Die Veränderung des Strafrechts durch die Digitalisierung der Lebenswelt

Michael Kubiciel

Angaben zur Veröffentlichung / Publication details:

Kubiciel, Michael. 2020. "Die Veränderung des Strafrechts durch die Digitalisierung der Lebenswelt." In *Zukunftsperspektiven des Strafrechts: Symposium zum 70. Geburtstag von Thomas Weigend*, edited by Elisa Hoven, Michael Kubiciel, and Thomas Weigend, 159–73. Baden-Baden: Nomos. https://doi.org/10.5771/9783748907978-159.

Beiträge zum Strafrecht –
Contributions to Criminal Law 2

Elisa Hoven | Michael Kubiciel (Hrsg.)

Zukunftsperspektiven des Strafrechts

Symposium zum 70. Geburtstag von Thomas Weigend

Nomos

Die Veränderung des Strafrechts durch die Digitalisierung der Lebenswelt

Michael Kubiciel

I. Digitalisierung der Lebenswelt: Von der Euphorie zur Ernüchterung

Die Digitalisierung der Lebenswelt begann in jenem „Scharnier-Jahrzehnt", in dem viele Veränderungen zwar nicht initiiert, aber für die breite Gesellschaft spürbar wurden: den 1980er Jahren.[1] Die Verbesserung der Hardware und die Entwicklung neuer Betriebsprogramme machten die in den 1970er Jahren entwickelten Personal-Computer gleichzeitig leistungsfähig, bezahlbar und nutzerfreundlich. Infolgedessen hielten sie in Büros und Kinderzimmern Einzug, erleichterten einer breiten Masse von Menschen die Arbeit und bescherten vielen ihrer Kinder eine neue Freizeitbeschäftigung. Wie von *Gordon Moore* Mitte der 1960er Jahre vorausgesagt, war es gelungen, die Komplexität integrierter Schaltkreise bei stabilen Komponentenkosten in regelmäßigen Abständen zu verdoppeln (sog. Mooresches Gesetz).[2] Diese Dynamik setzte sich in den 1990er und 2000er Jahren fort.[3] Die zunehmende Vernetzung der Computer sowie Einkaufs- und Kommunikationsplattformen verliehen dieser Entwicklung einen weiteren Schub: E-Mails beschleunigten die Kommunikation, das Internet und die sozialen Medien entwickelten sich zu Foren für den Austausch von Informationen und Meinungen, eCommerce-Plattformen machten das globale Waren- und Dienstleistungsangebot sichtbar. Auf diese Weise ist die digitalisierte Kommunikation zu einer „omnipräsenten Basisinfrastruktur" geworden.[4]

Euphorie begleitete die erste Phase der Entwicklung. Die Gesellschaft nahm die Digitalisierung überwiegend als positive Erweiterung persönli-

---

1 *Siebold*, APuZ 65 (2015), 3.

2 Locus classicus *Moore*, Electronics 38 (1965), 114.

3 Auf diese Weise hat sich die Rechenleistung innerhalb von 40 Jahren um den Faktor 1 Million erhöht; vgl. dazu *Schirrmacher*, Ungeheuerliche Neuigkeiten, 2014, S. 145, 147.

4 Treffend *Hoffmann-Riem*, AöR 142 (2017), 1, 6.

cher Freiheit und unternehmerischer Chancen wahr.[5] Manche träumten vom Internet als herrschaftsfreien Raum, in dem eine spontane, staatsfreie Ordnung entstehen sollte.[6] Andere sahen in den sozialen Medien gar einen virtuellen Diskursraum, der die Grundlage direkt-demokratischer Partizipationsmöglichkeiten bilden könne.[7] Auf der anderen Seite des Meinungsspektrums standen jene, die – nicht weniger optimistisch – darauf beharrten, dass nicht die Internet-Community, sondern der Staat (oder supranationale Organisationen) das Recht setzen sollten, und dass das Recht im Cyberspace in gleicher Weise gelte „wie überall sonst"[8].

Inzwischen ist die Euphorie der Ernüchterung gewichen.[9] Nicht nur der Diebstahl personenbezogener Daten oder digitaler Identitäten durch Hacker, sondern auch die Verwertung von Nutzerinformationen durch Plattformen wie Facebook oder Amazon haben uns gezeigt, dass jede Form der Verwendung sozialer Medien und eCommerce-Plattformen mit dem Verlust der Kontrolle über eigene Daten bezahlt wird. Selbst jene, die staatliche Regulierung im Internet ursprünglich abgelehnt haben, verlangen nunmehr nach einem stärkeren Schutz ihrer Grundrechte gegenüber global agierenden IT-Konzernen.[10] Indes ist deutlich geworden, wie schwer sich der Staat mit der Rechtsdurchsetzung gegenüber im Ausland ansässigen Unternehmen mit einer monopolartigen Marktmacht tut. Unternehmen wie Facebook fordern den Staat offen heraus, indem sie sich Regulierungsversuchen entziehen und eigene Regeln – in Konkurrenz zum staatlichen Recht – setzen und durchsetzen,[11] während sie sich lange geweigert haben, Rechtsverletzungen, die auf ihren Plattformen begangen werden, entgegenzutreten und rechtswidrige Inhalte zu löschen.

Aber nicht nur gegenüber Unternehmen fällt dem Staat die Rechtsdurchsetzung schwer. Auch Ermittlungen gegen einzelne Straftäter stoßen

---

5 *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 14 f.

6 Dazu *Gleß*, ZStrR 130 (2012), 3; *Kubiciel*, GA 2013, 226, 236.

7 Dazu *Kersten*, Schwarmdemokratie, 2017, S. 22 f.; *Thiele*, Verlustdemokratie, 2. Aufl. 2018, S. 159.

8 Siehe etwa Koalitionsvereinbarung zwischen CDU, CSU und FDP, 17. Legislaturperiode, 2009, S. 101: „Wir bekräftigen, dass Recht und Gesetz im Internet schon heute und in Zukunft ebenso gelten wie überall sonst." – Siehe zu diesem, oft floskelhaft verwendeten Satz *Di Fabio* (Fn. 5), S. 11; *Kubiciel*, ZIS 2018, 60, 63.

9 *Schallbruch*, in: Mair/Messner/Meyer (Hrsg.), Deutschland und die Welt 2030, 2018, S. 235. Ähnlich *Ingold*, Der Staat 56 (2017), 491, 492. Siehe auch *Kersten* (Fn. 7), S. 26: Aus dem „demokratischen Hype" um soziale Medien sei eine „undemokratische Depression" geworden.

10 Dazu *Di Fabio* (Fn. 5), S. 19, 43 ff.

11 *Schallbruch* (Fn. 9), S. 236 f.

an technische und rechtliche Grenzen. So werden Kinderpornographie, Ausweispapiere, Drogen oder Waffen nicht mehr nur hinter verschlossenen Wohnungstüren oder in dunklen Bahnhofsecken angeboten, sondern immer öfter in sog. P2P-Netzwerken. Während die Strafverfolgungsbehörden rechtlich wie tatsächlich in der Lage sind, Gespräche in Wohnungen abzuhören oder Personen zu observieren, können sie P2P-Netzwerke in aller Regel nicht von außen infiltrieren, weil die Beteiligten nur mit Usern kommunizieren, die als vertrauenswürdig anerkannt sind, und dabei verschlüsselte Kommunikationswege nutzen.[12] Angesichts dessen verwundert es nicht, dass das sog. Darknet inzwischen zum Synonym für die dunklen Seiten der Digitalisierung avanciert ist, an deren Aufhellung der Staat zu scheitern droht.

II. Rechtsdurchsetzung in digitalen Systemen

1. Ambivalenz digitaler Systeme

Nach einer Anfangsphase der Idealisierung haben sich das Internet und die sozialen Medien mithin als das erwiesen, was von Menschen ersonnene Werkzeuge stets sind: dual-use-Produkte, die sowohl zu sozialadäquaten als auch zu sozialschädlichen Zwecken genutzt werden können.[13] Soziale Medien *können* Orte der Deliberation und Integration sein;[14] häufig erweisen sie sich jedoch als Schauplätze strafbarer Formen der *hate speech* oder als Mittel der Desinformation und vertiefen damit die Risse in der Gesellschaft.[15] Geschlossene Netzwerke *können* zum harmlosen Tausch von Filmen oder Musikfiles verwendet oder in autoritären Staaten zur überwachungsfreien Kommunikation genutzt werden; ihre arkane Struktur macht die P2P-Kommunikation aber auch für Straftäter attraktiv.[16] Indes sollte man diese Ambivalenz bzw. Nutzungsoffenheit digitaler Systeme

12 Dazu *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1.

13 *De Negri Fischer*, Rethinking Law 2019, 18. Am Beispiel von File-Sharing-Software *Kubiciel*, wistra 2012, 453.

14 Dies schon allein deswegen, weil das Format der sozialen Medien eine Zuspitzung politischer Aussagen erfordert, welche die notwendige „Streittiefe" komplexer politischer Probleme nicht erreichen kann. Dazu *Thiele* (Fn. 7), S. 155 ff., 231 ff.

15 So bereits *Habermas*, Ach, Europa, 2008, S. 138, 161 f. Siehe ferner *Kersten* (Fn. 7), S. 127 ff.; *Magen*, VVDStRL 77 (2018), 67, 72 ff.

16 Dazu *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1.

nicht mit harmloser Neutralität verwechseln, die eine Regulierung von vornherein überflüssig macht. Denn mit *Carl Schmitt* gesprochen liegt die „Entscheidung über Freiheit und Knechtschaft (...) nicht in der Technik als Technik. Sie kann revolutionär oder reaktionär sein, der Freiheit und der Unterdrückung dienen (...)."[17] Die Technik sei immer „nur Instrument oder Waffe, und eben weil sie jedem dient, ist sie nicht neutral."

Vor dieser – nicht mit Neutralität zu verwechselnder – Ambivalenz digitaler Systeme kann der Gesetzgeber nicht kapitulieren. Er hat vielmehr die Aufgabe, gravierend sozialschädlichen Verhaltensweisen zu begegnen – auch mit dem Mittel des Strafrechts. Letzteres schützt subjektive Rechte und bedeutende gesellschaftliche und staatliche Institutionen, indem es die Verletzung von Normen, die sozialschädliches von sozialadäquatem Verhalten unterscheiden, unter Strafandrohung stellt. Um diese Stabilisierungsleistung erfüllen zu können, muss das Strafrecht grundsätzlich für sämtliche Orte Geltung beanspruchen, an denen die Verhaltensnormen in Frage gestellt werden und an denen der Staat diese Normen faktisch durchsetzen kann.

2. *Konsolidierung des materiellen Strafrechts*

Ob dazu auch das Internet und digitale Systeme gehören, ist indes noch keineswegs ausgemacht.[18] Bislang hält der Staat jedenfalls weder die rechtlichen noch die technischen Mittel zur Durchsetzung des Rechts in digitalen Welten bereit. Blickt man auf das materielle Recht, erkennt man ein eklektizistisches IT- und Datenschutzstrafrecht, das bemerkenswerte Strafbarkeitslücken mit Tendenzen zur Überkriminalisierung auf widersprüchliche Weise mischt.[19] Einerseits findet sich weder im StGB noch im BDSG ein (explizites) Verbot der rechtswidrigen Publikation personenbezogener Daten. Andererseits schützt das StGB Daten unabhängig von ihrem Informationsgehalt und ihrer Schutzwürdigkeit, weil die Tatbestände nicht auf den Inhalt der Daten, sondern die Art der Erlangung abstellen. Ursächlich für diesen Zustand des geltenden Strafrechts ist eine Ad-hoc-Gesetzgebung, die einzelnen Kriminalitätsphänomenen nachgeeilt ist, ohne nach dem Grund der Schutzwürdigkeit von Daten und personenbezogenen In-

17 Siehe dazu und zum Folgenden *Schmitt*, Der Begriff des Politischen, 7. Aufl. 1963, S. 90 ff. (Zitate: S. 90, 91, 93).

18 Vgl. auch *Di Fabio* (Fn. 5), S. 18.

19 Dazu und zum Folgenden *Kubiciel/Großmann*, NJW 2019, 1050, 1052 ff.; *Singelnstein*, ZIS 2016, 432, 433.

formationen zu fragen und auf dieser Basis ein Set stringenter Vorschriften zu entwickeln.[20] Eine systematisch-planvolle, wissenschaftlich beratene, auf Deutschen Juristentagen debattierte Gesetzgebung, die in den 1970er und 1980er Jahren das Wirtschafts- und Umweltstrafrecht hervorgebracht hat, hat es im Bereich des IT-Strafrechts – jedenfalls bislang – nicht gegeben. Ein Desiderat für die Zukunft des Strafrechts ist daher eine grundlegende Überarbeitung des materiellen Rechts, eine „digitale Agenda für das Strafrecht", die mehr leistet als den vorhandenen Fragmenten neue Teilstücke hinzuzufügen.

Dies setzt freilich Klarheit über den tragenden Grund des Datenschutz- bzw. IT-Strafrechts voraus. An dieser fehlt es. Den (strafrechtlichen) Datenschutz mit dem „Recht auf Schutz personenbezogener Daten" zu rechtfertigen, wie das Art. 1 Abs. 2 DS-GVO tut, ist offenkundig tautologisch. Das in den frühen 1980er Jahren entwickelte Grundrecht auf „informationelle Selbstbestimmung"[21] ermöglicht zwar in einfach gelagerten Fällen eine Unterscheidung zwischen zulässigen und unzulässigen Nutzungen fremder Daten: Wer etwa personenbezogene Daten eines Dritten ohne dessen Zustimmung im Internet publiziert, greift in das Recht auf informationelle Selbstbestimmung ein und handelt, jedenfalls nach meinem Dafürhalten, in strafwürdiger (allerdings *de lege lata* nicht strafbarer) Weise. Der Realität des in digitalen Systemen eingebundenen Einzelnen wird die Rede vom informationellen Selbstbestimmungsrecht hingegen nicht vollständig gerecht.[22] Der durchschnittliche Nutzer einer Smartphone-App, eines sozialen Netzwerks wie Youtube oder einer eCommerce-Plattform wie Amazon kann gar nicht überblicken, was mit seinen Daten geschieht, und will dies in der Regel auch gar nicht wissen. Zumeist werden die Allgemeinen Geschäftsbedingungen, in denen Hinweise auf die Datennutzung verborgen sind, nicht einmal gelesen. Mehr noch: Der Einsatz dieser Technologien wird – wie der Einsatz eines jeden alltäglich gewordenen Werkzeuges – vom Nutzer nicht mehr reflektiert. Anders als Autos oder andere Werkzeuge weisen digitale Systeme jedoch die Fähigkeit auf, das Verhalten der Nutzer unbewusst zu steuern.[23] Gerade wegen dieser „Digital Unconsciousness" bietet die „datenschutzrechtliche Einwilligung"[24] in die

20 Eine konzeptionelle und übergreifende Behandlung rechtlicher Fragen vermisst auch *Schallbruch* (Fn. 9), S. 241 ff.

21 Grundlegend BVerfGE 65, 1, 43.

22 *Veil*, NVwZ 2018, 686.

23 *Hoffmann-Riem*, AöR 142 (2017), 1, 6; *Martini*, JZ 2017, 1017.

24 Dazu *Brodowski/Nowak*, in: BeckOK-DatenschutzR, 27. Edition 1.1.2018, § 42 Rn. 38.1.

Verarbeitung der Daten *allein* keine Gewähr dafür, dass Daten in einer Weise verarbeitet werden, die die Interessen der einzelnen Nutzer hinreichend berücksichtigen. Es ist daher davor zu warnen, die Selbstbestimmung und Einwilligung als alleinige und zentrale Legitimationskriterien von Datennutzungen zu begreifen und die (strafrechtliche) Regulierung dieser Materie allein am Orientierungspunkt des autonom handelnden Einzelnen auszurichten.[25]

Ein alternatives Regulierungsmodell könnte den verwaltungsakzessorischen Ansatz des Umweltrechts übernehmen und beispielsweise vorsehen, dass Betreiber großer, gewerblich genutzter digitaler Systeme – soziale Netzwerke, eCommerce-Plattformen und dergleichen – ihre Allgemeinen Geschäftsbedingungen einer Regulierungsbehörde (etwa der Bundesnetzagentur oder dem Bundeskartellamt) zur Prüfung und Genehmigung vorlegen müssen, soweit darin Bestimmungen über die Verarbeitung personenbezogener Daten enthalten sind.[26] Eine Berechtigung zur Verarbeitung im Sinne des § 42 BDSG läge dann nur vor, wenn sich die sog. datenschutzrechtliche Einwilligung auf Allgemeine Geschäfts- bzw. Nutzungsbedingungen bezieht, die das skizzierte Prüfverfahren durchlaufen haben.

3. Fortlaufende Anpassung des Strafverfahrensrechts

Die Konsolidierung des materiellen Rechts und seine Anpassung an digitale Systeme ist für den Schutz der Bürger jedoch nur so viel wert, wie Strafverfolgungsbehörden und Gerichte in der Lage sind, das Recht durchzusetzen, d.h. dem Verdacht einer Straftat nachzugehen und diesen aufzuklären. Auch das Strafverfahrensrecht und seine Eingriffsermächtigungen müssen daher an den Handlungsort Cyberspace angepasst werden. Wenn Strafverfolgungsbehörden in nach außen abgeschotteten P2P-Netzwerken ermitteln wollen, stellt sich beispielsweise die Frage, ob ein Beschuldigter dazu verpflichtet werden kann, den Ermittlungsbehörden die Nutzung der eigenen, im Netzwerk als vertrauenswürdig anerkannten Identität zu ermöglichen. Eben dies sieht der im Frühjahr 2019 geleakte Referentenent-

25 Dass die Autonomie und (mutmaßliche) Einwilligung nicht als alleinige Legitimationskriterien fungieren können, zeigt sich eindrücklich auf dem Feld des Medizin(straf)rechts; vgl. zu den Grenzen dieser Figuren *Kubiciel*, GS Tröndle, 2019, S. 615.

26 Bislang ist die Prüfung von Geschäftsbedingungen nur unter den Voraussetzungen des § 19 GWB (Vorliegen einer marktbeherrschenden Stellung, Wettbewerbsverzerrung) möglich.

wurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme – Kurzform: „IT-Sicherheitsgesetz 2.0" – des Bundesinnenministeriums vor. Weigert sich der Beschuldigte, die Zugangsdaten herauszugeben, sollen gegen ihn Ordnungs- und Zwangsmittel nach § 70 StPO festgesetzt werden dürfen. Immerhin sollen die durch Nutzung der Zugangsdaten gewonnenen Erkenntnisse in einem Straf- oder Ordnungswidrigkeitenverfahren gegen den Verdächtigen oder einen in § 52 Abs. 1 StPO bezeichneten Angehörigen des Verdächtigen nur mit Zustimmung des Verdächtigen verwendet werden. Die daran geäußerte Kritik, die Vorschrift sei „verfassungsrechtlich bedenklich", weil sie den nemo-tenetur-Grundsatz aushöhle, lässt die Frage nach den Alternativen offen. Wie sollen Strafverfolgungsbehörden in geschlossenen Netzwerken ermitteln, wenn ihnen der Zugang verweigert wird?

Offen bleibt die Frage nach den Alternativen auch, wenn man die Auffassung zu Ende denkt, wonach Strafverfolgungsbehörden zur Durchführung einer Quellen-TKÜ oder einer Online-Durchsuchung *keine* Sicherheitslücken in Betriebsprogrammen nutzen dürfen, um IT-Systeme zu infiltrieren.[27] Folgt man dieser Ansicht, bliebe Staatsanwaltschaften nur die Möglichkeit, die Überwachungsprogramme mit Hilfe von Phishing-Mails zu platzieren oder diese händisch auf Smartphones oder PC zu installieren. Gerade Straftäter aber, die auf dem Feld der IT-Kriminalität tätig sind oder eine hohe kriminelle Energie aufweisen, werden keine E-Mail-Anhänge unbekannter Absender öffnen oder gar Dritten Zugang zu ihren Smartphones oder PCs ermöglichen. Untersagt man Staatsanwaltschaften die Ausnutzung von Sicherheitslücken, könnten sie in vielen Fällen – vor allem der Schwerkriminalität – gerade jene Kommunikationswege nicht überwachen, auf denen prekäre Themen besprochen werden: Messenger-Dienste wie WhatsApp oder Telegram. Wenn aber der Staat keine Alternativen hat, Täter in ihren „digitalen Schutzraum" zu folgen, könnten Straftaten erst und nur dann verfolgt werden, wenn Straftäter diese Räume verlassen. Tun sie dies nicht oder nur für einen flüchtigen Moment – wie beispielsweise beim Tausch von Kinderpornographie – blieben viele Straftaten ungeahndet.

Nicht nur mit Blick auf die betroffenen Rechtsgüter der Opfer kann das keine akzeptable Konsequenz sein. Auch das Strafrecht und der Staat können sich den Rückzug aus digitalen Räumen nicht leisten: Das Strafrecht geriete in eine Legitimationskrise, wenn einerseits Ladendiebstähle, Straßenverkehrsdelikte und andere Formen kleiner und mittlerer Krimina-

27 Dazu *Derin/Golla*, NJW 2019, 1111, 1114 f.; *Großmann*, GA 2018, 439, 454 ff.

lität konsequent verfolgt werden, während schwerwiegende Straftaten allein deswegen ungesühnt bleiben, weil die Täter ihre Aktivitäten in den Cyberspace verlegen.[28] Mit dem Strafrecht geriete auch der Staat in eine Legitimationskrise, betrifft die Durchsetzung des Rechts doch „das, was das Essentiale des modernen souveränen Staates ausmacht".[29] Daher wird er sich der strafprozessualen Mittel bedienen, die für die Umsetzung dieses Anspruchs in digitalen Systemen notwendig sind. Anders als der Etatist *Thomas Hobbes* im 17. Jahrhundert meinte, folgt aus der Legitimität des Zweckes zwar nicht das Recht auf den Einsatz jedweden effektiven Mittels; vielmehr müssen sich strafprozessuale Eingriffsbefugnisse unter der Herrschaft des Grundgesetzes an den Grundrechten und am Verhältnismäßigkeitsgrundsatz messen lassen. Wohl aber zeigt uns *Thomas Hobbes*, was geschieht, wenn der Staat als Durchsetzungsinstanz des Rechts ausfällt: Normen verlieren ihre Geltungskraft, d.h. sie können weder die Einzelnen schützen noch der Gesellschaft Orientierung bieten – zum Schaden aller. Angesichts dessen sollten wir uns davor hüten, jedwede Anpassung des Strafverfahrensrechts an die Veränderung digitaler Kriminalitätsräume *per se* zurückzuweisen, sondern die Kritik an einem Gesetzentwurf mit einem praktikablen Alternativvorschlag verbinden.[30]

III. Der Roboter als Richter: Rechtsdurchsetzung mit Hilfe von digitalen Systemen

Neben dem klassischen Problem, ob und wie sich Recht im Internet bzw. den sozialen Medien durchsetzen lässt, wird uns die Digitalisierung in naher Zukunft weitere grundlegende Fragen bescheren. Denn die exponentielle Steigerung der Rechenleistungen erlaubt es nicht nur, Maschinen, Autos, Fabriken und andere Dinge miteinander zu vernetzen und quasi in Echtzeit miteinander kommunizieren zu lassen.[31] Möglich werden auch

---

28 Treffend *Di Fabio* (Fn. 5), S. 24.

29 Treffend *Hobe*, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. XI, 2013, § 231 Rn. 3. Ebenso *Schallbruch* (Fn. 9), S. 239.

30 Im Fall der Quellen-TKÜ bzw. Online-Durchsuchung sollte zunächst genauer gesetzlich geregelt werden, wie und unter welchen Voraussetzungen Spyware auf Smartphones bzw. PCs installiert werden darf; zudem sollten die Sicherheitsbehörden verpflichtet werden, Softwareunternehmen auf bestehende Lücken hinzuweisen, um mit diesen zu erörtern, ob und wie die Sicherheitslücken verkleinert werden können.

31 *Hoffmann-Riem*, AöR 142 (2017), 1, 4 ff.; *Gleß/Weigend*, ZStW 126 (2014), 561.

sog. Formen des „deep learnings",[32] also das, was unter dem Label „künstliche Intelligenz" zusammengefasst wird. Diese technischen Möglichkeiten werden das Recht und seine praktische Anwendung tiefgreifend und auf allen Ebenen verändern – mein Vorredner hat das eindrucksvoll und systematisch abgeschichtet gezeigt.[33] Die folgenden Ausführungen beschränken sich daher auf einen Aspekt, der mit dem eben genannten klassischen Problemfeld verbunden ist: die automatisierte Rechtsdurchsetzung mit Hilfe digitaler Systeme, pointiert formuliert: den Rechner als Richter.

Was wie eine ferne Utopie erscheint, ist in Ansätzen bereits Wirklichkeit. Dies zeigt das berühmt-berüchtigte Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG).[34] Es verpflichtet bestimmte Anbieter sozialer Netzwerke dazu, Beschwerdemanagement-Systeme zu schaffen, die in der Lage sind, rechtswidrige Inhalte innerhalb eines sehr kurzen Zeitraumes zu löschen.[35] Möglich ist das nur, wenn digitale Systeme die Vielzahl von Beschwerden sichten und zumindest über eindeutig zutreffende bzw. eindeutig unzutreffende Beschwerden „autonom" entscheiden, so dass nur Grenzfälle von Menschen bearbeitet werden müssen.[36] Da § 1 Abs. 3 NetzDG den Begriff „rechtswidrige Inhalte" mit dem objektiven und subjektiven Tatbestand einer ganzen Reihe näher bezeichneter Straftatbestände gleichsetzt, muss der von den digitalen Systemen verwendete Algorithmus in der Lage sein, die Struktur dieser Rechtsvorschriften in binäre Codes umzusetzen und diesen mit dem Inhalt von Posts und Tweets zu vergleichen.

Bislang nutzen Strafverfolgungsbehörden und -gerichte diese Technik nicht. Man könnte sogar sagen: Der Grund für die Schaffung des NetzDG liegt gerade darin, dass staatliche Behörden mit der Bewältigung der Vielzahl von Fällen überfordert wären, da sie keine digitalen Systeme zur Sichtung und Bewertung der unzähligen mutmaßlich strafbaren Posts und Tweets im Netz nutzen. Stattdessen müssen sie bei jedem eingehenden Fall zunächst eine Akte (in Papierform) anlegen und ein umfangreiches Verwaltungsverfahren initiieren, in dem die Akte verschiedene Stationen durchläuft, bevor nach einigen Monaten – vielleicht – eine Entscheidung getroffen wird. Eine rasche Reaktion auf massenhaft begangene Taten in

---

32 Dazu *Hoffmann-Riem*, AöR 142 (2017), 1, 3; *Reichwald/Pfisterer*, CR 2016, 208.

33 *Hilgendorf* (in diesem Band), S. 137 ff.

34 Dazu *Kubiciel*, jurisPR-StrafR 7/2017 Anm. 1; *Wimmers/Heymann*, AfP 2017, 93.

35 Siehe § 3 Abs. 1 NetzDG, wonach „offensichtlich rechtswidrige Inhalte" innerhalb von 24 Stunden nach Eingang der Beschwerde, alle anderen rechtswidrigen Inhalte innerhalb von sieben Tagen zu löschen sind.

36 S. dazu bereits *Hoffmann-Riem*, AöR 142 (2017), 1, 18.

einem Medium, in dem rechtswidrige Inhalte mit einem Klick weiterverbreitet werden können, ist innerhalb eines derart arbeitenden Justizsystems nicht möglich. Wenn aber die Justiz aus technischen und rechtlichen Gründen keine „elektronischen Hilfsbeamten" selbst einsetzen kann und darf, liegt ein Outsourcing der (automatisierten) Rechtsdurchsetzung an private Unternehmen, die soziale Netzwerke betreiben, nahe, zumal diese nicht an die engeren Voraussetzungen des Strafverfahrensrechts gebunden sind. Wenn man diese Privatisierung der Rechtsdurchsetzung hingegen ablehnt, muss man die Justiz einerseits entlasten und sie andererseits mit den notwendigen digitalen Systemen ausstatten.

Schon heute ließe sich die Justiz durch den Einsatz von Algorithmen in Massenverfahren erheblich entlasten, nicht nur in dem gerade genannten Bereich. Ein scheinbar wenig aufregendes, aber praktisch wichtiges Beispiel sind einfach gelagerte Verkehrsstraftaten und -ordnungswidrigkeiten. Diese zeichnen sich dadurch aus, dass die Nachweisanforderungen niedrig sind und Betroffene im Einspruchsverfahren zur Verteidigung in aller Regel ein abgrenzbares Set von Argumenten vortragen, deren Relevanz oder Irrelevanz ein Algorithmus leicht erkennen kann.[37] Daher besteht hier nicht das Problem, komplexe Gesetzesformulierungen in binäre Programmcodes zu transferieren,[38] so dass sich der Richter durch einen Rechner ersetzen ließe, der Beweismittel auswertet und die Einlassung des Beschuldigten bzw. Betroffenen hört und bewertet.

Gegen den Vorschlag, die Straf- und Ordnungswidrigkeitenjustiz durch den Einsatz künstlicher Intelligenz zu ersetzen, wird oft eingewandt, es sei der Gesellschaft und dem konkret Betroffenen (noch) nicht zu vermitteln, die Strafrechtsanwendung in die Hände digitaler Systeme zu legen.[39] Dieser Einwand entspricht einer vordergründigen Intuition, ist aber bei näherem Hinsehen weitaus weniger stichhaltig. Denn schon jetzt erhält die Mehrheit von Beschuldigten eines Strafverfahrens bzw. Betroffenen eines Bußgeldverfahrens einen schriftlichen Strafbefehl bzw. einen maschinell erstellten Bußgeldbescheid, ohne dass hinter diesen eine dem Adressaten bekannte Person oder eine für ihn nachvollziehbare menschliche Leistung stünde. Ersetzte man letztere – die menschliche Entscheidung – in einfach gelagerten Fällen durch künstliche Intelligenz, dürften die so zustande gekommenen Strafbefehle oder Bußgeldbescheide den sog. Turing-Test be-

37 Vgl. auch *Gleß/Wohlers*, FS Kindhäuser, 2019, S. 147, 152 f.
38 Auf diese Schwierigkeiten weist *Rostalski*, Rethinking Law 2019, 4, 6, hin.
39 Vgl. *Hähnchen/Bommel*, JZ 2018, 334, 340; *Frese*, NJW 2015, 2090, 2092.

stehen, der prüft, ob ein menschlicher Adressat erkennt, dass er mit einer Maschine anstatt mit einem Menschen kommuniziert.

In rechtlich wie tatsächlich einfach gelagerten Fällen – man denke an Verkehrsordnungswidrigkeiten oder an das Schwarzfahren – könnte ein Algorithmus schon heute nicht nur eine richtige Entscheidung treffen. Er könnte diese auch so begründen,[40] dass sie vom Adressaten inhaltlich ebenso gut nachvollzogen werden kann wie ein von einem menschlichen Richter mit Hilfe von Textverarbeitungsmasken und Satzbausteinen produziertes Urteil.[41] Denn entscheidend für die Richtigkeit und Qualität einer Begründung ist nicht der biologische Status des Richters, sondern die Fähigkeit, einen Sachverhalt zu erkennen, die rechtlich entscheidungserheblichen Aspekte von nicht entscheidungserheblichen zu trennen und diesen Vorgang in Textform darzustellen. Dazu sind Algorithmen in den exemplarisch genannten, einfach gelagerten Fällen ebenso gut in der Lage, wie sie Kreditanträge aufnehmen, verarbeiten, entscheiden und die Entscheidung begründen können.

Letzteres aber soll durch Art. 22 DS-GVO (und dem korrespondierenden § 6a BDSG) ausgeschlossen sein.[42] Danach hat jede Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet. Warum ist das so? Wenn es nicht die Fähigkeit zur rechtstechnisch richtigen Entscheidung und stimmigen Begründung ist, die der Anerkennung eines digital produzierten Bußgeldbescheides oder Strafbefehls durch den Adressaten entgegen steht – was dann? Vielleicht gerade der Umstand, dass ein Roboter stets richtig, d.h. nach den immer gleichen Maßstäben entscheidet. Dem Algorithmus, so *Ernst*, fehle die Freiheit, von klar definierten Vorgaben abzuweichen, während dem Menschen „erweiterte Erkenntnismöglichkeiten" zur Verfügung stünden.[43] Dieser Einwand lässt sich in dreifacher Weise verstehen. Zum Ersten ist denkbar, dass die Entscheidung deshalb falsch ist, weil die vom Algorithmus verwendete Rechtsregel verfassungswidrig ist.[44] Zum Zweiten könnte

40 Siehe aber *Rostalski*, Rethinking Law 2019, 4, 11, die meint, ein „iudex ex machina" sei nicht ansatzweise in der Lage, dem Rechtsunterworfenen die Gründe der Entscheidung darzulegen. Ähnlich *Gleß/Wohlers* (Fn. 37), S. 159.

41 *Fries*, RW 2018, 414, 422, weist darauf hin, dass schon heute im Familien- und Erbrecht „Rechtsrechner" eingesetzt werden, deren Ergebnisse zumindest Familienrichter ungeprüft übernähmen.

42 *Ernst*, JZ 2017, 1026, 1029 f.

43 *Ernst*, JZ 2017, 1026, 1030.

44 *Rostalski*, Rethinking Law 2019, 4, 8.

die Entscheidung falsch sein, weil der Sachverhalt, den der Algorithmus bearbeitet, untypisch ist und daher nicht zur Regel passt.[45] Diese beiden Fälle zeichnen sich dadurch aus, dass sie sich weitgehend technisch korrigieren lassen, indem der Algorithmus stets mit den verfassungskonformen Regelungen versehen und in die Lage versetzt wird, Atypisches zu erkennen. Versagt diese Kontrolle, ist die Entscheidung falsch, aber reversibel, wie es auch menschliche Entscheidungen sein können. Die Notwendigkeit der Korrektur falscher Urteile mittels Anpassung des Algorithmus oder im Instanzenzug spricht also nicht gegen die Anwendung künstlicher Intelligenz als Richter.

Anders ist dies in der dritten Fallgruppe, die *Ernst* offenbar meint: Entscheidungen, die korrigiert werden sollen, weil sie zwar rechtlich richtig sind, dem menschlichen Richter aber als unbillig erscheinen. Gesteht man Richtern – auch im Strafrecht – die Möglichkeit einer solchen „Billigkeitskorrektur" des Rechts zu, kann man Roboter nicht einsetzen, da diese sich nicht vom persönlichen Judiz und Gespür leiten lassen, sondern von Routinen bzw. Regeln. Indes ist es – gerade im Strafrecht – rechtsstaatlich und gleichheitsrechtlich problematisch, die Entscheidungshoheit des menschlichen Richters mit dem Argument zu verteidigen, dass nur der Mensch in der Lage sei, im Einzelfall vom Recht abzuweichen und eine rechtlich falsche, ihm aber billig erscheinende Entscheidung zu treffen. Legitim mag diese Billigkeitskontrolle sein, wenn besonders schwere Strafen drohen. Zum Ausschluss des Roboters aus der Entscheidung einfach gelagerter Fälle von Straßenverkehrsrechtsverstößen taugt das Argument hingegen nicht: Gerade die Legitimität der Beurteilung von Massenfällen speist sich daraus, dass sie einheitlich und gleichmäßig, d.h. ohne Ansehen der Person und ohne Abweichung von der Regel erfolgt. Dazu ist ein Roboter in hervorragendem Maße geeignet.

Indes verweist *Rostalski* mit Recht darauf, dass ein Urteil (oder Bußgeldbescheid) nicht nur einen Verwaltungsvorgang in rechtlich richtiger Weise abschließen soll, sondern auch einen Akt der Kommunikation zwischen Rechtsgemeinschaft und Beschuldigten bzw. Betroffenen darstellt. Sie fügt an: „Eine solche Kommunikation kann nicht über ein technisches System geleistet werden. (...) Als Vertreter der Rechtsgemeinschaft ist eine Maschine, die selbst nicht die Eigenschaft eines gleichberechtigten Gesellschaftsmitglieds aufweist, nicht denkbar." Gleichberechtigte Gesellschaftsmitglieder seien nur „vernunftbegabte Subjekte".[46] In dieselbe Richtung geht der

45 *Gleß/Wohlers* (Fn. 37), S. 160. Vgl. auch *Fries*, RW 2018, 414, 425.
46 *Rostalski*, Rethinking Law 2019, 4, 13.

Hinweis *Sehers*, digitale Systeme seien deshalb keine Rechtspersonen, weil sie den Inhalt von Normen nicht reflektierend verstehen könnten.[47]

Indes bleibt dabei unklar, welches Niveau an Vernunft und Reflexion damit vorausgesetzt wird und ob menschliche Richter diesem Standard gerecht werden können und müssen. Sollte damit gemeint sein, dass ein Richter den Sinn einer Vorschrift nachvollziehen kann, steht diese Anforderung dem Einsatz künstlicher Intelligenz nicht im Wege, soweit diese die Vorschrift anwenden und typische Fälle von untypischen Fällen unterscheiden kann. Versteht man unter vernunftgemäßer Reflexion der Norm hingegen mehr, etwa eine durch Vernunftschlüsse ermöglichte Legitimation der Regelung, die dem eigenen Handeln Sinn und Rechtfertigung verleiht, ist ein Niveau erreicht, das Roboter vom Richteramt ausschließt. Ausgeschlossen wären jedoch auch viele Berufsrichter, die das Recht – gerade in Massen- und Bagatellfällen – anwenden, ohne dessen Vernünftigkeit reflektierend mitzubedenken. Das Beispiel zeigt, dass menschliche Richter diese Reflexionsleistung weder ständig noch als Selbstzweck erbringen müssen, sondern nur situativ und funktionsbezogen, also dann, wenn sie konkreten Anlass haben, an der Verfassungskonformität der Anwendung dieser Regelung auf diesen Fall zu zweifeln. In den genannten Beispielen dürfte dies kaum je der Fall sein.

Einer schrittweisen Digitalisierung der Strafjustiz stehen damit schon heute weder technische Gründe noch prinzipielle Erwägungen im Wege. Ihren Abschluss fände diese Entwicklung dann, wenn Algorithmen nicht nur den Richter ersetzten, sondern digitale Systeme auch zum Subjekt der Strafe werden.[48] Undenkbar ist das nicht. So steuern schon heute Algorithmen den Hochfrequenzhandel mit Wertpapieren. Sollten diese Algorithmen lernen können, dass sich eine gelegentliche Regelübertretung im Handel für sie lohnen kann, müsste dieser Tendenz zum *digital moral hazard* entgegengewirkt werden. Überwachungsalgorithmen könnten solche Täuschungsversuche und andere Regelverletzungen erkennen und müssten auf diese schnell und fühlbar reagieren und beispielsweise das delinquierende System für eine gewisse Zeit vom Handel abtrennen. Zudem müsste der Algorithmus den Vollzug dieser punitiven Reaktion anderen

47 *Seher*, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, 2016, S. 45, 49 f. *Seher* thematisiert diese Frage zwar im Hinblick auf die Fähigkeit, Täter einer Straftat zu sein; seine Überlegungen können aber von der Ebene der Verhaltensnorm und der personalen Voraussetzungen ihrer Adressaten auf die Ebene der Sanktionsnorm übertragen werden.

48 *Gleß/Weigend*, ZStW 126 (2014), 561, 566 ff.; *Simmler/Markwalder*, ZStW 129 (2017), 20. Vgl. auch *Cornelius*, ZRP 2019, 8; *der.*, ZIS 2020, 51, 60 ff.

Systemen mitteilen, damit diese daraus für ihr eigenes Handeln lernen: Crime doesn't pay. Hier – und nur hier – würde der lange gehegte Traum der Deterministen und Präventionstheoretiker, Entscheidungen mit Hilfe von Strafandrohung und Strafvollziehungen zu lenken, Wirklichkeit werden. Maschinen sind jedenfalls für derartige spezial- und generalpräventive Impulse erheblich empfänglicher als Menschen.[49]

III. Fazit

Die Digitalisierung verändert die Lebenswelt und mit dieser das Recht. Auch das Strafrecht, das personale Freiheit in einer konkreten Gesellschaft ermöglichen und sichern soll, reagiert mit der ihm eigenen zeitlichen Verzögerung auf diese Veränderungen. Einige von ihnen sind schon jetzt sichtbar: Straftatbestände und strafprozessuale Ermächtigungsgrundlagen werden den Besonderheiten digitaler Systeme fortlaufend angepasst oder gänzlich neue Vorschriften geschaffen, um in sozialen Medien, auf eCommerce-Plattformen und in anderen digitalen Räumen grundlegende Verhaltensnormen garantieren und auf Normverletzungen mit Strafe reagieren zu können. Den damit einhergehenden kriminalpolitischen Fragen sollte die Strafrechtswissenschaft nicht ausweichen, indem sie sich auf die Position der Kritikerin des Gesetzgebers zurückzieht.[50] Sie darf zwar die „dunklen Seiten des Strafrechts" – Grundrechtseingriffe und Dysfunktionalitäten – nicht unterschlagen,[51] sondern muss mögliche Folgewirkungen gerade in der schwer überschaubaren digitalisierten Lebenswelt einkalkulieren. Man kann aber von der Strafrechtswissenschaft *auch* erwarten, dass sie es nicht bei einer Kritik belässt, sondern realistische, praktikable und zielgenauere Vorschläge unterbreitet, wie beispielsweise das allgemeine Persönlichkeitsrecht in sozialen Medien gegen Beleidigungen geschützt, in Darknethandelsplätzen ermittelt oder die Kommunikation in verschlüsselten Messenger-Diensten überwacht werden kann. Nichts zu tun und auf staatliche Rechtsdurchsetzung zu verzichten, ist jedenfalls keine Option: Wenn sich der Staat aus diesen digitalen Orten und Kommunikationswegen zurückzieht, führt dies zu jenen Verhaltensnormerosionen, die gegenwärtig in den sozialen Medien zu beobachten sind. Der Strafrechtswissenschaft kommt daher gerade hier eine positiv-geltende kriminalpolitische

49 Vgl. *Seher* (Fn. 47), S. 56 f., 59.
50 *Kölbel*, NK 2019, 249.
51 *Kölbel*, NK 2019, 249, 263.

Aufgabe zu, der sie sich nicht verschließen sollte, falls sie den Gesetzgeber zu einem möglichst rational begründeten und problembewussten Handeln bewegen will.

Jede Rechtsfortbildung bedarf indes eines normativen Fundaments. Hier kommt der Strafrechtswissenschaft die Aufgabe zu, ein möglichst stimmiges Legitimationsmodell des Datenschutzstrafrechts zu entwickeln und das geltende Recht nach dieser Maßgabe zu restrukturieren. Dabei sollte sich die Strafrechtswissenschaft vor einer Überbetonung der Selbstbestimmung und der datenschutzrechtlichen Einwilligung hüten. Denn Entscheidungen im digitalen Raum sind einerseits leicht zu erteilen und andererseits so voraussetzungsreich und komplex, dass die in einen „Klick" hineingelesene Einwilligung nicht ohne weiteres eine plausible und tragfähige Grundlage für die Nutzung von (personenbezogenen) Daten darstellen kann. Zudem führt die Engführung der Problemlagen auf die Einwilligung zu jenen blinden Flecken, die – in anderer Gestalt, aber ebenso deutlich – im Medizinstrafrecht zu beobachten sind. Ein verwaltungsrechtsakzessorisches Gegenmodell könnte sich an das Umweltstrafrecht anlehnen.

Langfristig wird es bei solchen Strafrechtsänderungen kleiner und mittlerer Reichweite nicht sein Bewenden haben. Vielmehr wird sich ab einem Entwicklungsstand der Technik und bei einem fortschreitenden Schwund von zum Richteramt befähigten Absolventen auch die Frage stellen, ob und inwieweit Legal Tech die Arbeit des Richters bzw. der Richterin ersetzen kann.[52] Die verneinenden Antworten, die gegenwärtig verbreitet sind, scheinen jedenfalls nicht derart stark begründet, dass sie die Entwicklung hin zum Roboter als Richter mit normativ zwingenden Gründen kategorisch ausschließen. Daher liegt es nahe, dass die Strafrechtswissenschaft mit Vertretern anderer Disziplinen eruiert, was Algorithmen und digitale Systeme tatsächlich können und was auch mittelfristig nicht möglich sein wird. Erst wenn Klarheit darüber herrscht, was die digitale Technik tatsächlich leisten kann, lässt sich entscheiden, was sie fortan tun darf und was sie nicht können soll.

52 Dass sich der Glaube der Juristen an die eigene Unersetzbarkeit als trügerisch erweisen kann, meinen treffend *Gleß/Wohlers*, FS Kindhäuser, 2019, S. 147, 149. Siehe bereits *Martini/Link*, NVwZ 2017, 681.