher Verantwortung in diesen Lebensbereichen ist zu hinterfragen und neu zu justieren. Das betrifft die Schuld ebenso wie die Zurechenbarkeit, Nachweisfragen ebenso wie das Strafmaß. Auf diese Entwicklungen gibt es nicht die eine richtige Antwort, sondern verschiedene Antworten je nach konkretem Problemkontext. So ist eine Reduktion strafrechtlicher Verantwortung für bestimmte Aspekte nur ein erster Schritt bei der Lösung der Problematik, da dadurch das gesellschaftliche Bedürfnis nach Verantwortungszuschreibung, Absicherung gegen bestimmte gefährliche Technologien bzw. Technologieeinsätze und Schadensausgleich unbeantwortet bleibt. Hier werden in Zukunft weitergehende Lösungen gesucht werden müssen, die die mit Digitalisierung und KI/Lernenden Systemen einhergehende Verantwortungsdiffusion nachhaltig einhegen.

[87] Vgl. zu diesen Überlegungen auch *Beck*, ZIS 2018, 204 (205 f.).

[88] Zu diesem Konzept vgl. im Detail *Rademacher*, JZ 2019, 702.

[89] Darstellung anhand eines Beispiels bei Ionos by 1&1 v. 10.7.2019, abrufbar unter https://www.ionos.de/digitalguide/websites/online-recht/upload-filter/ (4.2.2020).

[90] Zur Verantwortungsfindung bei Lernenden Systemen *Bilski/Schmid*, NJOZ 2019, 657 (660).

[91] Geschlossen aus *Bolsinger*, PVS 2001, 3 (5–10).

„Künstliche Intelligenz“, Compliance und sanktionsrechtliche Verantwortlichkeit

Von Prof. Dr. **Kai Cornelius,** LL.M., Heidelberg

I. Einführung

In der mehr als sechzigjährigen „Geschichte“ der Forschung zur „Künstlichen Intelligenz“[1] hat sie Höhen und Tiefen erlebt, wurde nicht nur als marginal, sondern gar als Fehlentwicklung der Informatik betrachtet.[2] Das hat sich geändert: Dem Einsatz von „Künstlicher Intelligenz“ wird ein enormes Potential zugeschrieben. Die von der Europäischen Kommission eingesetzte „Hochrangige Expertengruppe für Künstliche Intelligenz“ sieht in ihr ein „vielversprechendes Mittel, um das Wohlbefinden von Individuum und Gesellschaft und das Gemeinwohl zu steigern sowie zur Förderung von Fortschritt und Innovation“ beizutragen.[3]

So soll *vertrauenswürdige* Künstliche Intelligenz (KI) in der Lage sein, dringende gesellschaftliche Probleme wie die Überalterung, eine wachsende soziale Ungleichheit und die Umweltverschmutzung wenn nicht zu lösen, so doch zumindest zu lindern.[4] Es lassen sich vielfältige Anwendungsbeispiele finden wie maschinelle Übersetzungsprogramme (z.B. deepl oder google translate), personalisierte Spracherkennungssoftware (z.B. Alexa, Siri oder google home) oder Systeme zum autonomen Fahren.[5] Insbesondere der Einsatz in der medizinischen Forschung ist vielversprechend, weil KI-Technologien genutzt werden könnten, um Krankheiten zielgerichtet – auf die jeweiligen Patienten zugeschnitten – zu behandeln, aber auch, um maßgeschneiderte vorbeugende Maßnahmen anbieten zu können.[6] Es darf aber nicht verkannt werden, dass KI-Systeme Risiken beispielsweise „im Hinblick auf Demokratie, Rechtsstaatlichkeit, Verteilungsgerechtigkeit oder den menschlichen Geist als solchen“ bergen.[7]

Um die Vorteile von KI-Systemen zu maximieren und gleichzeitig die mit deren Einsatz einhergehenden Risiken auszuschließen bzw. zu minimieren, hat die „Hochrangige Expertengruppe“ im April 2019 die „Ethik-Leitlinien für eine vertrauenswürdige KI“ vorgestellt.[8] Dabei geht sie davon aus, dass drei Komponenten erfüllt sein müssen: Das System muss a) rechtmäßig sein, also alle anwendbaren Gesetze und Bestimmungen einhalten, b) die Einhaltung ethischer Grundsätze und Werte garantieren, also ethisch sein und c) sowohl in technischer als auch in sozialer Hinsicht robust sein.[9] Dies betrifft den gesamten Lebenszyklus eines KI-Systems, also von der Entwicklung (einschließlich Forschung, Entwurf, Datenbereitstellung und Erprobung) über die Einführung (einschließlich der Umsetzung) und Nutzung[10] bis zur Postnutzungsphase (wie die Umsetzung von Löschkonzepten). Obwohl sich die genannten Ethik-Leitlinien nicht explizit mit der Frage einer rechtmäßigen KI beschäftigen, spiegeln sich die Komponenten b) und c) teilweise in bestehenden Gesetzen wider bzw. sind in solche zukünftig zu integrieren.[11]

Der nachfolgende Beitrag wendet sich auf der Grundlage dieser Ethik-Leitlinien der Frage zu, welche Risiken beim Einsatz von KI zu berücksichtigen sind, ob diese Risiken durch eine KI-Compliance eingedämmt werden können, inwieweit sanktionsrechtliche Verantwortlichkeiten betroffen

---

[1] Der Begriff der „Artificial Intelligence“ wurde geprägt durch *Carthy/Minsky/Rochester*, „A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence“, 1955, abrufbar unter http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html (3.2.2020); kritisch zum Begriff und zur deutschen Übersetzung als „Künstliche Intelligenz“ *Herberger*, NJW 2018, 2825 (2826 f.), der lieber von „extented intelligence“ spricht.

[2] *Kohlas*, in: Savory (Hrsg.), Expertensysteme: Nutzen für Ihr Unternehmen, 2. Aufl. 1989, S. 237.

[3] *Hochrangige Expertengruppe für Künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige KI, 2019, abrufbar unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425, S. 5 Abschnitt (9).

[4] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 42 Abschnitt (122), mit konkreten Anwendungsbeispielen in den Abschnitten (123 ff.).

[5] *Gaede*, Künstliche Intelligenz – Rechte und Strafen für Roboter?, 2019, S. 21 f.; *Lenzen*, Künstliche Intelligenz, 2018, S. 12 ff., 64 ff., 124 ff.

[6] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 42 f. Abschnitte (125 f.); vgl. die dort aufgeführten Beispiele zu den Projekten REVOLVER (Repeated Evolution of Cancer, https://www.healtheuropa.eu/personalised-cancer-treatment/87958, 3.2.2020), Live INCITE (personalisierte ehealth-Lösungen, www.karolinska.se/en/live-incite, 3.2.2020), CARESSES (Roboter für die Altenpflege, www.caressesrobot.org/en/project, 3.2.2020), MyHealth Avatar (digitale Sammlung und Zugänglichmachung von Langzeit-Gesundheitsdaten mit personalisierten Prognosen für Schlaganfall, Diabetes, Herz- Kreislauf-Erkrankungen und Bluthochdruckrisiko, www.myhealthavatar.org); vgl. auch *He/Baxter/ Xu/Zhou/Zhang*, Nature Medicine 25 (2019), 30 (34), mit KI-Beispielen, die bereits eine FDA-Zulassung in den USA erhalten haben.

[7] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 2 Abschnitt (2); vgl. auch die in Abschnitt 130 ff. aufgeführten KI-Beispiele zur Identifizierung und Ortung von Personen, zum verdeckten Einsatz, Bürgerinnen- und Bürgerbewertungen und tödlichen autonomen Waffensystemen.

[8] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 5 Abschnitt (10).

[9] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 2 Abschnitt (1), S. 6 Abschnitt (15).

[10] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 47 Abschnitt (147), zum Lebenszyklus von KI-Systemen.

[11] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 8 Abschnitt (24), S. 14 Abschnitt (49).

sind oder ob gegebenenfalls Handlungsbedarf für den Gesetzgeber besteht. Dabei geht es nicht um die Frage des Einsatzes von KI für die Lösung von Rechtsproblemen, sondern vielmehr um die durch die Nutzung von KI aufgeworfenen Rechtsprobleme.[12]

II. Künstliche Intelligenz (KI)

1. KI als Wissenschaftsdisziplin

Zunächst ist zu beachten, dass KI als wissenschaftliche Disziplin mehrere Ansätze und Techniken verfolgt wie das maschinelle Lernen („Deep Learning" mit der Fähigkeit der KI, durch die Auswertung von Datenmassen das eigene Leistungsvermögen selbständig zu steigern),[13] das maschinelle Denken (welches die Planung, Terminierung, Wissensrepräsentation und Schlussfolgerung sowie Suche und Optimierung betrifft) und die Robotik (welche die Steuerung, Wahrnehmung, Sensoren und Aktoren sowie weitere Techniken in cyber-physischen Systemen umfasst).[14]

2. Begriffsklärung

Um den Begriff der KI für die Zwecke des nachfolgenden Beitrages handhabbar zu machen, sei zunächst negativ beschrieben, dass es nicht um Systeme gehen soll, die ihre Umwelt selbständig erfassen, auf diese reagieren können und bestrebt sind, sie – ähnlich wie ein Mensch – als Grundlage der eigenen Existenz zu erhalten.[15] Denn solche selbstbewussten und sich die *Gründe* für ihr Handeln selbst setzenden KI-Systeme existieren (derzeit) ebenso wenig wie eine KI mit Gefühlen.[16] Es ist immer noch der Mensch, der das zu lösende Problem, die zu verfolgende Aufgabenstellung formuliert.[17] Den Algorithmen wird als Gebilde des menschlichen Geistes ihre Rolle durch den Menschen zugewiesen.[18]

Das Kennzeichen von KI-Systemen ist, dass sie „in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene agieren, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten und über die geeignete(n) Maßnahme(n) zur Erreichung des vorgegebenen Ziels entscheiden".[19] Andererseits wird unter Betonung des Aspektes der Nachahmung menschlichen Verhaltens schon dann von einem KI-System ausgegangen, wenn dieses menschliche Intelligenz nachahmt und Aufgaben erfüllen kann, deren Lösung bisher dem Menschen vorbehalten war.[20] Teilweise wird – unter Hervorhebung der Autonomie der Entscheidung des künstlichen Systems – von autonomen Softwareagenten[21] bzw. autonom agierenden Systemen[22] gesprochen. Um aus der Verwendung dieses Begriffes resultierenden etwaigen Missverständnissen vorzubeugen, ist zu betonen, dass die Autonomie dieser Systeme nur so weit geht, wie ihnen ein entsprechender Aktionsbereich durch den Menschen eingeräumt wurde.[23]

Entscheidend soll nachfolgend darauf abgestellt werden, dass die intelligenten Systeme ihre Entscheidungen aufgrund eigener Erfahrungs- und Lernprozesse treffen, die ihrem Verhalten zugrunde liegenden Algorithmen selbständig ändern und damit den Weg zur Lösung (der vom Menschen gestellten) Aufgabe[24] selbst bestimmen können,[25] wobei es sich um einen graduell stetig fortschreitenden Prozess handelt.[26] Es geht also entscheidend darum, dass ein „künstlicher Akteur vorliegt, der seine Umwelt wahrnimmt und auf Grund der Wahrnehmungen Akte ausführen kann".[27]

3. Risiken

Die enge Verbindung zwischen Mensch und Maschine und die Vernetzung der Systeme untereinander führen zu einer

[12] Vgl. *Herberger*, NJW 2018, 2825.
[13] *Eberl*, Smarte Maschinen, 2016, S. 41 ff., 91 ff.; dabei soll durch „deep" verdeutlicht werden, dass zwischen dem Input-Layer und dem Output-Layer noch ein oder mehrere Hidden-Layer liegen; *Frochte*, Maschinelles Lernen, 2019, S. 174; *Yuan*, RW 2018, 477 (490).
[14] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 47 Abschnitt (144).
[15] *Gaede* (Fn. 5), S. 22.
[16] *Gaede* (Fn. 5), S. 22; *Herberger*, NJW 2018, 2825 (2829).
[17] *Yuan*, RW 2018, 477 (492), mit einer genaueren Beschreibung des Trainings eines Lernalgorithmus.
[18] *Herberger*, NJW 2018, 2825 (2827).
[19] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 47 Abschnitt (143).
[20] *Gaede* (Fn. 5), S. 19.
[21] *Teubner*, AcP 218 (2018), 155 (156 Fn. 1); *Hengstenberg/Kirn*, Rechtliche Risiken autonomer und vernetzter Systeme, 2016, S. 59; *Zech*, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, 2016, S. 163 (168); *Gless/Weigend*, ZStW 126 (2014), 561; *Cornelius*, MMR 2002, 353; *ders.*, ZRP 2019, 8; dieser weite Begriff umfasst auch Roboter (hierzu *Hilgendorf*, in: Barton/Eschelbach/Hettinger/Kempf/Krehl/Salditt [Hrsg.], Festschrift für Thomas Fischer, 2018, S. 99 [101]; *Simmler/Markwalder*, ZStW 129 [2017], 20 [23], und cyberphysische Systeme, *Mansdörfer,* in: Barton/Eschelbach/Hettinger/Kempf/Krehl/Salditt [Hrsg.], Festschrift für Thomas Fischer, 2018, S. 155 [156]), soweit diese autonome Entscheidungen treffen können.
[22] *Schulz*, Verantwortlichkeit bei autonom agierenden Systemen, 2015, S. 44.
[23] *Herberger*, NJW 2018, 2825 (2827).
[24] Diese wird immer vom Menschen vorgegeben, da (bisher) keine selbstbewusste KI existiert, vgl. oben die Ausführungen zu Fn. 16.
[25] *Zech* (Fn. 21), S. 171; *Schulz* (Fn. 22), S. 44; *Yuan*, RW 2018, 477 (481).
[26] Vgl. *Silver/Hubert/Schrittwieser/Antonoglou/Lai/Guez/ Lanctot/Sifre/Kumaran/Graepel/Lillicrap/Simonyan/Hassabis*, Science 362 (2018), 1140, zum „Reinforcement Learning" bei welchem vorab nur noch grundlegende Regeln und Bewertungskriterien definiert werden, bevor das System in einen Selbstlernprozess eintritt; vgl. auch *Erhardt/Mona*, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, 2016, S. 61 (78 f., 92); *Yuan*, RW 2018, 477 (487).
[27] *Gaede* (Fn. 5), S. 21.

mangelnden Transparenz.[28] Es werden rechtliche Verantwortungslücken befürchtet. Es sei nur schwer erkennbar, worauf eine Entscheidung[29] – und damit die Verantwortung für die Folgen derselben – zurückzuführen ist.[30] Um diesen Lücken zu begegnen, hat das Europäische Parlament gegenüber der Kommission die Einführung einer elektronischen Person empfohlen.[31] Dieser Vorschlag wird von Experten in einem offenen Brief an die EU-Kommission „Artificial Intelligence and Robotics“ massiv angegriffen, da die Etablierung eines rechtlichen Status einer „Elektronischen Person“ auf einer „verzerrten Wahrnehmung“ beruhe und „unangebracht“ sei.[32] Technisch würden die „aktuellen Fähigkeiten selbst der am weitesten fortgeschrittenen Roboter“ überschätzt und auch ethisch und rechtlich dürfe ein Persönlichkeitsstatus nicht vom Modell der „natürlichen Person“ abgeleitet werden, da dies sowohl der Europäischen Grundrechtecharta als auch der Europäischen Menschenrechtskonvention widersprechen würde.[33]

Auch von juristischer Seite wird die Diskussion geführt, ob und inwieweit einem mit einer entsprechenden Intelligenz ausgestattetem Computersystem eine Rechtspersönlichkeit zuzusprechen ist.[34] Dabei wird dafür eingetreten, dass diesen „ein sorgfältig kalibrierter Rechtsstatus“ zuerkannt wird,[35] der autonome (KI-)Systeme durchaus als teilrechtsfähige Rechtssubjekte einordnet.[36] Denn nur Rechtssubjekte können Träger von Rechten und Pflichten und damit auch Adressaten von Rechtsnormen (also dem Recht unterworfen) sein.[37]

Dies ist insoweit nachvollziehbar, als es um eine enge Verflechtung von digitalen und humanen Handlungen geht, so dass das Ziel juristischer Haftungsnormen das Erfassen eines Gesamthandelns solcher Hybride bzw. eines umfassenden Vernetzungszusammenhanges sein sollte.[38] Deshalb geht es vorrangig nicht um die Frage entweder keiner oder einer vollen Rechtsfähigkeit (insbesondere durch Schaffung einer e-Person), sondern um die Entwicklung situationsadäquater Rechtskonstruktionen, die entsprechend der jeweiligen Rolle in der Mensch-Maschine-Interaktion abgestimmt sind.[39]

Bei der rechtlichen Bewertung geht es um die Einordnung des Autonomierisikos (resultierend aus „eigenständigen Entscheidungen“ der KI-Systeme), des Verbundrisikos (resultierend aus der engen Kooperation von Mensch und KI-System) und des Vernetzungsrisikos (resultierend aus der engen Verflechtung mit anderen elektronischen Systemen).[40]

a) Autonomierisiko

Dem Autonomierisiko kommt eine besondere Bedeutung zu, da dieses zu der Frage führt, ob KI-Systeme als handlungsfähige Akteure im Recht anerkannt werden.[41] In diesem Zusammenhang ist es von entscheidender Bedeutung, dass keine Parallelen zur Handlungsfähigkeit menschlicher Akteure gezogen werden, sondern es zielführender ist, solche zu anderen nicht-menschlichen Akteuren (wie juristischen Personen, dem Staat oder der Kirche) zu ziehen.[42]

Solche Gedankenkonstrukte wie das einer künstlichen Person („artificial person“)[43] sind im Rechtssystem nichts Ungewöhnliches.[44] Dabei werden diese Gebilde regelmäßig losgelöst von den sie konstituierenden Individuen betrachtet. So wird der Staat vom Herrscher getrennt, damit dieser nicht mit dem Tod des Menschen endet; Klöster bestehen unabhängig von Mönchen,[45] und Aktiengesellschaften unabhängig von den Vorständen. Dies verdeutlicht bereits das Vergeistigte an diesen Konstruktionen: Im Gegensatz zum Menschen, der in einem modernen Rechtsstaat mit seiner Geburt als Rechtssubjekt anerkannt wird, müssen die Gedankengebilde erst rechtlich verfasst und vom Rechtssystem anerkannt werden.[46]

Die Grundlage hierfür ist, als soziales Substrat nicht eine Vielheit konkreter Menschen zu sehen, sondern den Kollektivakteur als Kette von Mitteilungen bzw. Entscheidungs-

[28] *Spiecker*, CR 2016, 698 (701 f.).
[29] Vgl. zur systemtheoretischen Sicht, die autonome Entscheidung selbst (als Handlung) in die Verantwortung zu nehmen, die Ausführungen zu Fn. 71.
[30] Vgl. nur *Mayinger*, Die künstliche Person, 2017, S. 213 ff.
[31] Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103 (INL), Ziff. 59 f.), abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//DE (3.2.2020).
[32] Abrufbar unter http://www.robotics-openletter.eu/ (3.2.2020).
[33] Siehe erneut http://www.robotics-openletter.eu/ (3.2.2020).
[34] *Beck*, JR 2009, 229; *Cornelius*, MMR 2002, 353 (354); *Gless*, GA 2017, 324; *Wiebe*, Die elektronische Willenserklärung, 2002, S. 80; Entschließung des Europäischen Parlaments (Fn. 31), Ziff. 59 f.
[35] *Teubner*, AcP 218 (2018), 155 (177).
[36] *Teubner*, AcP 218 (2018), 155 (178 ff.); *Schirmer*, JZ 2019, 711 (716); einen anderen Ansatz (Transformation von Maschinenarbeit in Schuldnerverhalten qua Rechtsfiktion) bevorzugend *Klingbeil*, JZ 2019, 718 (721 ff.).
[37] *Schuhr*, Rechtstheorie 46 (2015), 225 (251); vgl. auch *Kelsen*, Reine Rechtslehre, 1934, S. 53; *Schirmer*, JZ 2019, 711 (715).
[38] *Teubner*, AcP 218 (2018), 155 (162).
[39] Ebenso *Schirmer*, JZ 2016, 660 (663 ff.); *ders*., JZ 2019, 711 (716 ff.); *Teubner*, AcP 218 (2018), 155 (163); *Gruber*, Bioinformationsrecht, 2015, S. 250 ff.
[40] *Teubner*, AcP 218 (2018), 155 (163 ff.; 196 ff.); *Cornelius*, ZRP 2019, 8 (9 f.).
[41] Vgl. *Zech* (Fn. 21), S. 191 ff.; *Cornelius*, ZRP 2019, 8 (9).
[42] *Teubner*, AcP 218 (2018), 155 (165); *Ortmann*, NZWiSt 2017, 241 (243 ff.).
[43] Vgl. nur *Hobbes*, Leviathan, 1651, Kap. XVI, wobei das Titelblatt den Staat als eigene Person symbolisiert, der aus vielen einzelnen Personen zusammengesetzt ist; *Schuhr*, Rechtstheorie 46 (2015), 225 (256 f.).
[44] *Schuhr*, Rechtstheorie 46 (2015), 225 (254).
[45] Zu diesen Beispielen *Schuhr*, Rechtstheorie 46 (2015), 225 (254).
[46] *Schuhr*, Rechtstheorie 46 (2015), 225 (255).

ketten.[47] Wenn es gelingt, entsprechende „Beiträge" von KI-Systemen als kommunikative Ereignisse in der Form einer Einheit von Information, Mitteilung und Verstehen einzuordnen,[48] werden die Parallelen zu anderen künstlichen Entitäten deutlich.[49] Dabei sollte man nicht der Fehlvorstellung unterliegen, den Algorithmen die psychischen Kompetenzen von Menschen zuzubilligen.[50] Vielmehr kommt es für das „Verstehen" innerhalb eines Kommunikationsprozesses zwischen Mensch und Maschine darauf an, dass die „Antwort" des Algorithmus die „Frage" des Menschen in der Form einer eigenen Differenz zwischen Mitteilung und Information „versteht" und nicht darauf, ob das Innere des Algorithmus die Äußerung eines Menschen nachvollzieht oder nicht.[51]

Die Teilnahme an der Kommunikation sowie Zielgerichtetheit und Mittelwahl (als intentionales Handeln) eines KI-Systems dürften zwar notwendige, aber noch nicht hinreichende Bedingungen sein, um eine rechtlich relevante Autonomie annehmen zu können. Allerdings würde es zu weit gehen, eine (irgendwie geartete – auch beschränkte) Rechtsfähigkeit erst bei einer Art digitalem Selbstbewusstsein anzunehmen.[52] Diese Argumentation orientiert sich mehr an Ähnlichkeiten zur natürlichen Person anstatt an künstlichen Entitäten.[53] Dabei wird Rechtsfähigkeit mit Rechtspersönlichkeit gleichgesetzt.[54] *Teubner* schlägt deshalb vor, bei einer „Entscheidung unter Ungewissheit" von einer rechtlich relevanten Autonomie auszugehen; zwischen solchen Entscheidungen ist dann der Zusammenhang zur (rechtlichen) Verantwortung (als Einstehenmüssen für Entscheidungen unter Ungewissheit) herzustellen.[55] Denn die Notwendigkeit, von einem autonomen Handeln im rechtlichen Sinne auszugehen, ist erst gegeben, wenn das KI-System (bei der Verfolgung der durch den Menschen gestellten Aufgabe) Entscheidungsvarianten hat, aus welchen es dann nach Gewichtung verschiedener Kriterien die nach seiner Programmierung und Lernleistung optimale auswählt und nicht prognostizierbare Entscheidungen trifft.[56] Die Voraussetzungen dafür sind eine Programmierung des Systems, die ihm die Möglichkeit gibt, zwischen mehreren Varianten zu entscheiden, wobei die KI selbst die Entscheidung nach einer von ihr vorgenommenen Optimierung treffen muss und auch ein Programmierer das Agieren nicht mehr voraussagen, sondern nur noch ex post korrigieren kann.[57]

Im Endeffekt ist es das Rechtssystem selbst, welches die rechtlich relevante Grenze zwischen instrumentalisiertem und autonomen Handeln festlegen muss, aber unter Zugrundelegung der wissenschaftlich erforschten Eigenständigkeit digitaler Entitäten.[58] Dabei hilft wieder ein Blick auf die formalen Organisationen: So wie es für deren rechtliche Handlungsfähigkeit nicht auf innere psychische Zustände (eine innere Denkfähigkeit) ankommt, ist dies ebenso bei KI-Systemen unerheblich; vielmehr kommt es auf die Kommunikation mit den Nutzern mitsamt den daraus erwachsenen Konsequenzen an (weshalb auch von artificial communication anstatt artificial intelligence gesprochen wird).[59]

Eine weitere notwendige Voraussetzung für Autonomie ist das willentliche Handeln, wobei es auch dort nicht um einen inneren psychischen Zustand des KI-Systems geht, sondern vielmehr um die Zuschreibung zielgerichteten Handelns durch die jeweiligen Beobachter.[60] Systemtheoretisch kann so der erhöhten Komplexität, die sich einer physikalischen Beschreibung entzieht, durch ein Sozialsystem (wie dem Recht) begegnet werden, indem KI-Systemen gewisse Intentionen zugerechnet und dementsprechend Konsequenzen für die Rechtswirkungen gezogen werden.[61]

b) Verbundrisiko

Insbesondere das aus der engen Kooperation von Mensch und KI resultierende Verbundrisiko kann angemessen nur durch eine Berücksichtigung des Handelns im Mensch-Maschine-Verbund als Kollektivphänomen Berücksichtigung finden.[62] Der Verbund aus Mensch und Maschine tritt mit den Dritten in eine kommunikative Beziehung, wobei auf diesen Verbund als eigenständiges Handlungssystem (als Einheit) und nicht auf den jeweils beteiligten Menschen oder Algorithmus abzustellen ist.[63] Dies entspricht auch der Selbstwahrnehmung einer formalen Organisation als korporativer Akteur.[64] Insoweit sind die Fragen ähnlich wie bei der Verantwortlichkeit formaler Organisationen, nämlich die Nicht-Personalisierbarkeit und Unaufklärbarkeit von Kausalzusammenhängen zwi-

[47] *Teubner*, AcP 218 (2018), 155 (165); *Ortmann*, NZWiSt 2017, 241 (243 ff.).
[48] Vgl. *Luhmann*, Soziale Systeme: Grundriß einer allgemeinen Theorie, 1984, S. 191 ff.
[49] So *Teubner*, AcP 218 (2018), 155 (164).
[50] *Esposito*, ZfSoz 2017, 249 (250); *Teubner*, AcP 218 (2018), 155 (167).
[51] *Teubner*, AcP 218 (2018), 155 (168).
[52] *Teubner*, AcP 218 (2018), 155 (173).
[53] Vgl. *Hacker*, RW 2018, 243, 251; *Mayinger* (Fn. 30), S. 14.
[54] *Schirmer*, JZ 2019, 711, der diese Differenzierung prägnant herausarbeitet; vgl. aber *Klingbeil*, AcP 217 (2017), 848 (859).
[55] *Teubner*, AcP 218 (2018), 155 (174 f.).
[56] *Mayinger* (Fn. 30), S. 14; *Teubner*, AcP 218 (2018), 155 (174).
[57] *Teubner*, AcP 218 (2018), 155 (174).
[58] *Matthias*, Automaten als Träger von Rechten, 2. Aufl. 2010, S. 43 ff.; *Teubner*, AcP 218 (2018), 155 (170); *Cornelius*, ZRP 2019, 8 (9).
[59] Vgl. *Teubner*, AcP 218 (2018), 155 (171 f.); *Esposito*, ZfSoz 2017, 249 (250); *Cornelius*, ZRP 2019, 8 (9).
[60] *Dennett*, The Intentional Stance, 1987, S. 17; *Matthias* (Fn. 58), S. 41 ff.; *Teubner*, AcP 218 (2018), 155 (172); *Cornelius*, ZRP 2019, 8 (9).
[61] *Teubner*, AcP 218 (2018), 155 (172); *Cornelius*, ZRP 2019, 8 (9).
[62] Vgl. *Teubner*, AcP 218 (2018), 155 (196); *Cornelius*, ZRP 2019, 8 (10).
[63] *Teubner*, AcP 218 (2018), 155 (198).
[64] *Ortmann*, NZWiSt 2017, 241 (246).

schen Straftaten und den Entscheidungen Einzelner aufgrund diffuser innerorganisatorischer Bedingungen.[65]

Deshalb kann – aus ganz ähnlichen Gründen wie bei der rechtlichen Erfassung von Verbänden – diskutiert werden, ob ein solcher Verbund als eine Zurechnungs- und Haftungseinheit angesehen werden sollte, ohne dass (wie vom individualrechtlichen Standpunkt aus gesehen) eine klare Trennung der jeweiligen Einzelhandlungen von Mensch und KI-System vorgenommen wird.[66] Eine solche kollektivrechtliche Verbundlösung ist gegenüber einer individualrechtlichen Repräsentantenlösung[67] sicherlich sehr viel weitgehender, dürfte die Realität der Mensch-Maschine-Interaktion aber dann am besten abbilden, wenn die KI-Systeme (z.B. als Chat-Bots) im Sozialleben nicht eindeutig identifizierbar teilnehmen, sondern nur in einem Interaktionszusammenhang mit anderen Akteuren wahrgenommen werden.[68]

c) Vernetzungsrisiko

Besondere Herausforderungen birgt das aus der engen Verflechtung mit anderen Computern resultierende Vernetzungsrisiko. Mit der Komplexität der Vernetzungen der KI-Systeme untereinander[69] steigt die Schwierigkeit, die Handlungsträger und Kausalzusammenhänge aufzuklären.[70] Die Zurechnung dieser Vielzahl sozialer und digitaler Prozesse an einen einzelnen (individuellen oder kollektiven) Akteur stößt an ihre Grenzen. Insofern wird aus systemtheoretischer (sich von Organisationen lösender und auf die Handlungen abstellender) Sicht vorgeschlagen, als Zurechnungspunkt nicht den einzelnen Entscheidungsträger (ob Mensch, Organisation, Netzwerk oder KI-System als Handlungsträger), sondern die autonome Entscheidung selbst (als Handlung) in die Verantwortung zu nehmen.[71] Dabei soll es letztlich um eine Art kollektives Risikomanagement zur Steuerung zukünftigen Verhaltens (wie die Programmierung und die Einsatzbedingungen von Algorithmen) gehen, so dass Risiken bereits präventiv eingedämmt werden.[72] In Ergänzung hierzu kommt auch eine retrospektive Betrachtung infrage, um aus aufgetretenen Fehlern für die Zukunft lernen zu können.

III. Einhaltung von Rechtsregeln

Die „Hochrangige Expertengruppe“ hat vollkommen zu Recht als erste Komponente für eine vertrauenswürdige KI darauf hingewiesen, dass sicherzustellen ist, dass Entwicklung, Produktion und Vertrieb sowie die Nutzung von KI-Systemen unter Einhaltung von rechtlichen Vorgaben zu erfolgen haben.[73] Dabei geht es nicht allein um die implementierte Technik im KI-System selbst, sondern es muss auf eine ganzheitliche Systemgestaltung geachtet werden, was auch die Einbeziehung von organisatorischen Prozessen, vertraglichen Zusammenhängen und (bei einem Unternehmen) unternehmensinternen Vorgaben bedeutet.

1. Ausgangspunkt

Relevante Rechtsquellen sind nicht nur das Primär- (also die EU-Verträge nebst der EU-Grundrechtecharta) und das Sekundärrecht (wie die Datenschutzgrundverordnung, aber auch Richtlinien zur Antidiskriminierung, Produktsicherheit und -haftung, Verbraucher- und Gesundheitsschutz) der Europäischen Union, sondern auf internationaler Ebene auch die Menschenrechtsverträge der Vereinten Nationen und die Übereinkommen des Europarates (insbesondere die Europäische Menschenrechtskonvention) sowie die nationalen Vorschriften.[74] Dabei ist zu beachten, dass es in Abhängigkeit von dem jeweiligen Anwendungsbereich der KI-Systeme zur Anwendung ganz unterschiedlicher rechtlicher Vorschriften kommen kann (z.B. sind bei einem Medizinprodukt die entsprechenden rechtlichen Vorschriften wie die Verordnung über Medizinprodukte im Gesundheitssektor oder das Medizinproduktegesetz zu beachten).[75]

2. KI-Compliance

Damit geht es im Endeffekt um eine typische Aufgabe, die der sog. Compliance zugeschrieben wird – das KI-System muss compliant sein (KI-Compliance). Die KI-Compliance selbst betrifft einerseits die Frage, ob die KI-Systeme alle relevanten allgemein geltenden rechtlichen Vorgaben nachweislich eingehalten haben.[76] Andererseits können auch solche Risiken berücksichtigt werden, die aus sonstigen externen Regelwerken (wie Verträgen, Normen oder Standards, Zertifikaten oder Richtlinien anderer Institutionen) aber auch internen Festlegungen (wie Unternehmensrichtlinien, Organisations- oder Verfahrensanweisungen, Service-Level-Agreements) resultieren.[77] Überdies zählen zu den rechtlichen Vorgaben auch die Rechtsprechung, durch die die jeweiligen Rechtsnormen und auch Sorgfaltspflichten konkretisiert und soweit notwendig auch den geänderten gesellschaftlichen Rahmenbedingungen angepasst werden (soweit dies mit dem

[65] *Bergmann*, MSchrKrim 2016, 3 (10); *Kölbel*, NZWiSt 2018, 407 (408) m.w.N. in Fn. 14 und 15; *Cornelius*, ZRP 2019, 8 (10).
[66] *Teubner*, AcP 218 (2018), 155 (198 f.).
[67] Vgl. *Gruber*, in: Günther/Hilgendorf (Hrsg.), Robotik und Gesetzgebung, 2013, S. 123 (158); *Klingbeil,* JZ 2019, 718 (723 f.).
[68] *Teubner*, AcP 218 (2018), 155 (200 f.).
[69] Vgl. *Beck,* in Hilgendorf/Seidel (Hrsg.), Robotics, 2017, S. 227 (233 f.); *Spiecker*, CR 2016, 698 (701); *Cornelius*, ZRP 2019, 8 (10).
[70] Vgl. *Zech* (Fn. 21), S. 170; *Cornelius*, ZRP 2019, 8 (10).
[71] *Teubner*, AcP 218 (2018), 155 (202 f.); *Cornelius*, ZRP 2019, 8 (10).
[72] *Teubner*, AcP 218 (2018), 155 (203); *Cornelius*, ZRP 2019, 8 (10).
[73] Siehe oben Fn. 9.
[74] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 8 Abschnitt (21).
[75] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 7 Abschnitt (20).
[76] Vgl. insoweit zur IT-Compliance *Klotz/Dorn*, HMD 2008, Heft 5 Bd. 263, 5 (8).
[77] *Klotz/Dorn*, HMD 2008, Heft 5 Bd. 263, 5 (11).

strafrechtlichen Gesetzlichkeitsprinzip nach Art. 103 Abs. 2 GG vereinbar ist).[78] Hierzu können Parallelen zum methodischen Ansatz der Automatisierung von Compliance ins Auge gefasst werden. Dieser sieht vor, dass rechtliche Vorgaben und jeweils relevante Regelwerke in IT-Systeme übersetzt werden, wobei für die Übersetzung der Compliance-Anforderungen in eine formale Form auf Policy-Sprache zurückgegriffen wird.[79] Jedoch sind – aus technischer Sicht – die jeweiligen Besonderheiten von KI-Systemen zu berücksichtigen. Denn KI-Systeme folgen gerade nicht – wie logische (automatisierte) Systeme – einer strengen Logik.

3. Erklärbare KI (oder explainable AI)

Hierbei kommt die Forschungsrichtung der so genannten erklärbaren KI (oder explainable AI) ins Spiel.[80] Durch sie soll sichergestellt werden, dass die jeweiligen Prozesse und Entscheidungen der KI-Systeme nachvollziehbar und erklärbar sind.[81] Dabei geht es auch darum aufzuklären, was Ursache und Wirkung und was ggf. nur eine Korrelation ist.[82] Letztlich ist diese Erklärbarkeit[83] nicht nur notwendig, damit die Nutzer ein Vertrauen zu den KI-Systemen entwickeln können,[84] sondern auch für die Frage der Feststellung von Verantwortlichkeiten für den Fall, dass es zu ungewollten Ergebnissen (wie beispielsweise einer Körperverletzung von Menschen) kommt.[85] Durch die Gewährleistung der Rückverfolgbarkeit und Nachprüfbarkeit der Daten, Algorithmen und Prozesse, die zu den entsprechenden Entscheidungen eines KI-Systems geführt haben, können nicht nur zukünftige Fehler verhindert, sondern auch die Gründe für eine fehlerhafte Entscheidung der KI ermittelt werden.[86] Eine besondere Bedeutung hat dies für sensible Situationen menschlicher Entscheidungsfindung (wie bei medizinischen Entscheidungsunterstützungssystemen), in denen den menschlichen Entscheidern zumindest eine Chance auf Überprüfung der Plausibilität der Ergebnisse eingeräumt werden muss, indem diese nachvollziehbar, transparent und erklärbar gemacht werden.[87] Dies gilt umso mehr, als aus Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h und Art. 22 DSGVO, insbesondere aus dem Recht auf aussagekräftige Informationen über die involvierte Logik, ein „Recht auf Erklärbarkeit" bei automatisierten Einzelentscheidungen abgeleitet werden wird.[88]

Allerdings ergibt sich eine besondere Schwierigkeit daraus, dass es nicht immer möglich ist, zu erklären, warum ein KI-System (insbesondere wenn es auf der Basis neuronaler Netze arbeitet) zu bestimmten Ergebnissen gekommen ist, also letztlich der Zusammenhang zwischen Eingabe- und Ausgabewerten nicht explizit darstellbar ist.[89] So ist es beispielsweise bei Deep-Learning-Algorithmen[90] eine besondere Herausforderung, zu erklären, warum es gerade zu bestimmten Ausgabewerten kommt und wie sich dies auf die Datenverarbeitung im gesamten Netzwerk auswirkt.[91] Dennoch wäre es ein Fehlschluss, deshalb davon auszugehen, dass eine

[78] Vgl. zum an die Rechtsprechung gerichteten Optimierungs- bzw. Präzisierungsgebot BVerfGE 126, 170 (198); *Cornelius*, GA 2015, 101 (118); *ders*., Verweisungsbedingte Akzessorietät, 2016, S. 352 f.

[79] Ausführlich hierzu *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 ff.

[80] *Waltl/Vogl*, Jusletter IT, 22.2.2018, abrufbar unter https://wwwmatthes.in.tum.de/pages/1hqrlk3h1m4l6/Explainable-Artificial-Intelligence-the-New-Frontier-in-Legal-Informatics (3.2.2020).

[81] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 27 Abschnitt (99).

[82] *Holzinger*, in: Gesellschaft für Informatik (Hrsg.), Informatiklexikon, Stand: 23.4.2018, abrufbar unter https://gi.de/informatiklexikon/explainable-ai-ex-ai/ (3.2.2020).

[83] Beim Verstehen als Brücke zwischen Wahrnehmen und Entscheiden kommt es auf die intellektuelle Erfassung des Zusammenhanges (den Kontext) an, während es beim Erklären (Interpretieren) darüber hinaus darum geht, die Ursachen eines beobachteten Sachverhaltes mit seinen logischen und kausalen Zusammenhängen sprachlich zu beschreiben. Dabei sind für den Menschen Bild, Sprache und Text direkt verständlich, nicht aber abstrakte Vektorräume, die dann in eine für den Menschen verständliche Form „zurückzuübersetzen" sind, vgl. *Holzinger*, in: Gesellschaft für Informatik (Hrsg.), Informatiklexikon, Stand: 23.4.2018, abrufbar unter https://gi.de/informatiklexikon/explainable-ai-ex-ai/ (3.2.2020).

[84] Zu diesem Aspekt vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 16 Abschnitt (53).

[85] Deshalb formuliert *Herberger*, NJW 2018, 2825 (2828), auch völlig zu Recht, dass „das Einfordern von Erklärungen in juristischer Hinsicht unabdingbar" ist.

[86] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 22 Abschnitt (76), zum Grundsatz der Rückverfolgbarkeit sowie S. 24 Abschnitt (88) zur Nachprüfbarkeit.

[87] *Holzinger*, in: Gesellschaft für Informatik (Hrsg.), Informatiklexikon, Stand: 23.4.2018, abrufbar unter https://gi.de/informatiklexikon/explainable-ai-ex-ai/ (3.2.2020); vgl. auch *He/Baxter/Xu/Zhou/Zhang*, Nature Medicine 25 (2019), 30 (32); *Gang Luo*, Health Information Science and System (HISS) Bd. 4 Nr. 2 März 2016, 1, abrufbar unter http://pages.cs.wisc.edu/~gangluo/explain_prediction_results.pdf (3.2.2020).

[88] *Dix*, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), Nomos Kommentar, Datenschutzrecht, 2019, DSGVO Art. 25 Rn. 25 m.w.N., wobei die Reichweite umstritten ist, vgl. *Wachter/Mittelstadt/Floridi*, Science Robotics, 2 (6), die davon ausgehen, dass „only a general, easily understood overview of system functionality is likely to be required".

[89] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 27 Abschnitt (99).

[90] Vgl. hierzu oben zu Fn. 13.

[91] *Yuan*, RW 2018, 477 (490); *Sachverständigenrat für Verbraucherfragen*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, 2018, S. 54 f.

Evaluation dieser Systeme nicht möglich ist.[92] Vielmehr ist es gerade bei diesen „Blackbox“-Algorithmen[93] notwendig, besonders auf die Rückverfolgbarkeit, Nachprüfbarkeit und transparente Kommunikation des Systems zu achten.[94] Dies bedeutet, dass die Daten, das System und die Geschäftsmodelle als systemrelevante Komponenten der KI für die Anwender transparent sein müssen.[95] Denn letztlich beruhen auch diese Algorithmen auf einem Training und damit auf einem menschlichen Verhalten. Der Mensch definiert, welche Aspekte vom System als positiv oder negativ anzusehen sind.[96]

4. Präventiver Ansatz: KI-Compliance by Design durch technologische Impossibility Structures

Mittels technikbezogener Vorgaben kann präventiv darauf hingewirkt werden, dass durch die KI-Systeme erst gar kein dem geltenden Recht widersprechendes – erst recht ein für den Menschen schädliches Verhalten – ausgeführt bzw. erlernt werden kann.[97] Solch eine Begrenzung der technischen Möglichkeiten kann möglichst frühzeitig – am besten bereits in der Entwicklungsphase des Systems – durch einen „By-Design Ansatz“ berücksichtigt werden.[98] Terminologisch kann hierfür auch der Begriff der impossibility structures fruchtbar gemacht werden, der für Mechanismen steht, die Rechtsverstöße bereits rein physisch unmöglich machen.[99] Allerdings geht es hier darum, dass es bereits dem KI-System selbst unmöglich gemacht werden soll, sich außerhalb der Grenzen des Rechts (bzw. auch weitergehender Vorgaben) zu bewegen.[100]

Ein solcher Ansatz erfordert, dass bereits ex ante die möglichen Aktivitäten und Zustände einschließlich etwaiger Ausnahmen erkennbar sind.[101] Auch wenn dies in Reinform nicht möglich ist, da alle Aktivitäten und Zustände nicht voraussehbar sind, lässt sich durch eine partielle Umsetzung die Komplexität verringern.[102] Dabei können zwei unterschiedliche Strategien verfolgt werden: Einerseits können in Form einer „Blacklist“ diejenigen Aktivitäten und Zustände spezifiziert werden, die als nicht-compliant angesehen und deshalb nicht zugelassen werden.[103] Andererseits können in Form einer Positivliste die Aktivitäten und Zustände spezifiziert werden, die compliant sind.[104] Soweit dann Abweichungen von diesen Zuständen festgestellt werden, bedeutet dies noch nicht zwingend, dass ein Verstoß gegen Compliance-Vorschriften vorliegt, aber dass zusätzliche Maßnahmen im Sinne des retrospektiven Ansatzes zu ergreifen sind.[105]

5. Retrospektiver Ansatz: KI-Compliance by detection durch intelligent surveillance

Der retrospektive Ansatz der KI-Compliance by Detection zielt darauf, dass durch eine vollständige und korrekte Aufzeichnung von tatsächlichen Aktivitäten und Zuständen eine ex-post-Bewertung ermöglicht wird, die den Abgleich der tatsächlichen Ergebnisse mit den Compliance-Anforderungen ermöglicht.[106] Hier können Parallelen zur Diskussion um eine technologisch durchgeführte intelligent surveillance gezogen werden. Während es durch die impossibility structures bereits objektiv ausgeschlossen wird, dass sich ein KI-System außerhalb rechtlicher oder vertraglicher Grenzen bewegt, ist ein entsprechendes Agieren bei einer intelligent surveillance noch möglich, wobei dann die aus dem Rechts- oder Vertragsbruch herrührenden Konsequenzen drohen.[107] Da so unerwünschte Aktivitäten oder Zustände nicht verhindert werden können, besteht die Herausforderung darin, technologische Werkzeuge zur Erkennung von Verstößen bereitzustellen, so dass einerseits gesetzte Anreize als tatsächlich erreichbar angesehen werden und andererseits auf die Verletzung von Compliance-Anforderungen (insbesondere von Rechtsverletzungen) schnell reagiert und gegebenenfalls gegengesteuert werden kann.[108] Neben dem nur eingeschränkt möglichen Einsatz von technischen Mechanismen wie der Unterbrechung des aktuellen Prozesses zur Herstellung eines früheren, regelkonformen Zustandes (Rollback) oder dem Starten weiterer Prozesse zur automatischen Beseitigung der für die Regelwidrigkeit verantwortlichen Bedingungen im KI-System (Recover) kommt insbesondere eine Information einer verantwortlichen Person (beispielsweise im

[92] *Yuan*, RW 2018, 477 (491).
[93] *Waltl/Vogl*, Jusletter IT, 22.2.2018, S. 3, abrufbar unter https://wwwmatthes.in.tum.de/pages/1hqrlk3h1m4l6/Explainable-Artificial-Intelligence-the-New-Frontier-in-Legal-Informatics (3.2.2020).
[94] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 16 Abschnitt (53).
[95] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 22 Abschnitt (75).
[96] *Yuan*, RW 2018, 477 (488), zum „Reinforcement Learning“, vgl. hierzu auch Fn. 26.
[97] Vgl. *Hilgendorf* (Fn. 21), S. 110 f.; vgl. auch Art. 6 Ziff. 2 des Verordnungsvorschlags der EU-Kommission KOM (2018) 640 endg. v. 12.9.2018, wonach Onlinedienste dazu verpflichtet werden sollen, proaktive Maßnahmen „einschließlich automatisierter Werkzeuge“ zu verwenden, um den Upload von terroristischer Kommunikation zu verhindern.
[98] Vgl. *Bedner*, Cloud Computing, 2012, S. 12.
[99] *Rademacher*, JZ 2019, 702 m.w.N. in Fn. 2.
[100] Zur Frage der Handlungsfähigkeit von autonom agierenden KI-Systemen bereits oben II. 3. a) Autonomierisiko.
[101] Allgemein zum „Compliance by Design“-Ansatz *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (43).
[102] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (43).
[103] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (43).
[104] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (43).
[105] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (43).
[106] Allgemein zum „Compliance by Detection“-Ansatz *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (44).
[107] Vgl. – auf das Handeln von Menschen bezogen – *Rademacher*, JZ 2019, 702 (703).
[108] Vgl. zur automatisierten Compliance by Detection *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (43).

Unternehmen des Compliance-Officers oder eines KI-Sicherheitsbeauftragten[109]) in Betracht.[110]

6. Kombination beider Ansätze

Der präventive Ansatz hat auf den ersten Blick den Charme, dass – in einer idealen Welt – Rechtsverstöße von vornherein unmöglich sind.[111] Jedoch stellt sich unmittelbar die Frage, ob es überhaupt möglich ist, dass die Grenze zwischen Recht und Unrecht für ein künstliches System erkennbar ist oder ob es nicht vielmehr zu einer Streubreite dahingehend kommt, dass auch Erlaubtes verhindert wird.[112] Wenn auch diese Gefahr des Overblockings in dem Maße geringer wird, in welchem die KI-Systeme zu einer ausreichenden Kontexterkennung in der Lage sind[113] – was bei einer so genannten starken künstlichen Intelligenz mit der (erwarteten) Fähigkeit, die Rechtmäßigkeit eines Verhaltens deduktiv aus Regeln abzuleiten prognostiziert wird[114] –, ist es derzeit schlichtweg unmöglich, alle (!) möglichen Varianten und Zustände bereits ex ante auf ihre Vereinbarkeit mit den jeweiligen Compliance-Anforderungen bewerten zu können. Dies führt bei einer strikten Erzwingung bzw. dem unbedingten Ausschluss bestimmter Aktivitäten dazu, dass auf unvorhergesehene Ereignisse oder einen sich ändernden Kontext nicht mehr angemessen reagiert werden kann.[115]

So zeigt die Erfahrung, dass mit einem „By-design"-Ansatz auch erhebliche Nachteile einhergehen. Eine besonders konsequente Form fand sich in dem Digital Rights Management (DRM) der Musik- und Filmindustrie. Dadurch wurde versucht, bereits durch die implementierte Technik sicherzustellen, dass Urheberrechtsverletzungen durch die Nutzer ausgeschlossen wurden. Jedoch wurde das DRM auf der Seite der Kunden als eine starke Gängelung empfunden und abgelehnt.[116] Als besonders gravierender Nachteil erwies sich die Tatsache, dass teilweise selbst die rechtmäßige Nutzung nicht mehr möglich war, wie dies durch die Abschaltung des Dienstes Playforsure von Microsoft passierte.[117] Ebenso zeigt die Diskussion um den berühmt-berüchtigten so genannten Upload-Filter die Brisanz von impossibility structures. So sollte den Plattformbetreibern nach dem ursprünglichen Entwurf der Urheberrechts-Richtlinie explizit vorgeschrieben werden, dass diese technologische Maßnahmen ergreifen müssen, damit es von vornherein unmöglich ist, urheberrechtlich geschütztes Material ohne eine entsprechende Lizenz hochzuladen.[118] Dies führte zur Diskussion um das urheberrechtliche Overblocking, wonach ein Hochladen auch rechtmäßiger Inhalte durch die Schaffung solcher impossibility structures von vornherein verhindert wird.[119]

Deshalb ist ein alleiniger „By-design"-Ansatz durch die technologische Implementierung von impossible structures nach wie vor nicht umsetzbar. Dessen Nachteile lassen sich durch eine Kombination mit dem retrospektiven Ansatz vermeiden. Durch diesen werden die Handlungsaktivitäten nicht beschränkt und es ist keine ex-ante-Kenntnis aller möglichen Aktivitäten und Zustände notwendig.[120] Damit bietet dieser Ansatz den größtmöglichen Handlungsspielraum und die Flexibilität, auch auf unvorhergesehene Ereignisse adäquat reagieren zu können.[121] Allerdings ist dies mit dem Nachteil verbunden, dass so keine präventiven Handlungsbeschränkungen möglich sind.

Bei der Wahl eines ausgewogenen Verhältnisses beider Ansätze zueinander gilt es, die jeweiligen Vor- und Nachteile sachgemäß gegeneinander abzuwägen.[122] Das ist die Sache der im jeweiligen Lebenszyklus[123] des KI-Systems Verantwortlichen.

7. Regelungsvorschlag in Anlehnung an Art. 25 Abs. 1 DSGVO

Der Gesetzgeber selbst könnte jedoch entsprechende Rahmenbedingungen schaffen. Da die zu beachtenden rechtlichen Vorgaben ständigen Änderungen unterworfen sind, die sich nicht allein in einem Eingreifen des Gesetzgebers äußern, sondern auch in der Dynamik der Rechtsprechung, entsteht ein ständiger Anpassungsdruck,[124] der dabei zu berücksichtigen wäre. Die DSGVO sieht bereits eine Regelung zum „Privacy by Design" bzw. „Datenschutz durch Gestaltung" in Art. 25 Abs. 1 vor.[125] Hier würde sich eine über den Bereich des Datenschutzes hinausgehende verallgemeinernde Regelung anbieten.[126] In Analogie dazu könnte eine Vorgabe für KI-Systeme wie folgt ausgestaltet sein:

> „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke des Einsatzes von KI-Systemen

[109] Zu diesem Vorschlag im Rahmen einer angedachten Kollektivverantwortlichkeit eines Verbandes vgl. die Ausführungen zu Fn. 181.
[110] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (44).
[111] Zur Ambivalenz einer solchen „idealen" Welt und der Forderung nach einem „Recht zum Rechtsverstoß" *Rademacher*, JZ 2019, 702.
[112] *Rademacher*, JZ 2019, 702 (706).
[113] *Rademacher*, JZ 2019, 702 (707).
[114] *Eberl*, APuZ 6-8/2018, 8 (12 f.).
[115] Vgl. *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (45).
[116] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (44).
[117] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (44).
[118] Zwar ist diese explizit noch in Art. 13 Abs. 1 des Vorschlags für eine Richtlinie über das Urheberrecht im digitalen Binnenmarkt (KOM [2016] 593 endg.) vorgesehene Regelung nicht mehr im Art. 17 der Richtlinie 2019/790 enthalten. Dennoch ist nicht klar, ob damit Upload-Filter ausgeschlossen sind oder nicht; hierzu *Rademacher*, JZ 2019, 702 (704) m.w.N. in Fn. 12.
[119] *Spindler*, NJW 2017, 2305 (2307).
[120] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (44).
[121] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (44).
[122] *Sackmann*, HMD 2008, Heft 5 Bd. 263, 39 (45).
[123] Zum Lebenszyklus vgl. oben zu Fn. 10.
[124] Vgl. *Rüpke/v. Lewinski/Eckhardt*, Datenschutzrecht, 2018, § 20 Rn. 9 ff.
[125] Zur Differenzierung dieser Begriffe vgl. *Hansen,* in: Simitis/Hornung/Spiecker genannt Döhmann (Fn. 88), DSGVO Art. 25 Rn. 23.
[126] *Herberger*, NJW 2018, 2825 (2828).

sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte Dritter und der Allgemeinheit sind durch die verantwortliche Stelle sowohl zum Zeitpunkt der Festlegung der Mittel für den Einsatz des KI-Systems als auch zum Zeitpunkt des eigentlichen Einsatzes geeignete technische und organisatorische Maßnahmen vorzusehen, die dafür ausgelegt sind, die Rechte Dritter und der Allgemeinheit wirksam zu sichern.“

Dabei haben Erfahrungen mit dem „Privacy by Design“-Ansatz gezeigt, dass diesem zunächst eine echte Durchschlagskraft verwehrt blieb, da es weder eine Sanktionierung noch Anreize (beispielsweise durch eine entsprechende Zertifizierung) gab.[127] Dies hat sich unmittelbar mit Einführung der DSGVO geändert. Nach Art. 83 Abs. 4a DSGVO sind bei einer Nichteinhaltung von allgemeinen Pflichten der Verantwortlichen oder Auftragsverarbeiter Geldbußen zu verhängen. Dazu gehören auch Verstöße gegen einen dem Stand der Technik entsprechenden Datenschutz, wonach die IT-Systeme so gestaltet sein müssen, dass sie die wirksame Umsetzung von Datenschutzgrundsätzen („privacy by design“) und die Forderung nach datenschutzfreundlichen Voreinstellungen („privacy by default“) gem. Art. 25 DSGVO fördern.[128]

IV. Verantwortlichkeiten beim Einsatz von KI-Systemen

Bei der Bestimmung der Verantwortlichkeiten kommt aus der Sicht der Fahrlässigkeitsdelikte eine Verschiebung der Sorgfaltsmaßstäbe in Betracht (hierzu 1.). Ferner käme es in Betracht, an eine Sanktionierung der KI-Systeme selbst zu denken (siehe hierzu 2.). So ließe sich ein „hinkendes Rechtssubjekt“ vermeiden, dem zwar die Fähigkeit zu rechtsgeschäftlichem und tatsächlichem Handeln (grundsätzlich aber im fremden Interesse) zugestanden wird, welches aber für rechtswidrige Taten nicht sanktioniert werden kann.[129] Außerdem sind die Möglichkeiten einer sanktionsrechtlichen Verbands(mit)verantwortlichkeit (hierzu 3.) sowie die Sicherstellung der menschlichen Aufsicht (hierzu 4.) zu bedenken.

1. Strafrechtliche Fahrlässigkeitshaftung

Bei der Entwicklung und dem Einsatz von KI-Systemen kann es bei den Fahrlässigkeitsdelikten (hier sind insbesondere die §§ 222, 229 StGB zu nennen) zu einer Verschiebung von einzuhaltenden Sorgfaltsmaßstäben kommen. Denn für eine Fahrlässigkeitshaftung kommt es insbesondere auf eine Sorgfaltspflichtverletzung an.[130] Dabei ist nach der überwiegenden Auffassung im Strafrecht auf der Ebene der Tatbestandsmäßigkeit ein objektiver Maßstab an die einzuhaltenden Sorgfaltsanforderungen anzulegen, während auf der Ebene der persönlichen Schuld danach zu fragen ist, inwieweit der Täter nach seinen individuellen Fähigkeiten subjektiv in der Lage war, den objektiven Sorgfaltsanforderungen zu entsprechen.[131] Hier kommt es entscheidend auf den Umfang von Verhaltensregeln an, die den Sorgfaltsmaßstab bilden und sich aus Rechtssätzen, aber auch aus nichtstaatlichen Regeln (wie Industrienormen) ergeben können.[132] Der Gesetzgeber selbst greift dabei auf generalklauselartige Beschreibungen wie den „Stand der Wissenschaft und Technik“ in § 1 Abs. 2 Nr. 5 ProdHG oder den „Stand der medizinischen Wissenschaft und Technik“ in § 5 Abs. 1 TFG zurück.[133] Soweit solche speziellen Verhaltensregeln nicht existieren, wird auf den „besonnenen und gewissenhaften Menschen aus dem Verkehrskreis des Täters“ abgestellt.[134]

Damit ist – soweit es aufgrund eines Programmierfehlers zur Schädigung (beispielsweise der körperlichen Integrität eines Menschen) durch ein KI-System kommt – die Frage zu beantworten, wie sich ein sorgfältiger Programmierer (bzw. KI-System-Entwickler) verhalten hätte bzw. ob ggf. eine Übernahmefahrlässigkeit vorgeworfen werden kann. Wegen der Komplexität bietet sich bei der Herstellung (bzw. Programmierung oder dem Training) von KI-Systemen eine Vielzahl von Anknüpfungspunkten für menschliche Sorgfaltspflichtverletzungen an.[135] Darüber hinaus müssen die Hersteller auch während des Betriebes der KI-Systeme noch produktbezogene Verkehrssicherungspflichten beachten.[136]

Es ist vorstellbar, dass der *Nichteinsatz* verfügbarer Systeme als eine Sorgfaltspflichtverletzung angesehen wird, wenn es dadurch zu vermeidbaren Schädigungen kommt.[137] So liegt im medizinischen Bereich ein Behandlungsfehler

[127] *Hansen* (Fn. 125), DSGVO Art. 25 Rn. 6.
[128] *Cornelius*, in Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XIV Rn. 61.
[129] Vgl. *Wagner*, NZWiSt 2018, 399 (400), allerdings im Hinblick auf die Verbandsstrafbarkeit.
[130] *Kühl*, Strafrecht, Allgemeiner Teil, 8. Aufl., 2017, § 17 Rn. 14 ff.
[131] *Sternberg-Lieben/Schuster*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 15 Rn. 118.
[132] *Sternberg-Lieben/Schuster* (Fn. 131), § 15 Rn. 135; jedoch ist hierbei zu beachten, dass vor dem Hintergrund der schadensorientierten Haftungsprinzipien des Zivilrechts keine unbesehene Übernahme zivilrechtlicher Sorgfaltsanforderungen für die Frage der strafrechtlichen Verantwortlichkeit erfolgen darf, BGH NJW 1990, 2560 (2562); ausführlich zu dieser Problematik *Blechschmitt*, Die straf- und zivilrechtliche Haftung des Arztes beim Einsatz roboterassistierter Chirurgie, 2017, S. 129 ff., mit der Nennung des Eckpunktes (S. 138), dass ein zivilrechtlicher Maßstab die Obergrenze möglicher Fahrlässigkeitsstrafbarkeit bildet, aber noch nicht zwingend zu einem strafrechtlich relevanten Sorgfaltsmangel führen muss.
[133] *Yuan*, RW 2018, 477 (494 f.).
[134] *Rengier*, Strafrecht, Allgemeiner Teil, 11. Aufl. 2019, § 52 Rn. 15; als „völlig nichtssagende Kunstfigur“ kritisierend *Duttge*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 1, 3. Aufl. 2017, § 15 Rn. 117.
[135] *Yuan*, RW 2018, 477 (496), mit Beispielen.
[136] *Yuan*, RW 2018, 477 (496 Fn. 95 m.w.N.).
[137] So bereits *Kilian*, in: Savory (Hrsg.), Expertensysteme: Nutzen für Ihr Unternehmen, 2. Aufl. 1989, S. 393 (395), mit Blick auf eine nicht erfolgte Konsultation verfügbarer medizinischer Expertensysteme.

dann vor, wenn eine gewählte Behandlungsmethode „veraltet und überholt“ ist, was dann anzunehmen ist, „wenn neue Methoden risikoärmer sind und/oder bessere Heilungschancen versprechen, in der medizinischen Wissenschaft im Wesentlichen unumstritten sind und deshalb nur ihre Anwendung von einem sorgfältigen und auf Weiterbildung bedachten Arzt verantwortet werden kann“.[138] Dies dürfte beispielsweise dann der Fall sein, wenn KI-Systeme so leistungsfähig sein sollten, dass deren Diagnose der Vorzug vor einer abweichenden ärztlichen Meinung gegeben wird, der Einsatz eines solchen Systems also medizinischer Standard ist.[139] Das ist keine in der Ferne spielende Musik, sondern für bestimmte medizinische Konstellationen aktuell. So ist bereits heute der Nachweis gelungen, dass deep-learning-Systeme besser als Dermatologen in der Lage sind, Hautkrebs zu erkennen.[140]

Wenn dagegen ein solches KI-System eingesetzt wird und sich die Diagnose im Nachhinein als fehlerhaft herausstellt, kommt eine Sorgfaltspflichtverletzung der (ärztlichen) Anwender nur bei einer fehlerhaften Auswahl (keine Kompatibilität des Systems mit dem Einsatzzweck), Bedienung (nicht entsprechend den Herstellervorgaben) oder Überwachung (keine regelmäßige Wartung, keine Beachtung offensichtlicher Sicherheitsmängel) des Systems in Betracht.[141] Dabei ist zu beachten, dass sich die jeweiligen Sorgfaltsanforderungen gegenseitig beeinflussen. So kann eine besonders sorgfältige Auswahl eines KI-Systems zu einer Verringerung der Überwachungspflichten führen (und andersherum).[142]

Daneben kommt noch eine Herstellerhaftung in Betracht.[143] Für diese ist es jedoch Voraussetzung, dass es sich um einen vermeidbaren und behebbaren Konstruktions- oder Trainingsfehler und nicht um eine Fehlreaktion im Einzelfall handelt.[144] Dabei kann es zu einer Verschiebung der Sorgfaltspflichten weg vom Nutzer hin zum Hersteller kommen.[145]

Weitere Voraussetzung für eine strafrechtliche Fahrlässigkeitshaftung ist die Vorhersehbarkeit des Erfolgseintritts im Zeitpunkt der Sorgfaltspflichtverletzung. Die Rechtsprechung stellt hauptsächlich auf den Eintritt des tatbestandlichen Erfolges ab,[146] während die Literatur noch die konkrete Art und Weise der Herbeiführung des Taterfolges mit einbezieht.[147] Bei Zugrundelegung des Maßstabes der Rechtsprechung kann die Vorhersehbarkeit regelmäßig dann bejaht werden, wenn es sich um KI-Systeme handelt, die bestimmungsgemäß mit Menschen interagieren und eine Verletzung derselben denkbar ist.[148]

Schließlich muss der Erfolg – nach Feststellung einer Kausalität im Sinne der conditio-sine-qua-non-Formel[149] – dem Täter zurechenbar sein. Dies erfordert die Schaffung eines rechtlich missbilligten Risikos, welches sich gerade im tatbestandlichen Erfolg verwirklicht.[150] Dabei wird neben dem Erfordernis eines bestehenden Schutzzweckzusammenhanges[151] auf einen Pflichtwidrigkeitszusammenhang[152] abgestellt. Dieser spezifische Ursachenzusammenhang ist dann zu bejahen, wenn auf der Grundlage eines hypothetischen Geschehensverlaufs bei Hinwegdenken des vorwerfbaren Tatumstandes und Hinzudenken eines pflichtgemäßen Alternativverhaltens des Täters der tatbestandliche Erfolg mit an Sicherheit grenzender Wahrscheinlichkeit[153] entfallen würde.[154] Hier wird wieder deutlich, wie wichtig eine entsprechende Nachvollziehbarkeit der Entscheidungsfindung eines KI-Systems für die Bestimmung des etwaigen Eintretens aufgrund eines rechtmäßigen Alternativverhaltens ist.

2. Sanktionierbarkeit von KI-Systemen?

Neben einer Fahrlässigkeitsverantwortlichkeit der beteiligten Personen stellt sich die Frage einer Sanktionierbarkeit der KI-Systeme selbst. Dem könnte das Erfordernis der Schuld entgegenstehen, welches nach dem üblichen Verständnis Voraussetzung für die Kriminalstrafe ist.[155] Denn eine auf den

[138] BGH NJW 1988, 763 (764); vgl. zur Verfehlung des medizinischen Standards aufgrund Anwendung einer veralteten Behandlungsmethode *Blechschmitt* (Fn. 132), S. 121 ff.

[139] *Meyer*, ZRP 2018, 233 (236).

[140] *Brinker/Hekler/Enk/Klode/Hauschild/Berking/Schilling/Haferkamp/Schadendorf/Holland-Letz/Utikal/v. Kalle*, European Journal of Cancer 113 (2019), 47.

[141] *Horner/Kaulartz*, CR 2016, 7 (8), haben diese Kategorisierung zwar unter Rückgriff auf § 831 BGB entwickelt, wobei jedoch nichts dagegenspricht, für den objektiven Maßstab auf diese Kategorisierung auch aus strafrechtlicher Sicht zurückzugreifen, vgl. oben Fn. 132.

[142] *Horner/Kaulartz*, CR 2016, 7 (8).

[143] *Meyer*, ZRP 2018, 233 (236).

[144] *Meyer*, ZRP 2018, 233 (236).

[145] *Horner/Kaulartz*, CR 2016, 7 (8).

[146] RGSt 54, 351; BGHSt 12, 75.

[147] *Sternberg-Lieben/Schuster* (Fn. 131), § 15 Rn. 180.

[148] *Yuan*, RW 2018, 477 (497).

[149] BGHSt 1, 332 (333).

[150] *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 29. Aufl. 2018, Vor § 13 Rn. 14 m.w.N.

[151] Dieser ist dann gegeben, wenn sich der eingetretene Erfolg als Verwirklichung des Risikos erweist, vor dem die übertretene Sorgfaltspflicht schützen sollte.

[152] *Duttge* (Fn. 134), § 15 Rn. 165.

[153] BGHSt 11, 1 (3); vgl. aber BGHSt 49, 1 (4), wonach der „Ursachenzusammenhang“ schon dann entfalle, wenn sich derselbe Erfolgseintritt bei verkehrsgerechtem Verhalten „aufgrund erheblicher Tatsachen nach der Überzeugung des Tatrichters nicht ausschließen“ lasse.

[154] Das Beweismaß ist umstritten. So wird in der Literatur schon das „überwiegend wahrscheinliche“ Ausbleiben des Erfolges als ausreichend angesehen; *Duttge* (Fn. 134), § 15 Rn. 184.

[155] BVerfGE 45, 187 (253 ff.); *Fischer*, Strafgesetzbuch mit Nebengesetzen, Kommentar, 67. Aufl. 2020, § 20 Rn. 2, wobei zwischen dem verfassungsrechtlichem und dem strafrechtsdogmatischem Schuldbegriff zu differenzieren ist; *Hörnle*, in: Sieber/Dannecker/Kindhäuser/Vogel/Walter (Hrsg.), Strafrecht und Wirtschaftsstrafrecht, Dogmatik, Rechtsvergleich, Rechtstatsachen, Festschrift für Klaus Tiedemann zum 70. Geburtstag, 2008, S. 325 (340); *dies*., Kriminalstrafe ohne Schuldvorwurf, S. 60, wobei sie (S. 49 ff.) unter Bezugnahme auf die Erkenntnisse der Hirnforschung

Menschenwürdegehalt des Grundgesetzes zurückgeführte Schuld[156] kann es für „künstliche“ Systeme nicht geben, so intelligent sie auch sein mögen.[157] Die Menschenwürde kann nur Menschen und nicht Tieren[158], Robotern und anderen „künstlichen Personen“ zukommen. Da das deutsche Strafrecht bisher nur die Strafbarkeit „natürlicher“ Personen kennt, weil (so zumindest die bisher herrschende Meinung) eine Verbandsperson weder handlungs- noch schuldfähig sei,[159] könnte die Betrachtung an dieser Stelle abgeschlossen werden.[160]

Damit weicht Deutschland aber zum Teil erheblich von den Modellen anderer Staaten ab. So wird in common law-Ländern wie England, Schottland und Zypern nicht zwischen der Strafbarkeit juristischer und natürlicher Personen differenziert. Die USA kennen die strafrechtliche Verantwortlichkeit von Kapitalgesellschaften ebenso wie Spanien, Frankreich, die Niederlande und Portugal.[161] Somit ist in den Ländern, die die Strafbarkeit juristischer Personen anerkennen, auch die Möglichkeit eröffnet, eine entsprechende strafrechtliche Haftung weiterer nicht-menschlicher Akteure zu etablieren. Hier reiht sich die aktuelle Diskussion in Deutschland um die Etablierung eines Unternehmenssanktionenrechts ein! Wenn der im Koalitionsvertrag geäußerte politische Wille[162] tatsächlich verwirklicht wird und eine direkte Sanktionierung von Unternehmen auch in Deutschland etabliert wird, können die angesprochenen Grundsatzfragen einer etwaigen Sanktionierbarkeit nicht-menschlicher Akteure wieder auf den Prüfstand kommen.

Das Grundgesetz selbst ist gegenüber einer Anpassung des Schuldbegriffs offen.[163] Dagegen lässt sich auch nicht die Lissabon-Entscheidung des Bundesverfassungsgerichts[164] anführen, denn diese bezieht sich nur auf den individualisierten – auf den Menschen bezogenen – Schuldgrundsatz.[165] Beispielsweise wird mit Blick auf die Diskussion eines Strafrechts von Verbänden – bei Akzeptanz des Ausgangspunktes, den Verband selbst als Akteur zu sehen – der „soziale Schuldvorwurf“ diskutiert, der auf ein Auswahl- und Organisationsverschulden des Verbandes abstellt.[166] Sowenig der Menschenwürdegehalt des (individualrechtlichen) Schuldprinzips der Einführung einer Verbandssanktionierung entgegensteht, sowenig steht dieser einer Sanktionierung von KI-Systemen entgegen.[167]

Allerdings sind (auch für die Frage der Sanktionsfähigkeit) die verfolgten Strafzwecke zu berücksichtigen. Die Überlegungen zu den Verbandssanktionen stellen vorwiegend auf Prävention ab,[168] wobei teilweise auch der Vergeltungs-

für die Aufgabe des Schuldbegriffs eintritt; vgl. auch (mit Blick auf juristische Personen) die Idee einer schuldgelösten Präventionsstrafe bei *Wohlers*, NZWiSt 2018, 412 (419), und einer parastrafrechtlichen Regelung bei *Jahn/Schmitt-Leonardy/Schoop*, wistra 2018, 27 (29).

[156] Vgl. BVerfGE 123, 267 (Lissabon), Rn. 364: „Das Strafrecht beruht auf dem Schuldgrundsatz. Dieser setzt die Eigenverantwortung des Menschen voraus, der sein Handeln selbst bestimmt und sich kraft seiner Willensfreiheit zwischen Recht und Unrecht entscheiden kann. Dem Schutz der Menschenwürde liegt die Vorstellung vom Menschen als einem geistig-sittlichen Wesen zugrunde, das darauf angelegt ist, in Freiheit sich selbst zu bestimmen und sich zu entfalten […]. Auf dem Gebiet der Strafrechtspflege bestimmt Art. 1 Abs. 1 GG die Auffassung vom Wesen der Strafe und das Verhältnis von Schuld und Sühne […]. Der Grundsatz, dass jede Strafe Schuld voraussetzt, hat seine Grundlage damit in der Menschenwürdegarantie des Art. 1 Abs. 1 GG […]. Das Schuldprinzip gehört zu der wegen Art. 79 Abs. 3 GG unverfügbaren Verfassungsidentität, die auch vor Eingriffen durch die supranational ausgeübte öffentliche Gewalt geschützt ist.“

[157] *Cornelius*, ZRP 2019, 8 (10).

[158] Zur Diskussion im Hinblick auf Tiere als „Personen im Recht“ vgl. *Raspé,* Die Anerkennung der tierlichen Person im Recht, 2013, passim.

[159] Vgl. zu dieser Frage *Jescheck/Weigend*, Strafrecht, Allgemeiner Teil, 5. Aufl. 1996, § 23 VII. 1.; *Lackner/Kühl* (Fn. 150), § 14 Rn 1a; *Laue*, JURA 2010, 339; *Roxin,* Strafrecht, Allgemeiner Teil, Bd. 1, 4. Aufl. 2006, § 8 Rn. 58 ff.; BGHSt 3, 130; 12, 295.

[160] Wenn nicht auf die Voraussetzung einer Schuld an sich verzichtet wird, vgl. hierzu oben Fn. 155.

[161] *Joecks*, in: Joecks/Miebach, (Fn. 134), Vor § 25 Rn. 16.

[162] Der Koalitionsvertrag zwischen CDU/CSU und SPD bekennt sich unter dem Stichwort Unternehmenssanktionen ausdrücklich hierzu: „Wir wollen sicherstellen, dass Wirtschaftskriminalität wirksam verfolgt und angemessen geahndet wird. Deshalb regeln wir das Sanktionsrecht für Unternehmen neu. Wir werden sicherstellen, dass bei Wirtschaftskriminalität grundsätzlich auch die von Fehlverhalten von Mitarbeiterinnen und Mitarbeitern profitierenden Unternehmen stärker sanktioniert werden. Bislang liegt es im Ermessen der zuständigen Behörde, ob auch das betreffende Unternehmen verfolgt wird. Durch die Abkehr vom Opportunitätsprinzip des bislang einschlägigen Ordnungswidrigkeitenrechts sorgen wir für eine bundesweit einheitliche Rechtsanwendung. Durch klare Verfahrensregelungen erhöhen wir zudem die Rechtssicherheit der betroffenen Unternehmen.“ Vgl. hierzu den bisher nur in Fachkreisen zirkulierenden Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Bekämpfung der Unternehmenskriminalität (Bearbeitungsstand: 15. August 2019).

[163] *Jahn*, in: Jahn/Schmitt-Leonardy/Schoop, Das Unternehmensstrafrecht und seine Alternativen, 2016, S. 53, 73 f.; *Simmler/Markwalder*, ZStW 2017, 20 (41), sehen „Schuld als Zuschreibung“; vgl. auch die Begründung zum Kölner Entwurf des Verbandssanktionengesetzes, S. 22.

[164] Vgl. oben Fn. 156.

[165] *Jahn* (Fn. 163), S. 53 (73 f.); vgl. auch die Begründung zum Kölner Entwurf des Verbandssanktionengesetzes, S. 22.

[166] *Tiedemann*, NJW 1988, 1169 (1172 f.); *Dannecker*, GA 2001, 101 (112); *Hilf*, NZWiSt 2016, 189 (190 ff.).

[167] *Cornelius*, ZRP 2019, 8 (10).

[168] *Kubiciel*, ZRP 2014, 133 (134 ff.); *Wagner*, NZWiSt 2018, 399 (401 f.); *Weigend/Hoven*, ZRP 2018, 30 (31).

gedanke berücksichtigt wird.[169] Dies lässt sich zwanglos auf KI-Systeme – ebenfalls als künstliche Gebilde – übertragen. Eine verhängte Strafe könnte als „kommunikative Vergeltung" eine vom Rechtsbruch eines KI-Systems ausgehende Botschaft im Sinne einer ausgleichenden Gerechtigkeit korrigieren.[170] Beim Abstellen auf den Gesichtspunkt der Generalprävention wäre eine Sanktionsfähigkeit zu bejahen, wenn die Wirkung einer verhängten Sanktion gegenüber anderen autonomen Systemen vergleichbar mit derjenigen ist, die die verhängte Sanktion gegenüber dem betroffenen System selbst hat.[171]

Dafür ist es notwendig, dass entsprechende Mechanismen etabliert werden, die die Verbreitung von rechtskräftig verhängten Sanktionen gewährleisten; sodass sie bei der Abarbeitung des Algorithmus (automatisch) mit berücksichtigt werden.[172] Außerdem müsste unter dem Gesichtspunkt der Generalprävention insbesondere bei dem durch eine Sanktion betroffenen KI-System eine Funktionalität implementiert sein, die dieses davon abhält, das bestrafte Verhalten noch einmal zu begehen.[173] Dies sind notwendige Voraussetzungen, damit die Adressierung von Sanktionen direkt an KI-Systeme sinnvoll ist. Solange diese nicht gegeben sind, ist eine Sanktionierung der KI-Systeme selbst nicht zielführend.

3. Möglichkeiten einer sanktionsrechtlichen Verbands(mit)-verantwortlichkeit

Damit schließt sich die unmittelbare Frage an, inwieweit die Risiken beim Einsatz von KI (Autonomie-, Verbund- und Vernetzungsrisiko) beim kommenden Verbandssanktionenrecht Berücksichtigung finden können. Zu dieser Frage wurde bereits an anderer Stelle herausgearbeitet,[174] dass sich frappierende Parallelen zwischen der Frage der Steuerung etwaigen rechtswidrigen Agierens von KI-Systemen durch das Recht und der Möglichkeit der Einführung einer Verbandsverantwortlichkeit ergeben, was Anlass dafür ist, die Berücksichtigung von rechtswidrigen „Handlungen" der KI-Systeme in eine strafrechtliche Unternehmenshaftung mit zu bedenken. So könnte eine Integration dergestalt erfolgen, dass der Normadressat von Verbandssanktionen nicht rechtlich formal, sondern funktional – an den faktischen Gegebenheiten ausgerichtet – erfolgt und sich so das (über die „Grenzen" einer juristischen Person hinausgehende) Verbund- und insbesondere Vernetzungsrisiko bei dem Einsatz autonomer KI-Systeme besser erfassen ließe.[175] Allerdings sind zuvor Kriterien zu erstellen, wie das soziale System als Normadressat selbst bestimmt werden soll, damit Rechtssicherheit (auch in der Wahrnehmung der Verteidigungsrechte) gewährleistet werden kann.

Ferner sollte eine Verantwortlichkeit des Verbandes für rechtswidrige (aber schuldlose) Handlungen von im Interesse des Verbandes eingesetzten KI-Systemen in das (noch zu schaffende) Verbandssanktionengesetz integriert werden. Der Grund für eine solche Zurechnung kann darin gesehen werden, dass dem Unternehmen (sozusagen als Prinzipal) ein rechtswidriges Verhalten des Algorithmus zugerechnet wird, welchen es zum eigenen Nutzen eingesetzt hat. Dabei käme es auf die tatsächliche Repräsentation des Verbandes (Prinzipals) durch das KI-System an, also wie sich der Repräsentant für Außenstehende darstellt.[176]

Insofern besteht beispielsweise nach dem Kölner Entwurf des Verbandssanktionengesetzes (nachfolgend: Kölner Entwurf) durchaus die Möglichkeit dazu, da nach dessen § 1 Abs. 3 eine Zuwiderhandlung bereits bei rechtswidrigen Handlungen gegeben sein sollte, die den objektiven Tatbestand eines Strafgesetzes erfüllte. Dies ließe sich beispielsweise durch eine Ergänzung des § 1 des Kölner Entwurfs dahingehend lösen, dass zu Mitarbeitern auch autonome KI-Systeme zählen, die im Interesse des Verbandes eingesetzt werden (wem diese Gleichstellung mit menschlichen Personen missfällt, könnte auch die Kategorie der autonomen KI-Systeme separat einführen). Außerdem ist es nach dem Kölner Entwurf noch erforderlich, dass eine Organisationspflichtverletzung der Leitungsebene vorliegt.[177] Es ist also eine personalisierbare Zuwiderhandlung notwendig, die mit einem Leitungsversagen zusammenfällt.[178] Es müssen „erforderliche und zumutbare Maßnahmen zur Verhinderung" der Zuwiderhandlungen von KI-Systemen durch eine Leitungsperson des Verbandes unterlassen worden sein.[179] Hier könnte dadurch Abhilfe geschaffen werden, dass von Unternehmen, die KI-Systeme einsetzen möchten, zwingend KI-Sicherheitsbeauftragte zu bestellen sind,[180] welche in § 1 Abs. 4 des Kölner Entwurfs als Leitungspersonen mit aufzunehmen wären.[181] Diese hätten dann mit Blick auf den Betrieb von KI-Systemen sicherzustellen, dass sich diese tatsächlich innerhalb der durch die Gesellschaft gegebenen und in das Recht gegossenen Grenzen bewegen.[182]

Inzwischen liegt ein Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (mit Bearbeitungsstand vom 15. August 2019) zur Sanktionierung von verbandsbezogenen Straftaten vor (VerSanG-E). Anknüp-

[169] *Dannecker/Dannecker*, NZWiSt 129 (2016), 162 (173); *v. Hirsch*, NZWiSt 2016, 161, stellt im Sinne der „Tadeltheorie" auf die normative Urteilsfähigkeit des führenden Personals ab; vgl. *Jahn/Schmitt-Leonardy/Schoop*, wistra 2018, 27 (28 f.).

[170] *Cornelius*, ZRP 2019, 8 (11); vgl. *Beale*, ZStW 126 (2014), 27 (39).

[171] *Cornelius*, ZRP 2019, 8 (11), unter Hinweis auf die Argumentation zur Sanktionsfähigkeit von Verbänden bei *Dannecker*, GA 2001, 101 (114).

[172] *Cornelius*, ZRP 2019, 8 (11).

[173] *Cornelius*, ZRP 2019, 8 (11).

[174] *Cornelius*, ZRP 2019, 8 (11 ff.).

[175] *Cornelius*, ZRP 2019, 8 (11 f.).

[176] *Wagner*, NZWiSt 2018, 399 (403).

[177] Kritisch dazu *Wagner*, NZWiSt 2018, 399 (404).

[178] *Kölbel*, NZWiSt 2018, 407 (408).

[179] Vgl. § 3 Abs. 2 des Kölner Entwurfs.

[180] Vgl. insoweit die nach dem IT-Sicherheitsgesetz bisher für die Betreiber kritischer Infrastrukturen vorgesehenen IT-Sicherheitsbeauftragten.

[181] *Cornelius*, ZRP 2019, 8 (12).

[182] *Cornelius*, ZRP 2019, 8 (12).

fungspunkt für eine Verbandsverantwortlichkeit ist eine Straftat, durch die Pflichten, die den Verband treffen, verletzt worden sind oder durch die der Verband bereichert worden ist oder werden sollte (§ 2 Abs. 1 Nr. 3 VerSanG-E). Daraus wird bereits deutlich, dass es sich um eine Straftat handeln muss, die tatbestandsmäßig, rechtswidrig und schuldhaft begangen wurde.[183] Insoweit ist nach diesem Entwurf ein rechtswidriges (aber nicht schuldhaftes) „Fehlverhalten“ von KI-Systemen nicht integrierbar. Zwar ist es für eine Zurechnung einer Verbandsstraftat schon ausreichend, dass eine Leitungsperson Vorkehrungen gegen die Begehung einer solchen Tat objektiv pflichtwidrig unterlassen hat und dadurch eine objektiv erkennbare Gefahr für die Begehung einer Straftat geschaffen wurde (vgl. § 3 Abs. 1 Nr. 2 VerSanG-E). Dies ändert jedoch nichts daran, dass der Anknüpfungspunkt für eine Verbandsverantwortlichkeit eine volldeliktisch begangene Verbandsstraftat ist.[184] Insoweit sollte im Laufe des Gesetzgebungsverfahrens eine Umorientierung und Öffnung (beispielsweise im Sinne des Kölner Entwurfs) erfolgen, um entsprechendes „Fehlverhalten“ von durch Verbände betriebenen KI-Systemen, welches durch eine unzureichende Überwachung seitens von KI-Sicherheitsverantwortlichen ermöglicht wurde, gegenüber dem Verband sanktionieren zu können.

4. Menschliche Aufsicht

Insoweit kommt der Sicherstellung der menschlichen Aufsicht eine besondere Rolle zu. Eine solche Aufsicht kann durch entsprechende Lenkungs- und Kontrollmechanismen wie die interaktive Einbindung eines Menschen (Human in the Loop – HITL), die Überprüfung und Kontrolle durch einen Menschen (Human on the Loop – HOTL) oder mittels der Gesamtsteuerung durch einen Menschen (Human in Command – HIC) erreicht werden.[185]

Der „Human in the Loop” (HITL) mit der Fähigkeit, in jeden Entscheidungsprozess eines Systems einzugreifen, stellt die Effektivität der KI-Systeme für sich genommen in Frage, sodass dies generell nicht unbedingt angestrebt werden sollte.[186] Dabei ist jedoch danach zu differenzieren, um welches Einsatzgebiet der KI es sich handelt.[187] Wenn es beispielsweise um den Einsatz im medizinischen Bereich mit unmittelbaren Auswirkungen auf Leib oder Leben der Patienten geht, wird nach wie vor der HITL erforderlich sein.[188] Die Verknüpfung zwischen künstlicher Intelligenz und (einem oder mehreren) Menschen zu einem „hybriden Multi-Agenten-Interaktionsmodell“ wird für diesen Bereich „als große Chance für die Zukunft“ gesehen.[189] Dieses Beispiel verdeutlicht einmal mehr, dass generelle Aussagen zur künstlichen Intelligenz schwierig zu treffen sind, sondern es vielmehr darauf ankommt, nach den verschiedenen Einsatzgebieten zu differenzieren.

Jedoch ist es wichtig, dass zumindest die Fähigkeit des Menschen aufrechterhalten bleibt, das Entwurfsstadium eines Systems zu steuern und den Systembetrieb zu überwachen (HOTL).[190] Grundsätzlich sollte der Gesamtbetrieb eines KI-Systems durch den „Human in Command“ beaufsichtigt werden und dieser Mensch die Fähigkeit haben, jederzeit über ein Ob, Wie und Wann eines Einsatzes des Systems zu entscheiden, einschließlich der Frage, inwieweit ein bestimmtes Maß an menschlichem Ermessen zugelassen und eine Entscheidung des Systems gegebenenfalls neutralisiert wird.[191] Gerade wegen der schwierigen Vorhersehbarkeit von Entscheidungen der KI-Systeme kommt deren Überwachung eine besondere Bedeutung zu, um sicherzustellen, dass sich das System auch nach seiner Einführung wie vorgesehen verhält bzw. sich innerhalb zuvor definierter Zielsetzungen bewegt (wozu auch die Einhaltung rechtlicher Vorgaben gehört).[192] Das korrespondiert auch mit dem Vorschlag, bei dem Einsatz von KI-Systemen durch Unternehmen eine entsprechend verantwortliche Person zu bestimmen, so dass etwaige rechtswidrige Aktionen der KI-Systeme bei einer fehlerhaften Überwachung durch die hierzu bestimmte Leitungsperson (wie einem KI-Sicherheitsbeauftragten)[193] direkt dem Verband zugerechnet werden können.

V. Ergebnis

Generelle Aussagen zur künstlichen Intelligenz sind mit Vorsicht zu genießen. Es ist vielmehr wichtig, auch bezüglich etwaiger regulatorischer Anforderungen nach den verschiedenen Einsatzgebieten zu differenzieren. Insoweit könnte es ein Ansatzpunkt sein, auf europäischer und nationaler Ebene eine im Bereich der KI tätige Behörde zu bestimmen, die Nutzen und Risiken von autonomen Systemen bewertet und

[183] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz, Entwurf eines Gesetzes zur Bekämpfung der Unternehmenskriminalität (Bearbeitungsstand: 15.8. 2019), S. 74.

[184] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz, Entwurf eines Gesetzes zur Bekämpfung der Unternehmenskriminalität (Bearbeitungsstand: 15.8. 2019), S. 78.

[185] *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 19 Abschnitt (65).

[186] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 19 Abschnitt (65).

[187] *Meyer*, ZRP 2018, 233 (235).

[188] *Kilian* (Fn. 137), S. 404; vgl. *He/Baxter/Xu/Zhou/Zhang*, Nature Medicine 25 (2019), 30, *Brinker/Hekler/Enk/Klode/Hauschild/Berking/Schilling/Haferkamp/Schadendorf/Holland-Letz/Utikal/v. Kalle*, European Journal of Cancer 113 (2019), 47 (52).

[189] *Holzinger*, in: Gesellschaft für Informatik (Hrsg.), Informatiklexikon, Stand: 23.4.2018, abrufbar unter https://gi.de/informatiklexikon/explainable-ai-ex-ai/ (3.2.2020).

[190] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 19 Abschnitt (65).

[191] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 19 Abschnitt (65).

[192] Vgl. *Hochrangige Expertengruppe für Künstliche Intelligenz* (Fn. 3), S. 27 Abschnitt (100 f.).

[193] Vgl. oben zu Fn. 180.

entsprechende Standards diskutiert und etabliert.[194] Diesbezüglich könnte es gegebenenfalls angebracht sein, eine solche Aufgabe der Agentur der Europäischen Union für Cybersicherheit sowie dem Bundesamt für Sicherheit in der Informationstechnik zuzuordnen.

Um die Rechtsmäßigkeit der KI-Systeme sicherstellen zu können, sollte bereits bei deren Entwicklung, aber auch bei der Einführung und Nutzung soweit wie möglich sichergestellt werden, dass die Rechtsregeln eingehalten werden (präventiver Ansatz). Außerdem wäre durch eine entsprechende Dokumentation zu ermöglichen, dass im Nachhinein die Beurteilung der Einhaltung von entsprechenden Sorgfaltsmaßstäben erfolgen kann (retrospektiver Ansatz). Deshalb muss gewährleistet sein, dass die KI-Systeme nicht nur vergangenheitsbezogen lernen, sondern offen für Regeländerungen (wie den Erlass neuer Gesetze oder die Änderung relevanter Rechtsprechung) sind. Insoweit können die rechtlichen Regelungen des „Privacy by Design"-Ansatzes nach Art. 25 DSGVO als für KI-Systeme zu verallgemeinernde Vorlage genutzt werden, soweit diese in kritischen Situationen eingesetzt werden (z.B. in der Medizin, aber ggf. auch bei der Steuerung wichtiger infrastruktureller Maßnahmen). Ob dann bei einer Nichtbeachtung eine Sanktionierung (wie in Art. 84 DSGVO für eine Nichtbeachtung des Art. 25 DSGVO vorgesehen) erfolgen sollte, wäre entsprechend der Sensibilität des Einsatzbereiches kritisch zu prüfen. Dies betrifft den gesamten Lebenszyklus[195] eines KI-Systems. Damit wird nur die an sich triviale Selbstverständlichkeit adressiert, dass das geltende Recht zu befolgen ist und für den Fall der Nichtbefolgung eine entsprechende Aufklärung möglich ist. Das ist auch deshalb notwendig, um die demokratische Basis unseres Rechtssystems auch für die Zukunft zu sichern und eine „Delegation" der Setzung der im Alltag wirksam werdenden Normen auf die Programmersteller und -betreiber zu verhindern.

Das Nutzungspotential der „künstlichen Intelligenz" hat einen unmittelbaren Einfluss auf die Sorgfaltsmaßstäbe und damit auf die Grenze zwischen rechtmäßigen und rechtswidrigen Verhaltensweisen. Wenn beispielsweise eine Weiterentwicklung des oben erwähnten deep-learning-Systems zur Erkennung von Hautkrebs[196] in der Lage ist, bessere „Entscheidungen" auf der Grundlage einer schnelleren und präziseren Interpretation von Ergebnissen zu erzielen, als dies menschliche Ärzte könnten, ist eine Bestimmung des erlaubten Risikos notwendig. Im Sinne einer Beobachtungspflicht sollte der Gesetzgeber regelmäßig evaluieren, inwieweit ein gesetzgeberisches Eingreifen erforderlich ist.

Eine Sanktionierung von KI-Systemen direkt ist derzeit nicht sinnvoll. Hierfür wäre zunächst die Etablierung entsprechender Mechanismen zur Verbreitung von rechtskräftig gegen KI-Systeme verhängten Sanktionen notwendig, die bei der Abarbeitung des Algorithmus (automatisch) mitberücksichtigt werden. Außerdem müsste unter dem Gesichtspunkt der Generalprävention insbesondere bei dem durch eine Sanktion betroffenen KI-System eine Funktionalität implementiert sein, die dieses davon abhält, das sanktionierte Verhalten noch einmal zu begehen. Insoweit sollten für die Frage der Sanktionierung Parallelen nicht zum Menschen, sondern zu künstlichen Akteuren (wie den juristischen Personen) gezogen werden.

Die sich abzeichnende Einführung eines Unternehmensstrafrechts sollte dazu genutzt werden, das Verbund- und Vernetzungsrisiko beim Betrieb von autonomen Systemen durch Unternehmen zu berücksichtigen. Dabei könnte das kommende Unternehmenssanktionenrecht vorsehen, dass der Normadressat für entsprechende Verbandssanktionen funktional danach bestimmt wird, wer faktisch die Regeln für den Einsatz von KI-Systemen festlegt. Außerdem sollte sichergestellt werden, dass das Fehlverhalten autonomer Systeme direkt dem Verband zugerechnet werden kann. Beispielsweise könnten „KI-Sicherheitsbeauftragte" als Leitungspersonen gefordert werden. Diese hätten dann zu beobachten und bei erkannten Abweichungen sicherzustellen, dass sich die eingesetzten KI-Systeme innerhalb der rechtlichen Grenzen bewegen. Hierfür ist zwingend eine effektive menschliche Aufsicht über die eingesetzten Systeme sicherzustellen. Dabei ist jeweils nach den Einsatzgebieten zu differenzieren, ob ein „Human on the Loop", „Human in the Loop" oder ein „Human in Command" erforderlich ist.

[194] Das Fehlen einer dem Paul-Ehrlich-Institut vergleichbaren Behörde kritisiert *Yuan*, RW 2018, 477 (495).
[195] Vgl. oben zu Fn. 10.
[196] Vgl. oben zu Fn. 140.

Zur Strafbarkeit von e-Personen

Von **Lasse Quarck**, Kiel

I. Die digitale Revolution und das Recht

In Alex Proyas Science-Fiction-Film „I, Robot" gibt es eine Szene, in der der humanoide Roboter Sonny dem menschlichen Protagonisten erzählt, er habe „geträumt". In dieser Szene verschwimmen die Grenzen zwischen Mensch und Maschine. Es ist nicht klar ersichtlich, ob es sich bei Sonny noch um einen Roboter oder doch schon um ein menschengleiches Wesen handelt. Nicht nur das Gesamtwerk Isaac Asimovs, dessen gleichnamiger Kurzgeschichtenband die Grundlage für Proyas Film war, zeigt, dass künstliche Intelligenz und ihre Auswirkungen die Menschen spätestens seit Ende der Zweiten Industriellen Revolution beschäftigen. Unzählige Werke in Literatur und Film befassen sich mit intelligenten Maschinen und deren Interaktionen mit dem Menschen. Dabei sind es in der Regel dystopische Visionen, die von den Autoren und Regisseuren gezeichnet werden. Angefangen bei Fritz Langs cineastischem Weltdokumentenerbe „Metropolis" über Stanley Kubricks zeitlosen Klassiker „2001: Odyssee im Weltraum" bis hin zu „Matrix" von den Wachowski-Geschwistern – ganz überwiegend werden Roboter und Super-Computer als Bedrohung für die Hauptfiguren dargestellt.

Glücklicherweise handelt es sich bei diesen Stilisierungen im wahrsten Sinne des Wortes um naturwissenschaftliche Fiktionen. Maschinen und Algorithmen haben sich bisher stets als nützliche Helfer des Menschen erwiesen und sind schon seit vielen Jahren aus dem Alltag nicht mehr wegzudenken. Digitale Sprachassistenten, automatisiert fahrende Autos, Medizin- oder Pflegeroboter sind nur einige Beispiele, die zeigen, dass moderne Technologien allgegenwärtig sind.

In den USA werden Algorithmen sogar zur Unterstützung der Rechtsprechung eingesetzt. So wurde beispielsweise vor einigen Jahren der Straftäter Eric Loomis deshalb zu einer sechsjährigen Haftstrafe verurteilt, weil der Algorithmus „Compas" ihm ein sehr hohes Rückfallrisiko attestierte.[1]

Auch wenn durch dieses jedenfalls fragwürdige Vorgehen wenig wünschenswerte Visionen von Roboter-Richtern hervorgerufen werden, so zeigen all diese Beispiele eindrücklich, was die Technik bereits heute zu leisten imstande ist. Möglich gemacht wird dies unter anderem durch die Verarbeitung großer Datenmengen verschiedenster Quellen in Sekundenbruchteilen, in der Fachsprache „Big Data" genannt. Dadurch sind Algorithmen inzwischen in der Lage, komplexe Aufgaben zu lösen und auch zu lernen.[2]

1. Die KI wird autonom

Die Lernfähigkeit intelligenter Systeme geht dabei über bloßes „Trial and Error" hinaus. Unter Zuhilfenahme neuronaler Netzwerke, also an die Struktur eines biologischen Gehirns angelehnte Schaltkreise, können Systeme Informationen auf mehreren Ebenen gleichzeitig verarbeiten.[3] Durch verschiedene Ansätze des maschinellen Lernens – Reinforcement Learning oder überwachtes oder unüberwachtes Deep Learning usw. – können neuronale Netze trainiert werden, Entscheidungen selbst zu treffen und auf Basis des Gelernten sogar kreativ zu sein.[4] Daraus erwächst die Fähigkeit des Systems, sich autonom zu verhalten, also auf eine Vielzahl von (ggf. unbekannten) Situationen und Problemen eigenständig und ohne menschliche Hilfe angemessen zu reagieren.[5] Diese Flexibilität und Anpassungsfähigkeit bergen riesiges Potenzial. Die konkreten Auswirkungen hingegen, die künstliche Intelligenzen auf unsere Gesellschaft haben werden, lassen sich heute kaum absehen. Angesichts des rasanten technischen Fortschritts der letzten Jahre und Jahrzehnte erscheint es zumindest nicht mehr außerhalb des Möglichen, dass uns in nicht allzu ferner Zukunft Entitäten begegnen, die ähnlich hoch entwickelt sind wie der eingangs erwähnte Sonny.

Klar jedenfalls ist: Der Einsatz von autonomer oder teilautonomer KI soll unsere Lebensbedingungen verbessern, indem dem Menschen bestimmte Aufgaben abgenommen oder erleichtert werden.[6] Dabei werden sich durch intelligente Agenten verursachte Rechtsgutsverletzungen wohl nicht vermeiden lassen. Das gilt insbesondere dann, wenn diese Systeme einerseits immer autonomer werden und nicht mehr ständig unter menschlicher Aufsicht stehen und andererseits vermehrt Einzug in den öffentlichen Raum halten. Eine Zunahme der möglichen eigenständigen Aktionen des intelligenten Agenten hat denklogisch auch ein erhöhtes Risiko für Rechtsgutsverletzungen zur Folge.

2. Die Strafzwecke als Ausgangspunkt des Bedürfnisses einer KI-Strafbarkeit

Schädigt nun eine KI, etwa in Form eines intelligenten Roboters ein geschütztes Rechtsgut, so ist fraglich, wer dafür zur Verantwortung gezogen werden kann. Angesichts des zunehmenden Maßes an Lernfähigkeit und Autonomie sind in nicht mehr allzu ferner Zukunft Fälle denkbar und wahrscheinlich, in denen der strafrechtliche Erfolg den dahinterstehenden Menschen, namentlich den Programmierern, Her-

---

[1] *Smith*, New York Times v. 22.6.2016, abrufbar unter https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?module=inline (4.2.2020); FAZ v. 11.6.2019, abrufbar unter https://www.faz.net/aktuell/rhein-main/algorithmen-werden-in-amerika-bei-gerichtsprozessen-genutzt-16230589.html (4.2.2020).

[2] Vgl. *Bräutigam/Klindt*, NJW 2015, 1137 (1138 f.).

[3] *Styczynski/Rudion/Naumann*, Einführung in Expertensysteme, 2017, S. 132 ff.

[4] Zu den verschiedenen Prozessen beim Maschinenlernen *Görz/Nebel*, Künstliche Intelligenz, 2003, S. 108 ff.; *Gopnik*, SdW kompakt v. 1.10.2018, S. 15 ff.; *Wolfangel*, SdW kompakt v. 17.20.2016.

[5] *Hilgendorf*, ZStW 130 (2018), 674 (675).

[6] Vgl. *Kirchschläger*, AJP/PJA 2017, 240 (241 f.).

stellern und Nutzern, aus verschiedenen Gründen nicht mehr zugerechnet werden kann.

Denkbar ist dieses Ergebnis, weil es ggf. schon an der Vorhersehbarkeit fehlt[7] oder aufgrund des ubiquitären Einsatzes von KI und der Unmöglichkeit, Schädigungen vollständig auszuschließen, der Einsatz sozialadäquat und damit nicht mehr sorgfaltswidrig ist.[8]

Da Autonomie ja gerade die Unabhängigkeit externer, in diesem Falle menschlicher Einflussnahme voraussetzt, ist diese Rechtsfolge intelligenten Agenten immanent. Unvorhersehbare Aktionen des Systems sind logische Konsequenz von Autonomie, beim Menschen wie bei der KI.[9]

Es muss daher die Aufgabe der Rechtswissenschaft sein, die juristischen Rahmenbedingungen für den Einsatz neuer Technologien und die Folgen des Einsatzes abzustecken. Das hat zweierlei zur Folge: Erstens wird dadurch die Verwendung außerhalb von Testumgebungen ermöglicht, auch weil die juristischen Maßstäbe bei der Programmierung berücksichtigt werden können. Zweitens trägt eine Klärung rechtlicher Fragen maßgeblich zur gesellschaftlichen Akzeptanz des Einsatzes von KI bei.[10]

Entsteht nämlich bei der Bevölkerung der Eindruck, dass der Rechtsstaat für die juristischen Herausforderungen der fortschreitenden Digitalisierung keine adäquaten Antworten hat, wird das Vertrauen in die normative Ordnung erschüttert.[11] Eine Schädigung geschützter Rechtsgüter ohne Reaktion darf nicht hingenommen werden, da es für dieses Vertrauen eines umfassenden Schutzes ohne planwidrige Regelungslücken bedarf. Sind das Strafrecht und seine Anwender nicht in der Lage, auf eine Rechtsgutsverletzung entsprechend zu reagieren, so kommt das einer Entwertung des nun ja offensichtlich nicht mehr schützenswerten Rechtsguts gleich.[12] Durch das Ergebnis, dass niemand für einen strafrechtlichen Erfolg verantwortlich gemacht werden kann, würde das Recht in seinen Grundfesten erschüttert.[13]

Zweck des Strafrechts ist es nämlich nicht nur, auf vergangenes Unrecht zu reagieren, sondern durch diese Reaktion darüber hinaus auch die Begehung künftigen Unrechts zu verhindern.[14] Das soll einerseits spezialpräventiv durch Einwirkung auf den Täter oder die Täterin passieren, andererseits generalpräventiv, indem der Gesellschaft (als Rezipientin der Strafrechtsanwendung) gezeigt wird, dass auf einen Rechtsbruch eine rechtsstaatliche Reaktion folgt.[15] Die flächendeckende Einhaltung von Rechtsnormen durch die Allgemeinheit kann aber nur dann gelingen, wenn eine Zuwiderhandlung durch die Rechtsprechung auch formell als solche bezeichnet und sanktioniert wird. Entsteht der Eindruck, dass Rechtsgüter ohne Folgen geschädigt werden können, wird das Strafrecht seinem Zweck nicht mehr gerecht.

Damit es beim Einsatz von KI nicht zu einer strafrechtlichen Regelungslücke in Form einer solchen „Verantwortungsdiffusion“[16] kommt, muss eine Strafbarkeit des intelligenten Agenten selbst diskutiert werden – und zwar unabhängig davon, ob man die baldige Existenz sowohl äußerlich, als auch hinsichtlich ihrer kognitiven Fähigkeiten menschengleicher KI für wahrscheinlich hält oder nicht. Die Rechtswissenschaft ist aufgefordert, den digitalen Wandel im Sinne unserer normativen Werteordnung mitzugestalten. Deswegen ist es angesichts der präventiven Strafzwecke nicht hinnehmbar, erst dann Lösungen für die rechtlichen Probleme im Zusammenhang mit KI zu finden, wenn diese sich bereits in einer Rechtsgutsverletzung niedergeschlagen haben. Die dogmatische Auseinandersetzung muss bereits vorher stattfinden.

II. Dogmatische Herausforderungen einer KI-Strafbarkeit

Hinsichtlich der praktischen Anwendbarkeit des Strafrechts auf intelligente Agenten werden drei zentrale Kritikpunkte angeführt, die zeigen, dass unsere Individualstrafrechtsdogmatik auf den Einsatz autonom agierender KI nicht vorbereitet ist.[17]

Erstens fehle es an der Fähigkeit der KI, eine Handlung im strafrechtlichen Sinne vorzunehmen. Zweitens könne sie auch nicht schuldfähig sein. Und drittens sei ein intelligenter Agent kein tauglicher Adressat einer Kriminalstrafe.

1. Handlungsbegriff im Zusammenhang mit KI

Für die Frage nach der Handlungsfähigkeit ist relevant, wie stark man den Handlungsbegriff im Zusammenhang mit KI am bisherigen Begriffsverständnis orientieren möchte.

Es könnte zunächst darauf ankommen, inwieweit man den Begriff normativ auflädt. Sieht man die Fähigkeit der KI zum wenigstens potenziellen Normverständnis als Voraussetzung der Handlungsfähigkeit, so wäre diese, zumindest zum jetzigen Zeitpunkt, abzulehnen.[18] Die Fähigkeit, einen unbekannten sensorischen Impuls als verpflichtend zu erkennen und dementsprechend zu handeln, besitzen intelligente Agenten (noch) nicht.

[7] Dazu *Gless/Weigend*, ZStW 126 (2014), 561 (581); vgl. auch *Markwalder/Simmler*, AJP/PJA 2017, 171 (177).
[8] *Gless/Weigend*, ZStW 126 (2014), 561 (583 f.); krit. *Gless/Janal*, JR 2016, 561 (566).
[9] *Borges*, NJW 2018, 977 (978).
[10] *Sternberg-Lieben*, in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, Robotik und Recht, Bd. 3, 2013, S. 119.
[11] *Brüning*, Das Verhältnis des Strafrechts zum Disziplinarrecht, 2017, S. 186 f.
[12] Vgl. *Meier*, Strafrechtliche Sanktionen, 4. Aufl. 2015, S. 36.
[13] *Brüning*, in: Gesk/Jing (Hrsg.), Digitalisierung und Strafrecht in Deutschland und China, noch unveröffentlichtes Manuskript des Vortrags vom 22.11.2018 an der Universität Osnabrück.
[14] *Meier* (Fn. 12), S. 18 ff.
[15] *Meier* (Fn. 12), S. 21 f.
[16] *Beck*, JR 2009, 225 (227 f.).
[17] *Brüning* (Fn. 13); *Seher*, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, Robotik und Recht Bd. 9, 2016, S. 46 f.
[18] *Seher* (Fn. 17), S. 48 ff.

Problematisch wird die Annahme einer Handlung aber auch dann, wenn man lediglich ein willensgetragenes Verhalten fordert. Hier ist dann fraglich, ob Wille in diesem Sinne in Abgrenzung zum bloßen Reflex, also kausalistisch verstanden werden muss oder die Zweckgerichtetheit, also Finalität, der Handlung verlangt wird.[19]

Es wäre in beiden Fällen bereits an dieser Stelle zu diskutieren, inwieweit intelligente Agenten ein Bewusstsein haben, um Normverständnis zu entwickeln bzw. die Fähigkeit zur Bildung eines zweckgerichteten Willens besitzen.

Doch schon diese Termini technici zeigen, dass unsere humanistisch geprägte Individualstrafrechtsdogmatik nur bedingt geeignet ist, die rechtlichen Probleme im Zusammenhang mit KI zu lösen. Das Strafrecht ist von Menschen für Menschen erdacht worden. Künstlich intelligente Maschinen kamen in der Vorstellung des Gesetzgebers und der Rechtswissenschaft bis vor wenigen Jahren nicht vor. Es fehlt daher bereits von vornherein an einer unmittelbaren Übertragbarkeit menschlicher Begriffskategorien. Auf das Erfordernis der Willensgetragenheit im menschlichen Sinne kann jedoch verzichtet werden, wenn für die Strafbarkeit nicht an die Begehung individuellen Unrechts, sondern an die Verwirklichung systemischen bzw. algorithmischen Unrechts angeknüpft wird.[20]

So ähnlich machen es Rechtsordnungen, die, anders als die Deutsche, bereits eine Unternehmensstrafbarkeit kennen. Die strafbewehrte Handlung des Unternehmens fußt demnach nicht auf menschlichem Vertreterverhalten, sondern auf seiner inneren Struktur, also der unternehmensinternen Organisation und Kommunikation.[21] Die Aktionen der menschlichen Organe und Vertreter des Unternehmens stellen dann lediglich die Umsetzung dieses übergeordneten Kommunikationsprozesses dar und sind daher keine eigenen Handlungen des jeweiligen Menschen, sondern solche des Unternehmens per se.[22]

Ebenso lässt sich nun für intelligente Agenten argumentieren: Wird für die Handlungsfähigkeit des Unternehmens auf dessen Eigendynamik rekurriert, so kann genauso auf den eigendynamischen algorithmischen Prozess abgestellt werden.[23] Bei der Prüfung der Strafbarkeitsvoraussetzungen ist die Handlung dasjenige Merkmal, welches kausal und objektiv zurechenbar den tatbestandlichen Erfolg herbeiführt. Ein solches rechtlich missbilligtes Risiko, das später Erfolg zeitigt, kann gleichermaßen durch Fehler innerhalb kommunikativer Strukturen in einem Unternehmen oder eben Fehler innerhalb des Algorithmus gesetzt worden sein. Mit einem Verständnis des Handlungsbegriffs, das über die Verwirklichung individuellen Unrechts hinausgeht, lassen sich die Bedenken hinsichtlich der Handlungsfähigkeit intelligenter Agenten somit entkräften.

2. Schuldfähigkeit intelligenter Agenten

Die Handlung, bzw. der algorithmische Fehler, welcher das Unrecht verwirklicht, muss dem intelligenten Agenten ferner auch persönlich vorgeworfen werden können – er muss schuldfähig sein. Schuldfähigkeit in diesem Sinne bedeutet, dass eine Entscheidung gegen das Unrecht und für das Recht möglich gewesen wäre, der Täter diese Möglichkeit aber bewusst nicht genutzt hat.[24] Grundvoraussetzung für die Schuldfähigkeit ist also die Willensfreiheit. Denn nur, wer einen freien Willen bilden kann, ist auch in der Lage, bei Kenntnis und Verständnis von Normbefehlen die eigene Handlung nach diesen Normbefehlen auszurichten oder eben nicht.

a) Willensfreiheit als zwingende Voraussetzung für die Schuldfähigkeit?

Allerdings ist die Willensfreiheit in diesem Sinne nicht dem Beweis zugänglich. Ihre Existenz wird in der Neurowissenschaft von den Vertretern des Determinismus zum Teil sogar abgelehnt, wenigstens aber angezweifelt.[25] Demnach sei lediglich das Erleben der freien Entscheidung real, der Prozess hingegen, der zu einer Entscheidung führe, sei vollumfänglich vorherbestimmt – determiniert.[26] Die Entscheidung sei also Ergebnis der genetischen Disposition, Erziehung und Sozialisierung des Menschen, Ergebnis der aktuellen Stimmungslage, der sonstigen situativen Umstände und unzähliger weiterer Faktoren, die in ihren Einzelheiten nicht hieb- und stichfest nachvollzogen werden können. Doch auch das Gegenteil ist richtig: So wie sich zum jetzigen Zeitpunkt die menschliche Willensfreiheit nicht positiv beweisen lässt, so kann auch nicht sicher davon ausgegangen werden, dass eine solche nicht vorhanden ist.

Dass das tatsächliche Vorhandensein von Willensfreiheit nun zwingende Voraussetzung der Strafbarkeit sein soll, mutet vor dem Hintergrund des eben Gesagten aber widersinnig an. Wie kann ein nicht beweisbares und damit rechtsunsicheres Merkmal ausschlaggebend dafür sein, ob eine Strafe verhängt wird oder nicht?

Um dieses Problem zu lösen, bedarf es schon für die Frage nach der Schuld des menschlichen Täters einer pragmatischeren Herangehensweise. Die Willensfreiheit wird lediglich zugeschrieben, begründet auf dem eigenen menschlichen Erleben derselben. Wenn ich selbst – vermeintlich – einen freien Willen habe, so muss das bei allen anderen Menschen doch auch der Fall sein. Die Schuld als Strafbarkeitsvoraussetzung stellt sich somit als eine Zuweisung der Verantwortlichkeit dar, welche deshalb vorgenommen wird, weil durch das begangene Unrecht ein Konflikt innerhalb unseres sozialen Systems hervorgerufen wurde, der durch diese Zuweisung

[19] *Roxin*, Strafrecht, Allgemeiner Teil, Bd. 1, 4. Aufl. 2006, § 8 Rn. 10 ff.; *Heinrich*, Strafrecht Allgemeiner Teil, 5. Aufl. 2016, Rn. 96 ff.
[20] *Brüning* (Fn. 13).
[21] *Ortmann*, NZWiSt 2017, 241 f.
[22] *Dannecker/Dannecker*, NZWiSt 2016, 162 (164).
[23] Vgl. *Teubner*, AcP 218 (2018), 155 (157 ff., 165 f.).
[24] *Roxin* (Fn. 19), § 19 Rn. 1 ff.; BGHSt 2, 194 (200); 18, 87 (94).
[25] Vgl. *Marlie*, ZJS 2008, 41 (44 in Fn. 47–49).
[26] Vgl. *Marlie*, ZJS 2008, 41 (44 in Fn. 52).

aufgelöst werden soll.[27] Das gesellschaftliche Bedürfnis an dieser Auflösung besteht, weil aus den genannten Gründen die Unrechtsverwirklichung nicht ohne Sanktion bestehen bleiben darf.

Ein solches funktionales Verständnis der Schuld ermöglicht nun auch eine Zuweisung der Verantwortlichkeit an intelligente Agenten. Ein durch KI begangener Rechtsbruch ist grundsätzlich ebenso wie menschliches Fehlverhalten geeignet, einen auflösungsbedürftigen sozialen Konflikt zu verursachen, sofern auch dem Algorithmus die Willensfreiheit durch unser soziales System zugeschrieben wird. Es kommt also weder bei Mensch noch Maschine darauf an, ob die getroffene unrechte Entscheidung auf determinierten biologischen bzw. algorithmischen Vorgängen basiert oder auf rechtlich fehlerhafter freier Willensbildung.

b) Gedanken zu einem e-Personenstatus

Eine solche Verantwortungszuweisung aufgrund eines sozialen Konflikts gelingt allerdings nur insoweit, wie der intelligente Agent auch als Person im Rechtssinne angesehen wird.[28] Die generalpräventive Wirkung der Strafe kann sich nur dann entfalten, wenn einerseits der Adressat von der Bevölkerung nicht mehr als Sache, sondern als Rechtssubjekt angesehen und andererseits auch rechtlich so behandelt wird.

Dass Menschen künstlichen Intelligenzen menschliche Eigenschaften zuschreiben, sie also anthropomorphisieren, ließ sich schon in den 60er Jahren beobachten. Das von dem Informatiker Joseph Weizenbaum entwickelte Programm ELIZA simulierte eine psychotherapeutische Sitzung, indem es auf bestimmte, von der menschlichen Person im elektronischen Dialog gelieferte Schlagwörter, mit vorgefertigten Phrasen reagierte.[29] Trotz der stark eingeschränkten Möglichkeiten von ELIZA führte die Konversation dazu, dass einige Teilnehmende dem Programm Verständnis für die eigene Situation zuschrieben. Die Anthropomorphisierung von Verhalten künstlich intelligenter Programme wird daher auch ELIZA-Effekt genannt.[30] Wenn dieser Effekt schon bei einem Programm eintreten kann, das nicht einmal einen Turing-Test bestehen würde, erscheint dies für hoch entwickelte und – ggf. auch in ihrer äußeren Erscheinung – dem Menschen ähnelnde KI umso naheliegender. Dass solche Entitäten von der Gesellschaft als etwas angesehen werden, das einen Status besitzt, der über denjenigen einer Sache hinausgeht, ist damit wahrscheinlich.

Darüber hinaus müsste ein solcher elektronischer Personenstatus dann auch rechtlich anerkannt werden. Es hat in der Politik bereits Vorstöße gegeben, die Einführung eines e-Personenstatus jedenfalls zu diskutieren. So hat etwa 2017 das EU-Parlament die Europäische Kommission aufgefordert, sich mit dieser Frage für das Zivilrecht zu beschäftigen.[31]

Dass die e-Person kein dogmatisches Luftschloss darstellen würde, zeigt sich an der Variabilität des Personenbegriffs im Recht. Unterscheidungen zwischen natürlichen und juristischen Personen, zwischen Volljährigen und Minderjährigen oder Differenzierungen im Hinblick auf die Strafmündigkeit machen deutlich, dass den verschiedenen Personenbegriffen stets eine Wertung innewohnt: Welche gesellschaftliche, rechtliche, moralische Stellung hat das betroffene Rechtssubjekt und welchen Schluss will die Rechtsordnung daraus ziehen?[32] Betrachtet man den bereits beachtlichen und künftig noch anwachsenden Stellenwert und die Allgegenwärtigkeit digitaler Technologien sowie die damit verbundenen Herausforderungen und rechtlichen Probleme, ist der Schluss meiner Ansicht nach folgender: Die Einführung eines e-Personenstatus ist sinnvoll und erforderlich – sowohl rechtspolitisch als auch aus strafzwecktheoretischen Erwägungen.

3. Bestrafbarkeit intelligenter Agenten

Schließlich wird noch eingewendet, dass eine elektronische Person gar nicht bestraft werden könne. Fraglich ist also zunächst, welche Merkmale die Kriminalstrafe spezifisch aufweist und schließlich, ob diese gegenüber einem intelligenten Agenten zur Geltung kommen können. Drei Charakteristika können hierbei unterschieden werden: der Übelscharakter, das mit der Strafe verbundene sozialethische Unwerturteil und der Missbilligungscharakter.

Betrachten wir zunächst die Übelszufügung. Durch die Strafe findet eine Einwirkung auf den Täter statt, die von diesem als nachteilig empfunden werden soll.[33] Dabei ist es unschädlich, dass dies nicht immer tatsächlich der Fall ist, denn es werden jedenfalls verfassungsrechtliche Garantien eingeschränkt, etwa die Fortbewegungsfreiheit und die Persönlichkeitsentfaltung – genannt sei an dieser Stelle das Lehrbuchbeispiel des Obdachlosen, der sich vor dem Winter intendiert einsperren lässt, um die kalte Jahreszeit in der beheizten JVA zu verbringen.[34]

Allerdings wird es den Betroffenen wohl wenig interessieren, ob das (auch als solches empfundene) Übel, also beispielsweise die Zahlung eines Geldbetrages, als eine Geld-

[27] *Markwalder/Simmler*, AJP/PJA 2017, 171 (180); *Gless/Weigend*, ZStW (126), 2014, 561 (574 f.); vgl. auch *Roxin* (Fn. 19), § 16 Rn. 39 ff.

[28] *Seher* (Fn. 17), S. 58; Zur Frage, ob eine Statusdebatte überhaupt sinnvoll ist, *Beck*, in: Hilgendorf/Günther (Hrsg.), Robotik und Gesetzgebung, Robotik und Recht, Bd. 2, 2013, S. 239.

[29] Siehe Österreichische Akademie der Wissenschaften v. 1.12.2017, abrufbar unter https://www.oeaw.ac.at/detail/news/gefangen-im-eliza-effekt/ (4.2.2020).

[30] Vgl. dazu *Gless/Weigend*, ZStW 126 (2014), 561 (565); *Herberger*, NJW 2018, 2825 (2826).

[31] Entschließung des Europäischen Parlaments von 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103 [INL]), abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//DE (4.2.2020).

[32] *Teubner*, AcP 218 (2018), 155 (168 f.); Vgl. zum Personenbegriff im Zoll- und Mehrwertsteuerrecht *Scheller/Zaczek*, UR 2015, 937.

[33] *Meier* (Fn. 12), S. 16.

[34] *Meier* (Fn. 12), S. 16.

strafe oder eine Geldbuße zu erfolgen hat.[35] Gleiches gilt für die Freiheitsstrafe, die Sicherungsverwahrung als Maßregel und den polizeilichen Gewahrsam. In allen Fällen, werden die gleichen verfassungsrechtlichen Garantien eingeschränkt. Die Übelszufügung ist also kein spezifisches Merkmal der Strafe.[36]

Ebenso wie die Übelszufügung ist auch das sozialethische Unwerturteil kein Merkmal, das spezifisch die Strafe kennzeichnet.[37] So wird im Falle einer Normverletzung sowohl im Straf- als auch im Disziplinar- und Ordnungswidrigkeitenrecht der staatliche Vorwurf erhoben, der Betroffene habe sich unrechtmäßig verhalten: Auch durch ein Falschparker-Ticket wird zum Ausdruck gebracht, dass dieses Verhalten im Widerspruch zum gesamtgesellschaftlichen Wertekonsens in Form der Rechtsordnung steht.[38]

Darüber hinaus lässt sich kaum bestimmen, inwiefern die Sozialethik als Charakteristikum dienen soll. Schon begrifflich ist sie denkbar wenig trennscharf.[39]

Und schließlich begegnet es verfassungsrechtlichen Bedenken, die Strafe explizit durch ein solches Werturteil zu kennzeichnen. Käme es der Strafe nämlich gerade auf die Herabwertung der moralisch-ethischen Wertigkeit des Täters an, so würde ihn dies in seinem durch die Menschenwürde garantierten persönlichen Geltungsanspruch betreffen[40] – staatliches Mobbing, wenn man so möchte.

Übrig bleibt damit die Missbilligung als zentrales Wesensmerkmal der Strafe und somit die unmittelbare Verknüpfung der Strafe mit der Schuld des Täters.[41] Die persönliche Vorwerfbarkeit, welche für die Verhängung der übrigen staatlichen Sanktionen gerade keine Voraussetzung ist, kennzeichnet den höheren Grad der Missbilligung des strafrechtlich relevanten Verhaltens und damit die auf dieses Verhalten folgende Strafe als solche. Wenn nun künstliche Intelligenzen, wie eben festgestellt, schuldfähig im Sinne einer (aus unserer sozialen Wirklichkeit folgenden) Verantwortungszuschreibung sind, dann kann die Strafe ihren missbilligenden Charakter auch gegenüber KI entfalten.

Die bloße Feststellung der Strafbarkeit reicht jedoch für die Erreichung der generalpräventiven Ziele nicht aus. Der Bevölkerung als Rezipientin muss das begangene Unrecht greifbar veranschaulicht werden, weshalb es einer Quantifizierung des Schuldvorwurfs durch ein möglichst gerechtes Strafmaß bedarf. Hierbei kann an gemeinnützige Arbeit, Eingriffe in den Roboterkorpus oder als ultima ratio auch an ein Abschalten gedacht werden.[42]

Zu denken ist ferner noch an eine Umprogrammierung durch eine Implementierung des Sinngehalts der verletzten Norm in den Algorithmus.[43] Das hätte sowohl maximale spezialpräventive als auch ggf. generalpräventive Wirkung, soweit mehrere intelligente Agenten miteinander vernetzt sind und die Implementierung somit flächendeckend erfolgen kann. Auch die Bestrafbarkeit von künstlichen Intelligenzen ist also möglich.

III. Fazit

Die vierte industrielle Revolution ist in vollem Gange. Diejenigen Wissenschaftsdisziplinen, die davon betroffen sind, sind daher aufgefordert, sie aktiv und im regen Austausch untereinander mitzugestalten. Andernfalls drohen sie abgehängt oder gar zur Bremse für den Fortschritt zu werden.

Aus diesem Grund muss die Rechtsordnung adäquate Antworten auf die Fragen und Probleme parat haben, die damit einhergehen. Die Einführung einer KI-Strafbarkeit wird dabei langfristig unumgänglich sein. Den gegenüber einer solchen Strafbarkeit geäußerten Bedenken kann dogmatisch fundiert entgegengetreten werden, indem in diesem Feld ein erweitertes, über die bisherigen Grenzen der Individualstrafrechtsdogmatik hinausgehendes Verständnis strafrechtlicher Begrifflichkeiten zugelassen wird. Das betrifft die Handlungsfähigkeit und insbesondere die Schuldfähigkeit und mit letzterer verknüpft das Verständnis von Strafe.

Auch wenn der technologische Fortschritt hinsichtlich seiner Ausmaße und seiner Geschwindigkeit bei Zeiten ein wenig beängstigend sein mag, so kann er wohl kaum aufgehalten werden. Und das soll er auch gar nicht. Die Vorteile dürften die rechtlichen wie technischen Risiken jedenfalls dann überwiegen, wenn diese rechtzeitig erkannt und minimiert oder gänzlich gelöst werden. So wird zumindest aus der Rechtswissenschaft keine „Technikverhinderin".

Enden möchte ich in Ansehung dessen mit einem Zitat von Kaiser Wilhelm II., der zu Beginn des 20. Jahrhunderts sagte: „Ich glaube an das Pferd. Das Automobil ist eine vorübergehende Erscheinung."

[35] Vgl. *Roxin*, in: Hassemer/Kempf/Dörr/Moccia (Hrsg.), In dubio pro libertate, Festschrift für Klaus Volk zum 65. Geburtstag, 2009, S. 602.
[36] A.A. *Meier* (Fn. 12), S. 16.
[37] *Brüning* (Fn. 11), S. 547 ff.
[38] *Brüning* (Fn. 11), S. 549.
[39] *Roxin* (Fn. 35), S. 603.
[40] *Brüning* (Fn.11), S. 543 f. m.w.N.
[41] *Brüning* (Fn. 11), S. 547 f.
[42] *Gless*, GA 2017, 324 (328).
[43] *Gless/Weigend*, ZStW 126 (2014), 561 (589).

Die Privatsphäre im Zeitalter von Big Data

Zum staatsanwaltschaftlichen Zugriff auf personenbezogene Daten in Speichern privater Dritter

Von Leitender Oberstaatsanwalt PD Dr. **Ralf Peter Anders**, Hamburg

I. Problemstellung

Der vorliegende Beitrag behandelt die Frage, ob die traditionellen Eingriffsgrundlagen für staatsanwaltschaftliches Handeln zur Ermittlung von elektronischen personenbezogenen Daten, nämlich § 161 Abs. 1 StPO und § 95 StPO, dem modernen Phänomen „Big Data" gerecht werden können. Elektronische Daten unterscheiden sich schon ihrer Art nach wesentlich von den herkömmlichen Beweismitteln; jedoch sind strafprozessuale Regelungen zum Umgang mit ihnen nur bruchstückhaft vorhanden, so dass Normen wie § 161 Abs. 1 StPO und § 95 StPO, die sich genuin auf körperliche Gegenstände beziehen, auf elektronische Daten angepasst werden.[1] Die Frage ist, ob diese traditionelle Vorgehensweise auch mit Blick auf Big Data noch angemessenen erscheint.

Big Data inhäriert das Potential einer totalen Kontrolle: Begriffe wie „embedded", „ubiquitous" und „wearable computing" sowie „smart home"[2] zeigen uns, dass wir im Alltag von speichernder Informationstechnologie, von einem sich ständig erweiternden Gedächtnis, dessen Einheiten durch permanenten Datenfluss miteinander „kommunizieren"[3], das wir durch unser Alltagsverhalten weitgehend unbemerkt mit riesigen Datenmengen beliefern, umgeben sind. Beispielhaft dafür stehen etwa internetfähige smart-Fernsehgeräte, smart-Kühlschränke und Sprachassistenzsysteme.[4] Diese Daten werden von privaten Dienstleistern, denen sie freiwillig und gutgläubig übertragen werden, nicht nur gesammelt, sondern von diesen auch sortiert, genauestens ausgewertet und über Algorithmen prognostisch und gewinnorientiert eingesetzt. Private Datensammler betreiben damit aus eigenem Interesse eine „Perfektionierung des Wissens über Personen"[5] und verfügen über eine machtvolle Datenherrschaft. Mit Blick auf die damit verbundene Gefahr für die Datenbetroffenen geht es im vorliegenden Beitrag nicht um den Schutz vor den privaten Datensammlern selbst, sondern um den „klassischen" Zugriff der Strafverfolgungsbehörden auf die privaten Speicher.

Anreize zur Zusammenarbeit zwischen privaten Datenspeichern und Strafverfolgungsbehörden bestehen hüben und drüben – die Rede ist von einer „public private partnership"[6]. Es ist von einer geringeren Grundrechtsgebundenheit der privaten Speicher gegenüber den privaten Nutzern auszugehen, so dass dem staatlichen Zugriff im Zweifel ein großer Datenbestand zu Grunde gelegt werden kann.[7] Der Staat spart zudem Ressourcen für die Sichtung und Aussonderung der relevanten Daten (muss dann allerdings auch auf deren Validität vertrauen können). Die privaten Unternehmen vermeiden Durchsuchungen und Beschlagnahmen und damit Reibungsverluste im Geschäftsbetrieb sowie eine negative publicity.[8]

II. Die „klassischen" Eingriffsgrundlagen: §§ 95, 161 Abs. 1 StPO

Die §§ 95, 161 Abs. 1 StPO sind für die Strafverfolgungsbehörden attraktiv, weil diese Vorgehensweisen eine richterliche Anordnung zunächst weitgehend obsolet machen: Bei § 161 Abs. 1 StPO reicht es in der Regel, wenn eine richterliche Beschlagnahmeanordnung (oder eine Zeugenvernehmung) in Aussicht gestellt wird, bei der Editionspflicht ist sie nach zutreffender Auffassung vorher nicht erforderlich, da der Richtervorbehalt des § 98 Abs. 1 StPO nur für die Beschlagnahme gilt.[9] Es handelt sich bei beiden Maßnahmen nach richtigem Verständnis um Vorfeldmaßnahmen: Private sind nach § 161 Abs. 1 StPO nicht zur Auskunft verpflichtet, Unternehmen genauso wenig wie Einzelpersonen; ihre informatorische Inanspruchnahme durch die Staatsanwaltschaft ist nur gemäß § 161a StPO (zeugenschaftliche Vernehmung) oder im Wege der Durchsuchung und Beschlagnahme möglich.[10] Die Staatsanwaltschaft kann daher unverbindliche Anfragen auf freiwillige Auskunft stellen, die in der Praxis zudem regelmäßig – rechtlich unbedenklich – unter Hinweis auf sonst beabsichtigte Ermittlungsmaßnahmen erfolgen.[11] Erst in diesem Zusammenspiel von Anfrage und Androhung kann in § 161 Abs. 1 StPO überhaupt eine *Eingriff*sgrundlage gesehen werden. Und § 95 StPO kann die Beschlagnahme abwenden, wenn diese aus Erwägungen der Verhältnismä-

---

[1] *Warken*, NZWiSt 2017, 417.

[2] Zur Abhörfähigkeit von smarten Haushaltsgeräten vgl. *Steigerwald* im Interview mit *Gießler*, Zeit Online v. 29.6.2019, abrufbar unter https://www.zeit.de/digital/datenschutz/2019-06/smart-home-haussteuerung-systeme-datensicherheit-gefahren-risiken (4.2.2020).

[3] *Blechschmitt*, MMR 2018, 361 (362).

[4] *Thür*, Jusletter IT 21.5.2005, 1 (1, 3).

[5] *Thür,* Jusletter IT 21.5.2005, 1 (6).

[6] *Peters*, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 527 (528).

[7] *Peters* (Fn. 6), S. 529.

[8] *Peters* (Fn. 6), S. 530.

[9] Vgl. LG Lübeck NJW 2000, 3148; LG Gera NStZ 2001, 276; LG Halle NStZ 2001, 276 (277); LG Koblenz wistra 2002, 359; *Bittmann*, NStZ 2001, 231; *Gerhold*, in: Graf (Hrsg.), Beck'scher Online Kommentar, Strafprozessordnung, Stand: 1.10.2019, § 95 Rn. 9; *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, Kommentar, 62. Aufl. 2019, § 95 Rn. 2; a.A. die ältere Rechtsprechung: KG NStZ 1989, 192; LG Bonn NStZ 1983, 327; LG Stuttgart NJW 1992, 2646; *Menges*, in: Erb/Esser/Franke/Graalmann-Scheerer/Hilger/Ignor (Hrsg.), Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 3, 26. Aufl. 2012, § 95 Rn. 20 m.w.N.

[10] *Kölbel*, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2016, § 161 Rn. 26.

[11] *Kölbel* (Fn. 10), § 161 Rn. 27; *Sackreuther*, in: Graf (Fn. 9), § 161 Rn. 10.

ßigkeit oder aus tatsächlichen Gründen erfolglos wäre.[12] Ein Defizit an gerichtlicher Kontrolle ist in beiden Fällen nicht gegeben: Betroffene können im Falle der Verweigerung des Auskunftsverlangens eine richterliche Beschlagnahmeanordnung abwarten. Jedenfalls die nachfolgende Durchsetzung der Herausgabeverpflichtung mit Zwangsmitteln steht unter Richtervorbehalt (§§ 95 Abs. 2 S. 1, 70 Abs. 3 StPO)[13] und das polizeiliche oder staatsanwaltschaftliche Herausgabeverlangen kann entsprechend §§ 98 Abs. 2 S. 2, 161a Abs. 3 StPO richterlich überprüft werden.[14]

Die beiden Eingriffsgrundlagen sollen am Beispielsfall der Abfrage von Kreditkartendaten dargestellt werden, über den bereits das BVerfG zu entscheiden hatte: Für den Zugang zu einer Internetseite mit kinderpornografischem Inhalt mussten 79,99 US-Dollar per Kreditkarte gezahlt werden. Die Staatsanwaltschaft versuchte, die Kunden dieser Internetseite als Beschuldigte dadurch zu ermitteln, dass sie die Institute anschrieb, die Mastercard- und Visa-Kreditkarten in Deutschland ausgeben, und forderte sie auf, alle Kreditkartenkonten anzugeben, die eine Überweisung des genannten Betrages an eine philippinische Bank aufwiesen, über die der Geldtransfer für den Betreiber der Internetseite abgewickelt wurde. Die Unternehmen übermittelten der Staatsanwaltschaft daraufhin die erbetenen Daten der betreffenden Karteninhaber. Die Beschwerdeführer, die Inhaber von jedenfalls nicht vom Datentransfer betroffenen Kreditkarten waren, erhoben nach erfolglosem Durchlauf des Instanzenzuges Verfassungsbeschwerde, die das BVerfG durch Kammerbeschluss bekanntlich nicht zur Entscheidung angenommen hat.[15] Das Gericht verneinte einen Eingriff in das Recht auf informationelle Selbstbestimmung; bei den Kreditkarteninhabern sei dieses Recht zwar betroffen, aber nicht verletzt, da § 161 Abs. 1 StPO eine ausreichende und hinreichend bestimmte Ermächtigungsgrundlage darstelle: Die Norm stehe unter dem begrenzenden Zweck der Straftataufklärung und wegen des Gewichts des Interesses an der effektiven Kriminalitätsverfolgung der in Frage stehenden Straftaten sei die Maßnahme auch verhältnismäßig.[16]

Dagegen wird aus datenschutzrechtlicher Sicht vorgebracht, dass von einer Freiwilligkeit der Auskunft nach Anfrage gem. § 161 Abs. 1 StPO keine Rede sein könne, da die ansonsten negative Publizitätswirkung der Durchsuchung im Raume stehe.[17] Diese Ansicht kann für sich in Anspruch nehmen, dass der Einwilligung gegenüber Behörden jedenfalls unter dem Regime der DSGVO generell wenig bis kaum mehr Gewicht beigemessen werden kann. So nimmt der Erwägungsgrund 43 der DSGVO die Unwirksamkeit der Einwilligung an, „wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbes. wenn es sich bei dem Verantwortlichen um eine Behörde handelt". Jedoch findet die DSGVO nach ihrem Art. 2 Abs. 2 lit. d keine Anwendung auf die Strafverfolgung, und die insoweit einschlägigen Umsetzungsgesetze der EU-RL 2016/680 v. 27.4.2016 sehen derartige Ressentiments gegen die Einwilligung nicht vor; diese verlangen vielmehr eine Rechtsvorschrift für freiwilliges Handeln, die mit den §§ 95, 161 Abs. 1 StPO jeweils gegeben sein dürfte (vgl. § 500 Abs. 1 StPO; 51 Abs. 1 BDSG).

Zudem wird jedenfalls bei verdeckten Ermittlungen – insbesondere gegenüber den Datenbetroffenen – angesichts der Grundrechtsbetroffenheit die Notwendigkeit einer spezifischen Eingriffsgrundlage angemahnt: Die fehlende Offenheit bedinge es, dass die Betroffenen gerichtlichen Rechtsschutz in der Regel erst nachträglich einholen könnten.[18] Auch hätten verdeckte Ermittlungsmaßnahmen oftmals eine große „Streubreite"[19]. Ob – wie behauptet – bei verdeckten Eingriffen mangels Transparenz die Rechtswidrigkeitswahrscheinlichkeit des Grundrechtseingriffs steige,[20] ist empirisch hingegen nicht belegt. Schließlich bestehe bei einigen verdeckten Ermittlungsmaßnahmen die Gefahr, dass ohne Wissen der Betroffenen in deren Kernbereich privater Lebensgestaltung eingegriffen werde. Antikritisch ist zu entgegnen, dass die Heimlichkeit zwar eines, aber für sich kein allein ausreichendes Kriterium für die Eingriffstiefe einer Maßnahme sein kann, welche eine (spezialgesetzliche) Ermächtigungsgrundlage zwingend erfordern würde.[21] Denn das Kriterium der Heimlichkeit trifft auch auf Ermittlungsmaßnahmen mit geringer Eingriffsintensität zu, wie etwa auf die nach den §§ 161, 163 StPO zulässige kurzfristige Observation.[22] Das BVerfG hat in seiner „Kreditkarten"-Entscheidung die Heimlichkeit des Vorgehens der Strafverfolgungsbehörden gar nicht erst in den Kriterienkatalog zur Bewertung der Eingriffsintensität eingebracht,[23] was damit erklärt werden kann, dass die Staatsanwaltschaft in dem betreffenden Fall gar keine andere Möglichkeit hatte als gegenüber den Datenbetroffenen nicht offen zu agieren, da diese zum Zeitpunkt der Abfrage nicht bekannt sein konnten. Diese faktische Alternativlosigkeit ändert gleichwohl im Ergebnis nichts an der intensiveren Grundrechtsbetroffenheit jedenfalls der Karteninhaber, deren Daten ausgefiltert und herausgegeben worden sind.

[12] LG Kaiserslautern NStZ 1981, 438 (439); LG Halle NStZ 2001, 276 (277); *Jahn*, in: Heinrich/Jäger/Schünemann (Hrsg.), Festschrift für Claus Roxin zum 80. Geburtstag am 15. Mai 2011, Strafrecht als Scientia Universalis, 2011, S. 1357 (1365).

[13] *Hauschild*, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 1, 2014, § 95 Rn. 7.

[14] LG Gera NStZ 2001, 276; LG Halle NStZ 2001, 276 (277).

[15] Vgl. BVerfG NJW 2009, 1405.

[16] Vgl. BVerfG NJW 2009, 1405 (1408).

[17] Vgl. *Petri*, StV 2007, 266 (268).

[18] Vgl. BVerfGE 107, 299 (321); 115, 116 (194 f.); *Hefendehl*, StV 2001, 700 (703); *Peters,* S. 533.

[19] *Klesczewski*, ZStW 123 (2011), 737 (749); *Schwabenbauer*, Heimliche Grundrechtseingriffe. Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung (2013), S. 176 ff.

[20] *Peters* (Fn. 6), S. 533.

[21] Vgl. BVerfG NJW 2008, 822 (830); NJW 2009, 1405 (1407).

[22] Vgl. *Sackreuther* (Fn. 11), § 161 Rn. 11.

[23] Kritisch *Peters* (Fn. 6), S. 532 f.

Mit Blick auf die Herausgabe der verlangten Daten wäre in dem vom BVerfG entschiedenen Fall wohl auch die Editionspflicht des § 95 StPO in Betracht gekommen, wobei die zu § 161 Abs. 1 StPO dargelegten Erwägungen zur Heimlichkeit auch für das Vorgehen im Rahmen der Editionspflicht gelten dürften. Voraussetzung für die Anwendung des § 95 StPO ist, dass sich der betreffende Gegenstand im Gewahrsam des Betroffenen befindet[24] und er dementsprechend definiert werden kann. Nach der Rechtsprechung des BVerfG kann sich das Herausgabeverlangen jedoch zum einen auch auf nichtkörperliche Gegenstände sowie zum anderen auf Gegenstände in diesem Sinne beziehen, die nicht bereits vorhanden sind, sondern erst aufgrund des Herausgabeverlangens geschaffen werden müssen (z.B. durch Zusammenstellung von Einzeldaten nach konkreten Suchkriterien aus einem Gesamtdatenbestand).[25] Diese Erweiterung auf (zu erstellende) digitale Daten wird insbesondere mit Blick auf einen fehlenden Grundrechtsschutz der Datenbetroffenen kritisiert.[26] Das BVerfG argumentiert damit, dass es der Wortsinn ohne Überschreiten des Wortlauts des § 94 StPO gestatte, als „Gegenstand" des Zugriffs auch nichtkörperliche Gegenstände zu verstehen; zudem werde diese Auffassung durch legislatorische Entwicklungen bestätigt.[27] Gegenüber der Beschlagnahme der Originaldatenträger mit umfangreichem Datenbestand stellt das Herausgabeverlangen von nach konkreten Kriterien zusammengestellten Einzeldaten in Kopie zudem das mildere Mittel dar. Auch streitet Art. 18 Abs. 1 der Convention on Cybercrime (CC)[28] für die Auffassung des BVerfG.

[24] *Hauschild* (Fn. 13), § 95 Rn. 2.

[25] Vgl. BVerfG NStZ-RR 2003, 176 (177); BVerfGE 113, 29 (50); BVerfG NJW 2009, 2431 (2434); *Greven*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, § 94 Rn. 4; *Hauschild* (Fn. 13), § 95 Rn. 8; *Menges* (Fn. 9), § 95 Rn. 5.

[26] Vgl. *Klesczewski*, ZStW 123 (2011), 737 (747) m.w.N.

[27] Neben den gesetzgeberischen Wertungen des § 97 Abs. 5 S. 1 StPO, vgl. BT-Drs. 7/2539, S. 11, und der §§ 98a ff. StPO, vgl. BT-Drs. 12/989, S. 36, würden die Gesetzesmaterialien zur Neufassung des § 110 Abs. 1 StPO durch das 1. Justizmodernisierungsgesetz v. 24.8.2004, vgl. BGBl. I 2004, S. 2189, dafür sprechen, vgl. BVerfGE 113, 29 (50); BVerfG NJW 2009, 2431 (2434).

[28] Art. 18 – Anordnung der Herausgabe: Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen, a) dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und b) dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat.

III. Auskunftsverlangen und Editionspflicht in Big-Data-Fällen

1. Die Entscheidung des BVerfG vom 16.6.2009 als „Blaupause"

Die Untergewichtung des heimlichen Vorgehens in der o.g. Kreditkartenentscheidung widerspricht der bekannten Rechtsprechungslinie des BVerfG, nach der lediglich die – insbesondere gegenüber dem Postfachinhaber – *offene* Beschlagnahme von E-Mails beim Internetprovider an den im Vergleich zu dem heimlichen Eingriff gemäß den §§ 100a f. StPO geringeren Voraussetzungen der §§ 94 ff. StPO gemessen werden darf.[29] Dem liegt zum einen eine angenommene zeitliche und situative Verlängerung des Grundrechtsschutzes aus Art. 10 GG betreffend den Kommunikationsinhalt zu Grunde, der an die (vermeintliche) Schutzbedürftigkeit des Grundrechtsträgers aufgrund der Einschaltung Dritter in den Kommunikationsvorgang anknüpft.[30] Zum anderen muss es überraschen, wenn das BVerfG trotz dieser Erweiterung des Schutzbereichs aus Art. 10 GG die strafprozessuale Schlussfolgerung zieht, dass die generellen Vorschriften der Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO als verfassungskonforme Eingriffsgrundlage beim Provider ausreichen sollen; insbesondere seien die Vorschriften wegen der strengen Begrenzung auf den Ermittlungszweck hinreichend bestimmt und auch in der Anwendung im konkreten Fall verhältnismäßig gewesen, wobei zur Sicherung des Grundsatzes der Datenminimierung konkrete Anforderungen betreffend den Schutz des Kernbereichs privater Lebensgestaltung sowie an die Sichtung und Trennung der zu erhebenden Daten nach Verfahrensrelevanz formuliert worden sind.[31] Die vom BVerfG zu Grunde gelegte Offenheit der Maßnahme ist dabei primär keine Forderung aus Gründen der Verhältnismäßigkeit, sondern eine Feststellung der vermeintlichen tatsächlichen Eigenheit des Eingriffs nach den §§ 94 ff. StPO.[32] Zwingend ist dies jedoch keinesfalls, da die Staatsanwaltschaft in der Regel jedenfalls ihre Herausgabeverlangen nach § 95 StPO mit dem Zusatz versieht, dass (etwa im Falle der Bankenanfrage) die Information des Kunden strafrechtliche Risiken nach sich ziehen könne. Auch ist bei einer Durchsuchung gemäß § 103 StPO die Unterrichtung des Beschuldigten über den Eingriff regelmäßig untunlich.[33] So legt das BVerfG dann auch relativierend die normative Forderung zu Grunde, dass der Postfachinhaber „im Regelfall" und „so früh, wie es die wirksame Verfolgung des Ermittlungszwecks erlaubt" über den Eingriff zu unterrichten ist.[34]

[29] Vgl. BVerfG NJW 2009, 2431 (2433 ff.).

[30] Vgl. BVerfG NJW 2009, 2431 (2432).

[31] Vgl. BVerfG NJW 2009, 2431 (2434 ff.).

[32] Vgl. BVerfG NJW 2009, 2431 (2435): „Hierbei ist zu berücksichtigen, dass die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers in der Regel nicht heimlich, sondern offen vollzogen wird." In diesem Sinne auch *Klein*, NJW 2009, 2996 (2998).

[33] *Klesczewski*, ZStW 123 (2011), 737 (749).

[34] BVerfG NJW 2009, 2431 (2437).

Im Rahmen der Verhältnismäßigkeitsprüfung prüft das BVerfG unter Hinweis auf seine Entscheidung zur Erlangung der bei einem Telekommunikationsunternehmen gespeicherten Verbindungsdaten[35] eine Beschränkung auf Ermittlungen betreffend Straftaten von erheblicher Bedeutung sowie Anforderungen an den Tatverdacht, die über den Anfangsverdacht einer Straftat hinausgehen.[36] Mit Blick auf Letztere müsse aufgrund bestimmter Tatsachen anzunehmen sein, dass der Beschuldigte mit hinreichender Wahrscheinlichkeit (solche) Straftaten begangen habe.[37] Die Begründung, mit der das BVerfG in seiner Entscheidung zur Beschlagnahme von E-Mails beim Provider neben dem Argument der offenen Vollziehung des Eingriffs eine solche Verschärfung der Eingriffsvoraussetzungen im Wesentlichen ablehnt – „(a)nderenfalls wäre es für jeden Nutzer ein Leichtes, belastende E-Mails durch eine Auslagerung auf den Mailserver seines Providers dem Zugriff der Strafverfolgungsbehörden zu entziehen“[38] – dürfte jedoch im Widerspruch zu der Argumentation des Gerichts stehen, welche für die Verlängerung des Grundrechtsschutzes aus Art. 10 GG stehen soll, nämlich den Mangel an Beherrschbarkeit bei Speicherung beim Provider und der daraus folgenden besonderen Schutzbedürftigkeit des Grundrechtsträgers. Die genannte Begründung ist nur in dem vom BVerfG nicht genannten Kontext verständlich, nämlich dass der Empfänger tatsächlich die Möglichkeit hat, auch im Bereich des Providers durch Löschen über das Schicksal der E-Mails zu entscheiden[39]. Insoweit besteht für den Postfachinhaber in den E-Mail-Fällen eine (Macht-)Missbrauchsmöglichkeit im Sinne eines safehouse.

Die Staatsanwaltschaft hätte über die E-Mails auch Auskunft nach § 161 Abs. 1 StPO verlangen können. Über die Problematik der Beschlagnahme von bei privaten Providern gespeicherten E-Mails hinaus dürfte diese Rechtsprechung des BVerfG auch sonstige Formen des Datentransfers von Datenbetroffenen an private Speicherstellen erfassen können.[40] Danach käme auch für die Big-Data-Fälle die Entscheidung des BVerfG zur Beschlagnahme von E-Mails beim Provider als „Blaupause“ im Sinne einer Lösung über ein an den materiellen Rechtfertigungsanforderungen und nicht an der Schutzbereichszuordnung orientierten Verständnis[41] in Betracht. Deren Tragfähigkeit soll anhand zweier Beispielsfälle aus dem Bereich Big Data untersucht werden.

2. Beispielsfälle

Wie eingangs dargelegt, ist Big Data nicht lediglich – wie im Kreditkartenfall – durch punktuelle Datenerhebungen und ihre Transfers an Dritte definiert, sondern durch einen permanenten Datenfluss und damit ein andauerndes Datensammeln und -verknüpfen beim privaten Speicher. Zudem kann zwar der Datenbetroffene – bestenfalls – Datenlöschungen veranlassen. Anders als im E-Mail-Fall besteht eine solche Möglichkeit für den Datenbetroffenen bei Big Data in der Cloud des speichernden Dritten jedoch entweder gar nicht oder zumindest nicht lückenlos. Dies ist ein Charakteristikum von Big Data: Die Abhängigkeit des Datenbetroffenen von der Wirkmacht des privaten Datensammelnden. Dazu zwei Beispielsfälle:

a) Carsharing

Das LG Köln verurteilte den Nutzer eines Carsharing-Unternehmens im Jahre 2016 wegen fahrlässiger Tötung zu einer Freiheitsstrafe von zwei Jahren und neun Monaten. Hintergrund war ein tödlicher Unfall, den der Fahrer in der Kölner Innenstadt verursachte.[42] Erst in der laufenden Hauptverhandlung stellte der Fahrzeughersteller in Erfüllung einer BMW gegenüber bereits im Juli 2015 ergangenen Herausgabeanordnung der Staatsanwaltschaft Köln die sog. Log-Daten des Carsharing-Moduls zur Verfügung. Dieses Carsharing-Modul nimmt eine lückenlose Speicherung unterschiedlichster Daten vor, u.a. von GPS-Positionen und Geschwindigkeiten,[43] deren Einführung in die Hauptverhandlung maßgeblich zur Verurteilung des Fahrers beigetragen hat.[44] Im „Carsha-

[35] Vgl. BVerfG NJW 2003, 1787 (1791).
[36] Vgl. BVerfG NJW 2009, 2431 (2435).
[37] BVerfG NJW 2000, 55 (67); 2003, 1787 (1791).
[38] BVerfG NJW 2009, 2431 (2435).
[39] Zutreffend VGH Kassel MMR 2009, 714; *Krüger*, MMR 2009, 680 (681).
[40] Vgl. *Singelnstein*, NStZ 2012, 593 (597).
[41] Vgl. *Gurlit*, NJW 2010, 1035 (1041).

[42] LG Köln BeckRS 2016, 17291 = ZD 2017, 192 (insoweit nicht abgedruckt); bestätigt von BGH NZV 2017, 135.
[43] Über Carsharing-Systeme hinaus sollen nach Angaben des ADAC und des Automobildachverbandes FIA über das Navigationssystem im PKW einige Fahrzeugtypen bestimmter Autohersteller, insbesondere BMW, Mercedes und Renault, folgende Daten speichern und an den Hersteller übermitteln: die erreichte Maximal-Drehzahl des Motors mit jeweiligem Kilometerstand (diese Daten erlauben Rückschlüsse auf den Fahrstil), die Anzahl der Fahrtstrecken zwischen 0 und 5, 5 und 20, 20 und 100 sowie über 100 Kilometer (diese Daten erlauben Rückschlüsse auf das Nutzungsprofil), die Dauer, wie lange der Fahrer in verschiedenen Modi des Automatikgetriebes (Dauer/Manuell/Sport) unterwegs war (diese Daten erlauben Rückschlüsse auf den Fahrstil), die Betriebsstunden der Fahrzeugbeleuchtung, getrennt nach einzelnen Lichtquellen, die Zahl der Verstellvorgänge des elektrischen Fahrersitzes (diese Daten erlauben Rückschlüsse auf die Anzahl der Fahrer), die Anzahl der eingelegten Medien des CD-/DVD-Laufwerks (diese Daten erlauben Rückschlüsse auf die Intensität der Nutzung der Baugruppe) sowie Zahl der elektromotorischen Gurtstraffungen, etwa aufgrund starken Bremsens (diese Daten erlauben Rückschlüsse auf den Fahrstil), vgl. ADAC v. 14.1.2020, http://www.adac.de/daten (4.2.2020).
[44] Zwar wird aus datenschutzrechtlicher Sicht vertreten, dass im konkreten Fall die Datenerhebung durch den Anbieter mangels rechtswirksamer Einwilligung des Betroffenen rechtswidrig gewesen sei, weil der Nutzer nicht nachvollziehbar und verständlich darüber aufgeklärt worden sei, dass im Fahrzeug Daten ermittelt werden, die im Ergebnis durch die Verknüpfung mit den Kundendaten zur Erstellung eines Bewegungsprofils führen können, vgl. *Bockslaff/Kadler*, ZD 2017, 166 (168). Hierbei handelt es sich jedoch um ein vertraglich gestaltbares Feld, da die Datenschutzerklärungen der

ring"-Fall wusste der Fahrer vermutlich weder von der Datenerhebung durch das Modul noch dem Transfer an den Autohersteller; jedenfalls konnte er beides nicht – allenfalls durch Verzicht auf die Nutzung des Fahrzeugs – beeinflussen.

b) Amazon Echo/Sprachassistenzsystem Alexa

Stationäre Varianten digitaler Assistenten, wie etwa Echo von Amazon mit dem Sprachassistenzsystem Alexa, sind in deutschen Haushalten schon weit verbreitet; 2017 findet sich ein solches Gerät bereits in fünf Prozent der Haushalte, knapp jeder zehnte Deutsche plant die Nutzung eines Apple Homepod und sogar jeder Fünfte die Nutzung von Google Home.[45] Alexa ist in unterschiedliche Hardware mit Namen Echo verbaut, für deren Nutzung WLAN zur Abwicklung von Spracheingaben über die Server von Amazon, ein Smartphone, auf dem die Alexa-App installiert ist, sowie ein Amazon-Konto erforderlich sind.[46] Die permanent online befindliche Alexa reagiert auf Zuruf, wobei nach Angaben des Herstellers Alexa nur dann Daten aufzeichnet, wenn ein bestimmtes Signalwort fällt.[47] Der mit dem Signalwort verbundene Sprachbefehl wird an die Server von Amazon weitergeleitet und dort weiterverarbeitet, wobei alle Sprachaufzeichnungen sowohl dort als auch in der dazugehörigen Alexa-App standardgemäß gespeichert werden.[48] Amazon Echo Spot besitzt zudem eine eingebaute Videokamera, Gleiches gilt für das auf dem US-Markt erhältliche Echo Look, deren Aufnahmen wie die Sprachbefehle ebenfalls in der Cloud gespeichert werden können.[49] Über Alexa werden Telefonverbindungen hergestellt, Bestellungen aufgenommen, Erinnerungen abgespeichert und allgemein Fragen beantwortet.[50] Amazon sammelt neben diesen Daten verknüpfend weitere Informationen wie die IP-Adresse, E-Mail-Adresse, Passwörter, Informationen über die Hard- und Software, die Reihenfolge der aufgerufenen Internetseiten und die gesuchten Produkte.[51] Der Betroffene kann die Daten jedenfalls auf seinem Gerät löschen. Nach Angaben von Amazon werden trotz entsprechender Bemühungen des Unternehmens in einigen Fällen die Daten jedoch nicht aus der Cloud gelöscht.[52]

Soweit ersichtlich sind in Deutschland bis heute keine Alexa-Geräte staatlicherseits mittels technischer Systeme abgehört oder infiltriert worden; Gleiches gilt für die Beschlagnahme des Hausgerätes nebst anschließendem Versuch des technischen Auslesens des Gerätes. Auch erfolgte bis heute keine Abfrage bei Amazon Echo nach den dort gespeicherten Daten. Im Übrigen speichert Amazon auf ausländischen Servern;[53] damit sind für die Strafverfolgungsbehörden weitere Schwierigkeiten verbunden, die hier jedoch nicht thematisiert werden sollen.[54] Veröffentlicht worden ist, dass in den USA in den Jahren 2017 in Arkansas (dort nach Zustimmung des Verdächtigen) Amazon die gespeicherten Daten herausgegeben hat[55] und 2018 in New Hampshire eine entsprechende gerichtliche Anordnung gegen Amazon erging.[56]

Anbieter entsprechend formuliert werden können, vgl. a.a.O., 170. Die Frage der Konsequenz ggf. rechtswidriger Beweiserhebung durch Private für die Editionspflicht nach § 95 StPO soll hier daher ausgeklammert werden.

[45] *Rüscher*, NStZ 2018, 687.

[46] *Blechschmitt*, MMR 2018, 361 (362).

[47] *Blechschmitt*, MMR 2018, 361 (362).

[48] *Blechschmitt*, MMR 2018, 361 (362). Vgl. Nr. 1.3 der „Alexa Nutzungsbedingungen" (Stand: 29.10.2019): „Alexa leitet Audiodaten in die Cloud, wenn Sie mit Alexa interagieren. Alexa lernt dabei und wird immer intelligenter; Alexa wird automatisch über die Cloud aktualisiert und neue Features und Skills werden hinzugefügt. Um den Alexa Dienst zur Verfügung stellen zu können, zu personalisieren und um unsere Dienste zu verbessern, verarbeitet und speichert Ihre Alexa Interaktionen, wie Ihre Spracheingaben, Musikwiedergabelisten und Ihre Alexa-To-do- und -Einkaufslisten in der Cloud",
https://www.amazon.de/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201809740 (4.2.2020).

[49] Vgl. *Blechschmitt*, MMR 2018, 361 (365); *Beuth*, Zeit Online v. 27.4.2017, abrufbar unter
www.zeit.de/digital/datenschutz/2017-04/echo-look-amazon-kamera-schlafzimmer-style (4.2.2020).

[50] *Rüscher*, NStZ 2018, 687 (689). Dazu *Hegemann*, Zeit Online v. 20.12.2018, über die Speicherpraktiken von Amazon: „Das Unternehmen […] weist explizit darauf hin, dass jedes Gespräch mit dem Lautsprecher Echo respektive dessen Stimme Alexa aufgezeichnet und in die Cloud gesendet wird, sobald das Codewort fällt. […] Man könnte aus den Daten mutmaßlich ableiten, wo die betroffene Person wohnt, wo sie arbeitet, welche Musik sie hört, wann sie aufsteht, wann (und vielleicht sogar wie oft) sie duschen geht.", abrufbar unter
www.zeit.de/digital/datenschutz/2018-12/amazon-datenschutz-alexa-nutzerdaten (4.2.2020).

[51] *Blechschmitt*, MMR 2018, 361 (362 f.).

[52] Vgl. *Huseman* von Amazon: „Wenn ein Kunde etwa Amazon Music abonniert, bei Amazon Fresh bestellt, sich ein Uber- oder Lyft-Taxi ruft, oder eine Pizza bestellt. […] Selbstverständlich braucht Amazon und/oder der Skill-Entwickler einen Beleg dafür." Zudem löscht Amazon nicht, wenn Nutzer über Alexa ihren Wecker stellen, Kalendereinträge machen, oder Freunden Nachrichten schicken, vgl. *Schießl*, BR24 v. 4.7.2019, abrufbar unter
www.br.de/nachrichten/netzwelt/was-alexa-wirklich-speichert,RVFTj6h (4.2.2020).

[53] *Blechschmitt*, MMR 2018, 361 (363).

[54] Vgl. dazu *Schiemann*, in: Kugelmann (Hrsg.), Migration, Datenübermittlung und Cybersicherheit (2016), S. 151 (156 ff.); *Warken*, NZWiSt 2017, 417 (419 ff.).

[55] Vgl. *Regensburger*, BR24 v. 7.3.2017, abrufbar unter
https://www.br.de/nachrichten/netzwelt/amazon-gibt-alexa-daten-an-ermittler-weiter,68w3gdht64wkjctk6gvkge1k60r3g (4.2.2020).

[56] Vgl. The Washington Post vom 14.11.2018:
https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/ (4.2.2020).

3. Möglichkeit der Herausgabe der Daten bzw. Auskunftserteilung nach den Vorgaben des BVerfG

Ausgehend von den Voraussetzungen der Entscheidung des BVerfG zur Erhebung der beim Provider gespeicherten E-Mails gilt für beide oben unter 2. genannten Beispielsfälle, dass der Wortlaut der §§ 95, 161 Abs. 1 StPO einer Herausgabe der Daten durch den privaten Datenspeicher bzw. entsprechenden Auskunftserteilung nicht im Wege stehen würde. Beide Normen dürften – nach der o.g. dargelegten Rechtsprechung des BVerfG wegen des begrenzenden Zwecks der Straftataufklärung[57]– hinreichend bestimmt sein, so dass es im Wesentlichen darauf ankommt, ob der Kernbereich respektiert und das Vorgehen verhältnismäßig wäre. In diesem Rahmen ist insbesondere zu überprüfen, ob eine Beschränkung auf Ermittlungen betreffend Straftaten von erheblicher Bedeutung sowie erhöhte Anforderungen an den Tatverdacht, die über den Anfangsverdacht einer Straftat hinausgehen, angezeigt sind. Zudem sollen vorgängig die – gedachten – vorgelagerten verdeckten Ermittlungsmaßnahmen in den Blick genommen werden. Denn die dargestellte, nach der Rechtsprechung des BVerfG vorgenommene Verlängerung des Grundrechtsschutzes könnte dafür sprechen, dass die Bedingungen, die für den potentiellen verdeckten „Ur"-Eingriff gelten würden, Auswirkungen auf den rechtlichen Rahmen der Datenerhebung beim privaten Dritten nach Datentransfer haben: Wäre für den Fall, dass für den verdeckten Eingriff eine gesetzliche Eingriffsgrundlage gänzlich fehlen würde, auch die nachfolgende Datenerhebung beim privaten Speicher unzulässig, bzw. sind die – ggf. vorhandenen – gesetzlichen Voraussetzungen für den „Ur"-Eingriff auf die nachfolgende Datenerhebung zu übertragen?

a) Carsharing

Im Falle des Carsharing wäre bei einer Infiltration des betreffenden Moduls durch die Strafverfolgungsbehörden das Grundrecht des Fahrers auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) nicht betroffen: Zwar erwähnt das BVerfG in seiner Entscheidung zur Konkretisierung dieses Grundrechts expressis verbis „elektronische […] Geräte, die in […] Kraftfahrzeugen enthalten sind"[58]. Es dürfte aber daran fehlen, dass es sich bei dem betreffenden Modul nach den Vorgaben des BVerfG um ein vom Fahrer genutztes System handelt.[59] Dabei kommt es nicht auf die sachenrechtliche Zuordnung an, sondern vielmehr darauf, ob eine „selbstbestimmte Nutzung ‚als' eigenes System" festgestellt werden kann.[60] Von einem solchen „eigenen" System kann jedoch gerade dann nicht die Rede sein, wenn sich ein Modul im Fahrzeug befindet, dass der Fahrer nicht einmal ansatzweise beeinflussen kann. Schließlich dürfte es auch an dem zusätzlichen Erfordernis einer besonderen Gefährdungslage für die Persönlichkeitsentfaltung des Betroffenen fehlen: Eine solche Persönlichkeitsgefährdung ist bei informationstechnischen Systemen gegeben, „die alleine oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten"[61]. Das BVerfG erwähnt diese Möglichkeit etwa bei einem PC bei der Auswertung des Nutzungsverhaltens,[62] das regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen lasse.[63] Ebenfalls wird eine spezifische Grundrechtsgefährdung mit Blick auf die in vielfältiger Art erfassten und gespeicherten personenbezogenen Daten von Mobiltelefonen oder elektronischen Terminkalendern mit großem Funktionsumfang angenommen.[64] Diese Voraussetzung dürfte indes nicht gegeben sein, wenn es – wie im Fall vor dem LG Köln – den Strafverfolgungsbehörden und Gerichten allein um ein im aktuellen Geschehensablauf für Verkehrsteilnehmer sichtbares Fahrverhalten auf öffentlichen Straßen geht. Von einem „getreuliche(n) Spiegelbild der persönlichen Interessen, Neigungen, der ökonomischen Situation sowie nicht zuletzt auch der physischen und psychischen Befindlichkeit"[65] bzw. einer Aggregation einzelner personenbezogener Daten zu einer „auf einmal und immer wieder zugänglichen, dynamischen Gesamtheit", die den Betroffenen bei unberechtigtem Zugang „in seiner persönlichen Lebensführung entblößen kann"[66],[67] kann hier nicht die Rede sein – wohlgemerkt bei einer Engführung auf das bloße Fahrverhalten.

Betroffen ist daher (allein) das Recht auf informationelle Selbstbestimmung des Fahrers. Geht es, wie im Fall, der vor dem LG Köln verhandelt wurde, allein um Daten, die Feststellungen zum Aufenthaltsort und zur Geschwindigkeit des vom Beschuldigten geführten Fahrzeugs erlauben, dürfte für den gedachten verdeckten Eingriff im Vorfeld § 100h Abs. 1 S. 1 Nr. 2 StPO als Maßnahme der längerfristigen Observation in Betracht kommen. Die Auffassung, welche „technische Mittel" allein als solche der Strafverfolgungsbehörden be-

[57] Kritisch *Klesczewski*, ZStW 123 (2011), 737 (749).
[58] BVerfG NJW 2008, 822 (824).
[59] Vgl. BVerfG NJW 2008, 822 (827): „Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf."
[60] *Hornung*, CR 2008, 299 (303).
[61] BVerfG NJW 2008, 822 (827).
[62] BVerfG NJW 2008, 822 (827).
[63] *Wehage*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das Bürgerliche Recht, 2013, S. 46.
[64] Vgl. BVerfG NJW 2008, 822 (827).
[65] *Kutscha*, NJW 2008, 1042 (1043).
[66] *Böckenförde,* JZ 2008, 925 (928).
[67] Beide zitiert von *Wehage* (Fn. 63) S. 47.

greift – im Rahmen des § 100h StPO etwa der Peil- bzw. GPS-Sender[68] – mit der Folge, dass für die Infiltration eines informationstechnischen Systems Software als nicht ausreichend angesehen, sondern daneben ein gesondertes physisches Gerät, das dem Staat zugerechnet wird, gefordert wird,[69] vermag angesichts der Weite des Gesetzeswortlauts und seiner Begründung[70] nicht zu überzeugen. Ein Verstoß gegen den Bestimmtheitsgrundsatz ist darin nicht zu sehen.[71] Für den Einsatz sonstiger für Observationszwecke geeigneter technischer Mittel muss die Anlasstat zudem eine solche von erheblicher Bedeutung (vgl. § 100h Abs. 1 S. 2 StPO) und damit mindestens dem Bereich der mittleren Kriminalität zuzuordnen sowie der Grundsatz der Verhältnismäßigkeit gewahrt sein. Im Kölner Fall waren diese Voraussetzungen erfüllt.

Einer Verlängerung des Grundrechtsschutzes betreffend das Recht auf informationelle Selbstbestimmung, wie sie das BVerfG in der o.g. Entscheidung zur Beschlagnahme von E-Mails auf dem Server des Providers mit Blick auf Art. 10 GG angenommen hatte, wäre hier schon nicht notwendig, da – mangels vorgehender spezieller Grundrechte – der Eingriff in das Recht auf informationelle Selbstbestimmung auch bei Abfrage der Daten nach § 161 Abs. 1 StPO bzw. beim Stellen des Herausgabeverlangens gemäß § 95 StPO gegenüber dem Fahrzeug-Hersteller gegeben wäre.

Eine Übertragung der Voraussetzungen des § 100h Abs. 1 StPO auf das Auskunfts- bzw. Herausgabeverlangen gegenüber dem Fahrzeughersteller – mangels Notwendigkeit eines Gerichtsbeschlusses[72], wegen der Nichtübertragbarkeit des § 100h Abs. 2 Nr. 2 StPO sowie der (bei einer faktisch offenen Maßnahme) Benachrichtigungspflichten aus § 101 Abs. 4 S. 1 Nr. 7 StPO kämen das Erfordernis einer erheblichen Straftat (§ 100h Abs. 1 S. 2 StPO) sowie die Subsidiaritätsklausel aus § 100h Abs. 1 S. 1 Hs. 2 StPO in Betracht – ist allerdings abzulehnen, da sich diese Norm prospektiv auf die Überwachung in Echtzeit bezieht[73] und ihr zudem die notwendigen bereichsspezifischen Regelungen für Beschlagnahmen fehlt.[74] Ferner würde eine solche Argumentation dazu zwingen, jegliches vorgefundene beweisrelevante Datum zu seinem Ursprung zurückzuverfolgen, was einen nicht mehr vertretbaren Aufwand bedeuten könnte.

Fraglich ist jedoch im Rahmen der Verhältnismäßigkeitsprüfung, ob – wie auch in der Entscheidung des BVerfG zur Beschlagnahme von E-Mails beim Provider angenommen – diese Maßnahme auch für Anlasstaten unterhalb der Schwelle der Straftat von erheblicher Bedeutung in Betracht kommt und ob auch erhöhte Anforderungen an die Verdachtsbegründung nicht erforderlich sein sollen. Das dafür vom BVerfG maßgeblich verwendete safehouse-Argument – ansonsten wäre es für den Nutzer ein Leichtes, die Daten durch Auslagerung zu entziehen[75]– trifft jedoch für den Carsharing-Fall gerade nicht zu: Die Auslagerung findet automatisch statt und die Betroffenen haben – anders als im Fall der auf dem Server des Providers gespeicherten E-Mails – keine Chance auf Beeinflussung des Schicksals der darin enthaltenen Daten; sie haben nicht einmal die Möglichkeit, das ursprüngliche Speichern der Daten im Fahrzeug zu beeinflussen. Daraus könnte gefolgert werden, dass auch für das Vorgehen gemäß §§ 95, 161 Abs. 1 StPO gegenüber den privaten Datenspeichern eine Straftat von erheblicher Bedeutung sowie ein konkreter Tatverdacht erforderlich sein müssten.

Jedoch dürfte die Verneinung einer Ausnahme – die safehouse-Situation – allein nicht ausreichen, um im Umkehrschluss den Grundsatz affirmativ anzunehmen. Es kommt dann vielmehr darauf an, aus welchen Gründen die Regelung konzipiert worden ist. Hier ist die Qualität der Grundrechtsbetroffenheit ausschlaggebend: Entscheidend ist das Gewicht des Eingriffs, das etwa bei der Offenlegung von Verbindungsdaten ein detailliertes Bild über Kommunikationsvorgänge und Aufenthaltsorte ermöglicht.[76] Davon dürfte jedoch bei einer Engführung auf das bloße Fahrverhalten auf öffentlichen Straßen nicht die Rede sein können, so dass insgesamt die Verhältnismäßigkeit des Eingriffs zu bejahen wäre.

b) Amazon Echo/Sprachassistenzsystem Alexa

Ein verdeckter Eingriff – Aufspielen einer Software – würde bei Sprachassistenzsystemen wie Alexa auf das Ziel hinauslaufen, eine akustische Wohnraumüberwachung durchzuführen, so dass entsprechend höhere Voraussetzungen an die Verhältnismäßigkeit der Maßnahme als im Carsharing-Fall anzusetzen wären. Zwar können über Alexa auch Telefonverbindungen hergestellt werden; gewöhnlich fehlt es im laufenden Betrieb bei Alexa aber an einem Telekommunikationsvorgang.[77] Insofern wären Art. 13 GG und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[78] betroffen, wobei es sich mit Blick auf das letztgenannte Grundrecht – anders als im Carsharing-Fall – um ein „eigenes" System des Verwenders handelt und auch die notwendige Eingriffstiefe erreicht wäre; es dürfte auf der Hand liegen, dass mit einer Kontrolle des zu dem Sprachassistenzsystem in der Wohnung gesprochenen Wortes ein „Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges

[68] *Bruns*, in: Hannich (Fn. 25), § 100h Rn. 5; *Günther*, in: Knauer/Kudlich/Schneider (Fn. 13), § 100h Rn. 5; *Hegmann*, in: Graf (Fn. 9), § 100h Rn. 5.
[69] Vgl. mit Blick auf § 100c Abs. 1 StPO im Wege der systematischen Auslegung: *Rüscher*, NStZ 2018, 687 (690).
[70] BT-Drs. 12/989, S 39 konkretisiert lediglich über das Erfordernis des Aussendens von Signalen und grenzt zudem negativ ab zum „Mithören, etwa durch einen Polizeibeamten, der in einem Park oder einer Gaststätte das Gespräch an einem Nachbartisch mitverfolgt und sich Aufzeichnungen macht".
[71] BVerfG NJW 2005, 1338 (1340).
[72] Vgl. *Bruns* (Fn. 68), § 100h Rn. 14; *Günther* (Fn. 68), § 100h Rn. 22; *Hegmann* (Fn. 68), § 100h Rn. 18.
[73] *Warken*, NZWiSt 2017, 417 (419).
[74] *Klesczewski*, ZStW 123 (2011) 737 (750).
[75] Vgl. BVerfG NJW 2009, 2431 (2435).
[76] Vgl. BVerfG NJW 2003, 1787 (1791).
[77] *Rüscher*, NStZ 2018, 687 (689).
[78] *Rüscher*, NStZ 2018, 687 (690).

Bild der Persönlichkeit zu erhalten“[79] ist. Mit Blick auf die Zulässigkeit des verdeckten „Ur“-Eingriffs de lege lata bestehen Zweifel nicht nur deshalb, weil die Innenpolitik sich offensichtlich Gedanken zur Rechtfertigung eines solchen Eingriffs de lege ferenda macht[80]. Daneben kommt *Rüscher* zu dem Ergebnis, dass nach geltendem Recht weder § 100b StPO noch § 100c StPO als Eingriffsgrundlagen für ein „Abhören“ von Alexa in Echtzeit in Betracht kommen: So soll es mit Blick auf § 100c StPO an einem gesonderten physischen Gerät, das dem Staat zugerechnet wird, fehlen,[81] was – wie bereits dargelegt – jedoch nicht überzeugt.[82] Zudem soll § 100b StPO nur hinsichtlich auf in Alexa bereits gespeicherte Daten passen, aber wegen des (unzulässigen) Eingriffs in das Wohnungsgrundrecht nicht mit Blick auf die Ausspähung von in Echtzeit über sensorische Systeme erfasste Beobachtungen.[83] Dem kann entgegengehalten werden, dass die Mikrofonaufnahmen in der Regel nachfolgend gespeichert werden, so dass allenfalls Raumgespräche, die das angeschlossene Mikrofon aufzeichnet und an das damit verbundene informationstechnische System überträgt, ohne dass aber diese Audioinformationen durch den Rechner aufgezeichnet bzw. gespeichert werden, erfasst wären[84]. Anderes dürfte aber für Kamera-Aufnahmen gelten, da im repressiven Bereich eine Rechtsgrundlage für die optische Wohnraumüberwachung fehlt[85].

Was bedeutet dies für ein Herausgabe- oder Auskunftsverlangen gegenüber dem privaten Datenspeicher nach den §§ 95, 161 Abs. 1 StPO? Nach der Systematik der dargelegten Rechtsprechung des BVerfG ist für eine Verlängerung des (in Echtzeit betroffenen) Grundrechtsschutzes jedenfalls aus Art. 13 GG kein Raum, da selbst eine Beschlagnahme, die nur mittelbar aus einer Durchsuchung folgen würde, nicht mehr Art. 13 GG unterfällt[86]; es verbliebe daher allein die Betroffenheit im Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Wäre de lege lata der – gedachte vorgelagerte – verdeckte Eingriff jedenfalls mit Blick auf ungespeicherte Audio- sowie Kamera-Aufnahmen mangels gesetzlicher Grundlage rechtswidrig, kann dies jedoch keine Auswirkungen auf das Datensammeln beim privaten Drittspeicher nach Datentransfer gem. den §§ 95, 161 Abs. 1 StPO in dem Sinne haben, dass diese Daten von vornherein nicht herausgabefähig wären. Denn damit würde in der Sache ebenfalls der Auffassung gefolgt werden, welche für die dem Datentransfer an (private) Dritte nachfolgende Eingriffe dieselben Voraussetzungen anmahnt, die für den (gedachten) verdeckten „Ur“-Eingriff gelten würden[87]. Dies ist jedoch – wie bereits dargelegt – abzulehnen.[88] Der Wortlaut der §§ 95, 161 Abs. 1 StPO erlaubt ein solches Vorgehen; es verbleibt daher beim einzuhaltenden Kernbereichsschutz sowie den Standards der Verhältnismäßigkeit, die sich im Wesentlichen auf das Gebot der Datenminimierung und damit den Grundsatz der Zweckgebundenheit beziehen.[89]

In diesem Rahmen bleibt die Frage, ob der Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach den §§ 95, 161 Abs. 1 StPO nur bei Straftaten von erheblicher Bedeutung und unter Zugrundelegung von über den Anfangsverdacht hinausgehenden Anforderungen möglich sein sollen. Einer der bereits genannten tragenden Gründe des BVerfG für die Ablehnung dieser Verschärfung der Eingriffsvoraussetzungen – „(a)nderenfalls wäre es für jeden Nutzer ein Leichtes, belastende E-Mails durch eine Auslagerung auf den Mailserver seines Providers dem Zugriff der Strafverfolgungsbehörden zu entziehen“[90] – käme hier aber schon deshalb nicht zum Tragen, weil bei gänzlich fehlender Eingriffsgrundlage für die verdeckte Maßnahme ein solches Auslagerungsinteresse des Bürgers zumindest unplausibel erscheinen muss. Soweit es um zulässige Aufnahmen geht – gespeicherte Audio-Daten –, gilt das bereits zum Carsharing-Fall Gesagte: Mangels Einwirkungskompetenz des Datenbetroffenen gibt es auch hier keine Rechtfertigung über das safehouse-Argument. Zudem dürfte – anders als im Carsharing-Fall – in Anlehnung an die Rechtsprechung des BVerfG zur Erlangung der bei einem Telekommunikationsunternehmen gespeicherten Verbindungsdaten[91] ein mit der Offenlegung von Verbindungs-

[79] BVerfG NJW 2008, 822 (827).

[80] Die Innenminister von Bund und Ländern wollten zwar auf ihrer 210. Sitzung der Innenministerkonferenz im Juni 2019 in Kiel über einen möglichen Zugriff auf Daten digitaler Sprachassistenten und „smarter“ Haushaltsgeräte in der Strafverfolgung beraten; neue Befugnisse für Strafverfolger in Bezug auf Daten aus dem Smart Home sollte es danach jedoch nicht geben, vgl. *Beuth*, Spiegel Online v. 14.6.2019 www.spiegel.de/netzwelt/gadgets/alexa-gespraeche-innenminister-wollen-keine-neuen-polizei-befugnisse-a-1272478-html (4.2.2020).

[81] *Rüscher*, NStZ 2018, 687 (690).

[82] Vgl. unter a).

[83] *Roggan*, StV 2017, 821 (826); *Rüscher*, NStZ 2018, 687 (691); *Schmitt*, in: Meyer-Goßner/Schmitt (Fn. 9), § 100b Rn. 2; a.A. *Eschelbach*, in: Satzger/Schluckebier/Widmaier (Hrsg.), Kommentar zur Strafprozessordnung, 3. Aufl. 2018, § 100b Rn. 4; *Blechschmitt*, MMR 2018, 361 (365).

[84] Vgl. *Graf*, in: Graf (Fn. 9), § 100b Rn. 55.

[85] *Bruns* (Fn. 68), § 100b Rn. 5; *Rüscher*, NStZ 2018, 687 (691); *Schmitt* (Fn. 83), § 100b Rn. 2.

[86] BVerfG NJW 2005, 1917 (1918); BVerfG NJW 2009, 2431 (2433).

[87] Vgl. LG Hamburg wistra 2008, 116 (117); *Brodowski*, JR 2009, 402 (411); *Härtling*, Internetrecht, 5. Aufl. 2014, Rn. 290 m.w.N.; *Korge*, Die Beschlagnahme elektronisch gespeicherter Daten bei privaten Trägern von Berufsgeheimnissen, 2009, S 86; *Malek*, Strafsachen im Internet, 2005, Rn. 372; *Sieber*, Straftaten und Strafverfolgung im Internet, Verhandlungen des 69. DJT, Bd. 1, 2012, Gutachten Teil C, S. 110 f.; *Störing*, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, 2007, S. 209.

[88] Vgl. unter a). Entsprechendes hat dann auch für die Beschlagnahme von Alexa und das „Auslesen“ des Geräts mittels Überwindung von Zugangscodes pp. zu gelten.

[89] Vgl. BVerfG NJW 2009, 2431 (2434 ff.).

[90] BVerfG NJW 2009, 2431 (2435).

[91] Vgl. BVerfG NJW 2003, 1787 (1791).

daten zumindest vergleichbares Eingriffsgewicht vorhanden sein, da es – nicht nur vergleichbar mit einem Bild über Kommunikationsvorgänge und Aufenthaltsorte, sondern darüber hinausgehend – um den Einblick in wesentliche Teile der Lebensgestaltung einer Person durch akustische Wohnraumüberwachung geht. Von einer Verhältnismäßigkeit des Herausgabe- oder Auskunftsverlangens kann daher im Alexa-Fall nur dann die Rede sein, wenn eine Straftat von erheblicher Bedeutung in Betracht kommt und insoweit ein konkreter Tatverdacht besteht.

IV. Folgerungen für die strafprozessualen Eingriffsgrundlagen

Mit speziellem Blick auf Big-Data-Fälle können aus der Rechtsprechung des BVerfG über die (Ausnahmen zulassende) Forderung nach einem offenen Vorgehen und den Geboten des Schutzes des Kernbereichs privater Lebensgestaltung sowie der Einhaltung des Grundsatzes der Datenminimierung hinaus keine (insoweit spezifischen) Eingrenzungen für die Zulässigkeit des Herausgabe- oder Auskunftsverlangens gegenüber privaten Datenspeichern gefolgert werden. Aus der „Verlängerung“ des Grundrechtsschutzes, wie sie im Falle der Beschlagnahme von E-Mails beim Provider vom BVerfG judiziert worden ist, kann insbesondere nicht geschlossen werden, dass im Falle der fehlenden Rechtsgrundlage für eine verdeckte „Ur“-Erhebung der Daten beim Privaten ein Eingriff über die §§ 95, 161 Abs. 1 StPO beim Dritten nach Transfer dieser Daten rechtswidrig wäre; auch die Forderung, für diese Maßnahme eine Beschränkung auf Straftaten von erheblicher Bedeutung vorzunehmen sowie Anforderungen an den Tatverdacht zu stellen, die über den Anfangsverdacht einer Straftat hinausgehen, vermag jedenfalls im kategorialen Sinne nicht zu überzeugen, da es de lege lata einzelfallbezogen auf die jeweilige Eingriffstiefe des Big-Data-Falles ankommt, welche nicht anhand des allgemeinen Kriteriums der Datenhoheit des privaten Speichers und – vice versa – der damit verbundenen Ohnmacht des Datenbetroffenen nach Datentransfer bestimmt wird. Die strafprozessuale Dogmatik gibt derzeit keine Instrumente für auf Big-Data-Fälle zugeschnittene spezifische Eingrenzungen; hier würde es des Handelns des Gesetzgebers bedürfen, was im Rahmen der zu Grunde zu legenden Grundrechtsbetroffenheit eine spezifisch an den Besonderheiten dieses Phänomens ansetzende Weiterentwicklung des Allgemeinen Persönlichkeitsrechts erfordern dürfte, die hier nicht geleistet werden kann.

Auswirkungen der Digitalisierung auf das Ermittlungsverfahren

Impulse aus der Strafverteidigungspraxis

Von Dr. **Frédéric Schneider**, Hamburg*

I. Einleitung

„Alles was digitalisiert werden kann, wird digitalisiert". Ganz diesem Zitat der ehemaligen CEO des Hewlett-Packard-Konzerns, Cara Fiorina, entsprechend, machen technische Fortschritte selbstverständlich auch vor dem Strafrecht nicht halt. Und anstatt digitale Neuerungen pauschal zu verteufeln, tun Strafrechtler angesichts der rapiden technischen Entwicklungen unserer Zeit gut daran, deren Auswirkungen und Vereinbarkeiten mit dem Strafrecht zu untersuchen.

Um ein Gefühl dafür zu bekommen, wie weit gefächert die Implikationen der Digitalisierung auch für das Strafrecht sind, reicht bereits ein Blick auf die vielen in dieser Sonderausgabe der ZIS behandelten Themen. Darüber hinaus drücken neue Formen der Kriminalität und damit einhergehend neue Straftatbestände auch der Strafverteidigung ihren Stempel auf.[1] So ergibt sich bereits aus dem Entstehungsdatum des StGB, dass die mit Hilfe etwa des Computerbetrugs gemäß § 263a StGB oder der Datenhehlerei gemäß § 202d StGB erfassten Phänomene digitaler Wirklichkeit strafrechtlich erst im Nachhinein erfasst werden konnten.[2]

Daneben lassen sich in der Praxis aber angesichts der digitalen Entwicklung auch Veränderungen hinsichtlich grundlegender Säulen des Ermittlungsverfahrens beobachten. Da die Arbeit des Strafverteidigers im Wirtschaftsstrafrecht aber ganz maßgeblich in diesem Verfahrensstadium erfolgt und sich Änderungen hier zugleich auf das gesamte materielle Strafrecht auswirken, erscheint die diesbezügliche Diskussion besonders dringlich.

Aus dem Bereich des Ermittlungsverfahrens näher betrachtet werden hier im Folgenden daher die Auswirkungen der Digitalisierung auf den strafprozessualen Anfangsverdacht und die Durchsuchung von EDV-Systemen. Dabei sollen nach einer sehr kursorischen Skizze des Ermittlungsverfahrens tatsächliche Auswirkungen der Digitalisierung sowie deren aktuelle Auswirkungen in der Praxis benannt und Vorschläge für eine Anpassung der Strafprozessordnung bzw. den Umgang mit dieser dargestellt werden.

II. Rahmen und Prinzipen des Ermittlungsverfahrens

Zur Betrachtung dieser Auswirkungen der Digitalisierung auf das Ermittlungsverfahren ist es zunächst notwendig, kurz dessen Rahmen und Prinzipien in Erinnerung zu rufen.

Ausgangspunkt ist der Anfangsverdacht, d.h. es müssen konkrete Anhaltspunkte vorliegen, die es nach den kriminalistischen Erfahrungen als möglich erscheinen lassen, dass eine verfolgbare Straftat begangen wurde.[3]

Die generelle Vorgabe ist gemäß § 152 Abs. 2 StPO sodann das Legalitätsprinzip, wonach Ermittlungen erfolgen müssen. Auch wenn dieses Legalitätsprinzip auf dem Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG beruht, ist es nicht grundgesetzlich festgeschrieben und eröffnet dem Gesetzgeber bei der konkreten Ausgestaltung einen Spielraum.[4] Im Kern geht es darum, einen möglichst objektivierten Maßstab zu schaffen, um sicherzustellen, dass strafrechtliche Ermittlungen nicht von den subjektiven Erwägungen des Ermittelnden im Hinblick auf Tat und Täter abhängen. Gerade weil Zweckmäßigkeits- und Effektivitätserwägungen sich – trotz begrenzter Ressourcen – nicht gut mit dem Legalitätsprinzip vertragen, ist es für die Funktionsfähigkeit der Strafrechtspflege und zur Vermeidung überbordender Sozialkontrolle von großer Bedeutung, ein Dunkelfeld zwar zu erforschen, aber zugleich zu akzeptieren.[5] Dessen vollständige Erhellung ist weder geschuldet noch einlösbar.[6] Sie ist anerkanntermaßen auch nicht gewollt. Entscheidend ist vielmehr, im Hinblick auf dieses Dunkelfeld Kapazitäten dergestalt einzusetzen, dass dem Legalitätsprinzip zu größtmöglicher Verwirklichung verholfen werden kann.[7]

Mit Hilfe einzelner Ermittlungen wird im Laufe des folgenden Ermittlungsverfahrens geprüft, ob sich der Anfangsverdacht zu einem hinreichenden Tatverdacht konkretisieren lässt.[8] Besonders einschneidende der stets grundrechtsrelevanten Ermittlungsmaßnahmen sind vom Gesetzgeber dabei in spezifischen Ermächtigungsgrundlagen der StPO ausgestaltet. Andere fußen auf den Generalklauseln in den §§ 161, 163 StPO.[9] Von besonderer praktischer Bedeutung ist dabei im Wirtschaftsstrafrecht die Durchsuchung gemäß §§ 102 ff. StPO und die – sich daran anschließende – Sicherstellung und Beschlagnahme von Daten und Unterlagen gemäß der §§ 94 ff. StPO.

---

* Der *Autor* ist Partner in einer auf das Strafrecht spezialisierten Kanzlei in Hamburg.

[1] Siehe etwa *Popp*, JuS 2011, 385; vgl. auch *Gercke*, ZUM 2017, 915 (917 ff.).

[2] Näher zur Entstehungsgeschichte dieser Regelungen etwa *Mühlbauer*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 3. Aufl. 2019, § 263a Rn. 11; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 5. Aufl. 2017, § 202d Rn. 1 ff., jeweils m.w.N.

[3] Vgl. BVerfG, Beschl. v. 23.7.1982 – 2 BvR 8/82 = NStZ 1982, 430.

[4] Ausführlich zum dogmatischen Hintergrund des Legalitätsprinzips *Peters*, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2016, § 152 Rn. 1 ff. m.w.N.

[5] Instruktiv zur Dunkelfeldforschung etwa *Kreuzer*, NStZ 1994, 10; *ders*., NStZ 1994, 164.

[6] Vgl. *Kölbel*, in: Knauer/Kudlich/Schneider (Fn. 4), § 160 Rn. 71 m.w.N.

[7] Vgl. *Peters* (Fn. 4), § 152 Rn. 7.

[8] *Gorf*, in: Graf (Hrsg.), Beck'scher Online-Kommentar, Strafprozessordnung, Stand 1.10.2019, § 170 Rn. 2.

[9] Zum Ganzen *Griesbaum*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, § 163 Rn. 1 m.w.N.

Konkretisiert sich der Anfangsverdacht durch die Ermittlungen zu einem hinreichenden Tatverdacht, ist die Staatsanwaltschaft gemäß § 170 Abs. 1 StPO grundsätzlich gehalten, Anklage zu erheben. Lässt sich der Verdacht indes nicht erhärten, stellt sie das Verfahren gemäß § 170 Abs. 2 StPO ein.

III. Was bedeutet Digitalisierung für das Ermittlungsverfahren?

Die digitale Entwicklung wirkt sich in der Praxis auf das vorstehend kursorisch skizzierte Ermittlungsverfahren in tatsächlicher Hinsicht in zweifacher Weise aus. Erstens gibt es mehr Daten und damit mehr Informationen und zweitens haben sich die technischen Möglichkeiten im Vergleich zu früher vervielfacht.

Mehr Daten bedeuten dabei „mehr Sachverhalt", wobei dies gerade nicht nur qualitativ, sondern vor allen Dingen auch quantitativ „mehr Sachverhalt" bedeutet. Der Zuwachs technischer Möglichkeiten führt wiederum zu mehr Auswertungsmöglichkeiten.

Diese Veränderungen sind faktische Gegebenheiten, mit denen man umgehen muss, und zwar unabhängig davon, ob man dem digitalen Wandel kritisch gegenübersteht oder nicht. Wer die Augen vor der technischen Entwicklung verschließt und es schließlich verpasst, erforderliche Änderungen in Bereichen des materiellen und prozessualen Strafrechts vorzunehmen, riskiert substantielle Unstimmigkeiten. Die Kohärenz des Systems Strafrecht ist aber auch aus Sicht eines Strafverteidigers ein hohes Gut, trägt sie doch ganz erheblich zu Akzeptanz und Vorhersehbarkeit bei. Stete Anpassungen des Systems an die Lebenswirklichkeit erscheinen mithin für alle Beteiligten sinnvoll.

Statt einer Diskussion über gegebenenfalls erforderliche Anpassungen und einer darauf aufbauenden einheitlichen, strukturierten Vorgehensweise der Ermittlungsbehörden erleben wir in der Verteidigungspraxis hingegen häufig das Gegenteil. Scheinbar aus Überforderung, mit der schieren Masse an Daten und Auswertungsmöglichkeiten umzugehen, werden Ermittlungen nicht mehr konsistent geführt. Zwar ergibt sich auch hieraus häufig beträchtliches Verteidigungspotential, doch kann dies – auch aus Verteidigerperspektive – letztlich nicht die sinnvolle Antwort auf eine sich digitalisierende Gesellschaft sein.

Als Beitrag für die mithin erforderliche Suche nach dieser Antwort werden im Folgenden einige Impulse für erforderliche Anpassungen gegeben.

IV. Auswirkungen der digitalen Entwicklung auf den Anfangsverdacht

Dass aufgrund der digitalen Entwicklung immer mehr Daten existieren und jene angesichts der technischen Entwicklung immer schneller analysiert werden können, führt zu einer immer häufigeren Annahme eines Anfangsverdachts.

Wie dargelegt hat jener eine sehr geringe Annahmeschwelle und liegt bereits vor, wenn tatsächliche Umstände es nach kriminalistischer Erfahrung für möglich erscheinen lassen, dass eine verfolgbare Straftat begangen wurde.[10] Gerade im Bereich des Wirtschaftsstrafrechts liegt eine Vielzahl an Daten aber bereits ohne Durchführung irgendwelcher Ermittlungsmaßnahmen vor. Die derzeit in aller Munde befindlichen Cum-Ex-Transaktionen etwa waren nicht geheim, sondern vielmehr vorab der BaFin angezeigt und über Börsen abgewickelt worden. Den Sozialversicherungsträgern liegt eine Vielzahl an Daten hinsichtlich der Versicherten vor, die etwa im Hinblick auf eine mutmaßliche Bestechlichkeit im Gesundheitswesen gemäß § 299a StGB oder ein Vorenthalten und Veruntreuen von Sozialversicherungsbeiträgen gemäß § 266a StGB geeignet sein können, einen Anfangsverdacht zu begründen. Im Bereich des Steuerstrafrechts haben Betriebsprüfer einen umfassenden Zugriff auf Unternehmensdaten. Aus den zunehmenden technischen Möglichkeiten wiederum folgt ein immer schnellerer Erstzugriff auf diese Daten.

Nun könnte man in einem ersten Zugriff davon ausgehen, diese immer neuen Möglichkeiten seien für die Ermittlungsbehörden ausschließlich eine willkommene Hilfe bei der Verbrechensbekämpfung. Wie eingangs geschildert, greift aber mit Feststellung eines Anfangsverdachts das Legalitätsprinzip, wonach Ermittlungen erfolgen müssen. Reine Zweckmäßigkeitserwägungen, etwa unzureichende Kapazitäten, vermögen hieran nichts zu ändern. Gerade in den besonders datenintensiven Bereichen des Wirtschaftsstrafrechts, in denen sich aus den vorstehenden Gründen häufig ein Anfangsverdacht ergibt, sind diese Ermittlungen aber erfahrungsgemäß besonders personal- und zeitintensiv. Eine Überforderung der Ermittlungsbehörden und unangemessen lange Bearbeitungszeiten sind die Folge.[11] Gerade für den Beschuldigten, über dem mit Anfangsverdacht das Damoklesschwert des Strafverfahrens schwebt, ist diese Situation nur schwer erträglich.

Eine im Gesamtsystem unangemessene Kriminalisierung datenintensiver Bereiche sowie eine fehlende Steuerungsmöglichkeit der Allokation von Kapazitäten ist darüber hinaus geeignet, die Idee eines erforderlichen Dunkelfeldes auszuhöhlen.

In einigen Bereichen reagieren die Ermittlungsbehörden auf diese Entwicklung bereits seit vielen Jahren faktisch mit Augenmaß. Nur so lässt sich etwa erklären, dass es in der Praxis verhältnismäßig selten zu Verurteilungen wegen Insolvenzverschleppungen kommt, wenn diese nicht zu sehr großen Schäden der Gläubiger geführt haben oder gar mit Betrugstaten einhergingen.[12] Viel häufiger sind trotz der genannten Schwierigkeiten in der Praxis aber gegenläufige Tendenzen zu beobachten. Neben der Ausweitung des sog. Vorermittlungsverfahrens und dem gezielten Einsatz von Software auch zur Ermittlung eines Anfangsverdachts finden

[10] Siehe Fn. 3.

[11] Vgl. zur besonderen Dauer und zum Umfang von datenintensiven Ermittlungsverfahren im Wirtschaftsstrafrecht ebenfalls *Peters*, NZWiSt 2017, 465.

[12] Vgl. zum kaum bestehenden Dunkelfeld im Rahmen der Insolvenzverschleppung *Hohmann*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 7, 3. Aufl. 2019, InsO § 15a Rn. 6 m.w.N.

sich in der Praxis etwa immer mehr Beamte, die sich durch eine Weitergabe von Informationen an Ermittlungsbehörden vor dem Risiko einer Strafvereitelung im Amt gemäß § 258a StGB schützen wollen.[13] Diese Sorge ist dabei so präsent, dass im Hinblick auf die Betriebsprüfer beispielsweise ein Anwendungserlass zu § 10 BpO existiert, der den Umgang mit Verdachtsmomenten zur Vermeidung strafrechtlicher Risiken für die Prüfer konkretisiert.[14]

Ausgehend von der eingangs geschilderten Bedeutung des Dunkelfeldes und der Notwendigkeit einer sinnvollen Allokation von Ressourcen der Kriminalitätsbekämpfung zur wirksamen Erfüllung unserer Strafzwecke brauchen wir eine Diskussion über den Inhalt und die Bedeutung des Anfangsverdachts in digitaler Zeit. Während ein solcher bislang anzunehmen war, wenn irgendwelche Anfangspunkte nach kriminalistischer Erfahrung eine verfolgbare Tat möglich erschienen ließen, existieren heute Bereiche, in denen aus vorliegenden Daten und der besonderen Weite von Straftatbeständen, etwa im Bereich der Korruption, immer entsprechende Anhaltspunkte folgen werden. Die hieraus folgende These ist, dass es einer strengeren Interpretation des Anfangsverdachtes bedarf. Nur auf diese Weise können eine Fehlallokation von Ressourcen vermieden und die Verfolgung der Strafzwecke aufrechterhalten werden. Erforderlich ist zur genauen Ausgestaltung eine intensive Diskussion in Strafrechtswissenschaft und -praxis. Möglich wäre etwa, für den Anfangsverdacht in betroffenen Bereichen nicht bereits die Möglichkeit, sondern die Wahrscheinlichkeit einer verfolgbaren Straftat zu fordern.

Eine Lösung des Problems mittels Einzelfallaugenmaß der Behörden oder über den § 153 StPO, wie sie heute häufig zu beobachten ist, ist demgegenüber rechtsstaatlich bedenklich.[15]

V. Durchsuchungen von EDV-Systemen

Erhebliche Probleme begründen für Ermittlungsbehörden erfahrungsgemäß die Durchsuchung und Auswertung von EDV-Systemen. Dabei soll es an dieser Stelle nicht um die sog. Online-Durchsuchung[16], sondern vielmehr um den praktisch besonders relevanten Fall gehen, in dem im Rahmen von Durchsuchungsmaßnahmen Datenträger sichergestellt worden sind. Der Durchsuchung von Privat- und Geschäftsräumen kommt gerade im Wirtschaftsstrafrecht eine große praktische Bedeutung zu und der Fokus liegt dabei immer mehr auf der EDV.[17] Letztere offenbart den Ermittlungsbehörden neben einer Vielzahl von Unternehmenszahlen und Dokumenten insbesondere auch Korrespondenz zwischen Beteiligten und gewinnt damit nicht nur hinsichtlich einer Konkretisierung der subjektiven Tatseite an besonderem Wert für die Ermittlungen.

Während der Gesetzgeber zwischenzeitlich immer wieder Regelungen getroffen hat, die sich mit dem Zugriff auf entsprechende Daten befassen – etwa den § 110 Abs. 3 StPO für den Umgang mit Daten, die außerhalb des Durchsuchungsortes gespeichert sind oder die Cyber-Crime-Konvention für im Ausland befindliche Daten[18] –, fehlt es an Vorgaben zur Auswertung dieser Daten. In der Praxis werden jene von den Ermittlungsbehörden regelmäßig zunächst zur Durchsicht gemäß § 110 StPO in Gänze kopiert, während die Durchsicht dann in den Räumen der Ermittlungsbehörden erfolgen soll. Diese Praxis wirft zunächst Fragen auf, inwieweit hier die richterlich kontrollierte Beschlagnahme gemäß §§ 94 ff. StPO zu Gunsten der Durchsicht gemäß § 110 StPO an Bedeutung verliert. Lange und umfassende Durchsichtsmaßnahmen beinhalten die Gefahr, sich immer wieder vom ursprünglichen Anfangsverdacht zu lösen und die Einhaltung eines verhältnismäßigen Vorgehens wird hier nicht richterlich überprüft. Verstöße hiergegen ziehen für die Ermittlungsbehörden keine Konsequenzen nach sich und können von der Verteidigung im Nachhinein nicht wirksam gerügt werden.[19] Große Bedeutung gewinnt aus Sicht der Verteidigung daher zunächst die Frage, ob für den Verteidiger bzw. den Rechtsbeistand des von der Durchsuchung betroffenen ein Anwesenheitsrecht bei dieser Durchsicht besteht.[20] Insbesondere aber ist auch an dieser Stelle noch nicht abschließend geklärt, wie mit dem aus der Digitalisierung folgenden Zustand „mehr Technik und mehr Daten“ umzugehen ist.

Mehr Technik bedeutet in diesem Zusammenhang nicht nur, dass immer mehr Speichermedien vorhanden sind, die diverse Daten sammeln (etwa Smartphones, Smartwatches, Lautsprecher mit Sprachsteuerung[21]), sondern vor allen Dingen auch, dass immer mehr Software zur Auswertung der Daten existiert und zum Einsatz gelangt. Seit das BKA mit der Rasterfahndung zur Bekämpfung der RAF die Grundlagen für technische Ermittlungsmaßnahmen gelegt hat, ist viel passiert. Mittlerweile haben sogar große Softwareanbieter die Ermittlungsbehörden und deren Erfordernis der Auswertung großer Datenmengen als relevanten Markt entdeckt und bieten speziell hierfür konzipierte Software an.[22] Deren Auswer-

[13] Kritisch zum Vorermittlungsverfahren bereits *Wölfl*, JuS 2001, 478; instruktiv hierzu *Peters* (Fn. 4), § 152 Rn. 62 ff.

[14] Gleichlautende Erlasse der obersten Finanzbehörden der Länder v. 31.8.2009 BStBl. I 2009, S. 829.

[15] Kritisch zum zunehmenden Rückgriff auf diese Regelung aus Komplexitätserwägungen ebenfalls *Peters* (Fn. 4), § 153 Rn. 3 ff.

[16] Ausführlich hierzu etwa *Soiné*, NStZ 2018, 497.

[17] Siehe zu Praxisproblemen bei der IT-Durchsuchung *Graßie/Hiéramente*, CB 2019, 191.

[18] Ausführlich zur Umsetzung der Cyber-Crime-Konvention *Gercke*, MMR 2004, 728; *ders.*, MMR 2004, 801.

[19] Eindrücklich und überzeugend zu diesen verschiedenen Kritikpunkten an der praktischen Vorgehensweise *Peters*, NZWiSt 2017, 465; vgl. ebenfalls *Basar/Hiéramente*, NStZ 2018, 681.

[20] Hierzu ebenfalls *Peters*, NZWiSt 2017, 465 (472); *Klose*, NZWiSt 2019, 93 (98).

[21] Siehe hierzu etwa die jüngste Diskussion auf der Innenministerkonferenz tagesschau.de v. 9.6.2019, abrufbar unter https://www.tagesschau.de/inland/innenminister-smart-home-geraete-101.html (4.2.2020).

[22] Ausführlich hierzu *Singelnstein*, NStZ 2018, 1; zum Einsatz der Software i2 Analyst‘s Notebook etwa *Borchers*, heise online v. 28.11.2012, abrufbar unter

tungs- und auch Vorhersagemöglichkeiten gehen dabei weit über das hinaus, was Ermittlungsbeamte auch unter Nutzung gängiger Software zu leisten vermögen. Besonders aktuell sind in dieser Hinsicht derzeit etwa Programme zur Vorhersage von Verhalten (sogenanntes „predictive policing“) und solche, die lernen, selbständig Muster zu erkennen, die das Programm dann in großen Datensätzen wiedererkennen kann (sog. „machine learning“).[23] Da eine derart intensive Datenverarbeitung indes besonders schwer in das Grundrecht des Betroffenen auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 GG eingreifen kann,[24] ist es fragwürdig, wenn jene allein auf den Ermittlungsgeneralklauseln der StPO fußt. Eine Erkenntnis der zunehmenden Digitalisierung muss daher sein, dass wir eine stete Diskussion über das Erfordernis neuer, einschränkender Ermächtigungsgrundlagen in der StPO benötigen. Dabei liegt es angesichts der besonderen Grundrechtsrelevanz des Umgangs mit Daten nahe, zu fordern, dass jeder Grundrechtseingriff mit Hilfe digitaler Werkzeuge einer speziellen Ermächtigungsgrundlage bedarf. Dies muss nicht zwingend eine neue (siehe etwa §§ 94 ff. StPO für den Eingriff in Art. 10 GG bei der E-Mail-Beschlagnahme), darf aber nicht die allgemeine Ermittlungsgenehmigung aus §§ 160, 163 StPO sein.

Besonders zweischneidig ist in der Praxis der richtige Umgang mit dem Umstand, dass den Ermittlungsbehörden angesichts der Digitalisierung immer mehr Daten zur Verfügung stehen. Hier stehen sich das Legalitätsprinzip und der Verhältnismäßigkeitsgrundsatz gegenüber. Während Ersterer eine möglichst umfassende Auswertung verlangt, streitet Letzterer zumeist für einen möglichst schonenden Eingriff. Bereits im Jahr 2005 hat das Bundesverfassungsgericht diesbezüglich ausgeführt: „Bei Durchsuchung, Sicherstellung und Beschlagnahme von Datenträgern und darauf vorhandener Daten muss der Zugriff auf für das Verfahren bedeutungslose Informationen im Rahmen des Vertretbaren vermieden werden.“[25]

Neben den Schwierigkeiten, die sich angesichts der – in Wirtschaftsstrafverfahren teils unvorstellbaren – Datenmengen für die Ermittlungsbehörden daraus ergeben, dass es an personeller und sachlicher Ausstattung fehlt, gewinnt man als Verteidiger häufig das Gefühl, dass die Behörden keine einheitliche Idee haben, wie die beiden vorgenannten Prinzipien im Rahmen der Auswertung in Einklang gebracht werden können. Um die Schwierigkeit und Berührungsängste zu verdeutlichen, kann man sich etwa vor Augen führen, dass der absolute Standard in deutschen Ermittlungsbehörden auch heute noch die Ermittlungsakte in Papierform ist.

Die StPO bietet an dieser Stelle jedenfalls keine Lösung und die häufig latente Sorge der Ermittler vor Datenverlust erschwert die Herangehensweise.[26] In der Folge werden die Daten immer häufiger zur Auswertung an private Dritte gegeben und damit eine besonders grundrechtsrelevante Aufgabe „outgesourct“ oder die Auswertung erfolgt unzureichend, etwa sehr punktuell und nicht mehr kontextual. Nicht selten retten sich die Ermittlungsbehörden in Opportunitätserwägungen und stellen Verfahren ein. Für Strafverteidiger eröffnet eine große Datenmenge vor diesem Hintergrund häufig ein weiteres Verteidigungsfeld, zumal die Auswertung jedenfalls meist lange Zeit in Anspruch nimmt, was sich zumindest strafmildernd auswirkt. Gleichwohl ist es auch aus Sicht der Verteidigung unangenehm, dass es an einem verbindlichen und damit für alle Beteiligten vorhersehbaren Maßstab fehlt, wie mit großen Datenmengen umzugehen ist.

Vor diesem Hintergrund benötigen wir dringend verbindliche Regelungen zum Umgang mit großen Datenmengen im Ermittlungsverfahren. Dabei können die Ermittlungsbehörden insbesondere auch von den diversen Privaten lernen, die interne Ermittlungen für Unternehmen anbieten und dabei immer weiter daran arbeiten, einen Standard zu entwickeln, wie eine entsprechende Aufarbeitung legitimerweise aussehen kann.[27] Positiv hervorzuheben sind in diesem Zusammenhang etwa Ausführungen des Bundesamts für Sicherheit in der Informationstechnik im „Leitfaden IT-Forensik“,[28] wohingegen enttäuschend zur Kenntnis genommen werden muss, dass auch der aktuelle Entwurf eines Verbandssanktionengesetzes keine Standards für die grundrechtskonforme Auswertung großer Datenmengen benennt.

VI. Schluss

Abschließend bleibt nur festzuhalten, dass die zunehmende Digitalisierung der Gesellschaft selbstverständlich auch vor dem Strafrecht nicht Halt macht. Besonders bedeutend und grundrechtsrelevant sind dabei die Fragen, die sich angesichts der tatsächlichen Veränderungen im Rahmen des Ermittlungsverfahrens ergeben. Eine stete und intensive Diskussion über eine grundrechtskonforme Ausgestaltung des Ermittlungsverfahrens ist hier von großer Wichtigkeit. Mit den Auswirkungen auf den Anfangsverdacht und die Durchsicht

https://www.heise.de/newsticker/meldung/Streit-um-Data-Mining-bei-deutschen-Polizeibehoerden-1758346.html; https://netzpolitik.org/2013/bundeskriminalamt-zum-schnupperkurs-fur-polizeiliche-vorhersagesoftware-bei-ibm-in-freiburg/ (4.2.2020).

[23] Siehe hierzu etwa die Meldung unter becklink 2009574; ZD-Aktuell 2017, 05455; *Singelnstein*, NStZ 2018, 1; *Meinicke*, K&R 2015, 377; *Gercke*, ZUM 2019, 798 (803).

[24] Vgl. *Hermann/Soiné*, NJW 2011, 2922; *Singelnstein*, NStZ 2018, 1.

[25] BVerfG, Beschl. v. 12.4.2005 – 2 BvR 1027/02.

[26] Ausführlich zu Löschungspflichten in diesem Zusammenhang *Basar/Hiéramente*, NStZ 2018, 681.

[27] Ausführlich zur Grundlage und Ausgestaltung solcher Internal Investigations diverse Monographien, etwa Knierim/Rübenstahl/Tsambikakis (Hrsg.), Internal Investigations, 2. Aufl. 2016; Spehl/Grützner (Hrsg.), Corporate Internal Investigations, 2013; Bay (Hrsg.), Handbuch Internal Investigations, 2013; Moosmayer/Hartwig (Hrsg.), Interne Untersuchungen, 2. Aufl. 2018; *Rieder/Menne*, CCZ 2018, 203; *Bittmann/Brockhaus/v. Coelln/Heuking*, NZWiSt 2019, 1.

[28] Abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 (4.2.2020).

von großen Datenmengen in EDV-Systemen konnten in diesem Beitrag nur zwei von vielen Bereichen dargestellt werden, in denen Anpassungen erforderlich sind. Es bleibt zu hoffen, dass die diesbezügliche Diskussion an Bedeutung und Intensität zunimmt, damit allen Beteiligten im Strafprozess auch weiterhin ein schlüssiges, legitimes und vorhersehbares Regelwerk zur Verfügung steht.