Einleitung

A. Transformative Technik – Transformation des Strafrechts?

1977 legte *Ulrich Sieber* sein Werk *Computerkriminalität und Strafrecht*[1] vor. Darin belegte er eindrucksvoll das Phänomen der Computerkriminalität – ein Kriminalitätsphänomen, dessen Existenz zur damaligen Zeit teilweise noch bestritten wurde. Einige Jahre später fügte der deutsche Gesetzgeber dem Strafgesetzbuch zwei Spezialstraftatbestände hinzu, den Computerbetrug (§ 263a StGB) und das Ausspähen von Daten (§ 202a StGB),[2] um auf diese Weise auch schon von *Sieber* identifizierte Strafbarkeitslücken zu schließen. Das strafrechtliche Spezialgebiet des Computerstrafrechts war geboren. Das Computerstrafrecht wurde in der Folgezeit um weitere Spezialtatbestände ergänzt[3] und entwickelte sich um die Jahrtausendwende hin zum Computer- *und* Internetstrafrecht. Dennoch führte es bis vor nicht allzu langer Zeit ein ausgeprägtes Nischendasein und die Auseinandersetzung damit wurde „den informatikinteressierten ‚Computernerds' der Strafrechtswissenschaft überlassen".[4]

Blenden wir zurück in diese Jahre der 1970er und frühen 1980er und richten den Blick auf den damaligen Stand der Computertechnik: Daten wurden nicht mehr auf Lochkarten, vielmehr auf Magnetplatten gespeichert,[5] hatten aber im Vergleich zur heutigen Zeit eine verschwindend geringe Speicherkapazität. Und auch die Rechenleistung von Computern bewegte sich weit unter dem heutigen Niveau.[6] Computer wurden in dieser Zeit – mit Ausnahme von einfachen Spielecomputern – fast ausschließlich im nicht-privaten Sektor genutzt: in der Wissenschaft, der Wirtschaft und im staatlichen Bereich mit Anwendungsbereichen bspw. in der Fertigungssteuerung, der Lohn- und Gehaltszahlung, der Lagerhaltung oder zum Aufbau von Datenbanken.[7]

Richten wir unseren Blick zurück in die heutige Zeit: Die Speicherkapazität und Leistungsfähigkeit von handelsüblichen Computern hat enorm zugenommen, für komplexe Rechenaufgaben stehen sog. Supercomputer[8] zur Verfügung und ein weiterer technologischer „Sprung" wird erwartet, sofern und wenn sich

1 *Sieber* 1977.
2 Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15.5.1986, BGBl. I (1986), S. 721.
3 Zur weiteren gesetzgeberischen Entwicklung *Kochheim* 2018, 133 ff.
4 *Fateh-Moghadam* ZStW 131 (2019), 863 (874).
5 *Klönne* 1986.
6 *Delvaux de Fenffe* 2019. Die Rechenleistung von Computern hatte dennoch im Vergleich zu den Anfängen des Computers bereits erheblich zugenommen und folgte dem „Mooreschen Gesetz" (dazu *Waldrop* 2016), mit welchem 1964 eine Verdoppelung der Rechenleistung alle 16 Monate vorhergesagt wurde.
7 Überblickartig *Sieber* 1977, 15 ff.
8 Dazu *statista* (Hrsg.) 2023.

sog. Quantencomputer realisieren lassen. Der Einsatz informationstechnischer Systeme ist so omnipräsent, dass eine Aufzählung ihrer Einsatzbereiche müßig ist – er durchdringt nicht mehr nur die Wirtschaft, Wissenschaft und Verwaltung, sondern ist auch im Privaten so vielfältig wie nie. Informationstechnische Systeme bedeuten nicht mehr nur Computer im eigentlichen Sinne, sondern „Smartphones", Fahrzeuge, die auch softwaregestützt operieren, Produkte des „Internet of Things" etc. Diese Systeme sind teilweise in der Lage, „autonom" zu agieren, weil sie Umgebungsdaten aufnehmen und berücksichtigen und weil sie die Regeln, auf Grund derer sie zukünftig agieren, selbst erlernen können – sie sind *künstlich intelligent*. Es geht um autonome Fahrzeuge, die aus Fahrern Passagiere machen, um Drohnen, die Pakete „selbstständig" ausliefern sollen, um Pflegeroboter, oder um generative Systeme, die Texte und Bilder auf Grund weniger Vorgaben erstellen können.

Während sich der Einsatz von Computern vor 40 bis 50 Jahren einem bestimmten, abgeschlossenen Lebensbereich zuordnen ließ, durchdringt die Computer- und Informationstechnologie inzwischen sämtliche gesellschaftliche Lebensbereiche. Auf der 38. Strafrechtslehrertagung in Hannover resümierte *Fateh-Moghadam* denn auch: „Die quantitative Leistungssteigerung und ubiquitäre gesellschaftliche Verbreitung der digitalen Informationstechnologie hat damit den Punkt erreicht, an dem sie qualitativ zu einer transformativen Technologie umschlägt."[9] Transformativ, weil sie auf „*die normative Verfasstheit einer Gesellschaft*" einwirke und namentlich eine „*digitale Transformation des Strafrechts*" bewirke.[10] In der Tat: Es geht nicht mehr um einen Spezialbereich des Computerstrafrechts, abgesondert vom „normalen Strafrecht" – der Prozess der Digitalisierung und damit einhergehende neue technische Möglichkeiten setzen vielmehr laufend neue Impulse, die sowohl auf Täterpersönlichkeiten und Tatmodalitäten einwirken und in rasanter Geschwindigkeit Fragen produzieren, die in das Strafrecht insgesamt hineinwirken und die Grundlagen des Strafrechts berühren.

Am Beispiel der *Künstlichen Intelligenz* als Teilbereich der Digitalisierung ergeben sich bspw. folgende Fragen:

- Was ist Handlung, was ist Schuld und ist schuldhaftes Handeln einer *autonomen* KI-Technik oder ausschließlich nur des Menschen denkbar? Was unterscheidet überhaupt eine leistungsstarke Technik vom „denkenden" Menschen?
- Wie rechnet das Strafrecht Erfolge zu, die nur mittelbar durch menschliches Handeln und unmittelbar durch ein technisches Artefakt herbeigeführt werden? Und ist eine solche Zurechnung bei einer autonomen und epistemisch opaken KI-Technik möglich?

9 *Fateh-Moghadam* ZStW 131 (2019), 863 (867).
10 *Fateh-Moghadam* ZStW 131 (2019), 863 (867 f.).

– Wie geht das Strafrecht mit dem technischen Risiko um und was ändert sich durch das KI-technische Risiko? Ist jegliches Risiko durch Technik verboten oder wenn nicht, wie sind erlaubte und unerlaubte Risiken zu unterscheiden? Wie fügt sich das Strafrecht in den Umgang mit dem technischen Risiko durch das Öffentliche Recht und das Zivilrecht ein?

Die „digitale Transformation" des Strafrechts wirft Fragen auf, die einer Rückbesinnung *ex negativo* auf die Grundlagen des Strafrechts bedürfen. *Hilgendorf* fasst dies wie folgt zusammen:

> „Bemerkenswert ist, dass die Digitalisierung zu der Notwendigkeit zu führen scheint, rechtliche Begriffe und Prozesse zu explizieren, ein Phänomen, welches die juristische Methodenlehre nicht als Übergriff, sondern als Herausforderung begreifen sollte."[11]

B. Untersuchungsgegenstand und Gang der Darstellung

Diese Arbeit widmet sich einem Teilbereich der Digitalisierung, der Technik der Künstlichen Intelligenz (KI), und untersucht, ob und wie der zunehmende Einsatz von KI-Produkten die strafrechtliche Produktverantwortung verändert. Denn mit KI entwickelt sich – so jedenfalls die Hypothese – eine Technik, die sich aus der (vermeintlichen) Steuerung und Beherrschbarkeit durch den Menschen herauslöst und als autonomer und in seiner Funktionsweise opaker Akteur dem Menschen als „zweite Natur" gegenübertritt. *Untersuchungsgegenstand* ist also ein Wandel der Technik und es ist zu fragen, ob sich hieraus Anlass für eine Neubewertung oder Änderung des Rechts – für einen Wandel auch des Rechts – ergibt. Ob KI als so verstandene Innovation auch rechtlichen Wandel anstößt bzw. zu einem solchen führen sollte, sei es seitens der Rechtsprechung durch eine Anpassung dogmatischer Strukturen im Bereich der strafrechtlichen Produktverantwortung oder durch ein Tätigwerden seitens des Gesetzgebers, ist das *Erkenntnisziel* dieser Arbeit.

Mit der strafrechtlichen Produktverantwortung beschäftigte sich monographisch erstmals u.a. *Hilgendorf*[12] und legte seiner Analyse dabei die von *Beck* 1985 aufgestellte Diagnose einer Risikogesellschaft zu Grunde – einer Gesellschaft, die mit „Wellen technologischer Großinnovationen" und als deren Nebenfolgen mit „wissenschaftlich-technischen produzierte[n] Risiken" konfrontiert sei.[13] Auch *Prittwitz*[14] nahm diese Gesellschaftsdiagnose in seiner Analyse von „Strafrecht und Risiko" auf und fragte, ob und wie das Strafrecht mit diesen „Großrisiken" umgehen könne und dürfe. Der Gesellschaftsbefund einer Risiko-

11 *Hilgendorf* 2019, 234. Ähnl. *Simmler* 2019, 466.
12 *Hilgendorf* 1993. Siehe daneben die Arbeit von *Kuhlen* 1989.
13 Dazu näher und mit Nachweisen unten Kap. 1, A.I.
14 *Prittwitz* 1993.

gesellschaft und der darauf aufbauende Diskurs um ein Risikostrafrecht beziehen sich auch auf technische Innovationen und haben Fragen aufgeworfen, die für die vorliegende Arbeit zu stellen sind.

Indes – es wird sich zeigen, dass die Perspektive der Risikogesellschaft für diese Arbeit nicht ausreicht. Um die oben beispielhaft aufgezählten Grundlagenfragen zu beantworten, bedarf es einer technikorientierten, interdisziplinären sowie intradisziplinären Perspektive, die dem Diskurs über das Risikostrafrecht fehlt. Zugrunde gelegt wird daher der Befund einer *Innovationsgesellschaft*.

Daraus ergibt sich folgender Gang der Untersuchung:

I. Die Untersuchung beginnt mit Grundüberlegungen zu „Risiko, Innovation und Verantwortung" (*Kapitel 1*) und in einem ersten Schritt zu „Risiko und Innovation" (A.). Es wird dargelegt, weshalb der Gesellschaftsbefund einer Risikogesellschaft für den Untersuchungsgegenstand dieser Arbeit unzureichend und der Befund einer Innovationsgesellschaft passender ist. Auf dieser Grundlage folgt ein Überblick über die „Innovationsforschung in der Innovationsgesellschaft" und speziell über die „rechtswissenschaftliche Innovationsforschung". Aus einer „Methodik der rechtswissenschaftlichen Innovationsforschung" ergibt sich, dass für die Verarbeitung des „Neuen" – der Technik der KI sowie der Frage der strafrechtlichen Produktverantwortung für KI-Produkte – zunächst ein Blick *ex negativo* erforderlich ist: Die Neuartigkeit der KI-Technik lässt sich nur bestimmen, wenn das Wesen „klassischer" Technik offengelegt wird; ein Innovationsbedarf für die strafrechtliche Produktverantwortung kann nur festgestellt werden, wenn die Grundlagen der (straf-)rechtlichen Verantwortung für „herkömmliche" Technik geklärt sind.

Entsprechend folgt in einem weiteren Abschnitt „Technik und Risiko" (B.) eine Analyse des Wesens von Technik, der Strukturen menschlichen Handelns in Bezug auf Technik (das technische Handeln) und der Erwartungen, die an „klassische" Technik geknüpft sind. In einem zweiten Schritt „Risiko durch Technik" wird das Verständnis von „klassischer Technik" mit dem Risikobegriff in Beziehung gesetzt, um das technische Risiko und den technischen Konflikt zu konturieren. Im Abschnitt „technische Innovation und Verantwortung" (C.) werden sodann – aus einer intradisziplinären Perspektive – die Grundlagen der (straf-)rechtlichen Verantwortung für technische Innovationen nachgezeichnet.

II. Das *zweite Kapitel* dieser Arbeit widmet sich dem Untersuchungsgegenstand dieser Arbeit und arbeitet heraus, was die Technik der Künstlichen Intelligenz ausmacht (A.). Dazu gehören verschiedene Begriffsmodelle, die prägenden Eigenschaften von KI – Lernfähigkeit und technische Autonomie – sowie das maschinelle Lernen. Beleuchtet wird insbes. das Phänomen einer epistemischen Opazität von KI-Systemen und die Frage des „Can machines think?" – beide Fragestellun-

gen sind relevant dafür, wie sich der Mensch zu KI-Technik ins Verhältnis setzen kann.

Für die Leserin und den Leser mögen in diesem Teil die Vielzahl wörtlicher Zitate aus der Primärliteratur zur Künstlichen Intelligenz auffällig sein. Ich habe mich bewusst dazu entschieden, an vielen Stellen die Experten vom Fach direkt zu Wort kommen zu lassen und mich selbst auf paraphrasierende Kommentare zu beschränken. Denn ich bin überzeugt davon, dass dies das Verständnis für die komplexen technischen Hintergründe fördert, weil die Experten vielfach besser beschreiben können, was sie tun, als die Verfasserin als in der Hinsicht technische Laiin.

In einem zweiten Schritt wird erörtert, ob und weshalb KI-Technik eine technische Innovation ist (B.). Dafür werden die Eigenschaften von KI an den Elementen einer „klassischen" Technik gemessen und untersucht, ob und inwiefern KI als „transklassische Technik" oder gar als „naturalisierte" Technik das technische Risiko verändert.

III. *Kapitel 3* schließlich widmet sich der strafrechtlichen Produktverantwortung für KI-Produkte. Dafür wird zunächst ihr Realbereich (B.) untersucht, d.h. welche tatsächliche Konfliktlage damit bewältigt werden soll; dabei erfolgt aus einem Blick *ex negativo* zunächst eine Bestandsaufnahme in Bezug auf „herkömmliche" Produkte und in einem zweiten Schritt wird untersucht, welche Veränderungen KI-Produkte bewirken.

Der Abschnitt „KI-Verantwortung statt Produzentenverantwortung?" (C.) geht der Frage nach, ob nicht ein KI-System selbst als *zusätzliches* Verantwortungssubjekt anzuerkennen ist, da es schließlich „technisch autonom" agiert und möglicherweise der Mensch wegen eines im KI-Kontext besonders diskutierten „Verantwortungsrisikos" nicht verantwortlich gemacht werden kann.

Die „strafrechtliche Produktverantwortung im Kontext der KI-Regulierung" (D.) nimmt einen intradisziplinären Blickwinkel ein und analysiert die KI-Strategie staatlicher Akteure, gibt einen Überblick über den Vorschlag für eine KI-Verordnung sowie über Vorschläge für eine Anpassung der zivilrechtlichen Produkthaftung in Bezug auf KI-Produkte.

Schwerpunkt des *3. Kapitels* bildet schließlich die Erörterung der „normativen Schwerpunkte bei der strafrechtlichen Produktverantwortung für KI-Produkte de lege lata" (E.). Untersucht wird, weshalb Produzenten Adressaten von KI-technischen Verhaltensnormen sind und wie der Umfang sog. unternehmensbezogener Pflichten auf der Grundlage der Rechtsfigur des erlaubten Risikos zu bestimmen ist (II.). Berücksichtigt werden dabei insbes. die technischen Verhaltensnormen der von der EU-Kommission vorgeschlagenen KI-Verordnung. Danach wird analysiert, wie die unternehmensbezogenen Pflichten angesichts des Grundsatzes individueller Zurechnung und im Zusammenhang mit dem „problem of many

hands“ auf einzelne Unternehmensangehörige individualisiert werden können (III.). Eine zentrale Rolle spielt dabei der Vertrauensgrundsatz. Sodann wird auf die Strafbarkeitsvoraussetzungen eingegangen, die neben dem tatbestandlichen Erfolg i.S.d. §§ 222, 229 StGB vorliegen müssen – auf die Kausalität und die objektive Zurechnung (IV.). Es werden die prägenden KI-typischen Eigenschaften – technische Autonomie, epistemische Opazität sowie – unter Einbeziehung des Fertigungsprozesses dieser Produkte – eine ausgeprägte soziale Opazität – zu Grunde gelegt und untersucht, inwiefern diese mit Herausforderungen beim Nachweis von Kausalität und/oder objektiver Zurechnung verbunden sein können.

Als Fazit vorstehender Erörterungen kann eine Verantwortungslücke bei der Zuweisung strafrechtlicher Produktverantwortung für KI-Produkte festgestellt werden; daher folgt in einem letzten Abschnitt die Frage nach einer „strafrechtlichen Produktverantwortung für KI-Produkte de lege ferenda“ (F.).

Schließlich werden die wesentlichen Ergebnisse der vorliegenden Untersuchung zusammengefasst und gewürdigt.