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).