Sammelband 2020

KriPoZ JuP

Kriminalpolitische Zeitschrift

KONTAKT
schriftleitung@kripoz.de

Herausgeber
Prof. Dr. Carsten Momsen
Mathis Schwarze, MSc

Strafrecht im Zeitalter von Digitalisierung und Datafizierung

- Sammelband -

aus der Reihe:

KriPoZ | Junges Publizieren

in Zusammenarbeit mit

University of Zurich[UZH]

Freie Universität Berlin

INHALT

VORWORT

Die in diesem Sammelband der JuP zusammengefassten Beiträge sind im Rahmen eines gemeinsamen Seminars der Freien Universität Berlin (*Carsten Momsen*) und der Universität Zürich (*Frank Meyer*) entstanden, der ersten gemeinsamen rechtswissenschaftlichen Lehrveranstaltung im Rahmen der strategischen Partnerschaft beider Universitäten.* Das Seminar fand im November 2019 an drei Tagen in Zürich statt mit insgesamt ca. 20 Teilnehmerinnen und Teilnehmern. Die Veranstaltung führte zu einem regen Meinungsaustausch, die Seminarsitzungen zogen sich teilweise bis in den Abend und die Diskussionen wurden im Rahmen des abendlichen Programms fortgesetzt. Auf hohem Diskussionsniveau zeigten sich dabei auch ganz erstaunliche Unterschiede in der Theorie und Praxis zweier benachbarter Strafrechtssysteme, so dass das Seminar auch viele rechtsvergleichende Erkenntnisse erbrachte.

Die „Digitalisierung und Datafizierung des Strafrechts und des Strafverfahrens" sowie weitergehend auch die Einführung vorhersagender Polizeiarbeit (Predictive Policing) führen zu einschneidenden Veränderungen in allen Bereichen. Alte Probleme erleben eine Widerauferstehung in neuem Gewand, neue Probleme – und Chancen – treten hinzu und in nicht wenigen Fällen verändert sich der Charakter von Ermittlungsmaßnahmen. Die möglicherweise folgenreichste Veränderung aber ist ein Bedeutungswandel von Begriffen und Institutionen, insbesondere im Bereich des Strafverfahrens. Durch die zunehmende Verwendung massenhaft erhobener Daten (Big Data), deren Verknüpfung und Auswertung mit Hilfe von durch Algorithmen gesteuerten Analysetools bis hin zum beginnenden Einsatz von künstlicher Intelligenz (KI/AI) gewinnen diese Entwicklungen ganz erheblich an Dynamik.

Vorliegend sind zunächst die Beiträge von Teilnehmerinnen und Teilnehmern aus Berlin zusammengefasst. Den Beginn macht ein Beitrag von *Kim Böttcher* zum Thema „Predictive Policing – Einsatzmöglichkeiten und Zulässigkeitsgrenzen". Sie beschreibt den gegenwärtigen Stand vorhersagender Polizeiarbeit und analysiert mit Blick auf Verfassungs- und Strafverfahrensrecht potentielle Grenzen und Legitimationsbedürfnisse. *Tinam Lorenso* widmet sich der „Nutzung von Big Data und Algorithmus-basierter Datenanalyse" in Strafverfahren und stellt nicht nur verschiedene Tools und Anwendungsbereiche dar, die gegenwärtig diskutiert werden, sondern zeigt gerade im Verhältnis zum ersten Beitrag auf, wie nahe sich die Methoden präventiver und repressiver Polizeiarbeit kommen. Obwohl er Fragen betrifft, die erst am Ende eines Strafverfahrens zu entscheiden sind, zeigt der Beitrag von *Malin Ebersbach* mit dem Titel" Big Data, Algorithmen und Bewährungsentscheidungen" nicht nur Potentiale und Gefahren der Verwendung von Algorithmen bei Bewährungsentscheidungen auf, sondern leitet zugleich über zu deren unter Umständen diskriminierender Auswirkung auf künftige Verfahren. Sehr eng damit zusammen hängen die Überlegungen von *David Heger* zu der Frage, wie sich die Verwendung von „Big Data (auf die) Unschuldsvermutung" auswirkt. Dies mündet in Fragen, ob derartige Vermutungen überhaupt durch Algorithmen angemessen erfasst werden können. *Leona May Jackson* wendet sich dem in bewusstem Widerspruch so betitelten Thema „Big Data und die Bestrafung künftiger Täter" zu. Bereits die Verwendung des Wortes „künftige Täter" zeigt, worum es geht. Die nicht zuletzt im „Minority Report" gestellte Frage, ob man Personen, die mit einer bestimmten

* Prof. Dr. *Frank Meyer*, LL.M. (Yale) ist Inhaber des Lehrstuhls für Straf- und Strafprozessrecht unter Einschluss des internationalen Strafrechts am Rechtswissenschaftlichen Institut der Universität Zürich.
Prof. Dr. *Carsten Momsen* ist Inhaber des Lehrstuhls für Vergleichendes Strafrecht, Strafverfahrensrecht, Wirtschafts- und Umweltstrafrecht am Fachbereich Rechtswissenschaft der Freien Universität Berlin.
Mathis Schwarze, MSc (Oxford) ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Vergleichendes Strafrecht, Strafverfahrensrecht, Wirtschafts- und Umweltstrafrecht am Fachbereich Rechtswissenschaft der Freien Universität Berlin.

Wahrscheinlichkeit Straftaten begehen werden, durch Sanktionen und Eingriffe im Vorfeld präventiv daran hindern kann. Hier stellen sich eine Vielzahl nicht nur verfassungsrechtlicher Probleme, die kritisch beleuchtet werden. *Katja Lentz* setzt mit ihrer Arbeit „Probleme und Möglichkeiten beim Einsatz von künstlicher Intelligenz als Hilfsmittel im deutschen Justizsystem“, an dem Punkt an, an dem die Analysen tatsächlich als Beweismittel in ein Strafverfahren eingeführt werden sollen. Können oder sollen sie, wie Protagonisten meinen, die Richterinnen und Richter in ihren Entscheidungen binden oder unterliegen sie freier Würdigung wie andere Beweismittel auch? Den Abschluss machen zwei konkrete Beispiele des Einsatzes digitaler Technologien bei strafrechtlichen Ermittlungen. *Delvin Sönmezer* befasst sich mit „Bodycams – Einsatzmöglichkeiten und Zulässigkeitsgrenzen“ und zeigt auch hier, dass die Technologie einen Einfluss auf den rechtlichen Rahmen, insbesondere von Durchsuchungen, gewinnt.

Hinzugenommen haben wir einen Beitrag von *Paula Benedict* aus einem vorangegangenen Seminar, der thematisch hier anschließt. Sie analysiert „WhatsApp-Nachrichten als Beweismittel“ und erläutert zugleich neue „digitale Ermittlungsmethoden“ wie bspw. die Online-Durchsuchung. Auch hier zeigt sich nicht nur ein immer präsenterer Konflikt zu den Anforderungen und berechtigten Interessen des Datenschutzes sowie der Durchsetzung der vom Bundesverfassungsgericht entwickelten „IT-Grundrechte“. Angelegt in der Regelung entsprechender – heimlicher – Ermittlungsmaßnahmen ist eine flächendeckende Überwachung, die legitimationsbedürftig ist. Der Beitrag schließt mit einer kurzen neu angefügten Analyse der „Tracking-Apps“, die ganz aktuell diskutiert werden, um mit dem „Corona-Virus“ (COVID-19) – infizierte Personen bzw. ihre potentiellen Kontaktpersonen mittels der Bewegungsdaten von Mobiltelefonen zu identifizieren.

In dieser Anthologie nicht enthalten ist der Beitrag von *Mathis Schwarze* zum Thema „Big Data, Algorithmen und Strafzumessung“. Dieser Beitrag ist Teil eines umfangreicheren Forschungsprojekts gemeinsam mit der University of Oxford und wird in einer anderen Publikation veröffentlicht. Auch *Marco Willumat* hat einen Diskussionsbeitrag zur „Nutzung von Big Data und Algorithmus-basierter Datenanalyse in der Beweisführung zum Nachweis von Kausalität“ geliefert, der ebenfalls bereits in einer anderen Veröffentlichung aufgegangen ist. *Cäcilia Rennert* schließlich hat über die „Nutzung von Big Data und Algorithmus-basierter Datenanalyse in der Beweisführung zum Nachweis des Tatverdachts und die Verwendung von Predictive Algorithms/Wahrscheinlichkeitsindikatoren“ referiert. Auch dieser Beitrag ist Teil eines umfangreicheren Forschungsprojekts gemeinsam mit dem „Center for International Human Rights“ am John Jay College of Criminal Justice der City University New York (CUNY). Die zugrundeliegenden Überlegungen sind Gegenstand einer umfassenderen Problemanalyse. Ein erster Bericht ist im Juni-Heft der KriPoZ erschienen.

Zur besseren Lesbarkeit wurden die Beiträge gekürzt und das für eine Seminararbeit obligatorische Literaturverzeichnis entfernt. Die Nachweise in den Fußnoten sind entsprechend angepasst.

Wir danken *Anja Schiemann* für die Möglichkeit, die Beiträge hier in der Kriminalpolitischen Zeitschrift veröffentlichen zu können. Der Freien Universität Berlin und der Universität Zürich ist für die Unterstützung bei der Durchführung des Seminars zu danken.

Carsten Momsen und *Mathis Schwarze*

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Kim Böttcher

Predictive Policing
Einsatzmöglichkeiten und Zulässigkeitsgrenzen

Inhaltsverzeichnis

I. Einleitung

„Aber träumen darf man ja mal von der gläsernen Welt und Tom Cruise beim predictive policing, und einem selbst am Drücker? Wer träumt nicht mal davon, die Herrin der Welt zu sein und die Linsen aus der Asche zu suchen: die guten hier hinein, die schlechten dort hinein, und am Schluss auf den Ball des Königssohns zu gehen ohne Blut im Schuh?“[1]

Es ist das alt bekannte Spiel von Räuber und Gendarm. Der eine will den anderen fangen und der Schnellere gewinnt. Doch was passiert, wenn sich die Spielregeln ändern und der Gendarm schon vor dem Räuber selbst weiß wo dieser sich aufhalten wird? Die Utopie der Gefahrenabwehr ist es, die Gefahr an sich gar nicht erst entstehen zu lassen. Also Straftaten zu verhindern, bevor sie verübt werden. Was wie eine Idealvorstellung klingt, scheint mit Predictive Policing bereits Realität geworden zu sein. Auch das Time Magazine schien von dieser Idee nicht unbeeindruckt und kürte „Predictive Policing“ als eine der besten 50 Erfindungen des Jahres 2011.[2] Big Data und deren Analysen stellen den neuen Lichtblick im dunklen Tunnel der Kriminalitätsbekämpfung dar. Doch wie jedes System, das eine finale Lösung verspricht, muss es sich an den Grenzen unserer Verfassung und denen der Realität messen.

II. Definition von Predictive Policing

Predictive Policing (auch vorhersagebasierte Polizeiarbeit) bezeichnet die polizeiliche Analyse von Falldaten und deren Anwendung im Wege der Big-Data-Auswertung.[3] Es ist dabei von „vorhersagebasiert“ zu sprechen, da Begriffe wie „vorhersagende oder vorausschauende Polizeiarbeit“ implizieren, die Vorhersagen seien absolut und nicht basierend auf reinen Wahrscheinlichkeitsrechnungen.[4] Die Berechnung von Wahrscheinlichkeiten des Eintritts von Straftaten, also die Vorhersage möglichen Täterverhaltens und frühzeitige Identifizierung aufkommender Kriminalitätsbrennpunkte stellt dabei das wohl wichtigste Ziel dar.[5] Auf Grundlage dieser Daten soll mit entsprechenden polizeilichen Maßnahmen reagiert werden, um fortan Straftaten zu verhindern oder die Aufklärung von Delikten zu verbessern.[6] Dies soll nicht nur zu einem gezielteren und effizienteren Einsatz von polizeilichen Ressourcen führen, sondern auch die Kriminalitätsrate im Allgemeinen senken.[7]

III. Ursprung

Vorhersagebasierte Polizeiarbeit begann in den Neunzigerjahren im amerikanischen Bundesstaat New York. Die „dunkelsten Jahre“[8] der Weltmetropole waren geprägt von massiver, die Sicherheit der Öffentlichkeit stark einschränkender Kriminalität.[9] Im Jahr 1990 verzeichnete die Polizeistatistik den absoluten Höhepunkt der damaligen

1 *Fischer*, Vor dem Gesetz ist jeder Glaube gleich, Spiegel Panorama, abrufbar unter: https://www.spiegel.de/panorama/justiz/kopftuch-urteil-vom-bundesverfassungsgericht-hauptsache-neutral-kolumne-a-7be575a3-4804-4c47-8402-c0aac93045f7 (zuletzt abgerufen am 10.3.2020).
2 *Grossman/Thompson/Kluger/Park/Walsh/Suddath/Dodds/Webley/Rawlings/Sun/Brock-Abraham/Carbone,* The 50 Best Inventions, Time Magazine, 18. November 2011.
3 *Egbert*, APuZ 33-32/2017, 17 (19); *Härtel*, LKV 2019, 49 (54).
4 Vgl. *Egbert/Krasmann*, Predictive Policing, Projektabschlussbericht, Universität Hamburg, 30.4.2019, S. 11.
5 *Härtel*, LKV 2019, 49 (54); Landeskriminalamt NRW, Abschlussbericht Projekt SKALA – Kurzfassung, 2018, S. 1.
6 *Härtel*, LKV 2019, 49 (54).
7 Website von *PredPol*, abrufbar unter: https://www.predpol.com/about/ (zuletzt abgerufen am 11.4.2020).
8 *Schweppe*, Als New York eine Mördergrube war, WELT, 11.1.2019, abrufbar unter: https://www.welt.de/politik/ausland/article186879194/New-Yorks-dunkelste-Jahre-Als-die-Weltstadt-eine-Moerdergrube-war.html, (zuletzt abgerufen am 11.4.2020).
9 *Knobloch*, Vor die Lage kommen: Predictive Policing in Deutschland, 2018, S. 11.

Kriminalitätswelle mit 2245 Morden.[10] Unter diesen Umständen etablierte der damalige Bürgermeister *Rudolph Giuliani* eine Zero Tolerance Policy, welche auf der von US-amerikanischen Sozialforschern *James Q. Wilson* und *George L. Kelling* entwickelten Broken Windows Theorie[11] basierte. Diese Theorie, welche auch als Ansatz für aktuell bestehende Predictive Policing Systeme verwendet wird, basiert auf der Annahme, dass eine nicht reparierte zerbrochene Fensterscheibe weitere Zerstörungen nach sich zieht und somit zu immer mehr Straftaten führt. Eine zerbrochene Scheibe steht nach diesem Ansatz für ein nicht sozial oder polizeilich kontrolliertes Gebiet und als Einladung für derartige Delinquenz.[12] Vermehrt setzte das New York City Police Departement zum ersten Mal ein datenbasiertes System (CompStat) ein, wodurch alle Festnahmen, Straftaten, Kontrollen und Beschlagnahmen gespeichert und für alle PolizistInnen zugänglich gemacht wurden.[13] Diese Verwendung von Statistik und Datenverarbeitung führte Jahre später zum Einsatz eines Predictive Policing Systems durch das Los Angeles Police Departement.[14] 2011 setzte dieses erstmals das bis heute am weitesten verbreitete System PredPol ein.[15] Es wurde von *George Mohler* und *Jeffrey Brantingham* an der University of California entwickelt und basiert auf einer Software zur Vorhersage von Erdbeben.[16] Dort gilt ein Prinzip ähnlich wie im später noch erläuterten Near-Repeat-Ansatz: Wenn ein Erdbeben stattgefunden hat, erhöht sich in der Nachbarschaft das Risiko, dass ein weiteres Erdbeben erfolgt. Mittlerweile haben sich auch Ableger und Eigenentwicklungen wie zum Beispiel das System KrimPro aus Berlin oder das in Bayern verwendete Programm Precobs entwickelt und etabliert.

IV. Technische Grundlagen und Einsatzmöglichkeiten

Predictive Policing kann in zwei Verfahren angewandt werden. Zum einen gibt es die raumbezogenen Verfahren, wo Orte und Zeiten bestimmt werden, an denen ein erhöhtes Risiko für das Auftreten von Kriminalität besteht. Daneben existieren die personenbezogenen Verfahren. Dort werden einzelne Personen identifiziert und mit einem Risikoprofil für die zukünftige Begehung von Straftaten versehen, Täterprofile im Hinblick auf vergangene spezifische Straftaten erstellt und Gruppen oder Personen ausgesondert, die einer erhöhten Gefahr ausgesetzt sind, Opfer einer Straftat zu werden.[17] Zur Gewinnung dieser Ergebnisse werden bestimmte Daten im Lichte unterschiedlicher kriminologischer Theorien und technischer Ansätze analysiert.

1. Raumbezogene Verfahren

Das raumbezogene Verfahren ist momentan die in Deutschland einzig zugelassene Form des Predictive Policing. Hier gilt es zwischen drei Ansätze zu unterscheiden: Dem Near-Repeat-Ansatz, der Hot-Spot-Methode und der Risk-Terrain-Analyse.

[10] Spiegel Panorama, Polizeistatistik – Zahl der Morde in New York sinkt auf Rekord-Tief, 2.1.2015, abrufbar unter: https://www.spiegel.de/panorama/justiz/kriminalitaet-in-new-york-zahl-der-morde-sinkt-auf-rekord-tief-a-1010993.html (zuletzt abgerufen am: 11.4.2020).
[11] *Wilson/Kelling*, Broken Windows – The Police and Neighborhood Safety, The Atlantic Monthly, März 1982.
[12] *Wilson/Kelling*, ebd.
[13] *Government Innovators Network*, Compstat: A Crime Reduction Management Tool, abrufbar unter: https://www.innovations.harvard.edu/compstat-crime-reduction-management-tool (zuletzt abgerufen am 13.4.2020).
[14] Vgl. *Montag*, Der Algorithmus des Verbrechens – Analysen und Argumente, Konrad Adenauer Stiftung (Hrsg.), Ausgabe 215, September 2016, S. 3.
[15] *Knobloch*, Vor die Lage kommen: Predictive Policing in Deutschland, 2018, S. 11.
[16] *Krieger*, in: Brettel/Rau/Rienhoff, Strafrecht in Film und Fernsehen, 2016, S. 193.
[17] Vgl. *Perry/McInnis/Price/Smith/Hollywood*, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, RAND Corporation, 2013, S. 8.

a) Near-repeat-Ansatz

Der Hauptanwendungsfall von Predictive Policing in Deutschland ist die Bekämpfung von Wohnungseinbruchdiebstählen. Und gerade hier wird meist der Near-repeat-Ansatz angewandt, welcher auf kriminologischen Thesen wie der Rational-choice-Theorie oder dem Routine-activity-Approach aufbaut.[18] Diese beruhen auf der Annahme, dass professionelle SerientäterInnen eine Art Gewinnabrechnung vornehmen, um so die Effektivität ihrer Delinquenz zu steigern. Sollten sie einmal in einer bestimmten Gegend erfolgreich gewesen sein, nutzen sie diese oft für Folgetaten, da sie die Risiken und Entdeckungsgefahren besser einschätzen können.[19] Es erfolgt also eine Maximierung ihres Gewinns, wobei der Aufwand vergleichsweise klein gehalten werden soll.[20] Für diese Folgetaten entwickelt die Predictive Policing Software dann eine Wahrscheinlichkeitsaussage. Es wird davon ausgegangen, dass die Wahrscheinlichkeit 48 Stunden nach der Anlasstat am höchsten sein soll.[21] Eigenschaften wie die Einsehbarkeit oder architektonische Gestaltung von Häusern, mögliche Überwachungsanlagen und Zugangs- sowie Fluchtmöglichkeiten spielen eine Rolle, da sie später als Kriterien in Datenform in das Prognosesystem einfließen. Dieser Ansatz kann aber nur effektiv sein, wenn das Verhalten von professionellen TäterInnen analysiert wird. Denn nur diese gehen oft einer bestimmte Vorgehensweise nach oder folgen distinktiven Mustern.[22]

b) Hot-Spot-Methode

Viele kennen das Bild der mit Stecknadeln übersäten Karte in amerikanischen Kriminalfilmen. Diese sollen Kriminalitätsentwicklungen und räumliches Täterverhalten aufzeigen. Diese Form des Crime Mapping[23] kann wie ein analoger Anfang des Predictive Policing in Form der Hot-Spot-Methode gesehen werden. Denn auch bei der Hot-Spot-Methode werden historische Falldaten verwendet, um ortsbezogene Kriminalitätszentren zu identifizieren.[24] Es sollen somit relativ dauerhafte Schwerpunktsorte aus der Vergangenheit in die Zukunft fortgeschrieben werden.[25] In solchen Risikobereichen wird dann mit polizeilichen Maßnahmen, wie beispielsweise verstärkter Kontrolle, Bestreifung und Polizeipräsenz reagiert. Ein anschauliches Beispiel dafür ist die Hamburger Reeperbahn, welche seit vielen Jahren eine hohe Anzahl an Straftaten verzeichnet, die vor allem am Wochenende auftreten.[26] Aufgrund einschlägiger Gründe, wie z.B. hoher Anteil an Nachtclubs, Rotlicht-Etablissements oder exzessiver Alkohol- und Drogenkonsum, geht die Polizei davon aus, dass sich dieses Muster auch in der unmittelbaren Zukunft abzeichnen wird.[27]

c) Risk-terrain-Analyse

Bei der Anwendung der Risk-terrain-Analyse wird die Datenverarbeitung in einer umfangreicheren Methode vollzogen. Es werden räumliche Risikoprofile für bestimmte Gebiete erstellt und diesen Einbruchswahrscheinlichkei-

18 *Egbert*, APuZ 32-33/2017, 17 (20).
19 *Egbert*, in: Schriftenreihe der Strafverteidigervereinigungen, Band 42, 2018, S. 241 (246).
20 *Knobloch*, Vor die Lage kommen: Predictive Policing in Deutschland, 2018, S. 16.
21 *Gluba,* Predictive Policing – eine Bestandsaufnahme, 2014, S. 3.
22 *Wolfangel*, Digitale Verbrechensvorhersage in Deutschland, Stadt Bauwelt, Heft 213, 20.3.2017, 53 (53).
23 *Ferguson*, Washington University Law Review, Vol. 94, Issue 5, 2017, 1109 (1124).
24 *Shapiro*, Predictive Policing – auf Streife mit Big Data, Stadt Bauwelt, Heft 213, 20.3.2017, 48 (49).
25 *Egbert*, in: Schriftenreihe der Strafverteidigervereinigungen, Band 42, 2018, S. 241 (245).
26 *Egbert/Krasmann,* Predictive Policing, Projektabschlussbericht, Universität Hamburg, 2019, S. 13.
27 *Egbert*, in: Schriftenreihe der Strafverteidigervereinigungen, Band 42, 2018, S. 241 (245).

ten zugeordnet.[28] Hierfür werden Daten aus der Kriminalitätshistorie mit geografischen und infrastrukturellen Daten zusammengeführt.[29] Beispielsweise werden Daten über bestehende Verkehrsanbindungen, Einwohnerstruktur, Gebäudestruktur, Nachtleben wie Bars oder Clubs und Einkommensverteilung erhoben und analysiert.[30] So ist ein Haushalt mit zwei Einkommen und ohne Kinder anfälliger für einen Wohnungseinbruch, da tagsüber voraussichtlich niemand zuhause ist. Ein aktuelles Beispiel für die Verwendung dieser Methodik ist die in Nordrhein-Westfalen etablierte Software SKALA, die Informationen unter dem Begriff „soziostrukturelle Daten" erfasst und verarbeitet.[31]

2. Personenbezogene Verfahren

Bei Verfahren, welche personenbezogene Daten verarbeiten, geht es hauptsächlich darum, potentielle TäterInnen genauso wie Opfer von Kriminalität zu bestimmen.[32] Als Basis hierfür dienen neben Vorstrafen auch sonstige polizeiliche Daten, z.B. der Wohnort oder auch das soziale Umfeld der Person, welches durch die Auswertung sozialer Medien ermittelt wird.[33] Anhand dieser Datenauswertungen sollen Wahrscheinlichkeiten errechnet werden, welche eine Aussage über das Risiko einer möglichen Beteiligung dieser Person an Straftaten, insbesondere Kapitalverbrechen treffen.[34] Diese Informationen werden anschließend an Polizeistreifen weitergegeben und auch im weiteren Sinne polizeipraktisch nutzbar gemacht.[35]

V. Aktuelles Lagebild in Deutschland

Die Entwicklung von Predictive Policing stellt sich in Deutschland überschaubar, wenn auch innovativ dar. Aktuell werden fünf verschiedene Systeme für ortsbezogene Wahrscheinlichkeitsaussagen in entsprechend fünf Bundesländern eingesetzt. In Bayern wird das an die US-amerikanische Software PredPol angelehnte Programm Precobs genutzt, wohingegen Berlin, Niedersachsen, Hessen und Nordrhein-Westfalen entweder selbst entwickelte oder weiterentwickelte Systeme nutzen.[36] Baden-Württemberg hatte nach einem Testlauf von Precobs den Einsatz im September 2019 eingestellt. Die in Deutschland eingesetzten Systeme verwenden nur ortsbezogene Daten. Eine personenbezogene Analyse erfolgt in der Bundesrepublik aktuell nicht.

Das Berliner Landeskriminalamt hat mit der Software KrimPro ein eigens entwickeltes Programm geschaffen, welches, wie Precobs, auf dem Near-repeat-Ansatz beruht. Es werden polizeiliche Falldaten untersucht, um per Kachelvisualisierung die Prognose für zukünftige Wohnungseinbruchsdiebstähle aufzuzeigen.[37] KrimPro verwendet als Datenquelle das polizeiliche Data-Warehouse, welches Daten aus mehreren Quellen (hauptsächlich aus dem polizeilichen Vorgangsbearbeitungssystem POLIKS) zusammenführt und kombiniert diese mit Daten des Amtes für Statistik Berlin-Brandenburg.[38] Die Berliner Software arbeitet mit einem Scoring-Modell: Eine hohe

28 *Egbert*, APuZ 32-33/2017, 17 (21).
29 *Hauber/Jarchow/Rabitz-Suhr*, Prädiktionspotential schwere Einbruchskriminalität, LKA Hamburg, 2019, S. 68.
30 *Egbert/Krasmann,* S. 18.
31 LKA Nordrhein-Westfalen, Abschlussbericht Projekt SKALA, 2018, S. 3.
32 *Egbert/Krasmann,* S. 20
33 *Ferguson*, Washington University Law Review, Vol. 94, Issue 5, 2017, 1109 (1137 f.); *Härtel*, LKV 2019, 49 (54).
34 *Knobloch*, S. 17.
35 *Egbert/Krasmann,* S. 20.
36 *Knobloch*, S. 13.
37 *Seidensticker/Bode/Stoffel*, in: Konstanzer Online-Publikations-System, August 2018, S. 3; *Egbert*, in: Schriftenreihe der Strafverteidigervereinigungen, S. 241 (246).
38 Senatsverwaltung für Inneres und Sport Berlin, Antwort auf die schriftliche Anfrage des Abgeordneten Bernd Schlömer (FDP), Abgeordnetenhaus Berlin, 1.2.2019, Drs. 18/17562.

Punktzahl erhalten Straftaten, die nach Einschätzung der Polizei auf professionelle Täterschaft schließen lassen, eine kleine Punktzahl gibt es für sog. „Gelegenheitstaten".[39] Dieser Score labelt dann einen ca. 400 mal 400 Meter großen Quadranten in der Stadt (bei insgesamt 5000 Quadranten in Berlin) und generiert eine Wahrscheinlichkeitsaussage für die nächsten drei Tage.[40] Im Jahr 2018 fanden an 58,1% aller Tage, an denen das Programm Wiederholungstaten vorausberechnet hatte, entsprechende Taten statt.[41]

VI. Lagebild in den USA

Besondere Popularität gewann Predictive Policing Anfang 2008 in den USA, wo es seitdem auch in der Polizeiarbeit regelmäßig eingesetzt wird. Aufgrund des zeitlichen Vorsprungs der Amerikaner sind die von ihnen angewandten Systeme nicht nur fortschrittlicher als die deutschen Programme, sondern basieren auch auf einem deutlich größeren und vielseitigeren Fundament an Daten.[42] In den USA wird nicht nur das Auftreten von Wohnungseinbruchsdiebstählen untersucht, es werden auch Aussagen über andere Tatbestände, wie zum Beispiel Gewaltdelikte getroffen.[43] Für raumbezogene Ansätze werden beispielsweise nicht nur Informationen aus Kriminalstatistiken und vorliegender Infrastruktur gesichtet, sondern auch Wetterdaten, Wohnorte von verurteilten Straftätern und mögliche Veranstaltungstermine ausgewertet.[44]

Anders als in Deutschland verwenden die USA nicht nur raumbezogene, sondern auch personenbezogene Verfahren und arbeiten mit individuell-persönlichen Daten.[45] Das am meisten Aufmerksamkeit erregende Beispiel der Verarbeitung personenbezogener Daten ist die Strategic Subject List (SSL) der Polizei in Chicago. Auch häufig von den Medien als „Heat List" bezeichnet,[46] erfasst die Polizei dort potentielle Opfer oder Verdächtige mit einem Hang zu Gewalttaten, insbesondere mit Schusswaffen.[47] Die Liste basiert auf der These, dass Personen, zu deren Bekannten- und Verwandtenkreis Opfer oder TäterInnen von Gewalttaten gehören, ein hohes Risiko besitzen, zukünftig ebenfalls in solche Taten verwickelt zu werden.[48] Wenn Personen dort registriert und eingeordnet werden, können sie nicht nur vermehrter Überwachung unterliegen, sondern erhalten sogenannte „Gefährderansprachen".[49] Die Polizei wendet sich entweder persönlich oder durch ein Schreiben an die in Frage kommende Person, wobei sie über ihr Risikoprofil informiert und aufgefordert wird, sich rechtstreu zu verhalten.[50]

In Chicago, wo es im Jahr 2016 rund 3.550 Auseinandersetzungen mit Waffen mit 762 Toten gab wird diese Liste seit ca. 7 Jahren geführt.[51] Sie begann mit einer Zahl von 400 Menschen und wurde seitdem auf knapp 400.000

39 *Heitmüller*, Predictive Policing, Heise Online (Hrsg.), 17.4.2017, abrufbar unter: https://heise.de/-3685873 (zuletzt abgerufen am 13.4.2020).
40 *Graupner*, Kommissar Glaskugel: Polizei-Software sagt jetzt Einbrüche voraus, abrufbar unter: https://www.bz-ber-lin.de/berlin/polizei-software-sagt-jetzt-einbrueche-voraus (zuletzt abgerufen am 13.4.2020).
41 Senatsverwaltung für Inneres und Sport Berlin, Antwort auf die schriftliche Anfrage des Abgeordneten Bernd Schlömer (FDP), Abgeordnetenhaus Berlin, 1.2.2019, Drs. 18/17562.
42 *Egbert,* APuZ 32-33/2017, 17 (20 f.); *Singelnstein*, NStZ 2018, 1 (2).
43 *Singelnstein*, NStZ 2018, 1 (2).
44 *Gluba,* Predictive Policing – eine Bestandsaufnahme, LKA Niedersachsen (Hrsg.), 2014, S. 11; *Rolfes,* Predictive Policing, Potsdamer Geographische Praxis, Heft 12, 2017, 51 (57 f.); *Singelnstein*, NStZ 2018, 1 (2).
45 *Egbert*, APuZ 32-33/2017, 17 (19); *Ferguson*, University of Pennsylvania Law Review, Vol. 163, 2015, S. 329 (373).
46 *Sommerer*, NK 2017, 147 (148).
47 *Ferguson*, Washington University Law Review, Vol. 94, Issue 5, 2017, 1109 (1139).
48 Vgl. *Leese*, Predictive Policing in der Schweiz, Bulletin zur schweizerischen Sicherheitspolitik, 2018, 57 (58 f.).
49 Allgemein dazu: *Jasch*, KJ 2014, 237 (239); *Härtel*, LKV 2019, 49 (54); *Singelnstein*, NStZ 2018, 1 (2).
50 *Kreuter-Kirchhof*, in: AÖR 2014, 257 (260).
51 Vgl. *Seibert*, Jeden Tag zwei Morde – Kriminalität in Chicago, Tagesspiegel Online (Hrsg.), abrufbar unter: https://www.tagesspiegel.de/gesellschaft/panorama/kriminalitaet-in-chicago-jeden-tag-zwei-morde/19203726.html (zuletzt abgerufen am 13.4.2020).

ausgeweitet, die als besonders gefährlich eingestuft werden.[52] Eine Skala von 0 bis 500 Punkten soll die Risikohöhe der einzelnen Personen markieren.[53] Darunter waren mehr als die Hälfte afro-amerikanische junge Männer.[54]

VII. Rechtliche Einordnung, Risiken und Wirksamkeit

1. Zwischen Strafrecht und Polizeirecht

Nun stellt sich die Frage in welches Rechtsgebiet Predictive Policing einzuordnen ist und was für rechtliche Folgen und Problematiken dabei entstehen können. Grundsätzlich befindet man sich beim Predictive Policing zwischen den Bereichen des Straf- und Polizeirechts.[55] Für das Polizeirecht stellt ein frühes Eingreifen keine Abnormität dar, zumal das unmittelbare Bevorstehen einer Straftat, also ein Gefahrverdacht auch unter den Gefahrentatbestand und mithin die Generalklausel fällt (vgl. in Berlin: § 1 Abs. 3 ASOG).[56] Doch auch dem Strafrecht ist der Gedanke der Prävention keinesfalls fremd. Ausflüsse einer vorverlagerten Anknüpfung der Strafverfolgung lassen sich nicht nur in Gefährdungsdelikten wie dem § 315c StGB, sondern auch in der Reformierung des 100d StPO, der Einführung des § 100a Abs. 1 S. 2 StPO und den bekannten Normen zu den Maßnahmen der Besserung und Sicherung erkennen. Diese können jedoch kaum derartige Eingriffsmöglichkeiten generieren, wie Predictive Policing es schafft.

2. Eingriffsmaßnahmen und ihre Grenzen

Welche Eingriffe dürfen nun aufgrund dieser Wahrscheinlichkeitsaussagen erfolgen? Was kann in Deutschland zulässig sein, wenn sich PolizeibeamtInnen in einem sog. „Hot-Spot-Gebiet" aufhalten? Das polizeiliche Streifen und Abfahren dieser Gebiete bleibt ohne weiteres möglich.[57] Andererseits unterliegen jedoch alle Maßnahmen, welche einen Grundrechtseingriff zur Folge haben, dem Gesetzesvorbehalt. Sie müssen bestimmte Gefahren- oder Verdachtsstufen voraussetzen.[58] Dies gilt auch für Interventionen, wie beispielsweise das Durchsuchen von Personen oder den Platzverweis.

Aber wo wird dann der Unterschied zwischen informatorischer Kontaktaufnahme und einem Eingriff in die Freiheitsrechte des Betroffenen durch die von der Software alarmierte Polizei gezogen?[59] Denn Eingriffe müssen an einer gewissen Schwelle gemessen werden, welche im Polizeirecht die Gefahr und im Strafverfahrensrecht grundsätzlich der Tatverdacht darstellt.[60] Unter dem Gefahrenbegriff im Polizeirecht versteht man eine Sachlage, in welcher bei ungestörtem Ablauf des zu erwartenden Geschehens in absehbarer Zeit mit hinreichender Wahrscheinlichkeit eine Rechtsgutsverletzung an einem Schutzgut eintreten wird.[61] Ein gesteigertes Risiko für das Begehen einer Straftat kann in bestimmten Fällen den auf eine hinreichende Wahrscheinlichkeit abstellenden Gefahrentatbestand erfüllen. Die Bestimmung dieser Wahrscheinlichkeit beruht vorliegend ausschließlich auf einer Aussage

52 *Ferguson*, The Police Are Using Computer Algorithms to Tell If You're a Threat, Time Magazine, 3. Oktober 2017, abrufbar unter: https://time.com/4966125/police-departments-algorithms-chicago/ (zuletzt abgerufen am 13.4.2020).
53 *Egbert/Krasmann,* S. 20.
54 *Tucek*, University of Chicago Legal Forum, Vol. 2018, Article 18, 2019, S. 427 (434).
55 *Singelnstein*, NStZ 2018, 1 (5).
56 *Schenke*, JuS 2018, 505 (508 f.); *Singelnstein*, NStZ 2018, 1 (5).
57 *Singelnstein*, NStZ 2018, 1 (7).
58 Vgl. *Härtel*, LKV 2019, 49 (56).
59 *Jasch*, KJ 2014, 237 (240).
60 *Singelnstein*, NStZ 2018, 1 (7).
61 *Poscher/Rusteberg*, JuS 2011, 984 (986 f.).

des Predictive Policing Systems. Nicht nur Nachweisprobleme der Wirksamkeit dieser Prognosen, sondern auch das stets zu wahrende Verhältnismäßigkeitsprinzip lassen an dieser Vorgehensweise Zweifel aufkommen. Das Prinzip der Verhältnismäßigkeit verlangt, dass mit jedem Grundrechtseingriff durch den Staat ein legitimes Ziel mit geeigneten, erforderlichen und angemessenen Mitteln verfolgt wird.[62] Aber ab welchem Zeitpunkt wird ein Eingriff in ein Freiheitsrecht durch eine polizeiliche Maßnahme angemessen sein, wenn diese lediglich auf die Wahrscheinlichkeit der Begehung einer Straftat gestützt wird, deren einzige Grundlage ein Datenverarbeitungsvorgang ist?

Im Polizeirecht wird an dieser Stelle besonders klar, dass für die Frage der Qualität der Maßnahmen neue Regelungen notwendig geworden sind.[63] Im Strafverfahrensrecht ist ein hinreichender Tatverdacht gegeben, wenn tatsächliche Anhaltspunkte vorliegen, die einen konkreten Verdacht der Begehung einer Straftat durch die betroffene Person begründen.[64] Bei der Anwendung von Predictive Policing fehlt jedoch gerade ein konkretes Geschehen in der Vergangenheit. Dieses wird ersetzt durch eine Wahrscheinlichkeitsaussage, ein erhöhtes Risiko. Das deutsche Strafrecht als Schuldstrafrecht[65] steht dem entgegen. Die individuelle Vorwerfbarkeit der Tat ist stets das wichtigste Kriterium. Dafür muss an eine bereits begangene Tat oder Handlung angeknüpft werden. Es ist der Kernbereich des Strafrechts sich mit der Vergangenheit zu befassen und zurückliegende Ereignisse zu bewerten. Genau diese Chronologie wird durch Predictive Policing unterbrochen. Anstatt an einen bereits erfolgten Normverstoß anzusetzen, wird hier das Risiko zum zentralen Anknüpfungspunkt erhoben.[66] Anstelle des Reagierens tritt ein vorzeitiges Agieren. Diese Vorverlagerung der staatlichen Eingriffsmöglichkeiten könnte dazu führen, dass eine Intervention erfolgt, noch bevor der Betroffene selbst weiß, dass er eine Straftat begehen wird.[67] Die damit provozierte Verschmelzung des Strafrechts mit dem Polizeirecht zu einem schwer zu begrenzenden „Sicherheitsrecht" scheint dabei fast unausweichlich.[68]

3. Risiken und Nebenwirkungen

Auf dem Techfest des indischen Instituts für Technik in Mumbai erklärte der ehemalige internationale Generalsekretär von Amnesty International, *Salil Shetty*, dass er durch Predictive Policing die Unschuldsvermutung aus Art. 6 Abs. 2 EMRK, Art. 20 Abs. 3 i.V.m. Art. 28 Abs. 1 S. 1 GG bedroht sehe. Er wies darauf hin, dass eine etwaige Diskriminierung von religiösen und ethnischen Minderheiten durch Predictive Policing intensiviert werden könnte.[69] In den USA konnte dies gegenüber afro-amerikanischen und lateinamerikanischen Personen im Rahmen von Bewährungsentscheidungen nachgewiesen werden, wo Richter eine bestimmte Software benutzten um das Rückfallrisiko einzuschätzen.[70] Bei den in Deutschland verwendeten raumbezogenen Verfahren erhalten die PolizeibeamtenInnen bei ihrem Einsatz nur Informationen über die Lage und Größe des Risikogebiets. Hier müssen die BeamtInnen nun auf persönliche Einschätzungen zurückgreifen um „verdächtige" Personen oder Umstände

62 *Härtel*, LKV 2019, 49 (55).
63 *Singelnstein*, NStZ 2018, 1 (5).
64 *Gaede*, in: MüKo-StPO, 2018, Art. 5 EMRK Rn. 43.
65 *Kinzig,* in: Schönke/Schröder, StGB, 30. Aufl. (2019), § 46 Rn. 4.
66 *Singelnstein*, NStZ 2018, 1 (3).
67 *Derin*, Strafrechtliche Vorverlagerung: Der Wandel zum Präventionsstrafrecht, Bürgerrechte und Polizei, Cilip 117, November 2018.
68 *Jasch*, KJ 2014, 237 (239).
69 *Shetty*, Technology: force for progress, or tool of repression?, Techfest in IIT Bombay, 16.12.2016, abrufbar unter: https://www.amnesty.org/en/latest/news/2016/12/salil-shetty-speech-techfest/ (zuletzt abgerufen am 13.4.2020).
70 *Angwin/Larson*, Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say, ProPublica, 30.12.2016, abrufbar unter: https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say (zuletzt abgerufen am 13.4.2020); *Knobloch*, S. 12.

zu identifizieren. Dabei kann oft der Rückgriff auf stigmatisierende Indikatoren wie fremdländisches Aussehen oder der Verfall in die Anwendung einer Art „Typisierung" erfolgen.[71] Es entsteht das Problem, dass nicht nur potentielle Straftäter in das Visier geraten, sondern Personen, welche keine Gefahr darstellen.[72] Aufgrund fälschlicher Analysen könnten Grundrechtseingriffe gegen unschuldige Personen gerichtet werden. In diesem Zusammenhang stellt sich auch die Frage der Verantwortlichkeit, insbesondere der Zurechenbarkeit für sich als unrichtig herausstellenden Prognosen und darauf basierten polizeilichen Eingriffen.[73] Weiterhin kann eine erhöhte Polizeipräsenz in diesen Gebieten eine bereits bestehende Stigmatisierung verstärken und möglicherweise erreichte Fortschritte in Hinsicht auf Diskriminierung zunichte machen.[74]

4. Wirksamkeit von Predictive Policing

Das wichtigste Kriterium für die Wirksamkeit von Predictive Policing ist die Qualität der erhobenen Daten, wovon die Leistungsfähigkeit des Systems entscheidend abhängt.[75] Insbesondere Aktualität, Vollständigkeit, Korrektheit, Genauigkeit und Verlässlichkeit der Informationen stützen die Treffsicherheit der entstehenden Wahrscheinlichkeitsaussagen. Etwaige Fehlinterpretationen können dabei Aussagen über ganze Risikogebiete verfälschen. Und Fehler schleichen sich auch bei datenbasierten Analysen durch Algorithmen ein. Die Auffassung, dass computergestützte Systeme neutrale Wahrscheinlichkeitsaussagen generieren, verkennt wie viel menschlicher Einfluss in diesen Systemen steckt.[76] Letztendlich sind Algorithmen nur so objektiv, wie die Programmierer, die sie geschaffen haben, bzw. die Daten, mit denen sie gefüttert werden.[77] Obwohl die Systeme Objektivität symbolisieren, heißt es nicht, dass sie mit der technischen Exaktheit Aussagen agieren, die sie zu versprechen scheinen.[78]

Eine Quelle der Unsicherheit kann auch die mögliche falsche rechtliche Einordnung von Straftaten oder eine zu späte Anzeige des Opfers, gerade bei Einbruchsdiebstahlen sein, welche die aufgenommenen Daten ungenau oder gar falsch machen können.[79] Es entsteht eine Art Dominoeffekt, der sich von den falsch erhobenen Daten bis zu der daraus ungenau generierten Wahrscheinlichkeitsaussage zieht. Dies wirkt sich nicht nur auf die Aussagen selbst aus, sondern auch auf die Wahrnehmung der Polizei, welche aufgrund dieser in spezifischen Gebieten mit bestimmten Erwartungen tätig wird. Außerdem bilden Kriminaldaten selten das reale Lagebild ab und spiegeln häufig eher das polizeiliche Registrierverhalten oder lediglich einen Ausschnitt der Gesamtsituation wider.[80] Da auch die polizeiliche Tätigkeit nicht durchgängig neutral ausgeübt werden kann, kommt es zu einer Verzerrung, welche einen Rückschluss auf die Effektivität der Systeme kaum zulässt.[81]

Ferner gilt zu berücksichtigen, dass in einem vermehrt von der Polizei aufgesuchten Gebiet automatisch auch mehr Straftaten dokumentiert werden, was wie ein Verstärker für bestimmte Wohnorte bei den Zukunftsprognosen wirkt

71 *Egbert/Krasmann,* S. 55.
72 Vgl. *Ferguson*, Washington University Law Review 2017, 1109 (1160).
73 Vgl. *Quinn*, in: Marks/Steffen: Prävention und Freiheit – Zur Notwendigkeit eines Ethik-Diskurses, S. 57 (169).
74 Vgl. *Knobloch*, S. 12.
75 *Singelnstein*, NStZ 2018, 1 (3).
76 *Egbert*, in: Schriftenreihe der Strafverteidigervereinigungen, S. 241 (259).
77 *Singelnstein*, NStZ 2018, 1 (4); *Härtel*, LKV 2019, 49 (55).
78 *Rolfes,* in: Potsdamer Geographische Praxis, Heft 12, 2017, S. 51 (67).
79 *Ferguson*, Washington University Law Review 2017, 1109 (1146).
80 *Leese*, Predictive Policing in der Schweiz, Bulletin zur schweizerischen Sicherheitspolitik, 2018, S. 57 (68); *Egbert*, in: Schriftenreihe der Strafverteidigervereinigungen, S. 241 (259).
81 *Egbert*, in: Schriftenreihe der Strafverteidigervereinigungen, S. 241 (259).

(sog. feedback loop[82]).[83] Durch den Einsatz der Software werden somit die Fallzahlen verändert und bestimmte Gebiete anvisiert, wobei die Gefahr der Entwicklung einer selbst erfüllenden Prophezeiung entsteht.[84]

Die Einschätzung der Wirksamkeit von Predictive Policing ist vor allem durch ihre Nachweisproblematik erschwert. Die Messung der Effektivität ist ein kaum lösbares Problem: trifft die Aussage der Software nicht zu, also geschieht in dem prognostizierten Zeitraum und Gebiet kein Einbruch, bleibt offen, ob die Software falsch lag oder die Polizei aufgrund dieser Aussage die Tat wirksam verhindern konnte (z. B. durch Abschreckung).[85] Auch wenn ein Rückgang der Fallzahlen zu verzeichnen ist, sagt dies nichts über die Kausalität des angewandten Predictive Policing Systems aus. Zunächst verkennt die im Rahmen der Analysen praktizierte Betrachtung von Kriminalität als ein eindimensionales Ereignis, welches durch simple Theorien erklärt werden könne, dass Kriminalität als ein multifaktorielles Vorkommen viele Ursachen haben kann.[86] Zum anderen ist die Prognose Teil eines umfassenden Bekämpfungskonzepts der Polizei, welches auch durch vorhersageunabhängiges polizeiliches Verhalten gesteuert und angetrieben wird.[87] In diesem Rahmen ist eine Beeinflussung der Analysen durch mögliche Verdrängungs- oder Ausnutzungseffekte nicht auszuschließen. Es besteht die Gefahr, dass bestimmte Täter die Algorithmen für ihren Vorteil nutzen und sich mithin auf die Strategie der Polizei einstellen.[88] Wenn jemand sich bewusst ist, dass ein Einbruch mehr Polizeipräsenz zur Folge hat, wird sich dieser potentielle Straftäter natürlich nicht an diesem Ort aufhalten oder dort eine Tat verüben.[89] Dies könnte weniger zu einer Bekämpfung oder Eindämmung, als zu einer Verlagerung der Kriminalität in die der Polizei weniger bekannten Risikogebiete führen. Es könnte somit zu einer Art Symptombehandlung kommen, die nur kurzweilige und oberflächliche Erfolge verzeichnen lässt.[90]

VIII. Entwicklungen und Perspektiven

Wie sich die vorhersagebasierte Polizeiarbeit weiter ausformen wird, bleibt unsicher. Da die Qualität der Daten so wichtig ist, kann dies zu einer Steigerung des Umfangs der Datengewinnung führen. Am Beispiel der USA ist zu erkennen welche Masse an Daten ohne die uns bekannten grundrechtlichen Grenzen erhoben werden können. Die Gefahr der Verselbstständigung des Prozesses ist dabei nicht zu unterschätzen.[91] Es verbleibt die ungeklärte Frage was ein Bürger preisgeben muss, damit der Staat seine Sicherheit gewährleistet.[92] In Deutschland werden jedoch der Verarbeitung personenbezogener Daten im Rahmen von Predictive Policing Grenzen gesetzt. Regelmäßig ist bei solchen Erhebungen das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG tangiert. Das *BVerfG* stellte deshalb fest, dass der Einsatz solcher Systeme grundsätzlich nur bei einem objektiv bestimmten und begrenzten Anlass zulässig sei.[93] Ein anlassloser Einsatz sei hingegen nur möglich, soweit damit auf ein gefährliches oder risikobehaftetes Tun reagiert werde.[94] Dieses Risiko kann sich auch aus einer

82 Vgl. *Ensign/Friedler/Neville/Scheidegger/Venkatasubramanian*, Runaway Feedback Loops in Predictive Policing, Proceedings of Machine Learning Research 81, 2018, S. 1 f.
83 *Lum/Isaac*, To predict and serve?, Significance, Vol. 13, Issue 5, Oktober 2016, S. 14, (15); *Egbert,* APuZ 32-33/2017, 17 (22).
84 *Ferguson*, Washington University Law Review 2017, 1109 (1149).
85 *Egbert,* APuZ 32-33/2017, 17, (22).
86 Vgl. *Singelnstein*, NStZ 2018, 1 (4).
87 Vgl. *Bode/Stoffel/Keim*, in: Konstanzer Online-Publikations-System, April 2017, S. 8.
88 *Rolfes,* in: Potsdamer Geographische Praxis, Heft 12, 2017, S. 51 (61).
89 *Singelnstein*, NStZ 2018, 1 (4).
90 *Rolfes,* in: Potsdamer Geographische Praxis, Heft 12, 2017, S. 51 (61).
91 *Leese*, Predictive Policing in der Schweiz, S. 57 (71).
92 *Di Fabio*, NJW 2008, 421 (421).
93 *BVerfG*, Beschl. v. 18.12.2018 – 1 BvR 142/15, Rn. 91.
94 A.a.O., Rn. 94.

territorialen Konstellation ergeben, insb. Grenznähe gestattet hier Ausnahmen.[95]

Aber könnte trotzdem bald eine personenbezogene Analyse in Deutschland wie in den USA erfolgen? Ein Beispiel für ein Projekt in den Kinderschuhen ist das vom BKA Anfang 2017 entwickelte Prognosesystem RADAR-iTE (regelbasierte Analyse potenziell destruktiver Täter zur Einschätzung akuten Risikos – islamistischer Terrorismus). Damit soll das Risiko der Begehung einer Gewalttat durch polizeilich bekannten islamistischen Gefährder bewertet werden.[96] Ähnlich wie in den USA wird hier mithilfe eines Programms ein Risikoprofil für potentielle Täter erstellt. Für die Analyse werden dabei laut Aussage des BKA Daten, „die ihnen bereits vorliegen oder die sie aufgrund der gültigen Rechtslage erheben dürfen", verwendet.[97] Das vom BKA entwickelte System lässt sich jedoch nicht mit den bereits laufenden Predictive Policing Programmen vergleichen. Wie ein Fragenkatalog strukturiert, leitet RADAR-iTE den Sachbearbeiter an und agiert auf Basis eines Punktesystems, was auch analog erfolgen könnte.[98] Als Beispiel für vorhersagebasierte Polizeiarbeit im personenbezogenen Verfahren eignet sich RADAR-iTE daher weniger.

IX. Fazit

Predictive Policing bleibt ein durchwachsenes Phänomen mit vielen Unklarheiten, aber auch fortschrittlichen Ansätzen. Das Bemühen Kriminalität einzudämmen ist ein wichtiges Staatsziel, welches jedoch nicht um jeden Preis erreicht werden darf. Wie jedes innovative Projekt muss es sich in die bestehende Struktur eingliedern können und den Grenzen unseres Strafverfahrensrechts und denen der Verfassung fügen. Auch wenn vorhersagebasierte Polizeiarbeit ein recht junges Phänomen ist, zeigt es doch einige Mängel auf. Fehlende Wirkungsnachweise und offene Fragen über Zurechnungsproblematiken decken dabei nur einen Teil der Unsicherheiten ab. Für die Zukunft wird die größte Herausforderung die Etablierung einer Balance zwischen öffentlicher Sicherheit und den Grundrechten des Einzelnen sein. Dafür wird der Gesetzgeber ein aktuelles und den fortschreitenden Eingriffsmöglichkeiten entsprechendes Strafverfahrensrecht und Polizeirecht erarbeiten müssen, welches den Betroffenen entsprechend schützt. Gerade auf die Einhaltung der bewusst gesetzten Grenze zum Tatverdacht und den sich ergebenen Beschuldigtenrechten sollte besonders geachtet werden. Bei der Verwendung von Predictive Policing Systemen muss man sich bewusst sein, dass Daten nicht immer die Realität wiederspiegeln und eine selbsterfüllende Prophezeiung keine reale Prognose ist, auch wenn sie dieser verlockend ähnlich sieht.

95 A.a.O., Rn. 117 ff., 123 ff., 139 ff.
96 BKA, Presseinformation: Neues Instrument zur Risikobewertung von potentiellen Gewaltstraftätern, 2.2.2017, abrufbar unter: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/170202_Radar.html (zuletzt abgerufen am 13.4.2020).
97 A.a.O.
98 *Wischmeyer*, Predictive Policing – Nebenfolgen der Automatisierung von Prognosen in Sicherheitsrecht, abrufbar unter: http://www.jura.unibielefeld.de/lehrstuehle/wischmeyer/dokumente/Wischmeyer_PredictivePolicing_20190513.pdf (zuletzt abgerufen am 13.4.2020), S. 5.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Tinam Lorenso

Nutzung von Big Data und Algorithmus-basierter Datenanalyse in der Beweisführung zum Nachweis des Vorsatzes

Inhaltsverzeichnis

I. Vorsatz: Ein nie abschließend festzustellendes Tatbestandsmerkmal

Das Strafverfahren besteht aus einer ewig langen Aneinanderreihung von entscheidungserheblichen Fragen, die vom Gericht beantwortet werden müssen. Dies trägt zur ständigen Überlastung des deutschen Justizsystems bei.[1] Insbesondere der Vorsatz führt immer wieder zu heftigen Diskussionen, da er sich als interne psychisch-kognitive Gegebenheit einer unmittelbaren Wahrnehmung als Faktum in der Außenwelt entzieht.

Grundsätzlich handelt es sich bei dem strafprozessualen Beweis der subjektiven Tatseite daher – wenn auch unterschiedlich ausgeprägt – immer um einen Indizienbeweis, d.h. auf die Tatsachen, welche für die Urteilsfällung relevant sind, kann nur mittelbar durch Beweisanzeichen (Indizien) geschlossen werden.[2] Die diesbezügliche Problematik bei der Feststellung des Vorsatzes ist spätestens durch den Fall der Ku'damm-Raser im Jahr 2017[3] auch in die Laienspähre übergeschwappt. Die Abgrenzung zwischen Vorsatz und Fahrlässigkeit ist jedoch auch zwischen Juristinnen[4] eine der meist diskutierten und brisantesten Problemstellungen im Strafrecht. Nicht zuletzt ist hieran auch die Inkonsistenz der Gerichte bezüglich der Bewertung des Vorsatzes schuld.

Definiert wird der Vorsatz als Wissen und Wollen der Tatbestandverwirklichung.[5] Allerdings ist weder das kognitive („Wissen"), noch das voluntative („Wollen") Merkmal des Vorsatzes abschließend und mit voller Sicherheit ermittelbar. Denn im Gegensatz zu den objektiven Tatbestandsmerkmalen ist dieses subjektive Tatbestandsmerkmal nur für die Angeklagte abschließend festzustellen, da die psychischen Gedankenabläufe der Angeklagten während der Tat nicht nachvollzogen werden können. Anhand verschiedener Indizien ist festzustellen, dass die Täterin den Tod des Opfers zumindest billigend in Kauf genommen hat.[6] Wenn ihr dies nicht gelingt, greift der Grundsatz „in dubio pro reo"[7], sodass – soweit die Tat auch bei Fahrlässigkeit bestraft wird – ein erheblich geringerer Strafrahmen zur Verfügung steht (z.B. bei einer fahrlässigen Körperverletzung bis zu drei Jahre (§ 223 StGB) im Vergleich zu bis zu fünf Jahre Haftstrafe bei einer vorsätzlichen Körperverletzung (§ 229 StGB). Die Richterin muss zur Feststellung des Vorsatzes auf ihre Erfahrungssätze zurückgreifen, sodass die Bewertung und Würdigung verschiedener Beweise und Indizien auf subjektiver Basis erfolgt.

Ebenso wie eine Richterin, können Algorithmen Prognosen bzw. Vermutungen aus Erfahrungssätzen erstellen. Hierdurch kann ermöglicht werden, dass in die Entscheidung des Gerichts nicht lediglich die Erfahrungswerte einer Richterin einfließen, sondern die aller Richterinnen. Dies wäre aufgrund der riesigen Datenmengen auf manuelle Weise kaum zu bewältigen. Hierdurch könnten inkonsistenten Bewertungen des Vorsatzes minimiert werden. Wie verschiedene Beweise und Indizien, die für bzw. gegen den Vorsatz sprechen, durch einen Algorithmus verwertet werden könnten und wie diese zu gewichten sind, wird im nächsten Schritt erörtert.

---

1 Justiz in Not – So überlastet sind deutsche Gerichte, MDR 30.04.2019, abrufbar unter: https://www.mdr.de/nachrichten/politik/gesellschaft/justiz- richter-mangel-und-verfahrenseinstellungen-100.html (zuletzt abgerufen am 04.10.2019)

2 *Velten*, in: SK-StPO, 5. Aufl. (2014), Vor § 261 Rn. 4.

3 *LG Berlin*, NStZ 2017, 471 (nicht rechtskräftig).

4 Aus Gründen der Einfachheit wird im Rahmen dieser Arbeit nur die weibliche Form verwendet, soweit nicht über eine bestimmte Person gesprochen wird. Gemeint sind hiermit allerdings alle Geschlechter.

5 *Hoffmann-Holland*, Strafrecht AT, 3. Aufl. (2015), Rn. 152; *Sternberg-Lieben/Schuster*, in: Schönke/Schröder, StGB, 30. Aufl. (2018), § 15 Rn. 9.

6 *Puppe*, in: NK-StGB, 5. Aufl. (2017), § 15 Rn. 31; *BGH*, NStZ 2007, 704 Rn. 9.

7 *Heintschel-Heinegg*, in: BeckOK-StGB, 43. Edition (2019), § 1 Rn. 39.

II. Indizien für den Vorsatz und ihre Geeignetheit für einen Algorithmus

Die Abgrenzung zwischen bedingtem Vorsatz und bewusster Fahrlässigkeit stellt sich aus den vorgenannten Gründen oft als große Herausforderung für die Gerichte dar. Insbesondere in Grenzfällen wie bei dem Berliner-Raser-Fall[8] oder dem Göttinger Transplantationsfall[9] kann der Vorsatz nur anhand einer Gesamtbetrachtung aller objektiven und subjektiven Umstände des Einzelfalls erfolgen.[10] Die Aspekte, die bei einer solchen Prüfung besonders zu beachten sind, werden im Folgenden erörtert und auf deren Geeignetheit für einen Algorithmus geprüft. Aufgrund der Aktualität beziehen sich die folgenden Ausführungen auf den Tötungsvorsatz.

1. Die objektive Gefährlichkeit der Tat

Ein besonders entscheidender Indikator für einen Tötungsvorsatz ist nach der Rechtsprechung die objektive Gefährlichkeit der Tat.[11] Wann genau eine solche besteht, lässt sich nicht generell-abstrakt feststellen, sodass sie anhand von Fallbeispielen zu bestimmen ist. Während die Abgabe von Schüssen regelmäßig auf eine Tötungsvorsatz schließen lässt,[12] ist bei Messerangriffen zwischen Stichen und Schnitten abzugrenzen.[13] Denn neben der mit dem Messer angegriffenen Stelle[14] ist auch entscheidend, wie tief das Messer in das Opfer eingedrungen ist. Dementsprechend ist sogar bei Angriffen in hochsensible Körperpartien die objektive Gefährlichkeit nicht ohne Weiteres anzunehmen, wenn es sich lediglich um Schnittverletzungen handelt.[15] Grds. ist allerdings nicht nur die Möglichkeit eines tödlichen Ausgangs ausreichend, um eine objektive Gefährlichkeit der Handlung anzunehmen, die auf einen Tötungsvorsatz schließen lässt. So sind Schläge auf den Rumpf eines Menschen zwar gefährlich, allerdings „führen [sie] grundsätzlich nicht ohne Weiteres zu Verletzungen, die wegen ihrer Gefährlichkeit mit hoher oder gar sehr hoher Wahrscheinlichkeit zum Tode führen."[16] Auch im Fall der Ku'damm-Raser stützte das *LG Berlin* den Vorsatz der beiden Angeklagten insb. auf die Gefährlichkeit der Tat, die durch die hohen Geschwindigkeiten in Verbindung mit dem hohen Verkehrsaufkommen am Berliner Kurfürstendamm erkennbar ist.[17] Sie hätten aufgrund der hohen objektiven Gefährlichkeit ihres Handelns nicht auf einen positiven Ausgang hoffen können,[18] da die Gefährlichkeit kaum noch zu toppen sei.[19]

2. Gegenindikatoren

Auch wenn die Rechtsprechung die besondere objektive Gefährlichkeit einer Handlung als eine ausschlaggebenden Faktor für die Feststellung des Vorsatzes sieht, sei „jedoch immer auch in Betracht zu ziehen, dass [die Täterin] die Gefahr der Tötung nicht [erkannt] oder jedenfalls darauf vertraut haben könnte, ein solcher Erfolg werde nicht

8 *LG Berlin*, NStZ 2017, 471 (nicht rechtskräftig).
9 *BGH*, NStZ 2017, 701 (Der Vorsatz wurde verneint, da der Arzt „begründet darauf vertraut", dass die „überholten" Patientinnen zu einem späteren Zeitpunkt das benötigte Organ transplantiert bekommen können.)
10 *BGH*, NStZ 2017, 701 (705); *BGH*, NStZ 2015, 216.
11 *BGH*, NStZ-RR 2015, 172; *Heinke*, NStZ 2010, 119 (123); *BGH*, NStZ 2015, 516; *BGH*, NStZ 2011, 210 (211).
12 *BGH*, NStZ-RR 1996, 323; *BGH*, Beck RS 1996 30390888.
13 *Schneider*, in: MüKo-StGB, 3. Aufl. (2017), § 212 Rn. 28.
14 *Schneider*, in: MüKo-StGB, § 212 Rn. 28.
15 *Schneider*, in: MüKo-StGB, § 212 Rn. 28.
16 *BGH*, NStZ 2009, 91.
17 *Lorenz/Sehl*, Und es war doch Mord, LTO 26.3.2019, abrufbar unter: https://www.lto.de/recht/hintergruende/h/lg-berlin-532-ks- 918-ku-damm-raser-zweites-urteil-mord-bedingter-vorsatz- kein-dolus-subsequens-mordmerkmale/ (zuletzt abgerufen am 29.9.2019).
18 Pressemitteilung v. 26.3.2019, Landgericht Berlin verurteilt Angeklagte nach tödlichem Zusammenstoß bei illegalem Autorennen auf dem Kurfürstendamm erneut wegen Mordes (PM 18/2019), abrufbar unter: https://www.berlin.de/gerichte/presse/pressemitteilungen- der-ordentlichen- gerichtsbarkeit/2019/pressemitteilung.796501.php. (zuletzt abgerufen am 29.9.2019).
19 *Lorenz/Sehl*, Und es war doch Mord, LTO 26.3.2019, abrufbar unter: https://www.lto.de/recht/hintergruende/h/lg-berlin-532-ks- 918-ku-damm-raser-zweites-urteil-mord-bedingter-vorsatz- kein-dolus-subsequens-mordmerkmale/ (zuletzt abgerufen am 29.9.2019).

eintreten."[20] Dementsprechend sind auch bei Feststellung der objektiven Aspekte der Handlung die „sorgfältige Prüfung des bedingten Vorsatzes nicht entbehrlich",[21] sodass festgestellt werden muss, ob Umstände vorliegen, die gegen den Vorsatz sprechen.[22] Solche Umstände können sowohl auf kognitiver als auch auf voluntativer Seite des Vorsatzes bestehen.[23]

a) Das kognitive Vorsatzelement

Bei Betrachtung der kognitiven Vorsatzelemente kann das Fehlen der Fähigkeit, die Gefährlichkeit des Handelns zu erkennen, da die Wahrnehmungsfähigkeit durch den Einfluss von Alkohol, anderen Rauschmitteln, oder durch eine affektiv belastete Situation[24] eingeschränkt war, zum Ausschluss des Vorsatzes führen. Allerdings kann diese Bewertung ausgeschlossen sein, „wenn der vorgestellte Ablauf des Geschehens einem tödlichen Ausgang so nahe ist, dass nur noch ein glücklicher Zufall diesen verhindern kann".[25] In solchen Fällen bestehen daher keine besonderen Anforderungen an die Darlegung der inneren Tatseite.[26]

b) Das voluntative Vorsatzelement

Ähnlich verhält es sich bei den voluntativen Aspekten der objektiven Gefährlichkeit. Soweit keine Indikatoren bestehen, die auf das Gegenteil hinweisen, kann bei besonderer Gefährlichkeit einer Handlung auf die Billigung des tödlichen Ausgangs geschlossen werden.[27] Der Tötungsvorsatz kann zwar entfallen, wenn die Täterin nicht nur vage darauf vertraut, dass die Todesfolge ausbleibt; allerdings reicht hierfür ein bloßes Hoffen auf einen nichttödlichen Ausgang nicht aus, da es tatsachenfundiert sein muss.[28] In Betracht kommen hier einige Indikatoren, welche im Folgenden erörtert werden.

aa) Spontanität der Tat

Ein oft gegen das Bestehen des voluntativen Vorsatzelements sprechendes Indiz ist die Spontanität einer Tat. So ist laut Rechtsprechung „insbesondere bei spontanen, unüberlegten, in affektiver Erregung ausgeführten Handlungen" auch bei bestehendem kognitiven Element der Vorsatz nicht ohne weiteres zu bejahen.[29] Dies wird vor allem in solchen Fällen angenommen, in denen die Täterin aus Wut oder Verärgerung gehandelt hat und bspw. durch Beleidigungen provoziert wurde.[30] Indizien für eine affektive Erregung können „zeitlich eng begrenzte totale Erinnerungslücke[n] oder inselhaft erhalten gebliebene Erinnerungsreste" sein.[31] Allerdings ist oft schwer feststellbar, ob die Erinnerungen tatsächlich fehlen, oder ob diese Aussage lediglich zum Selbstschutz angeführt wird,[32] sodass hier in jedem Fall die gutachterliche Betrachtung durch eine Sachverständige notwendig ist.

20 *BGH*, NStZ 2009, 91.
21 A.a.O.
22 *BGH*, NStZ 2011, 210 (211).
23 *Neumann/Saliger*, in: NK-StGB, § 212 Rn. 12 f.
24 *BGH*, NStZ-RR 2016, 204.
25 *BGH*, NStZ 2007, 150 (151).
26 *BGH*, NStZ 2004, 330.
27 *Neumann/Saliger*, in: NK-StGB, § 212 Rn. 13.
28 *BGH*, NStZ 2019, 208 Tz. 7; *Schneider*, in: MüKo-StGB, § 212 Rn. 70.
29 *BGH*, NStZ-RR 2011, 73; *BGH,* NStZ 2009, 91; *BGH*, NStZ 2003, 603.
30 *BGH*, NStZ 2011, 338 (339).
31 *BGH*, NStZ-RR 2003, 8.
32 *BGH*, NStZ-RR 2003, 8 (9).

bb) Vermeideverhalten oder Rettungswille

In Betracht kommt ein sogenanntes „Vermeideverhalten" der Täterin oder auf die Rettung des Opfers fokussiertes Nachtatverhalten[33]. Ein solches liegt vor, wenn die Täterin Vorkehrungen trifft, um die Wahrscheinlichkeit des Todeseintritts möglichst gering zu halten. Allerdings bleibt zu beachten, ob die Täterin die Handlung nur vornimmt, um die Folgen der Tat für sie selbst zu verringern oder ob es tatsächlich auf das Überleben des Opfers gerichtet ist.[34]

cc) Positive Beziehung/Einstellung zum Opfer

Auch die zwischen Täterin und Opfer bestehende Beziehung kann einen Einfluss auf die Bewertung des Vorsatzes haben. Einem Mann, der seine Partnerin über mehrere Tage hinweg misshandelt, woraufhin sie an inneren und äußeren Blutungen sowie einem hämorrhagischen Schock stirbt, ist nach der Bewertung des *BGH* anzurechnen, dass er sie liebte und mit Medikamenten und Nahrung versorgt hat.[35] Hier wird argumentiert, dass der Täter kein Anliegen an dem Tod seiner Partnerin gehabt habe. Weniger kritisch zu betrachten ist die Behandlung von Beziehungen in einem Fall, in welchen eine Täterin ihr Kind stark schüttelte, da sie es dazu bringen wollte, aufzuhören zu schreien. Laut *BGH* ist die Hemmschwelle für die Tötung des eigenen Kindes am höchsten, sodass hier nicht aufgrund der äußerst hohen objektiven Gefährlichkeit des Schüttelns eines Kindes auf Vorsatz geschlossen werden darf.[36]

3. Verarbeitung durch einen Algorithmus

a) Rationalisierbarkeit für regelbasierten Algorithmus

Fraglich ist, inwiefern dieser Vorsatzindikator durch einen Algorithmus erkannt und verarbeitet werden kann. Unterschieden wird hier zwischen beispielbasierten und regelbasierten Algorithmen. Während ein beispielbasierter Algorithmus verschiedene Fälle mit denen er „gefüttert" wird, derart analysiert, dass er ein eigenes Muster darin erkennt, erreicht ein regelbasierter Algorithmus sein Ziel durch die Anwendung von Regeln und Informationen, welche durch menschliche Expertinnen kodiert werden müssen. Die objektive Gefährlichkeit an sich kann anhand verschiedener Faktoren – sowohl regel- als auch beispielbasiert – festgestellt werden. Um Regeln zu implementiert, müssten Statistiken erstellt werden, welche untersuchen, welche Art von Verletzungshandlung typischerweise zum Tode führt. Wie hoch allerdings die Wahrscheinlichkeit des Eintritts des Todesfalls sein muss, um eine objektive Gefährlichkeit festzustellen, ist nicht klar abgrenzbar. Auch in der Rechtsprechung finden sich zu solchen Grenzen keine Angaben.

Nicht außer Acht zu lassen für die Gefährlichkeit der Handlung ist auch der Gesundheitszustand des Opfers.[37] So birgt das Schubsen einer älteren Person ein höheres Gefahrenpotenziell als bei einer jungen Person. Hier können allerdings nur solche Gesundheitsdefizite oder -risiken einbezogen werden, die die Täterin kannte, bzw. die für die Täterin erkennbar waren. Da der Gesundheitszustand einer Person objektiv ist, ist die Wertung dessen in Relation zur Tathandlung durch einen Algorithmus verwertbar.

33 *BGH*, NStZ 2003, 259 Tz. 4.
34 *BGH*, NStZ 2012, 443 (444).
35 *BGH*, NStZ-RR 2014, 139 f.
36 *BGH*, NStZ-RR 2007, 267.
37 *BGH* NStZ 2013, 75 (77); zu Recht kritisch: *Schneider*, in: MüKo StGB, § 212 Rn. 30.

Der Vorteil eines Algorithmus zur Feststellung der objektiven Gefährlichkeit wäre die gleiche Bewertung einer Handlung durch verschiedene Gerichte, insb. wenn diese keine Erfahrungswerte zur durchgeführten Handlung haben. Auf kognitiver Seite des Vorsatzes sind entsprechende Gegenindikatoren wie ein Rauschzustand miteinzubeziehen. Diese lassen sich (soweit nachweisbar) für einen Algorithmus rationalisieren, sodass dieser eine Abwägung zwischen der objektiven Gefährlichkeit und der eingeschränkten kognitiven Fähigkeit der Täterin vornehmen könnte. Schwieriger gestaltet sich die Rationalisierung des voluntativen Vorsatzelements. Bei Betrachtung der oben genannten Gegenindikatoren lässt sich schnell erkennen, dass diese nur subjektiv durch die Täterin feststellbar sind. So ist für eine Außenstehende kaum erkennbar, ob eine Rettungshandlung, welche die Täterin nach der Tat vornimmt, tatsächlich auf das Überleben des Opfers gerichtet ist oder lediglich der plötzlichen Realisierung der Täterin bezüglich der bevorstehenden Strafe geschuldet ist.

Auch die Beziehung der Täterin zum Opfer kann – insb. wenn das Opfer verstorben ist – kaum durch objektive Indizien festgestellt werden. Infrage kommen hier lediglich Aussagen von Zeuginnen aus dem Bekanntenkreis, wobei in Beziehungen bestehende Probleme oft kaum nach außen dringen.[38] Zudem ist bekanntermaßen die Zeugenaussage eine unverlässliche Quelle, da viele Faktoren die Wahrnehmung und Erinnerung eines Menschen beeinflussen können.[39] Die selektive Wahrnehmung von Menschen sorgt dafür, dass Geschehensabläufe nie im Gesamten wahrgenommen werden.[40] Die wahrgenommenen Bruchstück werden dann durch für die Aussagende sinnvolle Folgerungen ausgefüllt (sog. Logischer Ergänzungsmechanismus), welche auf den Erfahrungen des Individuums basieren.[41] Der durch Außeneinflüsse geprägte Erwartungshorizont der Befragten kann dazu führen, dass eine Außenstehende, die die Täterin nicht mochte, nun in all ihren Verhaltensweisen Anzeichen für eine aggressive und gewalttätige Art erkennt und damit ihr Vorurteil der Täterin gegenüber unterstützt (sog. knew-it-all-along-attitude).[42] Eine einheitliche und objektive Bewertung der Psyche der Täterin während der Tat ist daher nicht möglich. Dies gilt allerdings nicht nur für Algorithmen, sondern auch für Richterinnen.

aa) Normative Betrachtung des Vorsatzes

Aufgrund dessen haben sich in der Literatur einige Meinungen herausgebildet, die von der Einbeziehung des voluntativen Elements in die Bewertung des Vorsatzes absehen wollen. Solche normativ geprägten Herangehensweisen – wie *Puppe* sie vertritt – stellen lediglich darauf ab, ob die Täterin die Gefahr erkannt hat, denn „[o]b eine Gefahr ernst zu nehmen ist, hat […] nicht [die Täterin] zu entscheiden, sondern das Recht."[43] Dementsprechend sei ein vorsätzliches Verhalten dann zu bejahen, „wenn ein verständig denkender und handelnder Mensch an seiner Stelle nur dann so hätte handeln können, wenn er den Erfolg tatsächlich gewollt oder doch gebilligt hätte."[44] Dieser Bewertung ist das *LG Berlin* mit der Entscheidung im Berliner-Raser-Fall etwas entgegengekommen.[45] Hier wurde angenommen, dass die Täter – egal ob sie tatsächlich ernsthaft darauf vertraut haben – auf das Ausbleiben eines Todesfalls nicht mehr ernsthaft vertrauen konnten und durften.[46]

---

38 Deutschlandfunk, Gewalt in Deutschland – Jeden Tag versucht ein Mann seine Frau zu töten, 20.11.2018, abrufbar unter: https://www.deutschlandfunk.de/gewalt-in-deutschland- jeden-tag-versucht-ein-mann- seine.2852.de.html?dram:article_id=433613 (zuletzt abgerufen am 3.10.2019).
39 *Miebach*, NStZ-RR 2016, 329 ff.; *Nestler*, JA 2017, 10 (11 f.).
40 *Geipel*, Handbuch der Beweiswürdigung, 3. Aufl. (2017), § 22 Rn. 13.
41 *Geipel*, Handbuch der Beweiswürdigung, § 22 Rn. 14 f.
42 *Fischhoff/Beyth*: „I knew it would happen" – Remembered Probabilities of Once-Future Things, 1975, S. 3
43 *Puppe,* in: NK-StGB, § 15 Rn. 64.
44 *Puppe,* in: NK-StGB, § 15 Rn. 68.
45 *LG Berlin*, NStZ 2017, 471 (nicht rechtskräftig).
46 *LG Berlin*, NStZ 2017, 471 (475) (nicht rechtskräftig).

Diese Ansicht wird in abgewandelter Form auch von *Jakobs*[47] und *Herzberg*[48] vertreten. All diese Herangehensweisen haben gemeinsam, dass sie die Fokussierung der Abgrenzung zwischen Fahrlässigkeit und Vorsatz auf die voluntativen Elemente kritisieren. Diese Herangehensweisen erscheinen sinnvoll, da selbst die Wahrnehmung, Erinnerung und Reproduktion von Gedanken und Gefühlen der einzigen Person, die den inneren Sachverhalt tatsächlich wiedergeben kann – die Täterin – insbesondere bei Affekttaten erheblich fehlerhaft sein kann.[49]

bb) Kritik

Allerdings ist die Einbeziehung des voluntativen Elements vor allem bei Grenzfällen unabdingbar, wenn andere Indizien fehlen.[50] *Roxin* sieht in der Vorsatzgefahr kein geeignetes Abgrenzungskriterium zwischen Vorsatz und Fahrlässigkeit, da dies nur unter Einbeziehung aller Sachverhaltsumstände möglich sei.[51] Zudem kritisiert *Roxin* die Lehre von der Vorsatzgefahr in solchen Fällen als zu eng, in denen die von der Täterin geschaffene Gefahr nur gering oder mittel ist, da hier der Vorsatz kategorisch ausgeschlossen werden würde.[52]

Kritisiert wird auch, dass die Lehre von der Vorsatzgefahr dem Prinzip der individuellen Vorwerfbarkeit widerspricht.[53] Es ist „zutiefst ungerecht", einer Täterin, bei welcher kein Risikowissen bestand, vorzuwerfen, vorsätzlich gehandelt zu haben.[54] Denn ein Urteil kann nur gerecht sein, wenn „die individuelle Lebenswirklichkeit jedes einzelnen Menschen" beachtet und berücksichtigt wird, wobei auch Emotionen, Hoffnungen und Wünsche einbezogen werden müssen, auch wenn diese für andere irrational und unvernünftig wirken.[55]

Insbesondere bei Raser-Fällen zeigt sich bei der Annahme eines objektiv bewerteten Vorsatz folgendes Problem: Wenn bei einem Rennen mit tödlichem Ausgang für einen Dritten Mord angenommen wird, so muss konsequenter Weise bei einem gleichermaßen gefährlichen Rennen, welches nicht im Tod eines Dritten endet, versuchter Mord angenommen werden.[56] Dies würde zu abstrusen Ergebnissen führen, bei denen ohne die Verletzung eines Menschen oder auch nur die Konkretisierung der objektiv gefährlichen Handlung auf eine Person ein Strafrahmen von nicht unter drei Jahren besteht, §§ 23, 49 Abs. 1 Nr. 1 StGB. Das Urteil erscheint durch einen stark symbolischen Charakter geprägt zu sein, der zum einen einen Appell an den Gesetzgeber darstellt und zum anderen der Besänftigung der Bevölkerung dient.[57] Auch wenn die Bestrafung der Raser als Mörder in weiten Teilen der Gesellschaft als positives Zeichen seitens der Justiz und Abschreckung der Raser-Szene wahrgenommen wird, darf nicht außer Acht gelassen werden, dass die Aufgabe der Justiz nicht das Setzen von Zeichen, sondern die Findung von möglichst gerechten und angemessenen Strafen ist.[58]

47 *Jakobs*, Strafrecht AT, 2. Aufl. (1991), 8. Abschnitt Rn. 5 ff.
48 *Herzberg*, JuS 1986, 249 (261).
49 *Eschelbach*, in: BeckOK-StGB, § 212 Rn. 22.1.
50 *Eschelbach*, in: BeckOK-StGB, § 212 Rn. 22.1.
51 *Roxin*, Strafrecht AT, 4. Aufl. (2006), § 12 Rn. 50.
52 *Roxin*, Strafrecht AT, § 12 Rn. 51.
53 *Prittwitz*, Strafrecht und Risiko, 1993, S. 357.
54 *Prittwitz*, S. 357.
55 *Schweiger*, HRRS 2018, 407 (411).
56 *Walter*, NJW 2017, 1350 (1352).
57 *Momsen*, KriPoZ 2018, 76 (80).
58 *Walter*, NJW 2017, 1350 (1352 f.).

b) Abwägung der Indikatoren

Ein entscheidendes Problem bei der Verwendung von regelbasierten Algorithmen stellt sich bei der Frage der Abwägung der verschiedenen Indikatoren. Während im Vorangegangenen bereits erörtert wurde, dass die objektive Gefährlichkeit einer Handlung grds. die Annahme des Vorsatzes nahelegt, ist nicht zu generalisieren, wie stark einzelne Indizien für oder gegen einen Vorsatz sprechen. Auch durch eine Analyse der Rechtsprechung ist es nicht möglich, ein Muster für die Gewichtung von Indikatoren zu finden. Neben der Anforderung einer umfassenden Gesamtwürdigung aller Indizien bestehen keine genauen Anforderungen an die Verarbeitung derselben. Grundsätzlich liegt die Feststellung des Vorsatzes umso näher, desto gefährlicher die Tötungshandlung war. Aber auch hier können verschiedene Aspekte – wie die Fähigkeit zum „Dosieren der Wucht" bei Tritten gegen den Kopf[59] oder auch bei Hammerschlägen[60] – die Argumentationskraft der hohen Gefährlichkeit schwächen. Darüber hinaus kann allerdings auch das Bestehen aller anderen Indizien für einen Vorsatz nicht einfach bejaht oder verneint werden. Sie müssen nuanciert festgestellt werden. Im Rahmen der Verwertung durch einen regelbasierten Algorithmus müssten diese Nuancen erst durch einen Menschen festgestellt und an den Algorithmus weitergegeben werden. Eine Automatisierung ist in einem solchen Vorgang mit einem regelbasierten Algorithmus nicht vorstellbar, da in jedem Sachverhalt andere Gegebenheiten bestehen, die sich nicht verallgemeinern lassen.

Zusätzlich müssen auch die einzelnen Vorsatzindikatoren gegeneinander aufgewogen werden. Hierfür bestehen ebenfalls keine allgemein anzuwendenden Regeln, welche zur Programmierung eines Algorithmus herangezogen werden könnten. Lediglich die hohe Gewichtung der objektiven Gefährlichkeit ist erkennbar, sodass die Anforderungen an die Begründung der Verneinung des Vorsatzes umso höher sind, desto gefährlicher die Tathandlung war.[61] Insgesamt ist aufgrund der inkonsistenten Rechtsprechung kaum erkennbar, in welcher Weise die einzelnen Indikatoren zueinanderstehen. Dies erschwert die Möglichkeit, Regeln festzustellen, auf dessen Basis ein Algorithmus den Vorsatz begründen kann.

c) Einsatz eines beispielbasierten Algorithmus

Um zu umgehen, dass subjektiv belastete Beweismittel nicht rationalisiert und somit nicht als Regeln in den Algorithmus eingearbeitet werden können, besteht die Möglichkeit, einen beispielbasierten Algorithmus zu verwenden. Um diesem möglichst verlässlich zu gestalten, muss er mit so vielen Informationen aus Beispielen „gefüttert" werden, wie möglich.[62] Eine hohe Anzahl an Daten ist besonders entscheidend, da Computer im Gegensatz zu Menschen deutlich langsamer lernen.[63] So würde ein Mensch verstehen, was ein Auto ist und entsprechend andere Autos erkennen, wenn ihm eine Hand voll solcher gezeigt werden; Computer hingegen benötigen hierfür hunderttausende Bilder, da sie nicht verstehen, was ein Auto ist, sondern eher ein Muster für ein solches erstellen.[64] Entsprechendes gilt für die Feststellung dessen, welche Indizien in welcher Höhe für bzw. gegen eine vorsätzliche Tat sprechen. Notwendig sind somit hunderte von Fällen für jedes Delikt. Hierfür müssten neben den Indizien selbst auch deren Schlussfolgerungen in den Algorithmus eingearbeitet werden, sodass der Algorithmus darin ein Muster erkennen kann, welches er auf andere Sachverhalte und Indizienlagen anwenden kann. Dieses Muster muss

59 *BGH*, NStZ 2013, 581.
60 *BGH*, BeckRS 1988, 31105618.
61 *Schneider*, in: MüKo-StGB, § 212 Rn. 25.
62 *Geitgey*, Machine Learning Is Fun!, 2019, S. 255.
63 *Geitgey*, S. 254 f.
64 *Geitgey*, S. 255.

möglichst viele erdenkliche Sachverhalte abdecken, um sicherzustellen, dass bestimmte Daten nicht falsch einordnet und interpretiert werden. Allerdings ist kaum möglich, alle Szenarien im Rahmen eines Musters festzulegen. Denn Stimmnuancen in einer Reuebekundung können dazu führen, dass sie nicht als ernsthaft anzuerkennen ist und somit nicht gegen eine vorsätzliche Tat spricht. Inwiefern solche Nuancen durch den Algorithmus erkannt und darüber hinaus auch richtig gewertet und interpretiert werden, muss im Rahmen von Testläufen überprüft werden. Zu beachten ist zudem, dass sich die Rechtsprechung bezüglich der Feststellung des Vorsatzes bei bestimmten Konstellationen ändert. Dies würde dazu führen, dass die Daten, die bereits für eine bestimmte Konstellation gesammelt wurden, auf diese nicht mehr anwendbar sind. Erkennbar ist diese Problematik auch bei den Raser Fällen: Bis zum Prozess der Ku'damm-Raser gab es keine Verurteilung von Straßenrennfahrern zum Mord. Die Hamburger Raser wurden allerdings vom *LG Hamburg* wegen Mordes verurteilt.[65] Dies wurde vom *BGH* bestätigt.[66] Hiermit wurde die Möglichkeit „eröffnet" bei solchen Straßenrennen einen Tötungsvorsatz anzunehmen. Demnach sind ältere Fälle, in denen der Tötungsvorsatz verneint wurde, nicht mehr in vollem Maße auf die aktuelle Rechtsprechung anwendbar. Die bereits bestehenden Daten können in solcher Weise angepasst werden, dass sie der neuen Rechtsprechung entsprechen. Andernfalls wird es einige Jahre dauern, bis genügend Daten zu solchen Fallkonstellationen gesammelt wurden, um einen beispielbasierten Algorithmus auf die Daten zu stützen.

d) Risiken eines beispielbasierten Algorithmus

Allerdings stellt sich auch bei Umsetzbarkeit eines beispielbasierten Algorithmus folgendes Problem: Die Subjektivität, die in den Daten besteht, welche als Beispieldaten die Grundlage des Algorithmus bilden würden, würde auch in diesen einfließen. Dies kann zum einen förderlich sein, wenn man betrachtet, dass viele Indizien auch nur durch die subjektive Wertung einer Richterin interpretiert und aus ihnen Schlussfolgerungen gezogen werden können. Nicht außer Acht zu lassen ist allerdings, dass die subjektive Betrachtung durch Richterinnen nicht immer positiv gerichtet ist. Sie kann von Diskriminierung, Druck, Vorurteilen, politischer Einstellung oder Ähnlichem geprägt sein.[67] Wenn solche Daten in einen Algorithmus eingearbeitet werden, wird auch dieser solche Tendenzen übernehmen. Solche Fehler sind bereits in einigen Algorithmen aufgetreten. Sie können „harmlos" sein, wie wenn eine dunkelhäutige Person durch einen Gesichtsscanner nicht richtig erkannt wird, weil die künstliche Intelligenz mit hellhäutigen Menschen trainiert wurde.[68] Allerdings können solche Fehler auch gravierender sein: In den USA kam es dazu, dass ein Algorithmus, der voraussehen sollte, ob Straftäterinnen rückfällig werden würden („risk assessment"), als entscheidende Kriterium für den „risk factor" die Hautfarbe der Täterin heranzog.[69] Trotz der Verwendung von modernsten Lerntechnologien ist kaum erkennbar, ob der trainierte Algorithmus vorurteilsbelastet ist. Erkennbar wird dies oft erst, wenn der Algorithmus bedenkenswerte Ergebnisse herausgibt.[70]

Aufgrund des hohen Einflusses auf Entscheidungen, den ein solcher Algorithmus innehaben würde, ist es wichtig, dass er auch verantwortbar für seine Entscheidungen ist. Dies kann erreicht werden, indem der in der Justiz genutzt Algorithmus und seine Funktionsweisen offengelegt werden. Im anglo-amerikanischen Raum spricht man hier

65 *LG Hamburg,* BeckRS 2018, 39544.
66 *BGH*, NZV 2019, 306.
67 *Heussen*, NJW 2015, 1927 (1927 f.).
68 *Lohr*, Facial Recognition Is Accurate, If You're a White Guy, The New York Times 9.2.2018, abrufbar unter: https://www.nytimes.com/2018/02/09/technology/facial- recognition-race-artificial-intelligence.html (zuletzt abgerufen am 29.9.2019).
69 *Angwin/Larson/Mattu/Kirchner*, Machine Bias, ProPublica 23.3.2016, abrufbar unter: https://www.propublica.org/article/machine- bias-risk-assessments-in-criminal-sentencing (zuletzt abgerufen am 1.10.2019).
70 *Wolfangel*, Programmierter Rassismus, Zeit Online 19.6.2018, abrufbar unter: https://www.zeit.de/digital/internet/2018- 05/algorithmen-rassismus-diskriminierung-daten-vorurteile- alltagsrassismus/komplettansicht (zuletzt aufgerufen am 1.10.2019).

von „accountability“, also Verantwortbarkeit; hierdurch soll sichergestellt werden, dass die Entscheidungen, die der Algorithmus trifft, nicht willkürlich sind und nachvollzogen werden können.[71] Dies sieht auch die Europäische Union als Voraussetzung für eine vertrauenswerte künstliche Intelligenz und verlangt, dass die Systeme zurückverfolgbar sind.[72] Hiermit soll verhindert werden, dass Algorithmen unerkannt auf vorurteilsbehafteten Daten basieren. Eine solche Offenlegung würde es nicht nur der Richterin, sondern auch der Strafverteidigerin der Angeklagten möglich machen, nachzuvollziehen, wie es zu der Entscheidung kam und dementsprechend zu überprüfen, ob hierbei Indizien in einem zu hohen Maße eingespielt haben (bzw. nicht hinreichend einbezogen wurden) oder falsch interpretiert wurden, um den Vorsatz zu belegen. Allerdings kann es auch bei einer Offenlegung des Entscheidungsweges dazu kommen, dass für die Richterin nicht erkennbar ist, ob Indizien hier falsch gewertet wurden, da Fahrlässigkeit und Vorsatz nicht klar voneinander abgegrenzt werden können. Dementsprechend können hierdurch nur gravierende Fehler, die für die Verfahrensbeteiligten erkennbar sind, festgestellt und korrigiert werden.

III. Fazit

Die Richterin stellt das Zentrum des Verfahrens dar, da sie allein die Verantwortung für Entscheidungen innehält.[73] Ob ihr solche Entscheidungen durch einen Algorithmus abgenommen werden sollten, stellt die entscheidende Frage im Rahmen dieser Arbeit dar. Hierfür spricht vor allem die Entlastung der Gerichte und die sichergestellte Beachtung aller Aspekte im Rahmen der Feststellung des Vorsatzes. Allerdings ist insbesondere bei der Feststellung des Vorsatzes die Verwendung eines Algorithmus kritisch zu betrachten. Sowohl auf technischer als auch auf juristischer Ebene ergeben sich derzeit unlösbare Schwierigkeiten. Bei Betrachtung der technischen Aspekte ist entscheidend, dass der subjektive Tatbestand in jedem Sachverhalt anderes aufgebaut ist, sodass eine Verallgemeinerung für die Feststellung nicht möglich ist, ohne den Vorsatz an rein objektive Voraussetzungen wie die Gefährlichkeit einer Tötungshandlung zu knüpfen. Zudem bestehen in weiten Teilen der Gesellschaft noch Bedenken bezüglich der Anwendung von künstlicher Intelligenz. Diese Tendenzen zeigten sich in einer Umfrage des Weltwirtschaftsforums, wobei 41 % der 20.000 Befragten aus 27 Ländern ihre Sorgen vor der Verwendung von künstlicher Intelligenz geäußert haben.[74] Das Vertrauen in die Justiz ist allerdings eine grundlegende Voraussetzung für einen funktionierenden Rechtsstaat. Dieses Vertrauen kann erst dann erreicht werden, wenn Fortschritte in der Technologie zu einer Minimierung der Nachteile und Risiken führt, sodass sie im Gegensatz zu den Vorteilen verschwindend gering sind.

Um einen solchen Grad an Sicherheit und Gewissheit zu erlangen, müsste die eingesetzte künstliche Intelligenz ein derart genaues Persönlichkeitsprofil erstellen können, durch welches die Gedanken und Gefühle der Angeklagten im Zeitpunkt der Tat rekonstruiert werden können. Allerdings stellt sich selbst bei technischer Umsetzbarkeit dieser Voraussetzungen das Problem eines möglichen Eingriffs in die durch Art. 2 Abs. 2 i.V.m. Art. 1 Abs. 1 GG geschützte Intimsphäre.

---

71 *Martin*, Ethical Implications and Accountability of Algorithms, Journal of Business Ethics 7.6.2018, abrufbar unter: https://doi.org/10.1007/s10551-018-3921-3. (zuletzt abgerufen am 1.10.2019).

72 Europäische Kommission, Künstliche Intelligenz, 8.4.2019, abrufbar unter: https://ec.europa.eu/commission/news/artificial-intelligence-2019-apr-08_de (zuletzt abgerufen am 28.9.2019).

73 *Heussen*, NJW 2015, 1927 (1927 ff.).

74 World Economic Forum, Public Concern Around Use of Artificial Intelligence is Widespread, Poll Finds, abrufbar unter: https://www.weforum.org/press/2019/07/public-concern- around-use-of-artificial-intelligence-is-widespread-poll-finds (zuletzt abgerufen am 10.10.2019).

Trotz sich stetig verändernder Moralvorstellungen in Bezug auf die Offenlegung persönlicher Daten in der Gesellschaft ist nicht vorstellbar, dass sich die Akzeptanz dahingehend entwickelt, dass künstliche Intelligenzen angewendet werden, um zu entscheiden, ob ein Mensch wegen fahrlässiger Tötung zu bis zu fünf Jahren Haft oder wegen Mordes zu lebenslanger Haft verurteilt wird.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Malin Ebersbach

Big Data, Algorithmen und Bewährungsentscheidungen

Inhaltsverzeichnis

I. Einleitung

Neben dem Verhängen von Geldstrafen sind zur Bewährung ausgesetzte Freiheitsstrafen die häufigste Sanktion, die im Rahmen des allgemeinen Strafrechts in Deutschland verhängt wird.[1] Obwohl die Möglichkeit des Verhängens einer Bewährungsstrafe bereits seit 1953 im StGB verankert ist[2] und Freiheitsstrafen mehrheitlich (ca. 70%) zur Bewährung ausgesetzt werden,[3] ist die der Aussetzung zugrunde liegende Prognosepraxis weder einheitlich noch wissenschaftlich fundiert.[4] Nach empirischen Untersuchungen mangelt es insbesondere an der Sorgfalt, bisweilen auch Kompetenz und Objektivität der herangezogenen Sachverständigen.[5] Einerseits werden die gesetzlichen Vorschriften als dynamische Verweisung auf den aktuellen Stand der Forschung gelesen, andererseits ist die Methode der Kriminalprognose in den verschieden Bezugswissenschaften umstritten, wird teilweise sogar als unmöglich angesehen.[6] Hinzu kommt, dass davon ausgegangen wird, dass Rückfallraten, insbesondere hinsichtlich erheblicher Delikte, regelmäßig zu hoch eingeschätzt werden.[7]

Insoweit überrascht es nicht, dass vermehrt der Einsatz neuerer technischer Entwicklungen, die den Einsatz von Big Data und Algorithmen im Rahmen von Bewährungsentscheidungen ermöglichen, gefordert wird. Während sich in anderen Ländern, insbesondere in den USA, die Verwendung entsprechender Programme bereits durchgesetzt hat, ist dies in Deutschland bisher nicht umfassend denkbar.[8] Der vorliegende Aufsatz untersucht, inwieweit die bestehenden strafrechtlichen Regelungen den Einsatz von Big Data gestützten Algorithmen ermöglichen und ob ein solcher das Potential birgt aufgezeigte Missstände der Prognosepraxis nachhaltig zu beheben. Zunächst werden die Bewährungsvorschriften des StGB vorgestellt und der mögliche Einsatz von Algorithmen aufgezeigt. Anschließend werden mit dem Einsatz solcher Systeme verbundene Chancen und Risiken diskutiert und abgewogen.

II. Bewährungsentscheidungen in Deutschland

1. Rechtliche Rahmenbedingungen

Eine Strafaussetzung ist grundsätzlich nur im Rahmen einer verhängten Freiheitsstrafe i.S.d. § 38 StGB möglich. Verurteilte sollen durch die Aussetzung der Strafe die Möglichkeit erhalten durch positives Legalverhalten die Vollstreckung abzuwenden. So können Haftkosten reduziert, entsozialisierenden Wirkungen des Freiheitsentzuges entgegengewirkt oder diese vollständig vermieden werden.[9] Die rechtlichen Voraussetzungen für Bewährungsentscheidungen finden sich in den §§ 56 ff. StGB. Zu unterscheiden ist im Wesentlichen zwischen der Aussetzung der gesamten Strafe gemäß §§ 56-58 StGB und der Strafrestaussetzung zur Bewährung, geregelt in den §§ 57, 57a

1 *Grube*, Jura 2010, 759 (759).
2 *Grube*, Jura 2010, 759 (759).
3 *Braasch*, in: HK-StGB, 4. Auflage (2017), § 56 Rn.1; *Kinzig*, in: Schönke/Schröder, StGB, 30. Auflage (2019), § 56 Rn. 1; *Ostendorf*, in: NK-StGB, 5. Auflage (2017), vor § 56 Rn. 5.
4 *Grube*, Jura 2010, 759 (761); *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 19.
5 *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (38); *Schöch*, in: FS-Widmaier, 2008, S. 769 (969).
6 *Brettel*, Tatverleugnung und Strafrestaussetzung: ein Beitrag zur Praxis der Kriminalprognose, 2007, S. 19/23; *Kury/Adams*, Forum Strafvollzug 2010, 81 (81).
7 *Angwin/Larson/Mattu/Kirchner*, ProPublica 2016 machine Bias – There's software used across the country to predict future ciminals. And it's biased against blacks. Abrufbar unter: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, (zuletzt abgerufen am 17.10.2019); *Braasch*, in HK-StGB, § 56 Rn. 8; *Kury/Adams*, Forum Strafvollzug 2010, 81 (86).
8 *Cukier/Mayer-Schönberger*, Wirtschaftswoche 2013, 94 (95); *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (46); *Härtel*, LKV 2019, 49 (53).
9 *Braasch*, in: HK-StGB, § 56 Rn. 1; *Dünkel*, in: NK-StGB, § 57 Rn. 1; *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 1; *Ostendorf*, in: NK-StGB, § 56 Rn. 4; *Groß*, in: MüKo-StGB, 3. Auflage (2019), vor § 56 Rn. 1; *Grube*, Jura 2010, 759 (760).

StGB.[10] Die vollständige Aussetzung der Freiheitsstrafe ist nur bis zu einer Strafhöhe von maximal zwei Jahren möglich, § 56 StGB.[11] Daraus folgt, dass das Gericht zunächst die tat- und schuldangemessene Strafe gemäß § 46 Abs. 1 S. 2 StGB bestimmen muss, bevor eine Aussetzung der Strafe in Betracht gezogen werden kann.[12] Dogmatisch ist die Strafaussetzung zur Bewährung daher eine Modifikation der verhängten Freiheitsstrafe.[13]

Je nach Dauer der Gesamtstrafe hat das Gericht unterschiedliche Voraussetzungen zu prüfen. Bei einer Freiheitsstrafe von unter sechs Monaten ist die Aussetzung der Bewährung bei günstiger Kriminalprognose zwingend.[14] Gegenstand der Legalprognose ist das zukünftige strafrechtskonforme Verhalten des/der Angeklagten.[15] Bagatelltaten sowie sog. „Jedermannsdelikte" (z.B. Steuerhinterziehung) werden angesichts fehlender Prognostizierbarkeit nicht in die Verhaltensvorhersage einbezogen. Ebenso spielt generell sozialkonformes oder sozialerwünschtes Verhalten keine Rolle, soweit die Grenzen der Strafbarkeit nicht überschritten werden.[16] Insofern ist der teilweise synonym verwendete Begriff der Sozialprognose irreführend.[17] Die Legalprognose ist dann günstig, wenn das straffreie Verhalten des/der Angeklagten wahrscheinlicher ist als die Erwartung weiterer Straftaten.[18] Diesbezüglich gilt der Grundsatz „in dubio pro reo" nicht. Zweifel des Gerichts gehen bei hinreichend bewiesener Tatsachengrundlage zu Lasten des/r Angeklagten.[19]

Bei einer Freiheitsstrafe zwischen sechs und zwölf Monaten ist neben einer günstigen Legalprognose erforderlich, dass die Verteidigung der Rechtsordnung die Vollstreckung der Strafe nicht gebietet, § 56 Abs. 2 StGB. Dies ist nach der Rechtsprechung der Fall, wenn „eine Aussetzung der Vollstreckung im Hinblick auf schwerwiegende Besonderheiten des Einzelfalls für das allgemeine Rechtsempfinden schlechthin unverständlich erscheinen müsste und das Vertrauen der Bevölkerung in die Unverbrüchlichkeit des Rechts den Schutz der Rechtsordnung vor kriminellen Angriffen erschüttern könnte".[20] Die Verteidigung der Rechtsordnung ist demnach insbesondere dann geboten, wenn die begangene Tat einen hohen Schaden verursacht hat, erhebliche kriminelle Intensität aufweist, hartnäckiges rechtsmissachtendes Verhalten des/r Täters*in festgestellt wird, eine besondere Sozialschädlichkeit der Tat besteht oder der/die Täter*in die Tat aus einer besonderen beruflichen Stellung heraus begeht und dabei das ihm/ihr entgegengebrachte Vertrauen grob missbraucht.[21]

Bei einer Strafdauer zwischen einem und zwei Jahren sind neben den Voraussetzungen des § 56 Abs. 2 StGB besondere Umstände nachzuweisen, § 56 Abs. 3 StGB.[22] Dabei sind vor allem gewichtige mildernde Gründe, die in der Persönlichkeit des Täters liegen zu berücksichtigen.[23] Eine Verwertung dieser Kriterien im Rahmen der Strafzumessung, schließt eine nochmalige Berücksichtigung in der Strafaussetzungsentscheidung nicht aus.[24]

10 *Fischer*, StGB, 66. Auflage (2019), § 56 Rn. 2; *Groß*, in: MüKo-StGB, vor § 56 Rn. 2; *Ostendorf*, in: NK-StGB, § 56 Rn. 1.
11 *Fischer*, StGB, § 56 Rn. 2a; *Groß*, in: MüKo-StGB, vor § 56 StGB, Rn. 2; *Grube*, Jura 2010, 759 (760).
12 *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 6; *Grube*, Jura 2010, 759 (760/763).
13 *Braasch*, HK-StGB, § 56 Rn. 1; *Dünkel*, in: NK-StGB, § 57 Rn. 4; *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 4; a.A.: *Ostendorf*, in: NK-StGB, vor § 56 Rn. 1.
14 *Groß*, in: MüKo-StGB, vor § 56 Rn. 14; *Grube*, Jura 2010, 759 (760).
15 *Braasch*, HK-StGB, § 56 Rn. 5; *Grube*, Jura 2010, 759 (761).
16 *Groß*, in: MüKo-StGB, vor § 56 Rn. 18; *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 16; *Ostendorf*, in: NK-StGB, § 56 Rn. 5.
17 *Fischer*, StGB, § 56 Rn. 3.
18 *BGH*, NStZ-RR 2005, 38 (38); *BGH*, NStZ 1997, 594 (595); *Braasch*, in: HK-StGB, § 56 Rn. 6; *Fischer*, StGB, § 56 Rn. 4a; *Groß*, in: MüKo-StGB, vor § 56 Rn. 16/24; *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 17.
19 *BGH*, StV 92, 106 (107); *Braasch*, in: HK-StGB, § 56 Rn. 10; *Fischer*, StGB, § 56 Rn. 4a; *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 17; *Ostendorf*, in: NK-StGB, § 56 Rn. 24; *Grube*, Jura 2010, 759 (761).
20 BGHSt 24, 40 (46).
21 *Groß*, in: MüKo-StGB, vor § 56 Rn. 37; *Grube*, Jura 2010, 759 (763).
22 *Groß*, in: MüKo-StGB, vor § 56 Rn. 43; *Grube*, Jura 2010, 759 (760).
23 *Grube*, Jura 2010, 759 (763).
24 *Grube*, Jura 2010, 759 (763).

Gemäß §§ 57, 57a StGB kann eine Freiheitsstrafe bei günstiger Legalprognose und Einwilligung des Verurteilten auch nach teilweise vollstreckter Haft zur Bewährung ausgesetzt werden. § 57 Abs. 1 StGB regelt die sog. Zwei-Drittel-Aussetzung.[25] Demnach kann der Strafrest zur Bewährung ausgesetzt werden, wenn zwei Drittel der verhängten Freiheitsstrafe, mindestens jedoch zwei Monate vollstreckt worden sind.[26] Im Unterschied zur primären Strafaussetzung gemäß § 56 StGB ist die Legalprognose dann als günstig anzusehen, wenn die Abwägung zwischen den zu erwartenden Wirkungen des bereits erlittenen Vollzuges und den Sicherheitsinteressen der Gemeinschaft eine weitere Vollstreckung nicht erforderlich erscheinen lässt. Maßgebliches Abwägungskriterium ist daher die Bedeutung der bei einem etwaigen Rückfall gefährdeten Rechtsgüter.[27]

In Ausnahmefällen kommt auch eine sog. Halbstrafen-Aussetzung gemäß § 57 Abs. 2 StGB in Betracht. Demnach kann die Haftstrafe bereits nach hälftiger Verbüßung, mindestens jedoch nach sechs Monaten, zur Bewährung ausgesetzt werden, wenn es sich um eine Erstverbüßung handelt oder besondere Umstände eine Aussetzung ermöglichen.[28] Besondere Umstände können sich auch hier aus einer Gesamtwürdigung von Tat, Persönlichkeit des/der Verurteilten und seiner/ihrer Entwicklung während des Strafvollzuges ergeben, müssen allerdings, anders als i.R.d § 56 Abs. 2 StGB, überdurchschnittlich gewichtig sein.[29]

§ 57a StGB trifft eine Sonderreglung für die Aussetzung der Vollstreckung einer lebenslangen Freiheitsstrafe. Maßgebliche Gesichtspunkte sind neben der Kriminalprognose auch die Schuldschwere der Anlasstat und Aspekte der Generalprävention.[30] Die Aussetzung ist erstmalig nach 15 Jahren verbüßter Freiheitsstrafe denkbar. Zudem darf die besondere Schwere der Schuld die weitere Vollstreckung nicht gebieten.[31]

2. Kriminalprognose

Allen dargestellten Aussetzungsentscheidungen gemein ist die Erforderlichkeit einer günstigen Kriminalprognose. Das Begehen weiterer erheblicher Straftaten durch den/die Täter*in muss demnach einer Wahrscheinlichkeitsprüfung unterzogen werden.[32] Zur Erstellung dieser Prognose sind die Persönlichkeit der/des Verurteilten, ihr/sein Vorleben, die Umstände der Tat, Ihr/sein Verhalten nach der Tat, ihre/seine Lebensverhältnisse, der soziale Empfangsraum, die Wirkungen die von der Aussetzung für ihn/sie zu erwarten sind, sowie sonstige Umstände die Rückschlüsse auf das zukünftige Verhalten der/des Angeklagten zulassen, heranzuziehen. Dabei ist auch zu beachten, inwieweit positive Auswirkungen durch, während der Bewährungszeit zu erfüllende, Auflagen und Weisungen zu erwarten sind.[33] Präzisiert werden diese Anforderungen durch die Rechtsprechung des *BVerfG*. Demnach muss im Rahmen der Begutachtung „deutlich werden, in welchem Zusammenhang Ausgangsdelikt und frühere Delinquenz mit der Persönlichkeit stehen [...] und ob deliktspezifische Persönlichkeitszüge persistieren oder nicht. Dabei muss die prognostische Relevanz der Vortaten und der Anlasstat in die Gesamtpersönlichkeit

25 *Fischer*, StGB, § 57 Rn. 12.
26 *Dünkel*, in: NK-StGB, § 57 Rn. 4.
27 *Braasch*, in: HK-StGB, § 56 Rn. 8; *Fischer*, StGB, § 57 Rn. 12; *Boetticher/Kröber/Müller-Isberner/Böhm/Müller-Metz/Wolf*, NStZ 2006, 537 (538).
28 *Dünkel*, in: NK-StGB, § 57 Rn. 25, 26, 47; *Braasch*, in: HK-StGB, § 57 Rn. 16, 17.
29 *Braasch*, in: HK-StGB, § 57 Rn. 24.
30 *Fischer*, StGB, § 57 Rn. 14.
31 *Dünkel*, in: NK-StGB, § 57a Rn. 7; *Fischer*, StGB, § 57a Rn. 4-6.
32 *Groß*, in: MüKo-StGB, vor § 56 Rn. 3; *Grube*, Jura 2010, 759 (760).
33 *BGH*, StV 1992, 62 (64); 1987, 63 (63); *Dünkel*, in: NK-StGB, § 57 Rn. 31; *Groß*, in: MüKo-StGB, vor § 56 Rn. 26/27; *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 23.

des Betroffenen nachvollziehbar abgeleitet werden."[34] Welche konkrete Methode das erkennende Gericht jedoch zur Erstellung der Legalprognose anwendet, bleibt grundsätzlich diesem überlassen.[35] Zu unterscheiden ist zwischen der intuitiven (subjektive Überzeugung des Gerichts), statistischen (nomothetischen/aktuarischen), und klinischen (idiografischen) Prognosemethode.

Die intuitive Methode stützt sich im Wesentlichen auf die subjektive Überzeugung des Gerichts.[36] Obwohl diese nur eine geringe Validität aufweist und diese Unzulänglichkeit bereits seit über 100 Jahren bekannt ist, findet sie in der gerichtlichen Praxis überwiegend Anwendung.[37]

Die klinische Methode umfasst ein Sachverständigengutachten, welches anhand einer Anamnese, eines umfassenden Aktenstudiums und weiterer Instrumente unterschiedlicher Herkunft, insbesondere psychodiagnostischer Tests, erstellt wird.[38] Auf Grundlage der Ermittlung von kriminogenen und protektiven Faktoren wird eine individuelle Kriminalitätstheorie entwickelt, die Aussagen über künftiges Verhalten des/der Probanden*in ermöglichen soll.[39] Auch im Rahmen der klinischen Methode obliegt die Beurteilung und Einordnung der ermittelten Daten jedoch letztlich der Erfahrung und der Expertise des/r Gutachters*in, sodass die Objektivität, Reliabilität und Validität der grundsätzlich auf wissenschaftlichen Erkenntnissen beruhenden Prognosemethode geschwächt wird.[40]

Bei der statistischen Prognosemethode wird der/die Täter*in anhand von bestimmten Merkmalen einer Vergleichsgruppe zugeordnet. Gedanklicher Ausgangspunkt ist die Erkenntnis, dass bestimmte Merkmale in bestimmten Gruppen statistisch mit Straffälligkeit korrelieren. Kann der/die Proband*in einer bestimmten Gruppe zugeordnet werden und weist besonders viele oder wenige kriminogene/protektive Merkmale auf, die nach der empirischen Datengrundlage mit der Begehung von Straftaten in Zusammenhang stehen, kann eine Wahrscheinlichkeitsaussage über das zukünftige Legalverhalten getroffen werden.[41] Bei einigen Erhebungsinstrumenten werden Punktwerte ausschließlich nach dem Bestehen oder Nichtbestehen bestimmter Merkmale vergeben, bei anderen ist eine zusätzliche Gewichtung möglich, sodass die individuelle Merkmalsausprägung erfasst wird.[42]

Neuere Instrumente kombinieren statistische und klinische Prognosemethoden.[43] Ob dies einen Qualitätszuwachs verspricht, ist bislang nicht eindeutig geklärt.[44] Während in Deutschland statistische Prognosemethoden jedenfalls nicht ausschließlich zur Erstellung von Kriminalprognosen verwendet werden, gehört die Nutzung dieser Methode

34 *BVerfG*, NJW 2004, 739 (743).
35 *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 17; *Grube*, Jura 2010, 759 (761).
36 *Budde*, Bewährungshilfe 2014, 161 (162); *Grube*, Jura 2010, 759 (761); *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (29).
37 *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 19; *Brettel*, S. 34; *Urbaniok*, Validität von Risikokalkulationen bei Straftätern – Kritik an einer methodischen Grundannahme und zukünftige Perspektiven, 2004, S. 261; *Budde*, Bewährungshilfe 2014, 161 (162); *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39); *Grube*, Jura 2010, 759 (761); *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (30).
38 *Brettel*, S. 34.
39 *Dünkel*, in: NK-StGB, § 57 Rn. 86; *Kinzig*, in: Schönke/Schröder, § 56 Rn. 20; *Brettel*, S. 34; *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (38); *Schneider*, StV 2006, 99 (100).
40 *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39).
41 *Brettel*, S. 30; *Budde*, Bewährungshilfe 2014, 161 (162); *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39).
42 *Brettel*, S. 31; *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminolige 2018, 37 (38); *Schneider*, StV 2006, 99 (102); *Rosegger/Laubacher/Moskvitin/Villmar/Palermo/Endrass*, International Journal of Offender Therapy and Comparativ Criminology, 716 (716).
43 *Braasch*, in: HK-StGB, § 56 Rn. 11; *Döbele*, Standardisierte Prognoseinstrumente zur Vorhersage des Rückfallrisikos von Straftätern – Eine kritische Betrachtung des Einsatzes in der Strafrechtspflege aus juristischer Sicht, 2014, S. 18; *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminolige 2018, 37 (37); Schneider, StV 2006, 99 (100).
44 Dafür: *Dünkel*, in: NK-StGB, § 57 Rn. 107; *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 22; *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminolige 2018, 37 (37); Dagegen: *Boetticher/Dittmann/Nedopil/Nowara/Wolf*, NStZ 2009, 478 (580); *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (34); *Bock*, StV 2007, 269 (273).

im anglo-amerikanischen Raum zu den führenden Methoden. [45]

Die Rechtsprechung stellt auf Grundlage der dargelegten gesetzlichen Prognoseindizien hohe Anforderungen an die Individualisierung der Verhaltensvorhersage, sodass letztlich eine rein statistische Prognosestellung, die ausschließlich Aussagen über eine gruppenbezogene Wahrscheinlichkeit treffen kann, in Deutschland nicht möglich ist und allenfalls als Ergänzung der idiografischen Methode eingesetzt werden kann.[46] Im Rahmen einer interdisziplinären Arbeitsgruppe wurden, vor dem Hintergrund der defizitären Praxis, Mindestanforderungen für Prognosegutachten entwickelt, die diesen Befund bestätigen: „[Es] verbietet sich eine abstrakte, allein auf statistische Wahrscheinlichkeiten gestützte Prognose."[47]

III. Möglicher Einsatzbereich von Big Data und Algorithmen bei Bewährungsentscheidungen in Deutschland

Letztlich ist lediglich die statistische Prognosemethode der strukturierten Erfassung durch Algorithmen, welche die Auswertung von großen Datenbeständen aus sämtlichen Lebensbereichen (Big Data)[48] ermöglichen, zugänglich.[49] Denkbar wäre daher gegebenenfalls der unterstützende Einsatz von Tools, wie sie in den USA oder in der Schweiz bereits verwendet werden. Das amerikanische System COMPAS berechnet auf der Grundlage von insgesamt 137 Kriterien einen individuellen Risk-Score auf einer Skala von eins bis zehn.[50] Die erforderlichen Daten werden zum Teil über die Abfrage automatisierter Datenbanken, zum Teil über Erhebungen durch Justizangestellte gewonnen[51] und basieren auf Fragebogeninterviews mit den Delinquenten und der Erfassung verschiedener Umweltfaktoren, wie der Historie und der persönlichen Lage des/der Angeklagten, einschließlich soziologischer, psychologischer und biographischer Faktoren.[52] In der Schweiz kommt das Programm FOTRES zur Anwendung, welches mehrere hundert Kriterien erfasst und Informationen zur Rückfallwahrscheinlichkeit, Behandelbarkeit des Probanden und der Bewertung von Therapieerfolgen generiert.[53] Im Folgenden soll kritisch diskutiert werden, welche Chancen und Risiken der Einsatz derartiger Prognoseinstrumente in Deutschland birgt.

IV. Chancen und Risiken des Einsatzes von Big Data und Algorithmen bei Bewährungsentscheidungen in Deutschland

1. Leistungsfähigkeit, Effektivität und Kostenreduzierung

Im gerichtlichen Alltag ist eine wissenschaftlich basierte Prognose, aufgrund der immensen Kosten sowie des personellen Aufwands, nicht in jedem Fall möglich.[54] Insbesondere im Rahmen von Aussetzungsentscheidungen gemäß § 56 StGB sind in der Regel über die intuitive Prognose hinaus keine weiteren Möglichkeiten gegeben; der

45 *Kinzig*, in: Schönke/Schröder, StGB§ 56 Rn. 20; *Urbaniok*, S. 261.
46 BVerfGE 109, 242 (251); *Kinzig*, in: Schönke/Schröder, StGB, § 56 Rn. 22; *Brettel*, S. 32; *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminolige 2018, 37 (37, 41-48); *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (34).
47 *Boetticher/Kröber/Müller-Isberner/Böhm/Müller-Metz/Wolf*, NStZ 2006, 537 (539).
48 *Bilski/Schmid*, NJOZ 2019, 657 (657).
49 *Brettel*, S. 31; *Ernst*, JZ 2017, 1026 (1028); *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (31).
50 Shadowen, Ethics and Bias in Machine Learning: A Technical Study of What Makes Us „Good", 2017, S. 7, 12; *Ziegler*, c't 2017, 68 (68).
51 *Ziegler*, c't 2017, 68 (68).
52 *Müller/Pöchhacker*, in: Algorthmic Risk Assessement als Medium des Rechts – Medientechnische Entwicklungen und institutionelle Verschiebungen aus Sicht einer Techniksoziologie des Rechts, 2019, S. 157 (163).
53 *Adams/Kury*, Forum Strafvollzug 2010, 81 (81).
54 *Budde*, Bewährungshilfe 2014, 161 (162); *Ostendorf*, in: NK-StGB, § 56 Rn. 20.

erforderlichen intensiven Datenerfassung steht schon der Grundsatz der Verhältnismäßigkeit entgegen, sodass auch eine algorithmenbasierte Entscheidung verbunden mit der hohen Eingriffsintensität grundsätzlich ausscheidet.[55]

Ohne wissenschaftliche Rückkopplung der Prognosemethode steigt jedoch das Risiko einer Fehlprognose eklatant.[56] Der Rückgriff auf Big Data Systeme könnte die für eine solche Analyse erforderliche umfassende Datenerhebung und Datenanalyse um ein Vielfaches erleichtern, den Prozess beschleunigen und die Kosten des Gerichts wesentlich reduzieren.[57] Zudem wäre sichergestellt, dass jede/r Angeklagte auf Grundlage einer wissenschaftlich fundierten Wahrscheinlichkeitsaussage und nicht bloß einer subjektiven Eingabe des/r entscheidenden Richters/in zu einer bedingten/unbedingten Freiheitsstrafe verurteilt würde. Weiterhin steigt die Vorhersagegüte mit der Masse an generierten Daten. Von einem Algorithmus könnte diese Erhebung innerhalb kürzester Zeit übernommen werden.[58] Teilweise wird durch eine derart strukturierte und umfassende Auswertung auch ein genereller Erkenntnisgewinn über die Ursachen von Kriminalität erhofft, der in Folge dessen auch dem/der einzelnen Probanden*in wiederum zu Gute käme. Individuelle Fördermöglichkeiten und Unterstützungsangebote könnten bedarfsgerecht gestaltet werden und das Rückfallrisiko des/r Einzelnen wesentlich minimieren.[59] Gleichzeitig wird durch eine algorithmenbasierte Wahrscheinlichkeitsprognose die Möglichkeit eröffnet, die der standardisierten Prognose zugrundeliegenden Kriterien offenzulegen, mithin auch für den/die Verurteilte/n transparent, nachvollziehbar, sowie gegebenenfalls angreifbar zu machen.[60] Ein Algorithmus ist auch nicht tagesformabhängig oder lässt sich von individuellen Sympathien/Antipathien leiten. So konnte beispielweise gezeigt werden, dass Richter*innen mit fortschreitender Tagesstunde in ihren Aussetzungsentscheidungen zunehmend weniger risikofreundlich agieren.[61] Ein algorithmenbasiertes Entscheidungssystem könnte also auch die Rationalität der getroffenen Entscheidungen wesentlich erhöhen.[62]

2. Chancengleichheit und Gleichheit der Prognosemethode

Untersuchungen zeigen, dass klinische Prognosen von Psychiater*innen grundsätzlich eine geringe Reliabilität und damit auch eine geringe Validität aufweisen, während statistische Methoden unabhängig von den zur Verfügung stehenden Daten und der Berufserfahrung des Prognostizierenden besser abschneiden. [63] Mithin kann einzig die statistische Prognosemethode jedem einzelnen Probanden gleiche Chancen auf Grundlage der gleichen Methode und gleicher Kriterien gewähren und kommt so den Anforderungen des Art. 3 GG am nächsten. Insbeson-

55 *Albrecht*, in: FS-Frisch, 2013, S. 1063 (1064).
56 *Ostendorf*, in: NK-StGB, § 56 Rn. 17/19; *Boetticher/Dittmann/Nedopil/Nowara/Wolf*, NStZ 2009, 478 (579); *Gless*, in: GS-Weßlau, 2016, S. 167 (172).
57 *Kury/Adams*, Forum Strafvollzug 2010, 81 (81); *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (31).
58 *Brettel*, S. 88; *Martini*, Blackbox Algorithmus – Grundfragen einer Regulierung künstlicher Intelligenz, 2019, S. 27; *Zweig*, Wo Maschinen irren können – Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung, 2018, S. 24; *Bilski/Schmid*, NJOZ 2019, 657 (657); *Egbert*, APuZ 2017, 17 (21); *Ernst*, JZ 2017, 1026 (1028); *Gless*, in: FS-Weßlau, S. 167 (167); *Krüger/Lischka*, in: Mohabbat Kar/Thapa/Prycek, (Un-)berechenbar? – Algorithmen und Automatisierung in Staat und Gesellschaft, 2019, S. 441; *Singelnstein*, NStZ 2018, 1 (4).
59 *Belina*, Monatsschrift für Kriminologie und Strafrecht 2016, 85 (95); *Bislki/Schmid*, NJOZ 2019, 657 (657); *Martini*, DVBl 2014, 1481 (1482); *Singelnstein*, NStZ 2018, 1 (3).
60 *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39); *Kury/Adams*, Forum Strafvollzug 2010, 81 (81).
61 *Zweig/Krafft*, in: Mohabbat Kar/Thapa/Prycek, S. 205.
62 *Bundesverband Verbraucherzentrale*, Algorithmenbasierte Entscheidungsprozesse – Thesenpapier des Bundesverbands Verbraucherzentrale, 2017, S. 7; *Zweig*, S. 5, 15; *Cukier/Mayer-Schönberger*, Wirtschaftswoche 2013, 94 (94); *Krüger/Lischka*, in: Mohabbat Kar/Thapa/Prycek, S. 441; *Zweig/Krafft*, in: Mohabbat Kar/Thapa/Prycek, S. 205.
63 *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (32).

dere vor dem Hintergrund des Bestehens einer hohen Falsch-Positiv-Rate, könnte eine algorithmenbasierte Entscheidungsfindung zu einer wesentlichen Erhöhung der Strafaussetzungen beitragen.[64] Ebenso sind fundierte Aussagen über die Irrtumswahrscheinlichkeiten des jeweiligen angewandten Algorithmus möglich.[65]

3. Begrenzte Aussagekraft statistischer Methoden

Andererseits wird vielfach die Aussagekraft nomothetischer Prognosemethoden bezweifelt. So werden von diesen vorrangig Merkmale erfasst, die in der Vergangenheit der/s Proband*in liegen, auf welche er/sie jedoch zum Zeitpunkt der Urteilsfindung keinen Einfluss hat, gegebenenfalls nie hatte,[66] obwohl die neuere Prognoseforschung gezeigt hat, dass früh in der Biografie liegende Merkmale mit zunehmenden zeitlichem Abstand an Bedeutung verlieren.[67]

Auch ist davon auszugehen, dass verschiedenen Kriterien, je nach Einzelfall, eine unterschiedliche Gewichtung zukommt. Wechselseitige Beziehungen und das Zusammenwirken der unterschiedlichen Faktoren können in einem algorithmenbasierten System nicht hinreichend abgebildet werden.[68] Auch für den Einzelfall bedeutsame Faktoren, die bisher nicht in die Ermittlung der Verhaltensprognose aufgenommen worden sind, können von dem System nicht ohne weiteres erfasst werden.[69] Da grundsätzlich jedoch davon ausgegangen werden muss, dass kriminelles Verhalten multifaktoriell bedingt ist und nicht anhand von statischen Kontrollfaktoren zugerechnet werden kann, stellt dies einen erheblichen Mangel in dem Prognosesystem dar.[70] Eine allgemeingültige Kriminalitätstheorie konnte zudem bislang nicht aufgestellt werden.[71]

Des Weiteren ist das Verhalten des/r Probanden*in beispielsweise im Strafvollzug kritisch zu hinterfragen und nicht vorschnell durch den Einsatz eines Algorithmus einer Kategorie zuzuordnen. So sind Anpassungsleistungen von Strafgefangenen während der Dauer des Vollzuges bekannt (Gefängnis als totale Institution), ermöglichen gegebenenfalls aber nur einen geringen Aussagegehalt über das Verhalten des/r Probanden*in in Freiheit.[72] Sobald ein Manual jedoch eine individuelle Gewichtung der einzelnen Faktoren durch den/die Prognostizierende*n ermöglicht, werden Reliabilität und Validität wiederum beeinträchtigt.[73]

Weiterhin ergibt sich bei Anwendung rein statistischer Methoden das sogenannte „Mittelfeldproblem“ auf Grund der Gauß’schen Normalverteilung. Der Algorithmus neigt überproportional dazu, Probanden in mittlere Risikokategorien um die 50% einzuordnen, sodass das Gericht letztlich erneut eine intuitive Prognose treffen muss oder auf ein weiteres Sachverständigengutachten angewiesen ist. Nur in Extremfällen kann auf Grundlage der algorithmenbasierten Wahrscheinlichkeitsvorhersage eine eindeutige Entscheidung getroffen werden.[74]

64 *Rettenberger*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 28 (32).
65 *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39).
66 *Dünkel*, in: NK-StGB, § 57 Rn. 25; *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminolige 2018, 37 (39); *Schneider*, StV 2006, 99 (103).
67 *BVerfG*, NStZ 2000, 109 (110); *Dünkel*, in: NK-StGB, § 57 Rn. 25; *Bock*, StV 2007, 269 (273).
68 *Ostendorf*, in: NK-StGB, § 56 Rn. 21.
69 *Braasch*, in: HK-StGB, § 56 Rn. 21; *Ostendorf*, in: NK-StGB, § 56 Rn. 21; *Brettel*, S. 83; *Bock*, StV 2007, 269 (272); *Ernst*, JZ 2017, 1026 (1027).
70 *Egbert*, APuZ 2017, 17 (21).
71 *Brettel*, S. 83.
72 *Dünkel*, in: NK-StGB, § 57 Rn. 30; *Grube*, Jura 2010, 759 (762).
73 *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39).
74 *Braasch*, in: HK-StGB, § 56 Rn. 8; *Dünkel*, in: NK-StGB, § 57 Rn. 114; *Ostendorf*, in: NK-StGB, § 56 Rn. 21; *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39).

Ein weiterer Kritikpunkt folgt aus der Funktionsweise statistisch basierter Prognoseinstrumente, die letztlich eine empirisch bestehende Rückfallwahrscheinlichkeit einer bestimmten Gruppe dem einzelnen Probanden zuschreibt.[75] Die individuell durch das Programm errechnete Wahrscheinlichkeit suggeriert dabei eine für den Einzelfall in der Realität nicht bestehende Aussagesicherheit,[76] und enthält notwendiger Weise umfassende Generalisierungen, sodass Fehlprognosen unvermeidlich bleiben.[77] Gesetzlich vorgesehen ist jedoch ausdrücklich eine individuelle Wahrscheinlichkeitsprognose, nicht die Bestimmung eines Kollektivrisikos (s.o.).[78]

Die Aussagekraft von algorithmenbasierten Bewährungsentscheidungen ist ferner nur schwer überprüfbar. Da die Aussetzungsentscheidung bei Straftäter*innen, die als gefährlich eingestuft werden, i.d.R. negativ ausfällt, ist die Ermittlung der Anzahl falsch-positiver Prognosen faktisch kaum möglich.[79] Neben dem Individuum und der Gesellschaft erhält auch das Programm keine Rückmeldung über etwaige Fehlentscheidungen (Feedbackasymetrie), sodass selbstverstärkende Feedback-Schleifen entstehen.[80] Dieser Effekt wird durch eine anzunehmende wesentliche Verzerrung der empirischen Daten auf Grund von Hell- und Dunkelfeldeffekten noch verstärkt.[81] Zudem ist die Treffsicherheit eines Prognoseinstrumentes maßgeblich von der Basisrate[82] abhängig. Ist diese wesentlich niedriger als die Treffsicherheit des Systems wird statistisch gesehen die gesamte Gefangenenpopulation benachteiligt, sofern Individualprognosen erstellt werden. Ein besseres Ergebnis könnte erzielt werden, wenn alle Proband*innen in Freiheit entlassen werden. Im umgekehrten Fall, die Treffsicherheit des Instruments erreicht nicht die Höhe der Basisrate, würde man statistisch ein besseres Ergebnis erzielen, wenn alle Aussetzungsentscheidungen negativ beschieden würden.[83]

Weiterhin folgt aus der Etikettierung eines Individuums mit einem bestimmten Risiko-Score in der Regel ein erheblicher Stigmatisierungseffekt. Strafgefangene verhalten sich auf Grund des Labels mit hoher Wahrscheinlichkeit entsprechend der Vorhersage des Algorithmus. Ob der Algorithmus jedoch im Einzelfall die richtige Vorhersage getroffen hat oder die Prognose lediglich im Sinne einer sich selbst erfüllenden Prophezeiung als zutreffend angesehen werden muss, bleibt offen.[84] Selbst wenn ein Rückfall mit 75 prozentiger Wahrscheinlichkeit vorhergesagt werden könnte, bedeutet dies, dass in einem Viertel der Fälle die Bewährungsentscheidung die dem Algorithmus folgt, falsch ausfiele.[85]

Nicht zuletzt ist darauf hinzuweisen, dass keinesfalls ein allgemeingültiges Prognosemanual für alle Gruppen von Straftäter*innen existiert. So ermöglicht beispielsweise das auch in Deutschland verwendete Level of Service Inventory-Revised, im Rahmen der Prognose von Gewaltstraftäter*innen eine vergleichsweise verlässliche Prog-

75 *BGH*, StV 2010, 484 (485); *Dünkel*, NK-StGB, § 57 Rn. 123; *Belina*, Monatsschrift für Kriminologie und Strafrecht 2016, 85 (87); *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (39); *Schöch*, in: FS-Widmaier, S. 967 (958); *Singelnstein*, NStZ 2018, 1 (8); *Wisser*, American Criminal Law Review 2019, 1811 (1815).
76 *Ostendorf*, NK-StGB, § 56 Rn. 21; *Zweig*, S. 25; *Ernst*, JZ 2017, 1026 (1028); *Schneider*, StV 2006, 99 (102).
77 *Bilski/Schmid*, NJOZ 2019, 657 (658); *Boetticher/Dittmann/Nedopil/Nowara/Wolf*, NStZ 2009, 478 (579).
78 *Schneider*, StV 2006, 99 (101).
79 *Adams/Kury*, Forum Strafvollzug 2010, 81 (86); *Cukier/Mayer-Schönberger*, Wirtschaftswoche 2013, 94 (97); *Grube*, Jura 2010, 759 (762).
80 *Zweig*, S. 26; *Zweig/Krafft*, in: Mohabbat Kar/Thapa/Prycek, S. 221.
81 *Egbert*, APuZ 2017, 17 (21).
82 Anteil der Rückfälligen an einer bestimmten Population.
83 *Dünkel*, NK-StGB, § 57 Rn. 112.
84 *Bock*, StV 2007, 269 (272); *Cukier/Mayer-Schönberger*, Wirtschaftswoche 2013, 94 (96); *Egbert*, APuZ 2017, 17 (21); *Fröhlich/Spiecker*, Können Algorithmen diskriminieren?, Verfassungsblog 2018, abrufbar unter: https://verfassungsblog.de/koennen-algorithmen-diskriminieren/ (zuletzt abgerufen am 18.10.2019); *Krüger/Lischka*, in: Mohabbat Kar/Thapa/Prycek, S. 440 (444).
85 *Cukier/Mayer-Schönberger*, Wirtschaftswoche 2013, 94 (96); *Egbert*, APuZ 2017, 17 (19); *Singelnstein*, NStZ 2018, 1 (3).

nose. Schon bei der Anwendung auf muslimisch geprägte Gewalttäter*innen, ist eine überzufällige Prognose jedoch nicht mehr möglich.[86] Ein entsprechender Algorithmus müsste demnach zunächst die Kulturangehörigkeit des/r Probanden*in ermitteln, und erst danach eine Prognose anhand von kulturspezifisch ausgewählten Merkmalen erstellen, und somit je nach Kulturzugehörigkeit etc. unterschiedliche Voraussetzungen an eine positive Legalprognose stellen. Die Erstellung einer zuverlässigen Prognose würde daher zwangsläufig zu einer erheblichen Diskriminierung führen.

4. Weitere grundgesetzliche Fragestellungen

Die Kriminalprognose wird anhand einer Vielzahl von persönlichen Daten des Probanden erstellt.[87] So erfasst beispielsweise das System COMPAS nicht nur die Vorstrafen des/r Angeklagten, sondern auch Vorstrafen von Familienangehörigen, Erkenntnisse über Alkohol- oder Drogenmissbrauch in der Familie, soziale Bindungen des/r Probanden*in, der Umgang mit sog. „anti-sozialen" Freunden und Bekannten, Schulden, häufige Wohnort- oder Beschäftigungswechsel, Tendenzen zu Wut oder Aggression sowie eine kognitive Verhaltensprognose.[88] Insofern wird eine massive Beeinträchtigung des Allgemeinen Persönlichkeitsrechts sowie des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und das Recht auf Schutz von persönlichen Daten und auf Vergessen (Art. 8 GRCh) befürchtet.[89] Allerdings ist bei der Bestimmung der Eingriffsintensität zu berücksichtigen, dass der/die Angeklagte selbst den Anlass zur Erhebung und Auswertung der Daten geschaffen hat.[90] Zugleich handelt es sich bei den erfassten Daten jedoch um besonders sensible Informationen, die durch die digitale Verknüpfung im Rahmen eines algorithmischen Systems den Nutzer des Systems in die Lage versetzen spezifische Persönlichkeits- und Verhaltensprofile der Proband*innen zu erstellen.[91] Zumindest erscheint daher die Schaffung einer gesetzlichen Grundlage, die den legitimen Zweck für den Einsatz derartiger Systeme hinreichend konkretisiert, mithin die umfassende und unbedachte Verwendung limitiert, bestimmt, welche Daten in welchem Umfang verarbeitet werden, eine Löschung der Daten nach einem bestimmten Zeitraum zwingend vorsieht und Daten weitgehend anonymisiert, zwingend erforderlich.[92]

Auch das oben angeführte Argument der besseren Nachvollziehbarkeit und Transparenz ist vor dem Hintergrund neuerer technischer Entwicklungen nicht tragfähig. Die Entscheidungsfindungen komplex arbeitender Algorithmen, insbesondere sofern Deep Learning Systeme auf Basis neuronaler Netze eingesetzt werden, ist für den Menschen, zumindest nach dem derzeitigen wissenschaftlichen Kenntnisstand, nicht nachvollziehbar (Black-Box Phänomen). Das Ergebnis des Algorithmus ist weder überprüfbar, noch für die Proband*innen verständlich.[93] Auch wenn es in Deutschland nicht vorstellbar ist, dass der dem Algorithmus zugrunde liegende Code nicht öffentlich zugänglich gemacht wird, wie im Fall von COMPAS,[94] schafft ein extrem komplexer und sich zudem ständig

86 *Dahle/Schmidt*, Forensik/Psychiatrie/Psychologie/Kriminologie 2014, 104 (109); ähnlich: *Ostendorf*, in: NK-StGB, § 56 Rn. 21; *Bock*, StV 2007, 269 (272).
87 *Dahle/Lehmann*, Forensik/Psychiatrie/Psychologie/Kriminologie 2018, 37 (38).
88 *Ziegler*, c't 2017, 68 (68).
89 *Härtel*, LKV 2019, 49 (52, 53); *Martini*, DVBl 2014, 1481 (1483/1484); *Singelnstein*, NStZ 2018, 1 (6); *Werner*, NJOZ 2019, 1041 (1042, 1043).
90 *Härtel*, LKV 2019, 49 (55); *Singelnstein,* NStZ 2018, 1 (6).
91 *Härtel*, LKV 2019, 49 (55); *Martini*, DVBl 2014, 1481 (1483).
92 *Härtel*, LKV 2019, 49 (55); *Werner*, NJOZ 2019, 1041 (1042, 1043).
93 *Martini*, S. 27; *Bilski/Schmid*, NJOZ 2019, 657 (659); *Ernst*, JZ 2017, 1026 (1036); *Herberger*, NJW 2018, 2825 (2828); *Gless*, in: GS-Weßlau, S. 167 (171); *Müller/Pöchhacker* S. 158; *Wisser*, American Criminal Law Review 2019, 1811 (1812).
94 *Müller/Pöchhacker*, S. 164.

veränderner, da lernender Algorithmus mithin keine Nachvollziehbarkeit. Damit ist die Entscheidung nicht hinreichend rechtlich überprüfbar und mithin nicht mit dem Rechtsstaatsprinzip Art. 20 Abs. 3 GG und dem Recht auf effektiven Rechtsschutz Art. 19 Abs. 4 GG vereinbar.[95]

Vor dem Hintergrund der fehlenden Überprüfbarkeit ergibt sich noch ein weiterer Problemkreis: Diskriminierungen auf Grund von Programmierungsfehlern in dem zugrundeliegenden Code oder einer unzureichenden Auswahl der Trainingsdaten sind nur schwer sichtbar zu machen und werden vielfach jahrelang nicht bemerkt. Insoweit besteht insbesondere die Gefahr der Reproduktion von praktischen Relevanzen, impliziten oder expliziten Vorurteilen, sowie die Verzerrung der Datenanalyse (Algorithmic Bias).[96] Dieser Effekt wird noch dadurch verstärkt, dass einem Algorithmus keine ethische Orientierung immanent ist, sodass in der empirischen Datenbasis bestehende Korrelationen unreflektiert in den Code aufgenommen werden.[97] Ein Algorithmus ist nicht in der Lage zwischen Korrelation und Kausalität zu unterscheiden (Cum-hoc-ergo-propter-hoc Fehlschluss).[98] So steht beispielsweise mittlerweile fest, dass COMPAS Angeklagte mit dunkler Haut systematisch diskriminiert, obwohl die Hautfarbe oder Ethnie des Individuums nie in das System eingegeben worden ist.[99] Derartige diskriminierende Entscheidungen sind nicht zuletzt vor dem Hintergrund des Art. 3 GG selbstverständlich nicht hinnehmbar.[100]

Die Reproduktion von Vorurteilen kann weiterhin dazu führen, dass bestimmte Personen kategorisch durch das System benachteiligt werden. Dies ist zwar grundsätzlich auch bei einer vorurteilsbehafteten Person, die eine Entscheidung trifft denkbar, allerdings erlangt ein algorithmenbasiertes System einen weit größeren Einflussbereich als ein/e einzelne/r Richter*in, sodass nicht nur einmalig die Chance des/r Probanden/in auf eine positive Aussetzungsentscheidung beeinträchtigt wird, sondern er/sie gänzlich von der Chance einer positiven Prognose ausgeschlossen wird.[101] Die bei der Anwendung des Systems COMPAS zu Tage getretenen diskriminierenden Entscheidungen beruhen zudem auf einem statistischen Dilemma. Einem Algorithmus ist es mathematisch nicht möglich, objektive Fairness einzuhalten, wenn bestimmte Eigenschaften (Geschlecht/Hautfarbe) in den durch das Manual erfassten Gruppen unterschiedlich oft vorkommen.[102]

Probleme ergeben sich auch im Hinblick auf die richterliche Unabhängigkeit Art. 97 GG. Der/Die Richter*in muss die Möglichkeit der Wahrscheinlichkeitsprognose überprüfen und die vorgenommenen Wertungen nachvollziehen können. Dies ist in komplexen und intransparenten Systemen gerade nicht der Fall.[103] Zumindest müsste der/die einzelne Richter*in über fundiertes Wissen zur Bewertung der statistisch generierten Prognosewerte verfügen. Dies ist bislang nicht die Regel und würde umfassende Fortbildungsmaßnahmen notwendig machen.[104]

---

95 *Martini*, S. 40; Martini, DVBl 2014, 1481 (1489); *Singelnstein*, NStZ 2018, 1 (7); *Tinnefeld*, ZD 2019, 333 (333); *Werner*, NJOZ 2019, 1041 (1043).

96 *Ernst*, JZ 2017, 1026 (1029); *Gless*, in: GS-Weßlau, S. 176 (172); *Härtel*, LKV 2019, 49 (55); *Müller/Pöchhacker*, S. 166; *Werner*, NJOZ 2019, 1041 (1042).

97 *Zweig*, S. 26; *Bilski/Schmid*, NJOZ 2019, 657 (658); *Werner,* NJOZ 2019, 1041 (1042).

98 *Martini*, S. 60; *Belina*, Monatsschrift für Kriminologie und Strafrecht 2016, 85 (96).

99 *Angwin/Larson/Mattu/Kirchner*, ProPublica 2016 machine Bias – There's software used across the country to predict future ciminals. And it's biased against blacks; Zweig, S. 31; *Härtel*, LKV 2019, 49 (55); *Ziegler*, c't 2017, 68 (69).

100 *Tinnefeld*, ZD 2019, 333 (333); *Werner*, NJOZ 2019, 657 (659).

101 *Martini*, S. 89; *Zweig*, S. 28; *Zweig/Krafft*, in: Mohabbat Kar/Thapa/Prycek, S. 204 (208).

102 *Martini*, S. 55, 56; Zweig/Krafft, in: Mohabbat Kar/Thapa/Prycek, S. 214.

103 BVerfGE 109, 130 (164); *Boetticher/Kröber/Müller-Isberner/Böhm/Müller-Metz/Wolf*, NStZ 2006, 537 (539); *Boetticher*, Forensische Psychiatrie und Psychotherapie 2009, 3 (4).

104 *Boetticher/Dittmann/Nedopil/Nowara/Wolf*, NStZ 2009, 478 (579); *Gless*, in: GS-Weßlau, S. 176 (171); *Schneider*, StV 2006, 99 (102).

V. Schlussbetrachtung

Bislang finden algorithmenbasierte Entscheidungssysteme bei Bewährungsentscheidungen in der Praxis deutscher Gerichte noch keine Anwendung. Die Vorteile liegen jedoch auf der Hand. Die Anwendung einer wissenschaftlich basierten Prognosemethode, die allen Betroffenen die gleiche Chance auf eine positive Aussetzungsentscheidung ermöglicht, ist erstrebenswert. Zudem ermöglicht das Generieren eines prozentualen Wahrscheinlichkeitswertes die vergleichsweise einfache Subsumtion unter das gesetzlich bestimmte Tatbestandsmerkmal. Fest steht allerdings auch, dass bei einer Verwendung algorithmenbasierter Prognosemanuale eine neue Form der Expertise insbesondere bei Richter*innen gewährleistet sein muss. Nur so können die ermittelten Werte gewinnbringend nachvollzogen und für eine individuelle Prognose, wie vom BVerfG und BGH gefordert, nutzbar gemacht werden.[105] Gleichzeitig ergeben sich vielfältige Probleme und Risiken bei der Nutzung derartiger Prognosetools. Zunächst ist festzuhalten, dass algorithmenbasierte Instrumente nur im Rahmen von Extremfällen eindeutige Ergebnisse produzieren können. Der Einsatz dieser ist daher bereits systemimmanent beschränkt. Auch das Spannungsfeld zwischen dem Eingriff in die datenschutzrechtlichen Grundrechte des Betroffenen und der Erforderlichkeit hinreichend aussagekräftiger Datenmengen zur Erzeugung verwertbarer Prognosen, lässt sich nicht auflösen. Solange jedoch die komplexen Strukturen der Prognoseinstrumente nicht hinreichend transparent gemacht werden können, diese sich jeder Nachprüfung entziehen und gegebenenfalls jahrelang unbemerkt diskriminierende Entscheidungen treffen, kann ein umfassender Einsatz solcher Instrumente vor dem Hintergrund der grundgesetzlichen Wertungen nicht verantwortet werden.[106]

Allerdings ermöglichen auch herkömmliche Prognosemethoden, wie erörtert, keine vorzugswürdige Alternative. Deshalb sollte ein alternatives Regelungsmodell zumindest in Betracht gezogen werden. So wird teilweise vorgeschlagen, vor dem Hintergrund hoher Falsch-Positiv-Raten und der Erkenntnis, dass durch den Freiheitsentzug im besten Fall eine Nichtwirkung, in der Regel aber ein kontraproduktiver Effekt erwartet werden muss,[107] gegebenenfalls gänzlich von einer Wahrscheinlichkeitsprognose abzusehen und vorrangig normative Kriterien für Aussetzungsentscheidungen gesetzlich zu verankern.[108]

[105] Müller/Pöchhacker, S. 175.
[106] so auch: *Urbaniok*, S. 263; *Wisser*, American Criminal Law Review 2019, 1811 (1815); *Zweig/Krafft*, in: Mohabbat Kar/Thapa/Prycek, S. 204 (219).
[107] *Jasch*, KJ 2014, 237 (238).
[108] *Dünkel*, in: NK-StGB, § 57 Rn. 28, 112, 114.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

David Heger

Big Data und die Unschuldsvermutung

Inhaltsverzeichnis

I. Einleitung

Die neuen digitalen Datensammlungs- und Auswertungsmöglichkeiten ermöglichen eine breite Überwachung und die Anwendung von ausgefeilten Prognosetechniken schon weit vor der Straftatbegehung, wie auch im Gerichtsprozess. Im Namen der Sicherheit der Allgemeinheit geraten dabei immer mehr Menschen ins Visier der Strafverfolgungsbehörden. Dieser Tendenz steht die strafprozessrechtliche Unschuldsvermutung gegenüber. Die Seminararbeit untersucht, ob und inwieweit der wichtige strafprozessuale Grundsatz durch die Einsatzmöglichkeiten von Big Data erstens in der (vorsorgenden) Strafverfolgung, zweitens in der Gefahrenabwehr und drittens im Gerichtsverfahren gefährdet ist. Darüber hinaus wird die Frage gestellt, ob die Unschuldsvermutung, neben einer rein formal-rechtlichen, auch eine übergeordnete gesellschaftliche Bedeutung hat. Dieser Aspekt der Unschuldsvermutung wird viertens in der Beobachtung einer tendenziellen Verschiebung des Rechtsstaates in Richtung eines proaktiven Präventivstaates relevant.

II. Unschuldsvermutung

Eine Normierung der Unschuldsvermutung findet sich etwa in Art. 6 Abs. 2 EMRK: „Jede Person, die einer Straftat angeklagt ist, gilt bis zum gesetzlichen Beweis ihrer Schuld als unschuldig."

Verfassungsrechtlich wird die Unschuldsvermutung unterschiedlich abgeleitet: So wird die Unschuldsvermutung als Ausprägung der Menschenwürde, Art. 1 Abs. 1 GG und dem darin enthaltenen Schuldprinzip gesehen.[1] Andere sehen in der Unschuldsvermutung eine Spezifikation des Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[2] Nach dem *BVerfG* ergibt sich die Unschuldsvermutung aus dem Rechtsstaatsprinzip, Art. 20 Abs. 3 GG i.V.m. Art. 28 Abs. 1 S. 1 GG.[3] Diese Ansicht lässt sich auch mit anderen Grundrechtstheorien in Einklang bringen.[4] Zusätzlich wird in der Unschuldsvermutung eine Sicherung des Systems gesehen: Die Grundvorstellung eines Rechtsstaates beinhalte das grundsätzliche Vertrauen des Staates in die Rechtsbefolgung der Bürger im Gegensatz zum Polizeistaat, der als zentrales Element Misstrauen gegen die Bürger pflege.[5]

Umstritten ist die Rolle der Unschuldsvermutung außerhalb des Gerichtsprozesses, also etwa in Ermittlungs- und Gefahrenabwehrmaßnahmen. So wird vertreten, dass die Unschuldsvermutung als ein rein menschliches Problem ausschließlich ein Pol bei der richterlichen Überzeugungsbildung sei, der gegenüber dem Tatverdacht stehe. Nur wenn der Tatverdacht die Unschuldsvermutung verdrängen würde, könnte das Urteil gesprochen werden. Dies gebiete zu einer „vornehmen Verhandlungsführung" im Gerichtsprozess.[6] Anders wird die Unschuldsvermutung als ein rein rhetorisches Kuriosum interpretiert, denn wenn jemand vor Gericht angeklagt ist, wird eben nicht vermutet, dass diese Person unschuldig ist.[7] Das Spektrum der Meinungen reicht bis zu der Ansicht, nach der die Unschuldsvermutung als fundamental für das neuzeitliche Zusammenleben steht. Demnach sei die Unschuldsvermutung eine Kanalisierung von abweichendem Verhalten und umfasse somit alle Aspekte des gesellschaftlichen Zusammenlebens.[8] Da etwa im Ermittlungsverfahren die öffentliche Sicherheit ein legitimes Ziel sei, das mit der

1 *Sax*, in: Bettermann/Nipperdey/Scheuner, Die Grundrechte, Band HI/2, 1959, S. 987.
2 *Kühl*, Unschuldsvermutung, Freispruch und Einstellung, 1983, S. 20; *Lindner*, AöR 2008, 235 (253).
3 *Creifelds*, Rechtswörterbuch, 23. Auflage (2019), Unschuldsvermutung; BVerfGE 35, 311 (320); BVerfGE 82, 106 (114).
4 *Stuckenberg*, Untersuchungen zur Unschuldsvermutung, 1998, S. 50.
5 *Weßlau*, Vorfeldermittlungen, 1989, S. 300.
6 *Sax,* S. 971.
7 *Fletcher,* UCLA Law Review 1968, 1203 (1203, 1222).
8 *Marxen*, GA 1980, 365 (373 f.).

Unschuldsvermutung in Einklang gebracht werden müsse, sei eine relative Unschuldsvermutung dadurch gegeben, dass durch die Verhältnismäßigkeit bereits eine Steuerungsfunktion gegeben sei.[9] Nach einer anderen Ansicht soll eine Grundrechtsschonung nur aus dem Verhältnismäßigkeitsprinzip, dem Fair-Trial-Prinzip und dem Teilhaberecht des Beschuldigten entspringen und eben nicht aus der Unschuldsvermutung geboten sein.[10]

Das *BVerfG* will keine Konkretisierung der aus der Unschuldsvermutung folgenden Verbote und Pflichten vornehmen. Dies sei vielmehr Aufgabe des Gesetzgebers, in Einbeziehung der sachlichen Gegebenheiten.[11] Es bezieht aber in Fällen, in denen die Unschuldsvermutung Strafverfolgungsinteressen gegenübersteht, die Unschuldsvermutung im Rahmen der praktischen Konkordanz in die Abwägung mit ein.[12] Derweil sieht das *BVerwG* keine Anwendung der Unschuldsvermutung in der Gefahrenabwehr, wenn die Maßnahme keine (repressive) Strafe darstellt oder eine individuelle Schuldzuweisung enthält, sondern ausschließlich (präventiv) der Abwehr spezifischer Gefahren dient.[13] Für eine solche Auslegung spricht, dass es in der Gefahrenabwehr nicht um die Schuldfrage geht, sondern um Präventivmaßnahmen, für die auch ein komplett unverantwortlicher Nichtstörer herangezogen werden könnte.[14] Die Unschuldsvermutung schützt den Beschuldigten auch vor Maßnahmen, die Schuldspruch oder Strafe gleichkommen, denen aber kein rechtstaatlich prozessordnungsgemäßes Verfahren zur Schuldfeststellung vorausgegangen ist.[15] Die Unschuldsvermutung hat also einen formalen Anwendungsbefehl im Strafprozess, darüber hinaus aber auch einen materiell-grundrechtlichen Schutz. Daraus wird auch das Abstandsgebot von präventiv- zu strafrechtlichen Rechtsfolgen abgeleitet.[16]

Im Ergebnis ist die Unschuldsvermutung eine Konkretisierung des Übermaßverbotes in der Verhältnismäßigkeit. Sprachlich nähern sich daher *Roxin/Schünemann* treffenderweise an die Unschuldsvermutung an: Was einem Unschuldigen schlechterdings nicht als Aufopferung im öffentlichen Interesse zugemutet werden könne, dürfe auch einem noch so dringend Tatverdächtigen nicht zugeführt werden.[17] Des Weiteren darf auch ein Verdächtiger nicht willkürlich ungleich gegenüber einem Nichtverdächtigen behandelt werden, allein ein über den Tatverdacht hinausgehender Grund könne die besondere Belastung begründen.[18] In der Gefahrenabwehr gilt die Unschuldsvermutung grundsätzlich nicht, es sei denn, sie erreicht einen, mit einer Strafe gleichwertigen, pönalen Charakter.

III. Big Data

Die Definition von Big Data besteht aus zwei Elementen: Es geht erstens um große Datensätze, die zweitens von einer Technologie ausgelesen werden.[19] Einerseits lässt sich durch Big Data ein Mensch in Echtzeit nahezu vollständig überwachen und sein psychisches Befinden aus diesen Daten ablesen.[20] Andererseits kann Big Data durch

9 *Lindner*, AöR 2008, 235 (253, 259).
10 *Wolter,* in: Eser, Strafrechtsreform in Polen und Deutschland, Untersuchungshaft, Hilfeleistungspflicht und Unfallflucht, 1991, S. 89.
11 BVerfGE 82, 106 (115); Vgl. *Stuckenberg, ZStW* 1999, 422 (428 f.).
12 Vgl. *BVerfG*, NJW 1966, 243 (244); *Lindner,* AöR 2008, 235 (251, 253 f.).
13 Vgl. *BVerwG,* BeckRS 2016, 42102.
14 *Staudinger,* Welche Folgen hat die Unschuldsvermutung im Strafprozess?, 2015, S. 133.
15 BVerfGE 74, 358 (370 f.).
16 Vgl. BVerfGE 109, 133 (157 f.).
17 *Roxin/Schünemann*, Strafverfahrensrecht, 29. Auflage (2017), § 11 Rn. 3; BVerfGE 74, 358 (373 f.); Vgl. auch *Frister*, Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1998, S. 108; *Gropp*, JZ 1991, 804 (804, 807 f.).
18 *Gropp*, JZ 1991, 804 (807 f.).
19 *Ward/Barker*, Undefined By Data: A Survey of Big Data Definitions, 2013, S. 2, abrufbar unter; https://arxiv.org/pdf/1309.5821.pdf (zuletzt abgerufen am 27.5.2020).
20 Frankfurter Allgemeine Zeitung: Der Gläserne Mensch, 9.6.2013, abrufbar unter: https://www.faz.net/aktuell/wirtschaft/internet-der-glaeserne-mensch-12214568.html (zuletzt abgerufen am 27.5.2020).

Korrelationen von vergangenem Verhalten mit statistischen Wahrscheinlichkeiten auch eine Prognose für zukünftiges Verhalten abgeben[21], oder die Gefährlichkeit von Orten bewerten.[22] Relevant für die rechtliche Betrachtung werden also zwei Prozesse: erstens die Sammlung von Daten und zweitens die Verwertung der gesammelten Daten.

IV. Big Data in der (vorsorgenden) Strafverfolgung

Für Big-Data-Anwendungen in der Strafverfolgung muss der Staat zwingend auf Daten zugreifen, die durch Kommunikations-[23] und Freiheitsgrundrechte[24] geschützt werden. Durch eine zu expansive Überwachung kann die Verhaltensweise der Bürger beeinflusst werden und somit würde insbesondere das Freiheitsgrundrecht aus Art. 2 Abs. 1 GG beeinträchtigt.[25] So können beispielsweise psychische Krankheiten als Folge von ständiger Überwachung auftreten.[26] Dem gegenüber steht eine aktive Strafverfolgung, die im Sinne des Rechtsguts Sicherheit gewährleistet werden muss.[27] Unter dem Stichwort „Strafverfolgungsvorsorge" werden immer neue, umstrittene Maßnahmen auch gegenüber Unverdächtigen eingeführt, um (zukünftige) Straftaten besser aufklären zu können.[28] Auch greift die Polizei gerade in den USA bisweilen auf Daten Privater zurück, um Big-Data-Programme „zu füttern".[29] In Konflikt mit der Unschuldsvermutung geraten diese Rechte insbesondere dann, wenn das Interesse des Betroffenen wesentlich höher ist als das Strafverfolgungsinteresse[30] und damit ein ungerechtfertigtes Sonderopfer erbracht wird. Dabei sind dann höhere Eingriffsbedingungen für die Informationsbeschaffung zu stellen, je weiter die Maßnahme in das Vorfeld möglicher Rechtsgutsbeeinträchtigungen vorverlagert ist[31] und je nach Rang des Rechtsguts.[32] Bei verdachtslosen, aber individualisierbaren überwachungstechnischen Maßnahmen wäre die Rechtsgutbeeinträchtigung entsprechend sehr groß. Bei expansiver Anwendung dessen kehrt sich die Unschuldsvermutung in eine generelle Schuldvermutung um, da jeder behandelt werden würde, als wäre er potenziell Verdächtiger, und nicht grundsätzlich als Unschuldiger gelten würde. Die gebotene Zurückhaltung widerspricht gerade dem Prinzip von Big Data, bei dem – wie der Name schon sagt – erst durch Quantität eine Qualität der Daten geschaffen wird. Dagegen wird mit einer umgedrehten Logik argumentiert: Aufgrund der Unschuldsvermutung unterschieden sich Nichtverdächtige und Verdächtige nicht wesentlich – beide würden als unschuldig gelten und dürfen Adressat gleicher Maßnahmen sein.[33] Jedoch entgeht dieser Meinung, dass nicht die Verdächtigen damit den Unverdächtigen gleichgestellt werden würden, sondern Unverdächtigen willkürlich und massenhaft

21 *Shapiro*, Bauwelt Nr. 6 2007, 48 (49).
22 *Shapiro*, Bauwelt Nr. 6 2007, 48 (50).
23 Insbesondere das Fernmeldegeheimnis, Art. 10 GG.
24 Insbesondere das allgemeine Freiheitsgrundrecht, Art. 2 Abs. 1 GG, sowie das aus Art. 2 Abs. 1 i.V.m. Art. 1 GG entwickelte Recht auf informationelle Selbstbestimmung. Zu diesem betont das *BVerfG* in seinem Volkszählurteil die Wichtigkeit von Transparenz und begrenzter Datensammlung und -nutzung für die Entfaltung der Persönlichkeit: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung […] nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus." (BVerfGE 65, 1 [43 f.]).
25 *Eschelbach*, in: Institut für Kirche und Gesellschaft, Gefährdet Big Data unsere Demokratie?, 2007, S. 5, abrufbar unter: https://vdw-ev.de/wp-content/uploads/2016/11/2016.10_bigdata_vortrag_eschelbach.pdf (zuletzt abgerufen am 27.5.2020).
26 *Eschelbach*, S. 5.
27 *Staudinger*, S. 132 f.
28 Neben den klassischen erkennungsdienstlichen Behandlungen nach § 81b StPO derweil teils umstrittene Gesetze erlassen, wie etwa die Speicherung von „genetischen Fingerabdrücken" in der DNA-Analysedatei nach § 81g StPO oder die weiter unten benannte Diskussionen um die Vorratsdatenspeicherung. Auch werden bereits vorhandene Befugnisse der Polizei stärker genutzt werden, etwa beim Ausbau von Videohardware (Antwort des Ministeriums Inneres und Heimat vom 3.9.2018 – hib 638/2018).
29 *Singelnstein*, NStZ 2018, 1 (2).
30 *Frister*, S. 108; vgl. auch *Roxin/Schünemann*, § 11 Rn. 3.
31 *Singelnstein*, NStZ 2018, 1 (6).
32 BVerfGE 115, 320 (345 ff.); *BVerfG* NJW 2010, 833 (841).
33 Vgl. *Rogall*, Fachtagung zur Vorratsdatenspeicherung am 17.9.2007 in Berlin.

ein gewisser Verdachtsgrad auferlegt würde, und sich damit ohne Grund von – dann fiktionalen – Unverdächtigen abhebt. Die aus der Unschuldsvermutung abgeleitete grundsätzliche Gleichbehandlungspflicht von Unverdächtigen und Verdächtigen wird bei einem Generalverdacht durch die de facto Auflösung der Kategorie des Unverdächtigen ausgehöhlt. Damit würde auch die Pflicht, Maßnahmen nicht alleine auf den Verdacht zu stützen, sondern weitere Gründe hinzuzuziehen[34], umgangen werden. Somit sind Maßnahmen, die einen Generalverdacht verkörpern, nicht mit der Unschuldsvermutung vereinbar.

1. Vorratsdatenspeicherung

Besonders gut lässt sich das Zerren zwischen den Freiheitsrechten des Bürgers, der als unschuldig gilt, und dem Sicherheitsbedürfnis bei der Vorratsdatenspeicherung beobachten. Gemeint sind dabei Gesetze, die private Firmen zwingen, die Daten ihrer Nutzer für eine gewisse Zeit zu speichern, um diese potentiell für die Strafverfolgung nutzen zu können. In Rumänien hat das Verfassungsgericht das Vorratsdatenspeicherungsgesetz annulliert, da es alle Bürger als potenzielle Straftäter sieht und dadurch zu „exzessiv" sei. Es wurde für nicht mit der Unschuldsvermutung vereinbar erklärt.[35] In anderen Urteilen wird zwar nicht die Unschuldsvermutung direkt angesprochen, jedoch werden die weiten Grundrechtseinschränkungen in der Verhältnismäßigkeit mit den sicherheitspolitischen Zielen kritisch gesehen. So urteilte der *EuGH*, dass die Vorratsdatenspeicherung zu einem Grundrechtseingriff bei fast der gesamten europäischen Bevölkerung führen würde.[36] Das *BVerfG* sieht als Voraussetzung einer unmittelbare Nutzung der Daten, dass genau gesetzlich spezifizierte Fälle schwerster Kriminalität vorliegen müssen.[37] Sonst sei der Schaden, der durch die Überwachung der Bürger entstehe, nicht mit dem Nutzen für die Sicherheit aufgewogen.[38] Im Ergebnis entschieden die Gerichte gegen die Verhältnismäßigkeit.[39] Eine europarechtliche Überprüfung des Nachfolgegesetzes steht noch aus.[40] Neben dem Eingriff in die Rechte vieler Bürger wird auch kritisiert, dass auf der anderen Seite die Erfolgsrate der Vorratsdatenspeicherung als alleinige Maßnahme äußerst gering ist: Nur eine Hand voll zusätzlicher Fälle könnten so aufgeklärt werden.[41]

2. Videoüberwachung

Auch der Ausbau von staatlicher und privater Videoüberwachung hat in den vergangenen Jahren immer weiter zugenommen. Mancherorts kann man die Bewegung eines Menschen komplett nachvollziehen, da es keine blinden Orte mehr gibt.[42] Während es bei bloßen Übersichtsaufnahmen weiterhin umstritten ist, ob diese einen Grund-

34 *Gropp*, JZ 1991, 804 (807 f.).
35 Rumänisches Verfassungsgericht, Entscheidung Nr. 158, 298/2008, deutsche Übersetzung aufrufbar unter: http://www.vorratsdatenspeicherung.de/content/view/342/1/lang,de/#Urteil (zuletzt abgerufen am 27.5.2020).
36 *EuGH* NJW 2014, 2169 (2172 f.) zur Beurteilung der Richtlinie 2006/24, die der Vereinheitlichung der Vorratsdatenspeicherung dienen sollte. Das Gericht sah dies als ein Verstoß gegen Art. 7 EuGrdRCh (Achtung des Privatlebens) und Art. 8 EuGrdRCh (Schutz personenbezogener Daten), da die Richtlinie hinsichtlich dieser Rechte nicht auf das Notwendigste beschränkt wurde, *EuGH* NJW 2014, 2169 (2170 ff.).
37 *BVerfG,* NJW 2010, 833 (841 f.).
38 A.a.O.
39 *BVerfG,* NJW 2010, 833 (837 ff.); *EuGH,* NJW 2014, 2169 (2172 ff.).
40 Pressemitteilung des BVerwG Nr. 66/2019 vom 25.9.2019; Netzpolitik.org: Bundesverwaltungsgericht: Die Vorratsdatenspeicherung bleibt weiter ausgesetzt, 25.9.2019, abrufbar unter: https://netzpolitik.org/2019/bundesverwaltungsgericht-die-vorratsdatenspeicherung-bleibt-weiter-ausgesetzt/ (zuletzt abgerufen am 27.5.2020).
41 Süddeutsche Zeitung: Studie schürt Zweifel an Vorratsdatenspeicherung, vom 27.2.2012, abrufbar unter: https://www.sueddeutsche.de/digital/streit-um-ueberwachung-studie-zweifelt-am-nutzen-der-vorratsdatenspeicherung-1.1268529 (zuletzt abgerufen am 27.5.2020).
42 *Szuba*, Vorratsdatenspeicherung, 2011, S. 180.

rechtseingriff darstellen, wird bei Aufnahmen, die eine Identifikation möglich machen oder genau auf die Identifikation abzielen, in das Recht auf informationelle Selbstbestimmung eingegriffen.[43] Gerade eine uneingeschränkte, umfassende videotechnische Überwachung, die einen *gläsernen Menschen* zur Folge hätte, ist – im Gegensatz zu den USA – in Deutschland schon nicht mit dem Verhältnismäßigkeitsgrundsatz zu vereinbaren.[44] Ein konkretes Beispiel, wie Videoüberwachung im öffentlichen Raum genutzt wurde, ist die Strafverfolgung im Nachgang zu den G20 Protesten in Hamburg. Die Hamburger Polizei nutzte die Bilder von öffentlichen Kameras sowie privater Smartphone- und Kameraaufnahmen, um anhand von biometrischen Profilen Täter zu identifizieren. Die Datenmenge belief sich dabei auf über 100 TB. Es wurden zum Großteil Aufnahmen friedlicher Demonstranten, aber auch am normalen Stadtverkehr teilnehmender Personen analysiert. Die Erfolgsquote fiel mit gerade einmal drei namentlich identifizierten Verdächtigen sehr gering aus.[45] Der Datenschutzbeauftragte Hamburgs stoppte darauf die Auswertung – wegen fehlender Rechtsgrundlage und dem Einschnitt in die Grundrechte von zu vielen Personen.[46]

3. Zwischenfazit

Bei der Datensammlung ist die Unschuldsvermutung insofern relevant, als dass sich plötzlich viele Unschuldige – Verdächtige wie Unverdächtige – in Ihren Grundrechten beschnitten sehen, teilweise ohne etwas von der Maßnahme zu wissen. Dabei gebietet die Unschuldsvermutung, dass nur aus einem konkreten Grund eingeschritten werden darf. Besonders kritisch muss also eine extensive Überwachung Unverdächtiger betrachtet werden, wenn eine Individualisierbarkeit gegeben ist. Im Falle der Videoüberwachung muss dem Unschuldigen ein Grad an *überwachungstechnischer Unsichtbarkeit* zustehen, um nicht zum dauerüberwachten gläsernen Menschen zu werden. Die Vorratsdatenspeicherung und ähnliche Maßnahmen müssen eine hohe Eingriffsschwelle bei der Abrufung garantieren, dass nicht alle Bürger unter einen Generalverdacht gestellt werden.

IV. Big Data in der Gefahrenabwehr

Anders als in den Ermittlungsmaßnahmen, ist in der Gefahrenabwehr nicht vergangenes, sondern die Prognose für zukünftiges Verhalten einschlägig. Traditionell orientiert sich dafür das Gefahrenabwehrrecht an der „konkreten Gefahr"[47], die konkrete Tatsachen für einen Eingriff voraussetzt. Werden anhand eines solchen Verfahrens präventive Maßnahmen ergriffen, entziehen sich solche dem Anwendungsbereich der Unschuldsvermutung. Erst wenn diese Maßnahmen einen bestrafenden Charakter haben und somit die Frage nach zukünftiger Schuld stellen, wird die Unschuldsvermutung ausgehöhlt.

43 *Bartsch*, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachung öffentlich zugänglicher Orte in Deutschland und in den USA, 2004, S. 102.
44 Vgl. *Bartsch*, S. 261.
45 Süddeutsche Zeitung: Streit um Gesichtserkennung: Innenbehörde reicht Klage ein, 15.1.2019, abrufbar unter: https://www.sueddeutsche.de/politik/datenschutz-hamburg-streit-um-gesichtserkennung-innenbehoerde-reicht-klage-ein-dpa.urn-newsml-dpa-com-20090101-190115-99-574653 (zuletzt abgerufen am 27.5.2020).
46 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, 2019, S. 23 ff.: Bzgl. dem quantitativen Einschnitten in die Rechte wird auf § 48 BDSG verwiesen: „Eine Strafverfolgung um jeden Preis, die in die Grundrechte einer unbestimmten Vielzahl von Personen eingreift und eine umfassende Kontrolle von Menschen durch Profilbildung ermöglicht, ist jedoch mit Blick auf den Grundsatz der Verhältnismäßigkeit […] nicht zulässig." Außerdem fehle der Bezug zur Tat.
47 Vgl. *Ebert*, LKV 2017, 10 (12); *Schenke*, JuS 2018, 505 (505).

1. Predictive Policing

Das bedeutendste Beispiel, bei dem sich die Polizei Big Data zur Gefahrenabwehr zunutze macht, ist Predictive Policing. Dabei analysiert ein Algorithmus die Daten von Orten oder Personen, um herauszufinden, welcher Ort am wahrscheinlichsten von einer Straftat betroffen sein wird bzw. welche Person diese wahrscheinlich ausführen wird.[48] In Deutschland sind die Erfahrungswerte mit ortsbasiertem Predictive Policing noch relativ neu, es wird aber immer öfter eingesetzt.[49] Derweil ist Predictive Policing in den USA schon ein fester Bestandteil der Sicherheitspolitik mit weiten Befugnissen.[50] Darüber hinaus wird dort die Gefahr mittlerweile auch nicht nur örtlich, sondern auch personenbezogen analysiert.[51] In der Gefahrenabwehr ist eine computergenerierte Prognose grundsätzlich ähnlich einer Prognose, die von einem Polizeibeamtem erstellt wurde, und damit nicht im Anwendungsbereich der Unschuldsvermutung.[52] Jedoch bedarf es im Gefahrenabwehrrecht dafür einer konkreten Sachlage,[53] die ein Algorithmus nicht liefern kann, da sie nur eine abstrakte Risikobewertung aufstellt.[54] Prognoseentscheidungen mit Predictive Policing bedürfen somit immer eines zweistufigen Einschreitens der Polizei: Die Polizei muss bei der Person oder dem Ort, die/der von Predictive Policing ermittelt wurde, erst nach einer konkreten Gefahr, also einer diese begründenden Tatsache, suchen, bevor sie Maßnahmen ergreifen darf.[55] Würde man die Gefahrenprognose nur auf Predictive Policing stützen, wüsste man nicht, auf welchen konkreten Daten diese basiert.[56]

Problematisch ist dabei die Vermassung der Daten in einer statistischen Wahrscheinlichkeit: Dadurch, dass die Polizei schon vor der Tat eingreift, ist ein *false positive*, also ein bei Predictive Policing recht häufig auftretender statistischer Ausfall, als Adressat der vorverlagerten polizeilichen Intervention möglich, lediglich, weil die betroffene Person zu einer statistisch *wahrscheinlichen* Gruppe gehört.[57] Dies kann aufgrund von reproduzierten und sich teilweise noch verstärkenden, diskriminierenden Tendenzen von Big Data dazu führen, dass bestimmte Bevölkerungsgruppen ungleich öfter als potenzielle, zukünftige Täter gelten.[58] Soweit ein rein personenbezogenes Predictive Policing zum Einsatz kommen sollte, ohne dass die Prognose durch weitere verdachtsbegründende Tatsachen ergänzt werden, könnte ein wegen der Unschuldsvermutung unzulässiges Sonderopfer einer Gruppe begründet werden, sollten grob unverhältnismäßige Rechtsfolgen daran anknüpfen. Die Maßnahme hätte mangels einer konkreten Tatsache einen repressiven Charakter. Denn sie würde auf einer für eine Gefahrenprognose unerheblichen, abweichenden Eigenschaften oder vergangenem Verhalten basieren, und wäre dabei keine qualifizierte

48 *Shapiro*, Bauwelt Nr. 6 2007, 48 (49 f.).

49 In Bayern und Baden-Württemberg wird etwa ein System namens PRECOBS eingesetzt, das den Ort von Wohnungseinbrüchen vorhersagen soll, *Shapiro* Bauwelt Nr. 6 2007, 48 (51); *Knobloch*, Vor die Lage kommen: Predictive Policing in Deutschland, 2018, S. 11 f. In Nordrhein-Westfalen gibt es das Pilotprojekt *Skala*, das auch weitere Verbrechensorte vorhersagen soll, und dabei größere Datenmengen benutzt, Shapiro Bauwelt Nr. 6 2007, 48 (51). Hessen und Hamburg haben bereits Gesetze verabschiedet, die den Einsatz von Programmen der Firma Plantir zulässt, und diese teils schon mit der Entwicklung von Software beauftragt hat. Die Firma ist u.a. wegen Verbindungen zu US-Geheimdiensten wie der NSA umstritten, dazu Netzpolitk.org: Hamburg: Juristinnen kritisieren „Palantir-Paragraf" im geplanten Polizeigesetz, 24.9.2019, abrufbar unter: https://netzpolitik.org/2019/hamburg-juristinnen-kritisieren-palantir-paragraf-im-geplanten-polizeigesetz/ (zuletzt abgerufen am 27.5.2020). Ähnliche Entwicklungen sind in den meisten Bundesländern zu beobachten, vgl. *Knobloch*, S. 14 f.

50 Vgl. *Singelnstein*, NStZ 2018, 1 (2): Die Polizeibehörden nutzen dort unterschiedliche Daten, wie etwa Social Media, Wetter, sozioökonomische Daten, Wohnorte vorbestrafter Straftäter u.a. um eine genauere Standortbestimmung als Prognose zu erhalten.

51 So experimentiert zum Beispiel die Polizeibehörde in Boston mit Algorithmen, die die Social Media Auftritte von Verdächtigen auswerten und diese dann auf Beobachtungslisten setzen oder priorisieren, *Perry/McInnis/Price/Smith/Hollywood*, Predictive Policing, 2013, S. 99 ff.

52 Vgl. *Knobloch*, S. 7.

53 Vgl. *Trurnit* in: Möstl/Trurnit, BeckOK-PolRBW, 17. Edition (2020), PolG § 1 Rn. 18.

54 *Singelnstein,* NStZ 2018, 1 (8 f.).

55 Vgl. *Singelnstein,* NStZ 2018, 1 (8).

56 *Gless,* in: Bayamlioğlu/Baliuc/Janssens/Hildebrandt, Being Profiled, 2018, Teil 3, S. 3.

57 Vgl. *Singelnstein*, NStZ 2018, 1 (5); *Ostermeier,* in: Puschke/Singelnstein, Der Staat und die Sicherheitsgesellschaft, 2018, S. 103 ff.; *Martini*, DVBI 2014, 1481 (1488).

58 *Singelnstein*, NStZ 2018, 1 (4); *Shapiro,* Bauwelt Nr. 6 2007, 48 (50 f.).

Prognose einer zukünftigen Straftat.

2. Bestrafung zukünftiger Täter

Schließen sich an solche Prognosen auch noch Maßnahmen, die Strafähnlichkeit haben, an, wird der Gerichtsprozess umgangen und somit die Schuldfrage der Tat vorangestellt. Dadurch wird gegen die Unschuldsvermutung verstoßen. Leichte Tendenzen gibt es in diese Richtung: So wurde etwa in der Neuordnung des Bayerischen Polizeirechts die Schwelle für Präventivgewahrsam gesenkt und die mögliche Dauer auf drei Monate erhöht, die theoretisch ins Unendliche erweitert werden könnte.[59] Eine zu lange Präventivhaft hätte einen pönalen Charakter und hinterginge so die Unschuldsvermutung, da diese eine Verurteilung ohne Schuldspruch nicht zulässt. Ein sozialethisches Werturteil entsteht etwa bei Haftmaßnahmen unabhängig davon, ob die Straftat verhindert wurde oder man ihrer verdächtig ist.[60] Eine zu lange Haft wäre ein mit der Unschuldsvermutung unvereinbares Sonderopfer.[61] Die Schwelle, an der eine Maßnahme präventiven Charakter hat und dabei subjektiv als Strafe angesehen wird, ist fließend.[62] Eine konkrete Bestimmung würde jedoch das Format dieses Aufsatzes übersteigen. Eine Bestrafung vor Tatbegehung würde auf einem deterministischen Menschenbild beruhen. Die Freiheit des Menschen, über sein Handeln selbst zu entscheiden, sei die Kehrseite menschlicher Verantwortlichkeit.[63] Freier Wille ist nur durch persönliche Schuld erreichbar. Wenn man sich nicht mehr entscheiden könne, ob man sich schuldig mache, könne man auch keine Schuld mehr haben.[64] Mit der Abkehr vom Schuldprinzip entfällt auch die Unschuldsvermutung. Der Bürger würde somit vom Rechtssubjekt zum Rechtsobjekt werden.[65] Auch würde eine Präventivhaft, die aufgrund einer Big-Data-Analyse angeordnet wurde, sich eher an einer Krisenfiktion als an einem konkreten Gefahrenpotential orientieren.[66] Somit ist ein Schuldspruch aufgrund von Prognosen sowie eine Präventivhaft, die durch ihre Länge bestrafenden Charakter erlangt, nicht mit der Unschuldsvermutung in Einklang zu bringen.

3. Zwischenfazit

In der Gefahrenabwehr kann Big Data neue Erkenntnisse für die Polizei liefern. Jedoch muss diese im Sinne der Unschuldsvermutung nach einen Verdacht begründenden, konkreten Tatsachen suchen, bevor sie präventiv einschreiten darf. Es bedarf also immer noch einer menschlichen Interpretation der Gefahrenlage anhand der konkreten Tatsachen.[67] Die Präventivhaft darf nur zeitlich begrenzt erfolgen, da sie sonst einer Strafe ohne Tat gleichkäme. Sorgen diesbezüglich bereiten die neuen Entwicklungen im Polizeirecht, da die Eingriffsschwelle in Richtung eines abstrakten Begriffs von Gefährdungslagen herabgesetzt wird, wodurch das Verdachtsmoment zwingend nach vorne verlegt wird.[68] Ein Beispiel ist die Einführung des Begriffs der drohende Gefahr im Bayerischen PAG.[69] Gleichzeitig wird die Präventivhaft ausgeweitet. Erreicht diese Entwicklung Strafcharakter, käme eine Bestrafung aufgrund einer vom Computer berechneten Krisenfiktion infrage. Eine damit begründete Haft würde

59 Vgl. Art. 18, 20 Nr. 3 BayPAG.
60 Vgl. *Lindner*, AöR 2008, 235 (246, 255, 259): Zur Untersuchungshaft als ethisch-moralisches Unwerturteil. Diese knüpft zwar wiederum an vergangenes Verhalten, hat aber als Haft die gleiche Außenwirkung wie eine Präventivhaft.
61 Vgl. *Wolter*, ZStW 1981, 452 (455) zur Haftdauer bei der Untersuchungshaft.
62 *Mayer-Schönberger,* Big Data – Chancen und Risiken der Prävention, in: Marks/Steffen, Prävention braucht Praxis, Politik und Wissenschaft, 2015, S. 383.
63 *Mayer-Schönberger,* in: Marks/Steffen, S. 383.
64 *Mayer-Schönberger,* in: Marks/Steffen, S. 383.
65 Vgl. etwa *Eschelbach*, S. 16.
66 Vgl. *Legnaro*, in: Brunhöber, Strafrecht im Präventionsstaat, 2014, S. 31.
67 Vgl. auch *Martini*, DVBI 2014, 1481 (1488 f.).
68 *Waechter*, NVwZ 2018, 458 (359).
69 Vgl. Art. 11 Abs. 3 BayPAG.

die Schwelle der Unschuldsvermutung überschreiten.

V. Nutzung von Big Data im Gerichtsverfahren

Unumstritten ist die Anwendung der Unschuldsvermutung im Gerichtsverfahren. Dort wird die Schuldfrage direkt gestellt. Wenn der Richter Zweifel an der Schuld des Angeklagten hat, hat er die Unschuldsvermutung anzuwenden, die besagt, dass der Angeklagte freizusprechen sei.[70] Jedoch ist hier die Unschuldsvermutung von der richterlichen Beweiswürdigung zu trennen: In dem Schritt, in dem aus Big Data gewonnene Erkenntnisse eine Rolle spielen könnten – wie etwa vom Computer durch Algorithmen generiertes Scoring – fließen diese als Indizien oder Beweise ein. Daraus leitet der Richter Tatsachen ab, wobei er nur seiner persönlichen, subjektiven Gewissheit unterworfen ist.[71] Aus den gewonnenen Tatsachen wird in einem zweiten Schritt die Schuldfrage gestellt. Nur in diesem zweiten Schritt gilt die Unschuldsvermutung.[72]

Auf den ersten Blick kommt die Unschuldsvermutung mit aus Big Data gewonnenen Beweisen und Indizien überhaupt nicht in Kontakt. Die richterliche Beweiswürdigung unterliegt jedoch gewissen Einschränkungen hinsichtlich Logikgesetzen und gesicherten wissenschaftlichen Erkenntnissen.[73] Problematisch könnten etwa aus Algorithmus gewonnene Scorings sein, also die Analyse von Daten über einen Menschen und computergenerierte Einschätzungen, etwa über dessen Gefahrenpotential. Richter denken in menschlicher Logik, also in einer Ursache-Wirkung-Relation. Dem gegenüber steht die Maschine, die nur eine korrelative Logik beherrscht. Dies könnte zu Missverständnissen führen und damit zu falschen Tatsachenerkenntnissen.[74] Würden diese als Urteilsgrundlage dienen, wäre die Unschuldsvermutung verletzt. Obwohl der Algorithmus an sich neutral ist, sind Computer nicht zwingend objektiver als menschliche Gutachter. Auch sie sind nicht frei von Überverdächtigung, Sexismus, Rassismus und anderen Formen der Diskriminierung.[75] Für den Richter bleiben die Gründe des Scorings aus dem Algorithmus oft verborgen.[76] So ist die wissenschaftliche Validität bisher nur unzureichend erforscht.[77] Problematisch für die Unschuldsvermutung können Scorings also dann sein, wenn sie dem Richter eine falsche Objektivität vermitteln, aufgrund derer ein Richter schuldig spricht. Etwa in der Strafzumessung kann aber ein solches Scoring – wenn es richtig von Sachverständigen eingeordnet wird – zusätzliche Erkenntnisse bringen, ohne dass die Unschuldsvermutung verletzt wird.[78]

VI. Ausblick: Der Präventionsstaat ohne Unschuldsvermutung

Sind die einzelnen Maßnahmen für sich genommen nicht im Anwendungsbereich der Unschuldsvermutung oder erreichen nicht eine strafähnliche Qualität im Eingriff, um gegen die Unschuldsvermutung zu verstoßen, könnte eine Kumulierung und Verschränkung von neuen (technischen) Ermittlungs- oder Gefahrenabwehrmaßnahem im

70 *Eisenberg,* Beweisrecht der StPO, 10. Auflage (2017), Rn. 90.
71 *Ott,* in: KK-StPO, 8. Auflage (2019), § 261 Rn. 2.
72 *Eisenberg,* Rn. 90.
73 *Ott,* in: KK-StPO, § 261 Rn. 49; *Eisenberg*, Rn. 91.
74 Vgl. *Ostermeier*, S. 103.
75 *Dressel/Farid,* Science Advances, 2018, 1 (1 ff.).
76 Vgl. *Ostermeier*, S. 103.
77 Der in den USA beliebte Algorithmus COMPAS hat in der Genauigkeit keine Vorteile im Vergleich zu Sachverständigen oder zum Teil sogar juristischen Laien, (*Dressel/Farid*, S. 3 f.).
78 *Martini*, DVBI 2014, 1481 (1489).

Tatbestand und weitergehenden Befugnissen in der Rechtsfolge eine Vorverlagerung von strafähnlichen Maßnahmen in die Gefahrenabwehr bedeuten.[79] Perspektivisch kann befürchtet werden, dass der Staat hauptsächlich proaktiv und nicht mehr reaktiv agieren könnte. Dadurch würde sich die Abkehr vom Rechtsstaat in der heutigen Form abzeichnen[80] und ein Präventivstaat an dessen Stelle treten. Der Staat könnte nicht mehr versuchen, solche Taten aufzuklären, sondern zukünftige Täter im Vorhinein zu bestrafen.[81] In einen solchen Staat würden Mechanismen mithilfe von Big Data etabliert, in der der einfache Bürger nicht mehr unter der Prämisse der individuellen Unschuldsvermutung betrachtet werden würde, sondern stets unter einem kollektiven Schuldverdacht stehen würde.[82] So würde eine Doppelbödigkeit in dem Sinne entstehen, dass grundsätzlich alle Gesellschaftsmitglieder sowohl als mögliche Täterinnen und Täter, gleichzeitig aber auch potenzielle Opfer gesehen werden.[83] In Extremfällen wird befürchtet, dass Bürger sogar ihre Unschuld beweisen müssten,[84] was eine Beweislastumkehrung von der Unschuldsvermutung wäre.

Auch auf politischer Ebene hat dies Folgen: Durch die Ausweitung der Befugnisse könnte die Akzeptanz für ein allgemeines Lebensrisiko in der Politik immer weiter sinken und somit das Verhältnis von Freiheit und Sicherheit immer weiter auf die Seite von präventiver Sicherheit kippen – bis dies systemgefährdend werden könnte.[85] Die Aufgabe des Staates würde sich ändern: Der Staat wäre nicht mehr für die Sicherung von Rechtsgütern zuständig, sondern würde das Rechtsgut Sicherheit selbst produzieren, indem er andere Freiheiten beschneiden würde.[86] Dies kann auch ein demokratisches Problem werden: Wer sich nicht im Mainstream befindet, könnte zunehmend Adressat von Repressionen werden.[87] Somit wäre auch die Idee einer streitbaren Demokratie am Ende.[88] Die Unschuldsvermutung hat hier neben der individuellen eine systemsichernde Funktion zur Abgrenzung vom Rechts- zum Polizeistaat.[89]

Die Rechtsprechung hält sich dagegen mit einer gesamtsystematischen Betrachtung zurück. Eine Verfassungsbeschwerde forderte eine besondere gesetzliche Regelung für mehrere Ermittlungsmaßnahmen. Das *BVerfG* lehnte dies ab, forderte jedoch insbesondere bei verborgenen Ermittlungsmethoden eine erhöhte Anforderung an das Verfahren und eine umfassende Informiertheit der Staatsanwaltschaft.[90] Bei dieser Rechtsprechung wird kritisiert, dass sie nicht der Realität entspreche und durch Idealisierung das enorme Potential von Big Data verkenne.[91] Einer richterlichen Überprüfung würde es sich jedenfalls entziehen, da der Richtervorbehalt nur punktuell gilt.[92] Außerdem wäre eine Sensibilisierung auch von der Legislative für das Potential von verschränkten Maßnahmen für die Eingriffsintensität im Gesamtsystem wünschenswert. Dagegen wird die aktuelle Entwicklung in ihrer Gesamtheit weniger kritisch gesehen und vor einer freiheitspolitischen Dramatisierung gewarnt.[93] Sicherheit sei gerade eine Voraussetzung für Freiheit und könne dadurch nicht mit dieser abgewogen werden.[94] So wird den Kritikern des

79 Vgl. *Knobloch*, S. 34.
80 *Denninger*, KJ 1988, 1 (3).
81 *Legnaro*, S. 31.
82 *Legnaro*, S. 31; vgl. *Denninger,* KJ 1988, 1 (3).
83 *Legnaro*, S. 31.
84 *Hofmann/Zängerling,* in: Kloepfer/Meßerschmidt, Anmerkungen zum Katastrophenrecht, 2009, S. 5.
85 *Legnaro*, S. 32.
86 Vgl. *Denninger,* KJ 1988, 1 (12 f., 14).
87 Vgl. *Denninger,* KJ 1988, 1 (12).
88 Vgl. *Denninger,* KJ 1988, 1 (12).
89 *Weßlau*, S. 300; Vgl. auch *Volkmann,* JZ 2004, 696 (702 f.).
90 BVerfGE 112, 304 (319 f.); BVerfGE 130, 1 (24).
91 Vgl. *Eschelbach*, S. 8.
92 *Eschelbach*, S. 8.
93 *Bull*, NG|FH No. 4 2009, 77 (78).
94 A.a.O.

aktuellen Kurses vorgeworfen, dass die freiheitspolitische Panikmache in Sicherheitsaspekten eine Verabschiedung vom seriösen Diskurs sei.[95] Ein Blick auf subjektive Sicherheitsbedürfnis der Bürger und die stetig sinkenden Kriminalitätsraten, die in einem Missverhältnis stehen[96], unterstreichen dagegen die Befürchtungen der öffentlichen und politischen Akzeptanz eines ausufernden Sicherheitsstaates, der die Freiheiten Einzelner weniger stark gewichtet. Als eine Lösung wird eine Erweiterung der liberalen Grundrechte des 19. und 20. Jahrhunderts verlangt, die eine Limitierung der Möglichkeiten von Big Data veranlasst, um das Schuldprinzip und die Freiheitsgarantie der heutigen Zeit zu festigen.[97] Momentan kann man noch nicht von Deutschland als Präventivstaat reden, auch wenn es eine Entwicklungstendenz in diese Richtung gibt.[98]

VII. Fazit

Die Unschuldsvermutung limitiert die Einsatzmöglichkeiten von Big Data in der Quantität der Überwachung und in der Qualität des Eingriffs. Predictive-Policing-Programme und Scoring bedürfen außerdem einer menschlichen Überprüfung bzw. Einordnung. Der Ausruf eines Präventivstaates mag aus heutiger Sicht zwar noch nach einer fernen Dystopie klingen, doch zeigen viele einzelne Entwicklungen in diese Richtung. Durch die Verschränkung der technischen Maßnahmen könnte die Unschuldsvermutung durch immer stärkere präventive Maßnahmen ausgehöhlt werden. Daher sollten nicht nur die Maßnahmen für sich, sondern stärker auch eine Gesamtbeurteilung des Systems in den Blick der juristischen und politischen Debatte um die Unschuldsvermutung genommen werden.

95 Vgl. *Bull*, NG|FH No. 4 2009, 77 (79).
96 Frankfurter Allgemeine Zeitung: Kluft zwischen realer und gefühlter Kriminalität, 17.9.2018, abrufbar unter: https://www.faz.net/aktuell/gesellschaft/kriminalitaet/aengste-und-statistiken-zwischen-realer-und-gefuehlter-kriminalitaet-15791726/reizwort-messerkriminalitaet-15791728.html (zuletzt abgerufen am 27.5.2020).
97 Vgl. *Mayer-Schönberger*, S. 384.
98 *Hofmann/Zängerling*, S. 14.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Leona May Jackson

Big Data und die Bestrafung „künftiger“ Täter

Inhaltsverzeichnis

I. Einleitung

Seit Beginn der 90er-Jahre wurde mit innovativer Informationstechnologie ein gesellschaftlicher Wandel angestoßen.[1] Wo Computer und Netzwerke früher noch Spezialisten vorbehalten waren, sind sie heute omnipräsent. Informationstechnologien wie Internet, Mobilfunk und interaktives Fernsehen erleichtern den Zugang zu Informationen und verbessern ihre Nutzbarkeit für verschiedene Bereiche, wie bspw. die Wirtschaft. Zu Zeiten der Digitalisierung und der Allgegenwart von Smartphones und Social Media, kommen mit jedem Klick neue Daten auf. Das Resultat dieser Entwicklung ist Big Data, eine Informationsmenge, die in ihrer Größe unsere Vorstellungskraft weit überschreitet.[2] Diese Datenmengen haben ein immenses Potenzial, da durch die Menge an Informationen Zusammenhänge begriffen werden können, die zuvor nicht erkannt wurden. Mit der richtigen Einsatzweise von Big Data können sogar Prognosen erstellt werden. Die Prävention, die Verhinderung eines negativen Ereignisses, ist ein Ideal, das die Menschen seit Jahrhunderten verfolgen.[3] Insbesondere im Bereich des Strafrechts, dessen Aufgabe der Rechtsgüterschutz ist, ist die Prävention von Straftaten von besonders großem Interesse - denn wenn die Begehung einer Straftat verhindert werden kann, bevor ein Schaden entsteht, ist der Rechtsgüterschutz besonders effektiv. So ist es denkbar, sich die immensen Daten, die über einen Großteil der Bevölkerung vorliegen, im Bereich des Strafrechts nutzbar zu machen.

Diese Arbeit konzentriert sich auf die Prävention von Straftaten und beschäftigt sich konkret mit der Frage, inwiefern eine Bestrafung „künftiger Täter“ mithilfe von Big Data aus der Perspektive der Prävention denkbar ist. Die Bezeichnung „künftiger Täter“ ist bewusst in Anführungszeichen gesetzt, weil sie einen Antagonismus beschreibt. Im gängigen Sprachgebrauch haben wir uns an die Bezeichnung „Gefährder“ gewöhnt, die ebenfalls problematisch ist. Denn auch hier besteht nur eine Vermutung oder Wahrscheinlichkeitsprognose der Gefährlichkeit, ohne dass deren Nachweis erbracht wäre. Tatsächlich ist aber mit Blick auf strafrechtliche Ermittlungen etwas ganz Ähnliches gemeint -die Wahrscheinlichkeit einer konkreten Tatbegehung soll Maßnahmen legitimieren können. Dass dieser Ansatz kritisch zu sehen ist und nicht nur mit den rechtsstaatlichen Prinzipien des Strafverfahrens in Konflikt tritt, wird deutlich werden. Die Anführungszeichen stehen sinnbildlich für die mit der konkreten Tatbegehungsprognose als Anknüpfungspunkt für Ermittlungen versuchte Quadratur des Kreises.

II. Big Data

1. Definition und Anwendungsbereiche

Für Big Data lässt sich nur schwer eine exakte Definition konstruieren.[4] Big Data sind grundsätzlich große Mengen an aus dem Internet stammenden Daten, die dann anhand von besonderen technischen Mitteln gespeichert, ausgewertet und verarbeitet werden.[5] Ein Kernbereich, in dem Big Data Anwendung findet, ist die Wirtschaft, insbesondere im Bereich des Marketings.[6] So sammeln Unternehmen anhand von Kundenkarten und -konten Daten

1 *Kollmann,* Die Grundlagen des E-Business, 7. Aufl. (2019), S. 1.
2 *Radtke*, Was ist Big Data?, abrufbar unter: www.bigdata-insider.de/was-ist-big-data-a-562440/ (zuletzt abgerufen am 20.10.2019).
3 *Singelnstein,* NStZ 2018, 1 (1).
4 *Mayer-Schönberger/Cukier,* Big Data, 2013, S. 13.
5 *Bendel,* Definition: Big Data, Gabler Wirtschaftslexikon, abrufbar unter: wirtschaftslexikon.gabler.de/definition/big-data-54101/version-277155 (zuletzt abgerufen am 1.10.2019).
6 *Dastani,* Big Data Anwendungsgebiete und Chancen, abrufbar unter: predictive-analytics.com/big-data-anwendungsgebiete/ (zuletzt abgerufen am 18.10.2019).

über das Kaufverhalten ihrer Kunden, die sie dann nutzen können, um ihre Verkaufsstrategie zu verbessern.[7] Indem dem Kunden auf Basis der bereits ausgewählten Produkte, weitere Produkte zum Kauf vorgeschlagen werden, generieren Unternehmen wie Amazon höhere Umsatzzahlen.[8]

2. Korrelation und Vorhersage

Um Kunden gezielt Produkte vorzuschlagen, die ihnen gefallen, müssen Erkenntnisse über die Bedürfnisse des Kunden erzielt werden. Dies geschieht im Rahmen von Big Data über Korrelationen. Eine Korrelation stellt die Beziehung zwischen zwei Datenpunkten her.[9] Treten beispielsweise Datenpunkt 1 und Datenpunkt 2 gemeinsam auf, so können auf Grundlage von Datenpunkt 2 Aussagen, bzw. sogar Vorhersagen zu Datenpunkt 1 getroffen werden.[10] So lässt sich aufgrund der Korrelationen die Gegenwart festhalten und die Zukunft vorhersagen.[11]

3. Predictive Policing Software als Anwendungsgebiet von Big Data in der Strafverfolgung

Big Data hat sowohl in den Bereichen Wirtschaft, Verwaltung und Justiz Einzug gefunden – insbesondere hier spielt Big Data in Form des Predictive Policing für die Prävention von Straftaten eine zunehmend wichtige Rolle. Predictive Policing ist der Sammelbegriff für algorithmenbasierte Straftatprognosen, die durch eine computergestützte, automatische Auswertung von verschiedenen Daten die Wahrscheinlichkeit der Begehung einer Straftat feststellen kann.[12] Diese Feststellungen können sich auf einen bestimmten Ort oder bestimmte Personen beziehen.[13] Predictive Policing ermöglicht es den Strafverfolgungsbehörden, präventiv gegen Straftaten vorzugehen, sowie angemessen auf sie zu reagieren.[14]

Seit 2008 wird Predictive Policing Software in den USA von vielen Polizeibehörden genutzt.[15] Die in den USA verwendeten Systeme können eine Vielzahl von Delikten vorhersagen, da ihnen diverse kriminologische Ansätze zugrunde liegen und sie auf größere und umfassendere Datenmengen zurückgreifen können.[16] Um konkrete örtliche Vorhersagen zu treffen, wird von den amerikanischen Polizeibehörden mit komplexen Kriminalitätskartierungen gearbeitet.[17] Dabei werden Daten aus Kriminalstatistiken, Wohnorte von verurteilten Straftätern, Infrastrukturen, Wetterbedingungen, Veranstaltungen und sozialökonomische Daten wie Status oder Alter berücksichtigt.[18] Personenbezogene Vorhersagen lassen sich treffen, indem Risikoprofile auf Grundlage von Vorstrafen, Wohnort, sozialem Umfeld, sowie Lebensereignissen und Verhaltensmustern erstellt werden.[19] Es scheint grundsätzlich möglich, anhand von Big Data Vorhersagen darüber zu treffen, wann, wo und von wem eine Straftat begangen werden könnte.

7 *Kraus,* Big Data – Einsatzfelder und Herausforderungen, 2013, S. 10.
8 *Kraus,* S. 10.
9 *Mayer-Schönberger/Cukier,* S. 70.
10 A.a.O., S. 71.
11 A.a.O., S. 71.
12 *Singelnstein,* NStZ 2018, 1 (1).
13 A.a.O.
14 *Gluba,* Predictive Policing – Eine Bestandsaufnahme, 2014, S. 7.
15 A.a.O., S. 6.
16 A.a.O., S. 6.
17 *Singelnstein,* NStZ 2018, 1 (2).
18 A.a.O.
19 A.a.O.

III. Der „künftige Täter“ im Strafrecht

1. Strafrecht und Täterbegriff

Um beurteilen zu können, inwiefern eine Bestrafung von „künftigen Tätern“ mit Hilfe der Verarbeitung und Auswertung von Big Data möglich ist, muss zunächst festgestellt werden, ab wann der Mensch zum „Täter“ wird. Der Gesetzgeber definiert den Täter als denjenigen, der die Tatbestandsmerkmale einer strafrechtlichen Norm verwirklicht.[20] Mit anderen Worten, der Täter ist grundsätzlich derjenige, der fahrlässig oder vorsätzlich Straftaten begeht. Nach *Jakobs* entscheidet der dem Strafrecht zugrundeliegende Täterbegriff über dessen Charakter. Wird der Täter als Feind der Gesellschaft betrachtet, der nur Unrecht bringt, so kommt es zu einer feindlichen, gar polarisierenden Ausrichtung des Strafrechts, in dem es nur „gut“ und „böse“ gibt.[21] Aufgabe dieses Strafrechts ist, die Gefahrenquelle „Mensch“ möglichst effektiv abzuwehren[22], um so die Rechtsgüter der übrigen Menschen zu schützen. Ist die Gefährdung von Rechtsgütern der einzige Anhaltspunkt zur Definition des Täters, so kommt es schnell zu einer grenzenlosen Vorverlagerung des Beginns der Gefahr[23] - insbesondere, wenn dem Täter aufgrund seiner Degradierung zum Feind kein Bereich nicht-sozial-relevanten-Verhaltens gewährt wird.[24] Infolge des Rechtsgüterschutzgedankens müsste dann bereits der Gedanke an eine Rechtsgutsverletzung bestraft werden, da dieser das erste Anzeichen einer Gefahr darstellen kann.[25] Dieser feindlichen Ausrichtung soll der Täter als Bürger entgegengesetzt werden.[26] Ihm wird das Recht auf eine von Kontrolle freie Sphäre zugestanden[27] und er wird als Bürger und somit als Teil des Systems anerkannt[28]. Das Zugeständnis einer Privatsphäre muss unweigerlich zu einer Begrenzung der Vorverlagerung des Gefahrenbeginns führen.[29]

Was Big Data und deren Zusammenhang mit Predictive Policing betrifft, stellt sich die Frage, wer der „künftige Täter“ sein kann. Wenn aus der Perspektive des Feindstrafrechts der Gefahrenbeginn vorverlagert wird, so kommen zwei Arten von „künftigen Tätern“ in Betracht. Zum einen ist als „künftiger Täter“ derjenige denkbar, der vorbereitet, aber noch keine Rechtsgutsverletzung begangen hat, und andererseits derjenige, bei dem die Begehung einer Straftat prognostiziert wurde.

2. Täterschaft ohne Rechtsgutsverletzung

a) Die strafbaren Vorbereitungshandlungen

Bei der Begehung von Straftaten gibt es verschiedene Verwirklichungsstadien: vom ersten Gedanken an die Tat über das Ergreifen des Tatentschlusses bis hin zur Vollendung der Tat.[30]

---

20 *Jescheck/Weigend*, Lehrbuch des Strafrechts Allgemeiner Teil, 5. Aufl. (1996), S. 643.
21 *Kindhäuser,* Gefährdung als Straftat, 1989, S. 179.
22 *Kindhäuser,* S. 179.
23 *Jakobs,* ZStW 1985, 751 (753).
24 A.a.O.
25 A.a.O.
26 *Kindhäuser,* S. 179.
27 *Jakobs,* ZStW 1985, 751 (753).
28 A.a.O., 751 (755).
29 A.a.O., 751 (753).
30 *Rengier,* Strafrecht Allgemeiner Teil, 11. Aufl. (2019), § 33 Rn. 7.

Die Vorbereitung der Straftat besteht aus dem ersten Gedanken des Täters an die Tat. Zu den Vorbereitungshandlungen zählt in etwa das Besorgen einer Waffe oder die Besichtigung des späteren Tatorts.[31] Grundsätzlich sind Vorbereitungshandlungen straflos. Es gibt im Strafgesetzbuch allerdings einige Ausnahmen, bei denen bereits Vorbereitungshandlungen unter Strafe gestellt werden, z.B. § 149 I StGB. Danach macht sich jemand strafbar, der bspw. im Frühjahr einen Druckstock herstellt, um dann im Winter mit der Herstellung von Falschgeld beginnen;[32] hier kommt es zu einer zeitlichen Vorverlagerung der Strafbarkeit.

b) Legitimation der strafbaren Vorbereitungshandlungen

Solche Ausnahmen, in denen die Vorbereitung bereits unter Strafe steht, kommen stets bei einer „unselbstständigen Ausdehnung der Straftatbestände" vor.[33] Eine derartige Ausdehnung ist immer dann anzunehmen, wenn die Effektivität des Rechtsschutzes und der Tatbestand nach Ansicht des Gesetzgebers ein möglichst frühes Eingreifen notwendig machen.[34] Weiterhin wird die Vorverlagerung der Strafbarkeit oftmals mit dem erhöhten objektiven Gefahrenpotenzial, das sich aus der Planung und Organisation einer Straftat ergibt, begründet.[35] Diese Form „künftiger Täter" stellt keinen neuartigen Typus dar. Wie sonst auch, müssen Tatsachen dafür beweismäßig belegt werden, dass eine konkrete Person Handlungen bereits begangen hat, welche vom Tatbestand erfasst werden.

3. Täterschaft aufgrund von Prognosen

Wenn Anknüpfungspunkt der Bestrafung allerdings nicht die Handlung des Täters ist, sondern sein allgemeines bzw. im Verhältnis zur Verwirklichung von Tatbeständen noch unspezifisches Verhalten wird, könnten in einem weiteren Sinne verhaltensspezifische und individuelle Prognosen über den Täter die Strafbarkeit begründen. Eine fundierte Prognose basierend auf der Sammlung, Auswertung und Verwertung von Daten über das objektive Gefahrenpotenzial des Täters[36] stellt dann den „Strafgrund" dar, welcher Ermittlungen oder gar Sanktionen legitimieren würde.

a) Sozialprognose nach § 56 StGB

Prognosen innerhalb des Strafrechts sind keine Besonderheit. So werden bspw. Gefährlichkeitsprognosen für die Anordnung von Maßregeln vorausgesetzt[37] und im Rahmen der Strafaussetzung nach § 56 StGB Prognosen über die Wahrscheinlichkeit einer weiteren Deliktsbegehung erstellt. Letztlich beruhen also alle individualpräventiven Sanktionen auf der Möglichkeit von Prognosen. Nach § 56 StGB kann eine Freiheitsstrafe, die eine Dauer von zwei Jahren nicht übersteigt, zur Bewährung ausgesetzt werden, wenn davon auszugehen ist, dass der Betroffene sich auch ohne die Wirkungen des Strafvollzugs von weiteren kriminellen Handlungen fernhält. Voraussetzung hierfür ist eine günstige oder positive Kriminalprognose.[38] Diese ist anzunehmen, wenn eine durch Tatsachen begründete Wahrscheinlichkeit der straffreien Führung besteht.[39] Für die Bestimmung der Sozialprognose werden

31 *Rengier,* § 33 Rn.7.
32 *Hefendehl,* JR 1996, 353 (354).
33 *Hillenkamp,* in: LK-StGB, 11. Aufl. (2018), § 22 Rn. 7.
34 *Deckers/Heusel,* ZfR 2008, 169 (170); *Hillenkamp*, in: LK-StGB, § 22 Rn. 7.
35 *Deckers/Heusel*, ZfR 2008, 169 (171); *BGH*, NJW 1995, 2117 (2118).
36 *Rehder,* KP 2009, 4 (5).
37 *Dessecker,* Gefährlichkeit und Verhältnismäßigkeit, 2004, S. 182.
38 *Groß,* in: MüKo-StGB, 3. Aufl. (2019), § 56 Rn. 14; *Hein,* JA 2018, 542 (545).
39 *Hein,* JA 2018, 542 (546).

nach § 56 I S.2 StGB verschiedene Kriterien herangezogen, wie etwa das Vorleben des Täters, seine Persönlichkeit, sein Verhalten nach der Tat, sowie die Tatumstände selbst, aber auch seine allgemeinen Lebensverhältnisse. So tragen etwa ein gefestigtes soziales Umfeld, das Bestehen eines Beschäftigungsverhältnisses oder auch Bemühungen gegen ein Suchtproblem vorzugehen, zu einer positiven Prognose bei.[40] Andererseits kann sich die Tatsache, dass vorherige Strafen bereits zur Bewährung ausgesetzt wurden, sowie die Ausführung der Tat negativ auf die Prognose auswirken.[41] Es stellt sich also die Frage, ob eine Bestrafung basierend auf einer solchen Prognose möglich ist.

b) Grenzen von Sozialprognosen

Bei Kriminalprognosen können also lediglich Aussagen darüber getroffen werden, wie wahrscheinlich es ist, dass ein Straftäter rückfällig wird, nicht aber ob er tatsächlich rückfällig wird.[42] Demnach lassen es die Wahrscheinlichkeitsaussagen nicht zu, bestimmte Ereignisse komplett auszuschließen.[43] So lässt sich etwa im Rahmen von Sexualdelikten bei keinem Menschen eine Wahrscheinlichkeit der Begehung von null Prozent vorhersagen.[44] Vielmehr geht diese Gefahr unter gewissen Umständen grundsätzlich von jedem Menschen aus.[45] Auch wenn bestimmte Aspekte die Tatwahrscheinlichkeit vielleicht erhöhen, kann bei niemandem ein zukünftiges Delikt mit Sicherheit ausgeschlossen werden.[46] Um ein Rückfallrisiko so genau wie möglich bestimmen zu können, sind verschiedene Wahrscheinlichkeiten von einem Legalprognostiker zu berücksichtigen und Verhaltensmuster zu bestimmen.[47] Dabei ist jedoch zu beachten, dass sich diese Verhaltensmuster verändern, zum Beispiel durch eine Therapie, oder äußere Entwicklungen der Lebensumstände.[48] Weiterhin ist zu berücksichtigen, dass alle Menschen Stimmungsschwankungen unterliegen. Unter Umständen lässt sich die Variationsbreite der Schwankungen prognostizieren, allerdings nicht, wann welche Stimmung dominiert und wie ausgeprägt sie in schwierigen Situationen ist.[49] Unvorhersehbare physische Zustände wie Schmerzen, emotional belastende Situationen oder Intoxikation können die Wahrscheinlichkeit eines kriminellen Verhaltens gravierend beeinflussen.[50] Um eine völlig zutreffende Prognose über die Wahrscheinlichkeit krimineller Handlungen zu treffen, müssten Informationen über alle zukünftigen Situationen, in denen sich die betroffene Person befinden wird, vorliegen.[51] Die Persönlichkeit eines Menschen mag erforschbar sein, in welchen Situationen sich der Mensch wiederfinden wird und in was für einer Stimmung er sich dann befindet, wird ein Prognostiker allerdings nicht festlegen können.[52] Die Prognoseforschung hält daher Vorhersagen über individuelles Verhalten gar nicht für möglich.[53] Letztendlich spielt auch die Offenheit des Betroffenen eine nicht unerhebliche Rolle: Sobald ein Täter über sich keine Auskunft geben kann – bspw. mangels Reflexionsfähigkeit – oder will, weil er abschätzen kann, dass Teile seiner Persönlichkeit negativ bewertet werden, lassen sich der Charakter, persönliche Vorlieben und Interessen nicht ausmachen.[54]

40 *Hein,* JA 2018, 542 (546).
41 *Hein,* JA 2018, 542 (546).
42 *Rehder,* KP 2009, 4 (4).
43 A.a.O.
44 A.a.O.
45 A.a.O.
46 A.a.O.
47 A.a.O.
48 A.a.O.
49 A.a.O.
50 A.a.O.
51 A.a.O.
52 A.a.O.
53 *Dessecker,* S. 188.
54 *Rehder,* KP 2009, 4 (7).

IV. Möglichkeiten und Grenzen der Bestrafung „künftiger Täter“

1. Möglichkeiten der Bestrafung „künftiger Täter“

Eine Bestrafung im Vorfeld auf Grundlage von Big Data bietet im Hinblick auf die staatliche Aufgabe, Rechtsgüter zu schützen, ein großes Potenzial. So kann auf diesem Wege die Gesellschaft möglichst effektiv vor Rechtsgutsverletzungen geschützt werden. Es wundert daher nicht, dass die Protagonisten oftmals für eine weitreichende Sicherheitspolitik argumentieren. Allerdings ist eine präventive Bestrafung in Bezug auf Legitimität und Durchsetzungsmöglichkeiten kritisch zu betrachten.

2. Grenzen der Bestrafung „künftiger Täter“

a) Probleme der Bestrafung auf Grundlage von algorithmenbasierten Prognosen

Auch auf Big Data basierende Prognosen lassen keine Schlüsse zu äußeren Einwirkungen und Entwicklungen potenzieller Täter zu.[55] Eine präventiv wirkende Bestrafung verkennt, dass der betroffenen Person die Wahl genommen wird, die Tat nicht zu begehen.[56] Ein vorschnelles Eingreifen kann zwar die potenziell drohende Rechtsgutsverletzung verhindern, allerdings nie mit Sicherheit aufzeigen, wie der Täter tatsächlich gehandelt hätte[57].

b) Verfassungsrechtliche Grenzen

Aus verfassungsrechtlicher Perspektive ergeben sich bezüglich der Legitimation von Big Data als Grundlage für die Bestrafung weitere Bedenken: Eine weit reichende Sammlung und Auswertung der Daten von Bürgern, wie es im Rahmen von Big Data der Fall wäre, würde eine unzulässige Einschränkung des Grundrechts auf informationelle Selbstbestimmung bedeuten[58]. Dieses Grundrecht schützt die Privatsphäre eines jeden Einzelnen, die dem Zugriff staatlicher und privater datenverarbeitender Stellen entzogen sein soll.[59] So war Hauptbotschaft des Volkszählungsurteils des Bundesverfassungsgerichts, dass Datenerhebungen immer bestimmte Zwecke verfolgen müssen.[60] Im Rahmen von Big Data und Predictive Policing Software als Grundlage der Bestrafung müsste vorab die Art und Weise der Auswertung und die sich daraus ergebenden Informationen und deren Verwendung/Verknüpfung genau geklärt werden.[61] Dies wird in der Praxis aber nur schwer umsetzbar sein. Im Hinblick auf das Rückwirkungsverbot, das sich aus dem Rechtsstaatsprinzip ergibt[62], ist die auf Big-Data-Prognosen basierende Bestrafung kritisch zu sehen. Im Sinne des Rückwirkungsverbots darf weder der Gesetzgeber noch der Richter rückwirkend rechtstreues Verhalten determinieren.[63] Auf diese Weise wird der Bürger vor Willkür *ex post* geschützt.[64] Hier drängt sich die Frage auf, inwiefern eine „vorwirkende“ Bestrafung rechtens sein kann, wenn eine rückwirkende Bestrafung gegen das Rechtsstaatsprinzip verstößt.

---

55 *Dessecker,* S. 188; *Rehder,* KP 2009, 4 (5).
56 *Deckers/Heusel,* ZfR 2008, 169 (171).
57 A.a.O.
58 *Meinicke,* K&R 2015, 377 (382).
59 *Hufen,* Staatsrecht II Grundrechte, 7. Aufl. (2019), § 12 Rn. 4; *Meinicke,* K&R 2015, 377 (382).
60 *Meinicke,* K&R 2015, 377 (382).
61 A.a.O.
62 *Krey/Esser,* Deutsches Strafrecht Allgemeiner Teil, 6. Aufl. (2019), § 3 Rn. 52; *Wessels/Beulke/Satzger,* Strafrecht Allgemeiner Teil, 49. Aufl. (2019), § 2 Rn. 66.
63 *Krey/Esser,* § 3 Rn. 52; *Wessels/Beulke/Satzger*, § 2 Rn. 66.
64 *Krey/Esser,* § 3 Rn. 52.

Weiterhin ist eine Analogie, also die Ausdehnung eines Rechtssatzes, auf einen Sachverhalt, dem ersterer eigentlich nicht mehr zuzuordnen ist, zu Lasten des Angeklagten unzulässig.[65] Dieses Verbot ergibt sich aus Art.103 II GG und dient dem Schutz des Täters vor einer unzulässigen Ausdehnung des Tatbestandes.[66] An dieser Stelle drängen sich ebenfalls Zweifel hinsichtlich der Bestrafung im Vorhinein auf. Auch wenn die präventive Bestrafung auf Grundlage von Big Data keine Analogie darstellt, so ist sie dennoch eine unzulässige Ausdehnung der Rechtssätze - die Rechtssätze des StGB würden so ausgedehnt, dass Ausgangspunkt bzw. Merkmal der Rechtsnormen nicht die Vollendung oder der Versuch der Tat ist; hier wäre bereits der Gedanke oder die Vorbereitung und Planung der Tat strafbar. Es ist aber gerade der Wortlaut der Normen, der deutlich macht, dass eine Strafbarkeit erst mit der tatsächlichen Begehung oder zumindest mit dem Versuch eintritt.

Auch im Hinblick auf das Schuldprinzip ergeben sich Probleme. Das Schuldprinzip findet seine Grundlage in der Menschenwürde und der Eigenverantwortlichkeit des Menschen nach Artt.1 I, 2 I GG, sowie im Rechtsstaatsprinzip nach Art.20 III GG.[67] Schuld wird dabei als die persönliche Vorwerfbarkeit der Entscheidung des Täters zum Unrecht verstanden.[68] Für die persönliche Vorwerfbarkeit der Tatbegehung ist nach dem normativen Schuldbegriff irrelevant, ob der Mensch in seinem Handeln determiniert ist.[69] Maßgeblich ist, dass wir selbst uns als frei handelnde Menschen erleben. Eine präventive Bestrafung würde genau das tun: sie würde menschliches Handeln determinieren, indem sie den Anspruch erhebt, genaue Vorhersagen über das Handeln von potenziellen Tätern zu treffen[70]. Dabei wird allerdings dem Betroffenen die bis zur tatsächlichen Tatbegehung bestehende Wahl genommen, sich doch noch eines Besseren zu besinnen.[71] Big Data kann daher aus Perspektive des Schuldprinzips keine Grundlage für die Bestrafung darstellen, da dies das Ende von Gerechtigkeit und freiem Willen bedeuten würde[72].

c) Konzeption des Strafrechts und Charakter der Strafe als Grenzen für die algorithmenbasierte Bestrafung „künftiger Täter“

Strafe ist nach unserer Konzeption des Strafrechts die Konsequenz bestimmter Taten. Sie ist zum einen Vergeltung und gibt dem Täter die missbilligende Antwort auf sein Verhalten,[73] zum anderen ist sie Prävention[74]; der Täter wird für seine Taten verantwortlich gemacht, was einerseits dem Rechtsempfinden der verletzten Gesellschaft entspricht, andererseits wird zugleich für Abschreckung sorgt.[75] Im Wesentlichen wird zwischen general- und spezialpräventiven Strafzwecken unterschieden. Die Generalprävention zielt auf der einen Seite darauf ab, die Gesellschaft durch Verhängung von Strafen vor der Begehung von Straftaten abzuschrecken, während auf der anderen Seite das Vertrauen der Menschen in die Normgeltung gestärkt werden soll.[76] Die Theorie der Spezialprävention hat den Täter selbst zum Adressaten.[77] Einerseits wird sie von dem Gedanken geleitet, dass der Straftäter nicht besserungsfähig ist und aus diesem Grund die Gesellschaft vor ihm zu schützen ist.[78] Andererseits sieht sie die

65 *Rengier,* § 4 Rn. 31.
66 *Rengier,* § 4 Rn. 31, 34.
67 *Rengier,* § 24 Rn. 1.
68 A.a.O.
69 A.a.O.
70 *Mayer-Schönberger/Cukier,* S. 203.
71 *Deckers/Heusel,* ZfR 2008, 169 (171).
72 *Mayer-Schönberger/Cukier,* S. 190.
73 *Gallas,* Beiträge zur Verbrechenslehre, 1968, S. 4.
74 A.a.O.
75 A.a.O.
76 *Eisele*, Strafrecht Allgemeiner Teil, 2017, § 2 Rn. 23; *Kindhäuser,* § 2 Rn. 14; *Rengier,* § 3 Rn. 14.
77 *Roxin,* Strafrecht Allgemeiner Teil, 4. Aufl. (2005), § 3 Rn. 11.
78 *Rengier*, § 3 Rn. 18.

Strafe als Möglichkeit, den Täter wieder in die Gesellschaft zu integrieren.[79]

Um bewerten zu können, inwiefern eine Bestrafung „künftiger Täter" mithilfe von Big Data – basierten Prognosen möglich ist, muss zunächst ermittelt werden, wie ein solches Strafrecht strukturiert sein müsste. Da sowohl bei der präventiven Bestrafung als auch beim Feindstrafrecht der effektivste Rechtsgüterschutz das zentrale Interesse darstellt,[80] könnte ein solches Strafrecht zum Feindstrafrecht führen, innerhalb dessen Rahmen dem Täter aufgrund von Datensammlung und algorithmenbasierten Prognosen kein Bereich privater Lebensführung gewährt wird[81] und bereits der erste Gedanke an eine Straftat strafbar ist. [82] So macht das Feindstrafrecht die Vorverlagerung der Strafbarkeit möglich, die für algorithmenbasierte Bestrafung notwendig wäre. Dieses Strafrecht betrachtet den Täter im Sinne der negativen Spezialprävention als nicht besserungsfähig.[83] Er ist der Feind, vor dem es gilt, die Gesellschaft zu schützen. Dieser Schutz stellt den zentralen Strafgrund dar. Die Bestrafung „künftiger Täter" im Sinne der negativen Theorie der Generalprävention bewirkt die Abschreckung der Menschen vor der Begehung von Straftaten[84]. Dieser Aspekt ist im Rahmen der Bestrafung auf Grundlage von auf Big Data basierenden Vorhersagen besonders ausgeprägt, da bei dem Umgang staatlicher Behörden mit Big Data der Überwachungscharakter verschärft wird. Dem entgegen zu halten ist, dass nach dem Verständnis der Gesellschaft der Täter nicht grundsätzlich „gut" oder „böse" ist, sondern als ein Bürger betrachtet wird, der einen Fehler gemacht hat. Ziel ist es, ihn wieder in die Gesellschaft einzugliedern. Dies zeigt sich insbesondere in den Maßnahmen, die in den Justizvollzugsanstalten angeboten werden, wie bspw. die Möglichkeit, einen Schulabschluss zu erreichen[85] und so eine Perspektive für die Zukunft zu gewinnen. Die Gesellschaft geht also davon aus, dass der Täter besserungsfähig ist. Unsere Konzeption des Strafrechts ist von der Auffassung des Täters als Bürger geprägt. Dadurch, dass das Bürgerstrafrecht von positiven Strafzwecken geprägt ist, müssten wir also die gesamte Konzeption von Täterschaft und Strafe verändern, um eine präventiv ausgerichtete Bestrafung[86] anhand von Big Data zu ermöglichen. Der Charakter des bestehenden Strafrechts zielt darauf ab, auf begangenes Unrecht zu reagieren und abgeschlossene Lebenssachverhalte zu beurteilen.[87]

V. Fazit

Big Data wird in unserem Leben aufgrund der stets wachsenden Digitalisierung und der unaufhaltbaren Weiterentwicklung der Technologie, eine immer größere Rolle spielen. Daher lässt sich abschließend sagen, dass Big Data und algorithmenbasierte Prognosen in der Zukunft eine Ergänzung zum geltenden Strafrecht darstellen können; als alleinige Grundlage zur Ermittlung, Verfolgung und Bestrafung „zukünftiger Täter" jedoch kaum denkbar und erst recht nicht wünschenswert sind.

79 A.a.O., Rn. 19.
80 *Kindhäuser,* S. 179.
81 A.a.O.
82 A.a.O.
83 *Rengier,* § 3 Rn. 18.
84 *Eisele*, § 2 Rn. 23.
85 *Keller,* Drinnen lernen für draußen, abrufbar unter: https://www.zeit.de/2009/49/C-Gefaengnis (zuletzt abgerufen am 20.10.2019).
86 *Singelnstein,* NStZ 2018, 1 (5).
87 *Singelnstein,* NStZ 2018, 1 (5); *Jescheck/Weigend,* S. 4.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Katja Lentz

Probleme und Möglichkeiten beim Einsatz von künstlicher Intelligenz als Hilfsmittel im deutschen Justizsystem

Inhaltsverzeichnis

I. Einleitung

Im Frühjahr 2019 verkündete Estland, künstliche Intelligenz als Ersatz für menschliche Richter in Gerichten einsetzen zu wollen.[1] In Zivilrechtsfällen mit bis zu 7000 Euro Streitwert analysiert eine Software die von den Parteien hochgeladenen Unterlagen und entscheidet daraufhin über die geltend gemachten Ansprüche. Die Parteien können allerdings Rechtsmittel einlegen und so eine Entscheidung durch einen menschlichen Richter herbeiführen.[2] In Deutschland gibt es bislang keine vergleichbaren Bestrebungen. Solche Technologien erzielen aber möglicherweise eine Entlastung und Effektivierung der Justiz. Im Folgenden werden zunächst Einsatzmöglichkeiten von künstlicher Intelligenz bei Gericht vorgestellt. Diese sind besonders relevant für die Hauptverhandlung im Strafprozess. Anschließend werden die mit einem KI-Einsatz einhergehenden Gefahren und Probleme diskutiert.

II. Einsatzmöglichkeiten von KI in der Justiz

1. Beurteilung der Glaubwürdigkeit von Aussagen

Die Beurteilung hinsichtlich Glaubwürdigkeit von Zeugenaussagen und Einlassungen des Angeklagten unterliegt im Strafverfahren dem Gericht nach den Grundsätzen der freien, richterlichen Beweiswürdigung, § 261 StPO.[3] Sie ist „ureigene Aufgabe des Tatrichters“[4] und nur ihm kraft Gesetz übertragen, §§ 155 Abs. 2, 244 Abs. 2, 261, 264 StPO. Die Einschätzung erfolgt regelmäßig allein durch das Tatgericht. Verbindliche Vorgaben für Richter bezüglich der Glaubwürdigkeitsfeststellung gibt es seitens des *BGH* allerdings nicht.[5] Es ist daher zu befürchten, dass Glaubwürdigkeitseinschätzungen stark intuitiv geprägt sind. Die Frage ist deshalb, ob eine KI die Glaubwürdigkeit von Zeugen und Angeklagten besser bewerten kann als ein Mensch. Letzterem bleibt nur die eigene Überzeugung, die aufgrund seines persönlichen Eindrucks von der Person entsteht. Aussagen werden vor Gericht heutzutage unter Zeitdruck gemacht, sind meist kurz und auf das Beweisthema beschränkt. Unter diesen Bedingungen lässt sich der Vorsitzende laut *Bender/Nack* besonders leicht täuschen.[6] Auch eine langjährige Berufserfahrung führt eher zu einer Selbstüberschätzung bezüglich des Erkennens von Lügen.[7] Die Beurteilung einer Person wird zudem durch den „Halo-Effekt“ verzerrt. Dieser sagt aus, dass herausstechende, bekannte Eindrücke einer Person die Zuschreibung weiterer, unbekannter Eigenschaften beeinflusst. Attraktive Angeklagte haben beispielsweise bessere Chancen auf mildere Urteile als unattraktive.[8] Während einer Vernehmung hat der Vorsitzende mehrere Aufgaben gleichzeitig, weshalb ihm Ungereimtheiten in der Sachverhaltsschilderung oder non-verbale Signale[9] weniger gut auffallen könnten. Wortwörtliche Dokumentationen erfolgen nur in den Ausnahmefällen der §§ 273 Abs. 2 S. 2 und Abs. 3 StPO. Es ist fraglich, ob eine Glaubwürdigkeitseinschätzung allein basierend auf subjektiven Empfindungen des Richters dem „verfassungsrechtlich verankerten Gebot rational begründeter und

1 *Niiler*, Can AI Be a Fair Judge in Court? Estonia Thinks So, 25.3.2019, abrufbar unter: www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/ (zuletzt abgerufen am 19.4.2020); *Shelton*, Estonia: From AI judges to robot bartenders, is the post-Soviet state the dark horse of digital tech?, 16.6.2019, abrufbar unter: www.abc.net.au/news/2019-06-16/estonia-artificial-intelligence-technology-robots-automation/11167478 (zuletzt abgerufen am 19.4.2020).
2 *Niiler,* a.a.O.
3 *Groh*, in: Creifelds kompakt, 2019, Glaubwürdigkeit von Zeugen(Kinder)aussagen.
4 *Miebach*, NStZ 2020, 72 (76).
5 *Prechtel*, ZJS 2017, 381 (385).
6 *Bender/Nack*, Tatsachenfeststellung vor Gericht, Bd. 2, 2. Aufl. (1995), Rn. 214; *OLG Celle*, Urt. v. 4.2.1999 – 11 U 19/98.
7 *Geipel,* Handbuch der Beweiswürdigung, 2. Aufl. (2013), Kap. 16 Rn. 48: „wesentlicher Faktor für Fehlurteile“; *Wendler/Hoffmann,* Technik und Taktik der Befragung, 2. Aufl. (2015), Rn. 89; *Prechtel*, ZJS 2017, 381 (392).
8 *Schweizer*, Kognitive Täuschungen vor Gericht: eine empirische Studie, 2005, Rn. 708.
9 *Prechtel*, ZJS 2017, 381 (393).

tatsachengestützter Beweisführung“[10] entspricht. Eine analytischere Herangehensweise wäre wünschenswert. Ein Beispiel hierfür ist der Lügendetektor. Durch die Messung körperlicher Reaktionen soll herausgefunden werden, ob eine Person lügt oder nicht. Laut dem *BGH* ist es aber nicht möglich, eine körperliche Reaktion ohne weiteres auf eine bestimmte Ursache zurückzuführen. Das Ergebnis einer polygraphischen Untersuchung darf daher nicht als Beweismittel in die Hauptverhandlung eingeführt werden.[11] Ein alternativer Lösungsansatz ist die Einführung einer audiovisuellen Aufzeichnung von Aussagesituationen in der Hauptverhandlung. Mithilfe von künstlicher Intelligenz könnten dann Verhaltensweisen, Gesprochenes und Mikromimik ausgewertet werden, um menschliche Fehlinterpretationen der Aufzeichnungen zu vermeiden.[12] Die verfassungsrechtlichen Anforderungen an eine richterliche Überzeugungsbildung wären gewahrt. Grundlegende Rechte der Verfahrensbeteiligten wie beispielsweise der Schutz des allgemeinen Persönlichkeitsrechts oder die Selbstbelastungsfreiheit müssten bei der Umsetzung berücksichtigt werden. Letztere erlaubt es dem Beschuldigten, die aktive Mitarbeit an der Sachaufklärung zu verweigern.[13] Bei der videotechnischen Aufzeichnung von Einlassungen des Angeklagten muss differenziert werden zwischen dem Filmen mit und ohne Einwilligung der betroffenen Person. Sofern der Angeklagte über die Vorteile und Risiken einer videotechnischen Aufzeichnung belehrt wird, besonders bezüglich Mikromimik, und er dann freiwillig entscheiden kann, ob er sich einem solchen Vorgehen aussetzen will oder nicht, würde die Selbstbelastungsfreiheit nicht gefährdet.

2. Urkundenbeweise

Auch im Zusammenhang mit der Auswertung von Urkundenbeweisen in der Hauptverhandlung könnte der Einsatz eines Algorithmus Potenzial haben. Nach dem Mündlichkeitsprinzip gem. § 261 StPO darf sich das Gericht bei der Urteilsfindung nur auf den mündlich erörterten Prozessstoff stützen. Grundsätzlich sind Urkunden und andere Schriftstücke daher stets gem. § 249 Abs. 1 StPO zu verlesen. Eine Auswertung von Urkunden durch künstliche Intelligenz würde diesen Anforderungen nicht gerecht. Eine Ausnahme des Verlesungsgrundsatzes ist das Selbstleseverfahren, § 249 Abs. 2 StPO. Es hat den Zweck, die Beweisaufnahme zu straffen und zu vereinfachen, indem die Richter und Schöffen längere und komplexere Urkunden selbstständig außerhalb der Hauptverhandlung lesen.[14] Der in dem Selbstleseverfahren gewonnene Beweisstoff gilt dann als im Inbegriff der Hauptverhandlung gewonnen.[15] Abgeschlossen wird die Beweisaufnahme im Selbstleseverfahren, nachdem der Vorsitzende in der Hauptverhandlung festgestellt hat, dass die Vorsitzenden und Schöffen vom Wortlaut der Urkunde Kenntnis genommen haben, „das heißt sie tatsächlich gelesen haben“.[16] Den Leseprozess auszulagern, sieht das Gesetz gerade nicht vor. Auch in diesem Fall würde eine Auswertung durch künstliche Intelligenz den Anforderungen nicht gerecht.

[10] *BGH*, Urt. v. 18.9.2008 – 5 StR 224/08, Rn. 16.
[11] *BGH*, Urt. v. 17.12.1998 – 1 StR 258/98; *BGH*, NStZ 2011, 474; *Prechtel*, ZJS 2017, 381 (390); *Momsen*, KriPoZ 2018, 142 (148).
[12] Bereits ein Kamerawinkel, der ausschließlich den Vernommenen frontal zeigt, sorgt bei Betrachtung der Aufnahme für eine Verzerrung der Vernehmungssituation, siehe *Gerson,* KriPoZ 2017, 376 (382).
[13] *Kasiske*, JuS 2014, 15 (17).
[14] *Kreicker,* in: MüKo-StPO, 2016, § 249 Rn. 51.
[15] *Diemer,* in: KK-StPO, 8. Aufl. (2019), § 249 Rn. 39.
[16] *Diemer*, in: KK-StPO, § 249 Rn. 39; *Kreicker*, in: MüKo-StPO, § 249 Rn. 61.

3. Eigene Gutachtenerstellung – Sachverständiger

Die Aufgaben eines Gutachters im Strafprozess lassen sich in drei wesentliche Bereiche einteilen. Dazu zählen die Vermittlung allgemeiner Erfahrungssätze, um dem Gericht zu ermöglichen, den Tatsachenstoff richtig einordnen zu können, die Anwendung von Fachwissen auf einen für erwiesen erachteten Fall sowie das Ziehen von Schlussfolgerungen durch Kombinieren der gegebenen Tatsachen mit den allgemeinen Erfahrungssätze und Fachwissen.[17] Im Hinblick auf Verkürzung und Effizienz der Beweisaufnahme in der Hauptverhandlung lässt sich fragen, ob eine KI den Sachverständigen ersetzen kann. Grundannahme der folgenden Überlegungen ist, dass künstliche Intelligenz als ein solcher im Sinne der StPO vor Gericht gelten würde. § 78 StPO überträgt die Leitung darüber, was ein Sachverständiger begutachten soll, dem Richter. Darunter fällt die klare Vorgabe aller Punkte, die für die Urteilsfindung relevant sind. [18] Indem der Vorsitzende selbst den Auftrag für die Gutachtenerstellung in das Programm eingibt, wäre diese Voraussetzung gewahrt. Kosten sowie Erstellungszeit würden reduziert. Die Anhörung des Sachverständigen entfiele, da der Richter selbst das automatisch erstellte Gutachten verlesen oder der Inhalt, sofern die wortwörtliche Wiedergabe des Urkundeninhalts nicht relevant für die Urteilsbildung ist und ihr kein Verfahrensbeteiligter widerspricht, zusammengefasst werden könnte.[19] Zwar gilt im Strafprozessrecht gem. § 250 StPO der Vorrang des Personen- vor dem Urkundenbeweis. Allerdings würde ein solches Vorgehen insbesondere durch § 251 Abs. 1 Nr. 3 Alt. 2 StPO gedeckt. Sofern eine künstliche Intelligenz als Sachverständiger gelten könnte, wäre das von ihr erstellte Gutachten eine Urkunde. § 251 Abs. 1 Nr. 3 Alt. 2 StPO sieht für den Fall, dass ein Sachverständiger in absehbarerer Zeit nicht gerichtlich vernommen werden kann, ihre Verlesung vor. Da eine gerichtliche Vernehmung der künstlichen Intelligenz nicht möglich ist, wäre der Tatbestand des § 251 Abs. 1 Nr. 3 Alt. 2 StPO mithin anzunehmen. Eine automatisierte Gutachtenerstellung durch eine Software wäre so vom Gesetz gedeckt. Es wird darauf hingewiesen, dass sich ein solcher Ersatz in einigen Bereichen eher bewähren wird, als in anderen. Ein gutes Beispiel ist die Ermittlung der Schadenshöhe von Autoschäden, die immens vereinfacht werden würde.[20]

4. Vernehmungen und Zeugen

Gegen das vollständige Ersetzen eines Richters durch eine KI bei der Vernehmung von Zeugen im Strafprozess spricht der Grundsatz der Unmittelbarkeit gem. § 250 StPO. Demnach muss das Gericht die Beweisgegenstände persönlich sinnlich wahrnehmen.[21] Ein Richterersatz müsste in der Lage sein, Vernehmungen eigenständig durchzuführen. Vernehmungen setzen gerade keine maschinell-analytische Logik voraus, sondern direkte Interaktion mit den Prozessbeteiligten. Ein völliger Richterersatz im Rahmen des Strafprozesses ist damit ausgeschlossen.

III. Mit dem Einsatz einhergehende Probleme und Gefahren

Im Rahmen von künstlicher Intelligenz bei Gericht müssen auch die mit dem Einsatz einhergehenden Gefahren angeschnitten werden. Probleme bestehen vorrangig im Zusammenhang mit der verfassungsrechtlich garantierten

[17] Beispiel: Der Rückschluss beruhend auf vorliegenden Befunden, dass eine Fehlintubation anzunehmen ist; *Ulsenheimer*, Der Anaesthesist 1998, 818 (820); *Schlund*, Der Anaesthesist 1998, 823 (824).
[18] *Monka*, in: BeckOK-StPO, 36. Edit. (2020), § 78 Rn. 3.
[19] *Diemer*, in: KK-StPO, § 249 Rn. 29.
[20] *Witte*, AssCompact 11/2018, 100 (100 f.).
[21] *Diemer,* in: KK-StPO, § 250 Rn. 1.

Unabhängigkeit der Justiz, dem Datenschutz der Angeklagten, insbesondere wenn die KI durch Dritte bereitgestellt wird, sowie vorurteilsbehafteter künstlicher Intelligenz, die ein wesentliches Argument gegen den Einsatz bei Gericht darstellt.

1. Unabhängigkeit der Justiz

Art. 97 GG schützt die richterliche Unabhängigkeit, die garantiert, dass die Gerichte ihre Entscheidung allein an Recht und Gesetz ausrichten.[22] Der Einsatz einer KI könnte dazu führen, dass ein Richter eigene Entscheidungen überdenkt und vielleicht abändert. Da „kollegiale Empfehlungen" unter Richtern, sobald sie psychischen Druck auslösen, die richterliche Unabhängigkeit verletzen, trifft das auch auf die KI zu.[23] Es ist zu bezweifeln, dass sich ein Richter gegen eine Entscheidung der KI wenden würde, wenn er jahrelang mit ihr verlässlich gearbeitet hat. Ein von privaten Firmen entwickeltes Programm greift in die Unabhängigkeit der Justiz ein. Das Abgeben rechtsstaatlicher Verantwortung an Private steht der inneren Unabhängigkeit des Richters sowie der selbstständigen Judikative als imminenter Teil der rechtsstaatlichen Demokratie und dem damit einhergehenden „Prinzip der Sicherung und ergänzenden Ausgestaltung der Gewaltenteilung"[24] unvereinbar entgegen. Auch staatlich entwickelte Programme, die mit künstlicher Intelligenz arbeiten, würde die Justiz in ihrer Unabhängigkeit verletzen. Art. 97 GG würde in allen beschriebenen Szenarien immens gefährdet oder verletzt.

2. Datenschutz und Transparenz

Datenschutz und Transparenz sind bei von privaten Dritten entwickelten Programmen nicht zwingend gewährleistet. In Europa gewährt die Datenschutz-Grundverordnung (DSGVO) der betroffenen Person unabhängig von ihrer Staatsbürgerschaft in Art. 17 Abs. 1 h) der EU-Verordnung Nr. 45/2001 grundsätzlich ein Informationsrecht in Bezug auf die Logik der Entscheidungsfindung bei automatisierter Verarbeitung von personenbezogenen Daten.[25] Mit dem Zugeständnis eines solchen Transparenzrechts schwingt gleichzeitig eine gewisse, europäische Skepsis gegenüber uneinsehbaren Entscheidungssystemen mit.[26] Komplexe Algorithmen sind Black Boxes und damit der Öffentlichkeit verschlossen.[27] Unterdessen ist die Entscheidungslogik für Menschen nicht immer nachzuvollziehen,[28] auch wenn es mittlerweile vielversprechende Ansätze zu ihrer Interpretation gibt.[29] Eine KI, die automatisiert über Verurteilung oder Freispruch entscheidet, würde das fair trial-Prinzip gem. Art. 20 Abs. 3 GG, Art. 6 Abs. 1 EMRK verletzen, das die Möglichkeit des Beschuldigten beinhaltet, aktiv auf Verfahrensgang und -ergebnis Einfluss zu nehmen, um seine Rechte zu wahren.[30] Außerdem käme es zur Verletzung des allgemeinen Persönlichkeitsrechts, das in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG Ausdruck findet. Es umfasst unter anderem die Freiheit der Person, selbst darüber zu entscheiden, was für ein Persönlichkeitsbild sie von sich darstellen will.[31]

22 BVerfGE 107, 395 (403); *Hillgruber,* in: GG-Kommentar, 89. EL (2019), Art. 97 Rn. 26.
23 *Hartmann/Schmidt*, Strafprozessrecht: Grundzüge des Strafverfahrensrecht, 7. Aufl. (2018), Rn. 29; *Volk/Engländer,* Grundkurs StPO, 9. Aufl. (2018), § 5 Rn. 2.
24 *Brüggemann,* Die richterliche Begründungspflicht: verfassungsrechtliche Mindestanforderungen an die Begründung gerichtlicher Entscheidungen, 1971, S. 126.
25 *E*uropäisches Parlament und Europäischer Rat: Verordnung (EU) 2018/1725, abrufbar unter: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:32018R1725 (zuletzt abgerufen am 19.4.2020).
26 *Holm*, Science, Vol. 364 (6435), 5.4.2019, S. 26, abrufbar unter: DOI: 10.1126/science.aax0162 (zuletzt abgerufen am 19.4.2020).
27 *Kwong*, Harvard Journal of Law & Technology 2017, 275 (297).
28 *Holm*, S. 27.
29 *Murdoch et al.,* PNAS 2019, S. 22071-22080, abrufbar unter: https://doi.org/10.1073/pnas.1900654116 (zuletzt abgerufen am 2.5.2020); *Krakovna/Doshi-Velez*, abrufbar unter: https://arxiv.org/pdf/1606.05320.pdf (zuletzt abgerufen am 2.5.2020).
30 *Beulke/Swoboda,* Strafprozessrecht, 14. Aufl. (2018), § 2 Rn. 28.
31 BVerfGE 82, 236 (269); vgl. *Fröhlich/Spiecker*, abrufbar unter: https://verfassungsblog.de/koennen-algorithmen-diskriminieren/, 26.12.2018, Abs. 8 (zuletzt abgerufen am 19.4.2020).

Durch die Zuordnung bestimmter Eigenschaften basierend auf Daten, die Dritte über den Angeklagten gesammelt haben, wird es verletzt.[32] Es ist einzuwenden, dass eine solche Verletzung ebenfalls durch die Vorverurteilung des menschlichen Richters erfolgt. Durch die DSGVO ist nach heutigem Stand zumindest schon der erste Schritt hin zu mehr Transparenz in automatisierten Entscheidungsprozessen getan.

3. Vorurteile

Ein menschlicher Richter ohne Vorurteile ist eine Utopie. Subjektive Annahmen über Angeklagte und Zeugen entstehen schon beim Aktenlesen im Zuge der Sitzungsvorbereitung.[33] Solche Vorverurteilungen missachten unterbewusst die in Art. 6 EMRK verankerte Unschuldsvermutung. Eine KI könnte die Unschuldsvermutung wiederherstellen, soweit sie eine neutralere Sichtweise hat. Ein Algorithmus ist aber stets nur so gut wie sein Programmierer. Sobald die Datensätze, durch die die KI Muster erlernt, verzerrt sind, gibt die KI auch ein verzerrtes Resultat aus. Oftmals sind diese Datensätze Polizeiberichte. Sobald diese beispielsweise „Racial Bias" aufweisen, lernt die KI diese Muster und wendet sie auf ihre eigenen Entscheidungen an. Um dem entgegenzuwirken, nutzt die Staatsanwaltschaft in San Francisco eine vom Stanford Computational Policy Lab entwickelte, für US-Behörden kostenlos zur Verfügung gestellte Software, die die schriftlichen Ermittlungsakten der Polizei mithilfe von KI automatisch anonymisiert. Hinweise auf Tatorte oder die Namen der Verdächtigen werden durch neutrale Passagen ersetzt, um „Racial Bias" entgegenzuwirken.[34] Auf Wunsch können die Staatsanwält*innen auch die Originale einsehen. Ähnliches Vorgehen könnte zur Minimierung von Vorverurteilung beitragen und ist daher auch in Deutschland wünschenswert.

IV. Fazit

Ein Einsatz von KI bei Gericht hat das Potenzial, ein Verfahren zu verkürzen und es objektiver zu machen, besonders im Fall von Sachverständigen oder bei der Beurteilung von Glaubwürdigkeit. Die Grenzen von KI sind die Auswertung von Urkundenbeweisen oder die eigenständige Vernehmung von Zeugen, da sie direkte Interaktionen mit oder aktive Handlungen der Verfahrensbeteiligten betreffen. Beim Einsatz von KI sind hohe Datenschutz- und Transparenzstandards geboten. Bei den verwendeten Daten wird es sich um hochsensible persönliche Informationen handeln. Es muss garantiert werden, dass die betroffene Person das Recht hat, bei automatisierten Entscheidungen angehört zu werden, sich einer automatisierten Entscheidung zu widersetzen sowie Rechtsbehelfe einzulegen.[35] Bei einer KI, die von privaten Dritten entwickelt wurde und deren Logik nicht öffentlich einsehbar ist, ist die Unabhängigkeit der Justiz hochgradig gefährdet. Außerdem führt ein Einsatz von KI nicht automatisch zu gerechteren Entscheidungen. Sobald der Datensatz vorurteilsbehaftet ist, lassen sich dahingehende Tendenzen auch im Endergebnis feststellen. Deshalb müssen unbelastete Datensätze als Lernstoff bereitgestellt werden. Der Ansatz der Staatsanwaltschaft in San Francisco ist ein erster Schritt in diese Richtung.

---

32 *Fröhlich/Spiecker*, Abs. 9

33 *Haisch,* Psychologie der Gerichtsverhandlung und richterliche Urteilsbildung, Kriminal-Psychologie: Grundlagen und Anwendungsbereiche, 1983, S. 169; *Bernhardt*, Probleme der Verständigung zwischen Richter und psychologischem Gutachter im deutschen Strafverfahren, 2011, S. 140.

34 *Kemmerich*, San Francisco verwendet KI-Tool zur vorurteilsfreien Beurteilung von Ermittlungen, abrufbar unter: https://www.it-boltwise.de/san-francisco-verwendet-ki-tool-zur-vorurteilsfreien-beurteilung-von-ermittlungen.html, 15. Juni 2019 (zuletzt abgerufen am 19.4.2020).

35 Europäische Kommission für die Effizienz der Justiz (CEPEJ), European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, 2018, abrufbar unter: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (zuletzt abgerufen am 19.4.2020), S. 57 Rn. 145.

Die gesetzlichen Hürden für eine Verwendung von KI bei Gericht sind hoch. Nichtsdestotrotz bietet ein intelligenter Einsatz die Möglichkeit, das deutsche Justizsystem an bestimmten Stellen zu entlasten.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Delvin Sönmezer

Bodycams
Einsatzmöglichkeiten und Zulässigkeitsgrenzen

Inhaltsverzeichnis

I. Einleitung

„*New bodycam video shows handcuffed man led by horseback*“[1]
„*Erst Drohung mit Bodycam beruhigt aufgebrachten Bräutigam*“[2]
„*Von der Verfolgungsjagd bis zum Schäferstündchen – was Bodycams alles aufzeichnen*“[3]

Aktuell finden sich weltweit immer mehr Schlagzeilen zu polizeilichen Einsätzen in den Nachrichten, welche Aufnahmen von Bodycams beinhalten. Dabei handelt es sich um eine Miniatur-Kamera, die über der Uniform an der Schulter von Polizeibeamten angebracht wird.[4] Mit Hilfe der Bodycam werden Bild- und teilweise Tonaufzeichnungen von polizeilichen Einsätzen ermöglicht. Eine Aktivierung und Speicherung der Aufnahme erfolgt manuell durch den kameraführenden Polizeibeamten. Die kleine Kamera bringt allerdings große Konsequenzen mit sich. Ihr Einsatz wirft zahlreiche rechtliche Bedenken auf, insbesondere steht er in einem Spannungsverhältnis zwischen den Rechten von Bürgern und dem Schutz der Polizeibeamten. Inwiefern der Einsatz von Bodycams in diesem Spannungsfeld möglich und sinnvoll ist und wo die Grenzen seiner Zulässigkeit liegen, soll im Folgenden erörtert werden. Kernpunkt der Diskussion bildet dabei die Diskussion der Schutzrichtung des Einsatzes der Bodycam.

Zunächst wird ein Überblick über die Zwecke und Ziele des Einsatzes gegeben, um ein Grundverständnis für die folgenden rechtlichen Bewertungen zu verschaffen. Anschließend wird der Prozess der Einführung näher betrachtet. Der Hauptteil der Arbeit dient zur Darstellung der besonders problematischen rechtlichen Rahmenbedingungen für den polizeilichen Einsatz von Bodycams. Obwohl eine Verallgemeinerung der Regelungen von Einsatzmöglichkeiten in Bundesländern und Bund schwer möglich ist, werden Gemeinsamkeiten bezüglich der Art und Weise des Einsatzes herausgearbeitet. Dabei werden die verfassungsrechtlichen Anforderungen, welche größtenteils von Stimmen in der Literatur gefordert werden, als Zulässigkeitsgrenzen diskutiert.

II. Gründe für den Einsatz von Bodycams

Die Einführung der Bodycams wird mit verschiedenen Zielrichtungen begründet. Hauptsächlich soll mithilfe von Bodycams präventiv der Schutz von Polizeibeamten bezweckt werden.[5] Im Einsatz sehen sich Polizeibeamte häufig aggressivem Verhalten von Bürgern ausgesetzt.[6] Seit der ersten Erfassung von Daten zum Thema „Gewalt

[1] *Shamliam,* https://www.cbsnews.com/news/bodycam-video-shows-handcuffed-man-led-by-horseback-2019-10-02/ (zuletzt abgerufen 13.10.2019), die Aufnahmen einer Bodycam zeigen wie Polizisten einen angeleinten Afroamerikaner, wie er durch die Straßen von Texas geführt wird.
[2] *Thurnes,* https://boostyourcity.de/erst-drohung-mit-bodycam-beruhigt-aufgebrachten-braeutigam (zuletzt abgerufen 13.10.2019).
[3] *Vonarburg,* https://www.aargauerzeitung.ch/schweiz/von-der-verfolgungsjagd-bis-zum-schaeferstuendchen-was-bodycams-alles-aufzeichnen-132989993 (zuletzt abgerufen 13.10.2019).
[4] *Möllers*, Wörterbuch der Polizei, 3. Aufl. (2018) S. 384; *Kipker*, DuD 2017, 165 (165).
[5] Sachstandsbericht „Auswertung der Pilotprojekte zum Einsatz von Body-Cams“ anlässlich der 59. Sitzung des UA FEK, S. 2; *Petri,* Handbuch des Polizeirechts, 6. Aufl. (2018), Rn. 796.
[6] Gewerkschaft der Polizei, Mobile Videoüberwachung- „Body-Cam“, https://www.gdp.de/gdp/gdpber.nsf/id/DE_GdP-fordert-Body-Cam-als-schuetzendes-Einsatzmittel/%24file/bodycam-positionspapier-2016.pdf (zuletzt abgerufen am 7.10.2019).

gegen Polizeibeamtinnen und -beamten“ im Jahr 2011 sind die Fallzahlen im Jahr 2018 im Hinblick auf die Erfassung von Polizeivollzugsbeamten als Opfer bundesweit von 54.843[7] auf 79.598[8] und hinsichtlich der Opfererfassungen der Polizeivollzugsbeamten von 31.072[9] auf 38.413[10] Fälle gestiegen. Die Opfererfassung erfolgt unter der Maßgabe, dass die Tatmotivation im personen-, berufs- bzw. verhaltensbezogenen Merkmal begründet ist oder in Beziehung dazu steht. Bei den Angaben zu den Opferzahlen wurde die Häufigkeit des „Opferwerdens“ gezählt, sodass eine Person, die mehrfach Opfer wurde auch mehrfach als Opfer gezählt wird. Zudem ist bei den statistischen Entwicklungen der Einfluss von einzelnen Ereignissen, wie beispielsweise des G20-Gipfels 2017 in Hamburg zu berücksichtigen.[11]

Für den Einsatz von Bodycams wird weiterhin argumentiert, dass in konfliktbehafteten Situation der potentielle Angreifer nun durch die Erkennbarkeit der Videodokumentationen zu einem kooperativen Verhalten neige.[12] Durch die Nutzung von Bodycams wird zudem seitens des Gesetzgebers eine repressive Zielrichtung verfolgt. Es soll mittels der Videoaufzeichnungen die Ermittlung des Geschehens als Beweismittel im Straf- und Ordnungswidrigkeitsverfahren verbessert werden.[13]

Während sich die Einführung der Bodycam auf Gewalt gegen die Polizei fokussiert, ist die Eindämmung rechtswidriger Polizeigewalt ebenfalls in Deutschland als Zielrichtung zu betrachten. In den USA stellt das wesentliche Motiv die Dokumentation der Polizei dar, um „police accountability“, also die Rechenschaftspflicht der Polizei, zu erreichen.[14] Inwieweit in Deutschland Polizeigewalt existiert, kann anhand der Untersuchungen des Statistischen Bundesamtes hinsichtlich der Korruptionsdelikten und Straftaten von Amtsträgern näher betrachtet werden.[15] Die statistische Auswertungen bieten dabei Befunde zu vorsätzlichen Tötungsdelikten, zur Gewaltausübung und Aussetzungen sowie zu Zwang und Missbrauch des Amtes durch Polizeibedienstete bei Ausübung ihres Dienstes in Deutschland.[16] Zwar ist im Hinblick auf Gewaltausübung und Aussetzung durch Polizeibedienstete ab 2016 (2383 Fälle[17]) betrachtet ein Rückgang festzustellen (2018: 2126[18]), dennoch könnten die erheblichen Zahlen als Indiz für die Notwendigkeit von Maßnahmen zur Eindämmung von Gewalt durch die Polizei sprechen.[19] Während die Gewerkschaft der Polizei das Motiv der Dokumentation einer „vermeintlichen Polizeigewalt“ bereits aus technischen Gründen ablehnt, da binnen kurzer Zeit eine große Ansammlung von Daten entstehen würde[20], kann gerade hinsichtlich der genannten Fallzahlen ein Interesse für Bürger an Videoaufzeichnungen bestehen.[21] Die Aufzeichnung einer Bodycam könnte etwa als Beweismittel in Strafverfahren gegen Polizeibeamte oder für ein verwaltungsgerichtliches Verfahren zur Feststellung der Rechtswidrigkeit einer polizeilichen Maßnahme verwendet werden.[22]

7 BKA, Gewalt gegen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte, Bundeslagebild 2012, S. 9.
8 BKA, Bundeslagebild 2018, S. 69.
9 BKA, Bundeslagebild 2012, S. 9.
10 BKA, Bundeslagebild 2018, S. 69.
11 *Schmidt*, Polizeiliche Videoüberwachung duch den Einsatz von Bodycams, 2016, S. 46.
12 *Donaubauer,* Internationales und Europäisches Strafverfahrensrecht – Der polizeiliche Einsatz von Bodycams, 2017, S. 67.
13 BT-Drs. 18/10939, S. 1.
14 *Lehmann,* SIA-Journal 2/2017, 28 (32).
15 Statistisches Bundesamt, Rechtspflege Staatsanwaltschaften, Fachserie 10 Reihe.
16 Statistisches Bundesamt, Rechtspflege Staatsanwaltschaften, Fachserie 10 Reihe 2.6-2015, S. 22.
17 A.a.O.
18 A.a.O.
19 Vgl. 2015: 2233 Fälle Statistisches Bundesamt, Fachserie 10 Reihe 2.6-2015, S. 22; 2016: 2383 Fälle Statistisches Bundesamt, Fachserie 10 Reihe 2.6-2016, S. 22; 2017: 2177 Fälle Statistisches Bundesamt, Fachserie 10 Reihe 2.6-2017, S. 22.
20 Gewerkschaft der Polizei, Mobile Videoüberwachung- „Body-Cam“. https://www.gdp.de/gdp/gdpber.nsf/id/DE_GdP-fordert-Body-Cam-als-schuetzendes-Einsatzmittel/%24file/bodycam-positionspapier-2016.pdf (zuletzt abgerufen am 7.10.2019).
21 *Schmidt*, S. 48.
22 A.a.O.

III. Rechtsgrundlage des Einsatzes von Bodycams

Die Nutzung von Bodycams findet mittlerweile sowohl in den Bundesländern als auch im Bund ihre Rechtsgrundlage. Seit mehreren Jahren werden in einigen Bundesländern Bodycams erprobt. Während einige Länder die Nutzung gesetzlich verankert haben[23], findet der Einsatz ohne eigenständige Normen in Berlin, Brandenburg, Niedersachsen, Rheinland-Pfalz, Sachsen und Thüringen statt, wobei teilweise legislative Prozesse bereits angestoßen wurden.[24] Hessen nimmt als erstes deutsches Bundesland, das bereits 2013 die Nutzung der Bodycams im Rahmen eines Pilotprojektes einführte, eine Vorreiterrolle ein.[25] Dabei sollten die Auswirkungen von Videokameras hinsichtlich Übergriffen auf Polizeibeamte und der Aufklärung der Sachlage im Frankfurter „Kneipenviertel" Alt-Sachsenhausen ermittelt werden.[26] Bereits nach 6 Monaten erwies sich der Einsatz von Bildaufnahmen als „deeskalierend"[27] und „präventiv".[28] Hinsichtlich der subjektiven Wahrnehmung schilderten Teilnehmer der Erprobungen, dass sie von kontrollierten Personen respektvoller behandelt wurden.[29] Seitens der Störer wurde eine positive Verhaltensänderung bezüglich der Kooperationsbereitschaft wahrgenommen.[30] Unter anderem konnte eine Verringerung der Widerstandshandlung gegen Polizeibeamte von 40 auf 25 Fälle festgestellt werden.[31] Zudem konnten 24 Sequenzen als Beweismittel eingesetzt werden.[32] Hierbei ist allerdings die begrenzte „statistische Aussagekraft" zu beachten, da es sich um einen „verhältnismäßig kleinen Datenbestand" handelt.[33] Darüber hinaus sei zu berücksichtigen, dass das Datenmaterial von der Polizei selbst gesammelt und ausgewertet wurde.[34] Trotz dessen führte die positive Resonanz der Erprobung zur Einführung von Regelungen hinsichtlich der Nutzung von Bodycams in weiteren Bundesländern. Infolgedessen startete die Bundespolizei Anfang des Jahres 2016 ebenfalls Pilotprojekte in verschiedenen Städten (Hamburg, Köln, Düsseldorf, Berlin und München).[35] Am 5. Mai 2017 wurde dann der § 27a BPolG zur Verbesserung der Fahndung bei besonderen Gefahrenlagen und zum Schutz von Bundespolizeibeamten eingeführt.[36] Zudem befinden sich weitere Einzelheiten zur Nutzung von Bodycams in der durch eine vom Bundesinnenministerium (BMI) und Bundespolizeihauptpersonalrat beim BMI (BHPR) gemeinsam erlassenen Dienstvereinbarung vom 15. Februar 2019.[37]

IV. Einsatzmöglichkeiten von Bodycams

Aufgrund der diversen Ausgestaltungen in den einzelnen Gesetzen sowie der spezifischen Systematik der Landes- und Bundesgesetzgebung ist eine Verallgemeinerung der Einsatzmöglichkeiten schwer möglich. Im Folgenden

---

23 § 21 Abs. 4, S. 2 PolG Baden-Wüttenberg; Art. 32 PAG Bayern; § 29 V Brem- PolG Bremen; § 8 I DVPolG Hamburg; § 14 Abs. 6 HSOG Hessen; § 15c PolG NRW; § 32a MVSOG Mecklenburg-Vorpommern, § 27 Abs. 3 Saarl-PolG Saarland, § 16 Abs. 3a – 4a LSASOG Sachsen-Anhalt, § 184 Abs. 3 SchlHLVwG Schleswig-Holstein.

24 *Köhler/Thielicke,* NVwZ-Extra 13/2019, 1 (2).

25 *Parma,* DÖV 2016, 809 (809).

26 A.a.O.

27 Sachstandsbericht „Auswertung der Pilotprojekte zum Einsatz von Body-Cams" anlässlich der 59. Sitzung des UA FEK TOP 2.4, S. 6.

28 A.a.O.

29 *Parma,* DÖV 2016, 809 (809).

30 Sachstandsbericht „Auswertung der Pilotprojekte zum Einsatz von Body-Cams" anlässlich der 59. Sitzung des UA FEK TOP 2.4, S. 6.

31 A.a.O.

32 A.a.O.

33 *Zurawski*, Landtag NRW 16. Wahlperiode, Stellungnahme 16/2456 A09; Innenminister Boris Rhein: „Body-Cam" verhindert Gewalt gegen Polizeibeamte (Pressemitteilung), S. 6

34 *Schmidt*, S. 56.

35 *Parma,* DÖV 2016, 809 (813).

36 *Ruthig,* in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. (2019), BPolG, § 27a Rn. 1; BT-Drs. 18/10939.

37 BMI Dienstvereinbarung über die Nutzung von körpernah getragenen Aufzeichnungsgeräten (Bodycams), der zum unmittelbaren Betrieb der Bodycams notwendigen technischen Geräte und Systeme zur Datenverarbeitung sowie der erzeugten Bild- und Tonaufnahmen, 22.2.2019.

werden deshalb insbesondere Gemeinsamkeiten bezüglich des sachlichen Anwendungsbereichs dargestellt. Zudem beschränkt sich die Ermittlung der Zulässigkeitsgrenzen auf verallgemeinerungsfähige Aussagen und es wird beispielhaft auf einzelne Regelungsmaterien Bezug genommen, die besonders problematisch erscheinen.

1. Aufzeichnungsanlass

Eine Aufnahme des Geschehens erfolgt allein durch die Entscheidung der das Aufnahmegerät tragenden Polizeibeamtinnen und -beamten. Unter Berücksichtigung der konkreten Umstände des Einzelfalls ist unter der Voraussetzung, dass eine „Gefahr für Leib und Leben“[38] vorliegt, die Anfertigung der Aufzeichnung gestattet. Demnach soll die Aufzeichnung in Situationen angestoßen werden, die nach polizeilichem Erfahrungswissen auf eine Eskalationsgefahr schließen lassen.[39] Die Daueraufnahme des gesamten Streifengangs ist unzulässig.[40] Inwieweit dies das Vertrauensverhältnis von Bürgern zur Polizei verbessern könnte, erscheint zweifelhaft.[41]

Angesichts des Gebots der Datensparsamkeit[42] sei seitens des Gesetzgebers eine anlasslose und dauerhafte Aufzeichnung abzulehnen, da sonst ein Verstoß gegen das rechtsstaatliche Übermaßverbot vorliegen würde.[43] Des Weiteren würden in massivem Umfang personenbezogene Daten unbeteiligter Passanten aufgezeichnet werden.[44] Unter dem Gesichtspunkt der Polizeigewalt hätte eine Daueraufnahme den Vorteil, dass die Polizei nicht durch selektives Ein- und Ausschalten der Kamera eigenes Fehlverhalten verbergen könnte.[45] Insbesondere in den USA werden Bodycams zum Schutz des Bürgers eingesetzt, um polizeiliche Übergriffe zu dokumentieren. Im Gegensatz dazu besteht in Deutschland durch das Ermessen der Polizei für Betroffene kein Anspruch auf den Einsatz der Bodycam.[46] Die einseitige Ausrichtung der Maßnahme nach den Interessen der Polizei hat zur Folge, dass die Rechte von Betroffenen aus Art. 19 Abs. 4 GG nicht ausreichend geschützt werden.[47] Letztlich ist die Debatte abhängig davon, unter welchem Gesichtspunkt – Gewalt gegen Polizeibeamte oder von diesen ausgehende rechtswidrige Gewalt – der Einsatz von Bodycams begründet wird. Sowohl hinsichtlich der Zweckrichtung des Schutzes von Polizeibeamten als auch des Schutzes von Dritten wäre eine Daueraufnahme vorteilig. Allerdings unterscheiden sich die Motive in Bezug auf die daraus resultierenden Nachteile.

Somit ist eine Entscheidung nur unter der Interessenabwägung zwischen dem Interesse der Polizeibeamten, durch die Bodycam keiner „Totalüberwachung“ an ihrem Arbeitsplatz ausgesetzt zu sein, und dem Interesse der Betroffenen, eine ihren Schutz vor unzulässigen Maßnahmen untergrabende selektive Handhabung zu vermeiden, möglich. Jedoch wurde mit Blick auf die technischen Kapazitäten eine Daueraufnahme ohnehin vorerst verneint. Um eine Alternative zu bieten, wurde in verschiedenen Bundesländern das Pre-Recording eingeführt.[48]

38 Bspw. § 27a BPolG.
39 *Martini/Nink/Wenzel,* NVwZ-Extra 24/2016, 1 (9).
40 *Arzt/Schuster*, DVBI 2018, 351 (354).
41 *Kipker/Gärtner,* NJW 2015, 296 (298).
42 gem. § 3a BDSG.
43 *Lachenmann,* NVwZ 2017, 1424 (1426).
44 *Kipker/Gärtner,* NJW 2015, 296 (298).
45 A.a.O.
46 *Arzt/Schuster,* DVBI 2018, 351 (354).
47 *Arzt/Schuster*, DVBI 2018, 351 (355).
48 gem. § 27 a BPolG, § 21 Abs. 5, Abs. 6 BWPolG, Art. 33 Abs. 4 BayPAG, § 29 Abs. 5 Brem-PolG, § 14 Abs. 6 Hess-SOG, § 32a MVSOG, § 15c NRWPolG, § 27 Abs. 3 Saarl-PolG, § 16 Abs. 3a – 4a LSASOG, § 184 Abs. 3 SchlHLVwG.

2. Pre-Recording

Bei dem sogenannten Pre-Recording-Modus nimmt die Kamera das Geschehen im Dauerbetrieb auf und überschreibt die Daten zeitgleich.[49] Betätigt der Beamte nun den Auslöseknopf zur Aufnahmespeicherung, wird dabei die beginnende Sequenz und das bereits Geschehene (bspw. in Hessen 30 Sekunden) gespeichert.[50] Dies dient der Sicherstellung einer umfangreichen Beurteilung in Notfallsituationen hinsichtlich der Ursache und des gesamten Geschehensverlaufs.[51] Jedoch erscheint eine vorherige Aufnahme zweifelhaft in Anbetracht der Tatsache, dass das Pre-Recording dem Betroffenen in der Regel nicht offenkundig ist.[52] Weil es sich nicht um eine stationäre Videoüberwachung an öffentlichen Orten wie beispielsweise Bahnhöfen handelt, die dem Betroffenen von vorneherein bekannt ist, besteht keine Möglichkeit, sich der Aufnahme zu entziehen. [53]

3. Pre-Recording als Grundrechtsverletzung

Fraglich ist, inwiefern das Pre-Recording einen Eingriff in die Grundrechte der Betroffenen darstellt. Dabei könnten das Allgemeine Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hinsichtlich des Rechts auf informationelle Selbstbestimmung, des Rechts am eigenen Bild oder am gesprochenen Wort betroffen sein. Werden die durch die Rechtsprechung des *Bundesverfassungsgerichts* hinsichtlich der automatischen Kfz-Kennzeichnungserfassung entwickelten Kriterien übertragen, ist ein Grundrechtseingriff abzulehnen.[54] Ein Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung wurde hier verneint, „soweit Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym [...] ausgesondert werden“[55]. Dagegen spricht bereits, dass die Rechtsprechung auf das Pre-Recording nicht übertragbar ist, weil es an einer rein technischen Verarbeitung fehlt, in der ein sofortiger spurenloser Löschungsvorgang erfolgen kann „ohne die Möglichkeit, einen Personenbezug herzustellen“[56]. Das Pre-Recording ermöglicht dem Kameraträger nämlich die Herrschaft über die Videosequenz.[57] Demnach ist die Frage der Speicherung und Auswertung von der subjektiven Einschätzung eines Polizeibeamten und nicht eines Computers abhängig.[58] Zudem ist die Datenqualität zwischen einer automatischen Kennzeichenerfassung und einer Bodycam-Aufzeichnung zu unterscheiden. Während ersteres lediglich Buchstaben und Zahlen erfasst, werden bei der Ton- und Bildaufnahmen personenbezogene Daten erhoben, sodass ein rein technischer Funktionsablauf nicht vorliegt.[59] Somit stellt die Pre-Recording-Funktion einen Eingriff in das Allgemeine Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. [60]

---

49 *Lachenmann,* NVwZ 2017, 1424 (1427); Stellungnahme des Deutschen Anwaltsvereins durch den Ausschuss Gefahrenabwehrrecht zum Einsatz von Bodycams bei der Polizei https://www.bundestag.de/rsource/blob/494776/248d5d35c5d066614a2476440b1af03b/18-4-728-data.pdf (zuletzt abgerufen am 7.10.2019).
50 *Parma,* DÖV 2016, 809 (810); *Ruthig,* in: Schenke/Graulich/Ruthig, Rn. 19 f.
51 *Parma,* DÖV 2016, 809 (810).
52 A.a.O.
53 *Möllers*, S. 384.
54 *BVerfG*, Urt. v. 11.3.2008 – 1 BvR 2074/05 und 1 BvR 1254/07.
55 A.a.O.
56 A.a.O.
57 *Parma,* DÖV 2016, 809 (810).
58 Stellungnahme des Deutschen Anwaltsvereins durch den Ausschuss Gefahrenabwehrrecht zum Einsatz von Bodycams bei der Polizei, S. 5., abrufbar unter: https://www.bundestag.de/rsource/blob/494776/248d5d35c5d066614a2476440b1af03b/18-4-728-data.pdf (zuletzt abgerufen am 7.10.2019); *Zöller*, Der Einsatz von Bodycams zur polizeilichen Gefahrenabwehr, 2017, S. 64.
59 *Zöller*, S. 64.
60 *Möllers*, S. 384.

a) Rechtfertigungsmöglichkeiten

Trotz weiterer Versuche wie beispielsweise des hessischen Gesetzgebers, der Kritik einer klaren Eingriffsschwelle gerecht zu werden, indem die kurzfristige technische Erfassung an eine Identitätsfeststellung und eine konkrete Gefahr von erheblichen Rechtsgütern knüpft, bestehen weiterhin Bedenken hinsichtlich der verfassungsrechtlichen Rechtfertigung. Hierbei wird vertreten, dass eine Rechtfertigung unvorstellbar sei[61], da der verfolgte Zweck der Maßnahme nicht eindeutig feststeht und insbesondere die Erforderlichkeit im Rahmen einer Verhältnismäßigkeitsprüfung fraglich erscheint.[62] Infolge der Gesetzesänderung des § 14 Abs. 6 S. 1 HSOG steht Polizeibeamten im Rahmen des Auswahlermessens zu, ob während der Identitätsfeststellung bei einer zunehmenden Aggressivität nun das Pre-Recording oder die unmittelbare Aufnahmefunktion betätigt werden soll.[63] Allerdings wird dabei der Zweck einer Pre-Recording-Funktion verfehlt. Eine Aufnahme der Gefahrensituation im Vorfeld ist lediglich möglich, soweit das Pre-Recording dauerhaft eingeschaltet werden kann oder die Aktivierung an eine niedrige Eingriffsschwelle anknüpft.[64] Weiterhin mangelt es an der Transparenz, da hierbei zumindest kein Hinweis auf die laufende Aufzeichnung erfolgt.[65] Somit lässt sich festhalten, dass die Nutzung der Pre-Recording-Funktion einen nicht zu rechtfertigenden Grundrechtseingriff darstellt.

b) Mögliche Bedingung für die Zulässigkeit

Das Pre-Recording könnte verfassungsrechtlich als zulässig angesehen werden, soweit die gesetzlichen Rechtsgrundlagen der Kritik angepasst werden. Beispielsweise könnte bestimmt werden, dass die Aufnahme nach einer festgelegten Zeitdauer unwiderruflich gelöscht und überschrieben wird, wenn kein manueller Start der Kamera erfolgte.[66] Zudem könnte die Erkennbarkeit für den Betroffenen hergestellt werden, indem an der Kamera ein Licht signalisiert, dass die Kamera angeschaltet ist. Es empfiehlt sich allerdings, bei einer Bodycam-Nutzung nicht nur faktisch die Pre-Recording-Funktion ausgeschaltet zu lassen, sondern den Verzicht auf die Nutzung dieser Option auch gesetzlich ausdrücklich zu bestimmen.[67]

4. Speicherung

Zur Sicherung der Videos werden aktuell zwei Systeme verwendet, das so genannte Blackboxing und das Clouding.[68] Durch das Blackboxing ist es Unberechtigten nicht möglich einen Zugriff auf die Aufnahmen zu erlangen.[69] Die Aufzeichnungen bleiben verschlossen und durchlaufen regelmäßig einen systematisierten Löschungsprozess. Lediglich mithilfe eines Zwei-Schlüssel-Prinzips[70], wird ein Zugriff auf die Daten ermöglicht.[71] Beim Clouding werden die aufgenommenen Daten über das Internet an eine virtuelle Cloud (Server) übermittelt und dort gesichert, wodurch sie weltweit gesehen werden können.[72] Insbesondere das Clouding, welches bspw. von der Bundespolizei

61 *Parma,* DÖV 2016, 809 (810); *Zöller*, S. 64; *Dembrowski,* Polizeispiegel 2015, Heft 4, 22 (24).
62 *Ruthig,* in: Schenke/Graulich/Ruthig, Rn. 20.
63 *Parma,* DÖV 2016, 809 (811).
64 A.a.O.
65 *Zöller*, S. 65.
66 *Lachenmann,* NVwZ 2017, 1424 (1427).
67 *Zöller*, S. 65.
68 *Köhler/Thielicke,* NVwZ-Extra 13/2019, 1 (1).
69 A.a.O.
70 Gemeinsames Handeln zweier Personen.
71 *Lachenmann,* NVwZ 2017, 1424 (1428).
72 *Köhler/Thielicke,* NVwZ-Extra 13/2019, 1 (1).

verwendet wird, ist aus datenschutzrechtlicher Sicht kritisch zu beurteilen. Wie aktuell bekannt geworden ist, nutzt die Bundespolizei derzeit den amerikanischen Dienstanbieter „Amazon" zur Sicherung und Verarbeitung von Daten.[73] Infolgedessen kann ein Zugriff von US-Behörden nicht ausgeschlossen werden, da nach dem Cloud-Act amerikanische Firmen den Sicherheitsbehörden unter bestimmten Anforderungen zur Herausgabe aller Daten, gleich ob im In- oder Ausland erhoben und/oder gespeichert, verpflichtet sind.[74] Die Aussage der Bundesregierung, dass die Sicherung von Daten auf AWS-Servern keine Gefahr darstelle, erscheint diskussionswürdig.[75]

5. Löschung

Die gesetzlichen Regelungen hinsichtlich der Löschungsfrist der gespeicherten Aufnahmen sind uneinheitlich. Dabei unterscheiden sich die Regelungen bezüglich der Vorgehensweise (manuell[76] oder automatisch[77]) und der Länge der Speicherfrist[78], die nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten (Zweckänderungsklausel) erforderlich sind. In Hinblick auf die Festlegung einer Speicherfrist von Aufnahmen, welche nicht der Strafverfolgung dienen, wie bspw. § 15c Abs. 4 S. 1 BPolG NRW[79], lässt sich nach einer Ansicht die Notwendigkeit einer Mindestspeicherfrist nicht erschließen. Regelmäßig ist bereits unmittelbar nach Schichtende die Zweckänderung zur Strafverfolgung der Aufnahme offenkundig.[80] Des Weiteren ist hierbei auch der Grundsatz der Datensparsamkeit zu berücksichtigen, sodass die Regelung als verfassungswidrig betrachtet wird.[81] Allerdings ermöglicht die Speicherung einer Aufnahme für den Betroffenen die Ausübung eigener Rechte zur späteren Sachverhaltsaufklärung.[82] Insbesondere im Hinblick auf das Recht der Einsichtnahme des Betroffenen würde bei der Möglichkeit der unverzüglichen Löschung der Aufnahme der Zweck „faktisch ins Leere laufen".[83] Einen Anspruch auf Einsicht und Zugriff der Aufnahmen wird mit der Waffengleichheit, Transparenz staatlichen Handelns und dem Gebot des effektiven Rechtsschutzes begründet.[84] Dabei kann dies nicht unmittelbar aus den Richtlinien zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung abgeleitet werden, da es sich um ein Auskunftsrecht handelt. Jedoch kann sich das Auskunftsrecht „je nach Antrag der betroffenen Person und den weiteren Umständen des Einzelfalls zu einem Einsichtsrecht verdichten"[85]. Somit erscheint die Voraussetzung einer Mindestspeicherfrist angemessen.

73 ZD-Aktuell 2019, 06560.
74 A.a.O.
75 BT-Drs. 19/8180, S. 15.
76 Bspw. in Bremen und Hamburg.
77 Bspw. in Hessen und Rheinland-Pfalz.
78 Bspw. Schleswig-Holstein § 184 Abs. 3 S. 2 LVwG SH spätestens nach 3 Tagen, Bremen nach 2 Monaten nach § 29 Abs. 5 S. 4 und 5 BremPolG, Badenwüttenberg § 21 VII 1 BWPolG statt einer festgelegten Löschungsfristwird an das Gebot der Unverzüglichkeit zugegriffen.
79 Innerhalb von 2 Wochen sind Aufzeichnungen zu löschen.
80 Stellungnahme Innenausschluss 16/4207, S. 4 abrufbar unter: https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMST16-4207.pdf;jsessionid=AB6A012271C8ED647138EE486A880F6F (zuletzt abgerufen am 8.10.2019); *Meixner/Fredrich*, Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG), 12. Aufl. (2016), § 14 Rn. 23.
81 *Arzt,* in: BeckOK-GG, 41. Edition, Stand: 15.5.2019, PolG NRW, § 15c Rn. 57.
82 *Lachenmann,* NVwZ 2017, 1424 (1428).
83 *Schmidt*, S. 312.
84 *Petri*, S. 797.
85 *Petri*, S. 802.

6. Datenauswertung

Die Speicherung von Aufnahmen mithilfe von Bodycams hat zur Folge, dass die Art und Weise der Datenauswertung geregelt werden muss. Hierbei mangelt es an gesetzlichen Regelungen, welche die Zugriffsperson und Voraussetzungen der Weiterverarbeitung von Daten festlegen.[86] Mithin soll insbesondere sichergestellt werden, dass der Polizei keine Möglichkeit zusteht, „unliebsame" Aufzeichnungen zu löschen.[87] Der Notwendigkeit einer diesbezüglichen Regelung wird die Bindung der Polizei an Recht und Gesetz gem. Art. 20 Abs. 3 GG entgegengehalten.[88] Polizei- und Datenschutzgesetze sollen bereits spezifische Regelungen zur weiteren Datenverarbeitung enthalten, sodass eine Überfrachtung der Normen hinsichtlich der Nutzung von Bodycams entgangen werden kann.[89] Inwiefern dies einen ausreichenden Schutz für den Betroffen darstellt, steht offen, insbesondere wenn eine Alterative zur transparenten Datenverarbeitungen vorgeschlagen wird. Dabei handelt es sich um eine unabhängige Treuhandstelle, welche eine unabhängige Kontrolle durch nicht weisungsgebundene Mitarbeiter bereitstellt.[90] Dagegen wird auf bürokratische Hemmnisse bezüglich der Effektivität der Auswertung und schnellen Löschung aufmerksam gemacht. Jedoch ist nicht ersichtlich, weshalb die Auswertung durch Mitarbeiter, die im Gegensatz zu Polizeibeamten lediglich die Aufgabe ausführen, an der Effektivität scheitern würden. Einer gesonderten Einrichtung bedarf es dabei nicht, sodass eine interne Stelle innerhalb der Polizei als ausreichend betrachtet werden könnte.[91]

V. Fazit/ Ausblick

Abschließend ist festzustellen, dass Bodycams ein nützliches polizeiliches Einsatzmittel zur Abschreckung potentieller Gewalttäter und zur Beweissicherung des Einsatzgeschehens darstellen. In absehbarer Zeit könnte die Bodycam zum Standardinstrument werden. Allerdings müssen die Bundes- und Landesgesetze ausdrücklich bestimmte Ermächtigungsgrundlagen zur Nutzung vorsehen, welche Verfassungskonformität ausweisen. Unverkennbar lässt sich festhalten, dass hinsichtlich der Einsatzmöglichkeiten Ausgangspunkt der Debatten die Zweckrichtung der Bodycam ist. Obwohl sich der Gesetzgeber darum bemüht, die Grundrechte der Betroffenen zu berücksichtigen, muss er sich eingestehen, dass ein Teil der Debatte auch unter dem Gesichtspunkt der Polizeigewalt betrachtet werden muss. Dementsprechend muss die Gesetzeslage so angepasst werden, dass die Aufnahme nicht allein im Ermessen der Polizei steht und der Zugang zu dem Datenmaterial gesichert wird.

86 *Kipker/Gärtner*, NJW 2015, 296 (299); *Martini/Nink/Wenzel,* NVwZ-Extra 24/2016, 1 (11).
87 So *Arzt,* Schriftliche Stellungnahme v. 15.2.2017, S. 16.
88 *Schmidt*, S. 314.
89 *Schmidt*, S. 314.
90 *Kipker/Gärtner*, NJW 2015, 296 (299 f.); *Kipker*, DuD 2017, 165 (167).
91 *Lachenmann,* NVwZ 2017, 1424 (1429).

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Paula Benedict

WhatsApp-Nachrichten als Beweismittel

Inhaltsverzeichnis

I. Einleitung

Die rasante technische Entwicklung hat einen großen Einfluss auf die Gesellschaft und verändert so auch die Kommunikation. Mithin werden technische Geräte und die mit ihnen verarbeiteten Daten auch immer relevanter für das Recht. In Bezug auf das Strafprozessrecht stellen diese Daten enormes Potential dar, da sie viel Aufschluss über das Leben von Tätern und Straftaten geben können. Vor allem Nachrichten über Messengerdienste wie WhatsApp spielen eine große Rolle. Sie sind oft so persönlich wie ein privates Telefongespräch, werden jedoch im Unterschied zu diesen ohne Weiteres auf den Endgeräten gespeichert. Täter teilen möglicherweise Motive, Abläufe und Standorte mit ihren Kommunikationspartnern. Die Nachrichten können folglich eine hohe Beweiskraft haben. Allerdings kann eine Verwendung im Strafverfahren einen starken Eingriff in die Privatsphäre darstellen. In dieser Arbeit werden WhatsApp-Nachrichten als Beweismittel näher betrachtet. Zunächst wird das Beweisrecht vorgestellt, um in diesem Kontext die WhatsApp-Nachrichten als Beweismittel einordnen zu können. Dabei wird sowohl auf den Zugriff auf diese im Ermittlungsverfahren als auch auf die Einführung als Beweismittel in die Hauptverhandlung eingegangen.

II. WhatsApp-Nachrichten als Beweismittel

1. WhatsApp-Nachrichten

WhatsApp ist ein Instant-Messaging-Dienst, mit dem Nutzer Textnachrichten, Ton-Dateien, Dokumente, Standort und Kontaktinformationen verschicken sowie internetbasiert telefonieren können.[1] Die Nachrichten werden seit 2016 von WhatsApp in Echtzeit mittels einer sogenannten „End-to-End-Verschlüsselung“ gesichert.[2] Dies gilt sowohl für Nachrichten zwischen zwei Personen als auch für solche, die in „WhatsApp-Gruppen“, also an mehrere Teilnehmer, versendet werden.[3] WhatsApp als Unternehmen speichert nur nicht-zugestellte Nachrichten auf seinen Servern, jedoch auch das nur verschlüsselt und kann selbst nicht auf diese zugreifen.[4]

a) Telekommunikationsvorgang

WhatsApp-Nachrichten fallen unter den Begriff der Inhaltsdaten des Telekommunikationsvorgangs. Telekommunikation umfasst alle Formen der Nachrichtenübermittlung unter Raumüberwindung in nichtkörperlicher Weise mittels technischer Einrichtungen.[5] Als „wesentliche Orientierungshilfe“ wird zur Definition des Begriffs § 3 Nr. 22 TKG herangezogen, welcher Telekommunikation als den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen bezeichnet.[6] Inhaltsdaten sind dabei alle Daten, die den tatsächlichen Nachrichteninhalt umfassen.[7]

---

1 *Graf*, in: BeckOK-StPO, 28. Edition, § 100a Rn. 71.
2 WhatsApp Encryption Overview, Technical White Paper, 2017, abrufbar unter: https://scontent.whatsapp.net/v/t61.22868-34/68135620_760356657751682_6212997528851833559_n.pdf/WhatsApp-Security-Whitepaper.pdf?_nc_sid=41cc27&_nc_ohc=e-uwISyWn80AX9WAcN-&_nc_ht=scontent.whatsapp.net&oh=60952870742ce73726838cb700385350&oe=5ED81153 (zuletzt abgerufen am 27.5.2020).
3 WhatsApp Encryption Overview, Technical White Paper.
4 https://www.WhatsApp.com/security/ (zuletzt abgerufen am 8.1.2018).
5 *Bruns,* in: KK-StPO, 7. Aufl. (2013), § 100a Rn. 4; *BGH*, NStZ 1997, 247.
6 *BGH,* NJW 2001, 1587.
7 Graf, in: BeckOK-StPO, § 100a Rn. 39.

b) Ermittlungsverfahren

Fraglich ist, auf welche Art und Weise die Strafverfolgungsbehörden im Ermittlungsverfahren Zugriff auf die in den Inhaltsdaten verschlüsselten Nachrichten erlangen können.

aa) Telekommunikationsüberwachung eines laufenden Vorgangs § 100a StPO

Ein Zugriff auf die Nachrichten während des laufenden Telekommunikationsvorgangs kann in bestimmten Fällen über die richterlich angeordnete Telekommunikationsüberwachung nach § 100a StPO erfolgen. Diese kann auch ohne das Wissen des Betroffenen stattfinden (verdeckte Ermittlungsmaßnahme). Zunächst muss es sich dafür um Telekommunikation handeln, die überwacht werden soll.[8] Weiterhin muss ein auf bestimmten Tatsachen beruhender, ausreichender Tatverdacht vorliegen. Das Vorliegen dessen liegt im Beurteilungsspielraum des anordnenden Ermittlungsrichters.[9] Der Tatverdacht muss sich auf eine der in § 100a Abs. 2 StPO benannten Katalogtaten beziehen. Ausreichend ist dabei auch der bloße Versuch einer solchen oder eine Vorbereitungstat.[10] Zudem sind die Strafverfolgungsbehörden nach § 100a Abs. 1 Nr. 2 StPO zu einer Einzelfallprüfung verpflichtet, bei der sie jede Tat darauf prüfen müssen, ob sie in diesem konkreten Fall besonders schwer wiegt.[11] Eine Telekommunikationsüberwachung darf ferner nach § 100a Abs. 1 Nr. 3 StPO nur angeordnet werden, wenn die Sachverhaltserforschung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Weiterhin muss auch diese immer dem Verhältnismäßigkeitsgrundsatz entsprechen.

Auch während der Nachrichtenübermittlung, also vor Empfang auf dem Gerät des Adressaten, kann eine Telekommunikationsüberwachung der Inhaltsdaten auf § 100a StPO gestützt werden.[12] Eine solche Telekommunikationsüberwachung kann durch den Anbieter der Telekommunikationsdienste erfolgen, in diesem Fall WhatsApp Inc. Dieser müsste den Strafverfolgungsbehörden eine Kopie der zu überwachenden Telekommunikationsinhalte bzw. –daten zur Verfügung stellen. Problematisch erscheint hierbei, dass WhatsApp aufgrund der „End-to-End"-Verschlüsselung der Nachrichten selbst nicht auf diese zugreifen kann. Daher können die Behörden selber die Überwachung durchführen. Bei der Quellen-Telekommunikationsüberwachung werden technische Vorkehrungen getroffen, die Kommunikationsdaten noch vor ihrer Verschlüsselung bzw. nach ihrer Entschlüsselung auf dem Gerät abfängt.[13] Diese ist jedoch nur verfassungsgemäß, sofern sie sich ausschließlich auf Daten aus dem laufenden Telekommunikationsvorgang beschränkt, was technisch sichergestellt sein muss.[14] Im Falle der WhatsApp-Nachrichten wird aber auch dies kaum möglich sein, da die Daten, selbst wenn sie noch nicht beim Empfänger angelangt sind, auf Servern von WhatsApp verschlüsselt gespeichert sind,[15] der Vorgang also bereits abgeschlossen ist. § 100a StPO kann mithin in Bezug auf WhatsApp-Nachrichten keine Anwendung finden.

8 Zur Begriffsdefinition s. oben.
9 *BGH*, NJW 1995, 1974 ff.; *Günther,* in: MüKo-StPO, 2014, § 100a Rn. 74 f.
10 *Bruns*, in: KK-StPO, § 100a Rn. 31.
11 BT-Drs. 16/5846, S. 40.
12 *Bär*, TK-Überwachung, 2009, § 100a Rn. 12.
13 *Bruns*, in: KK-StPO, § 100a Rn. 27.
14 *BVerfG*, NJW 2008, 822.
15 Siehe oben.

bb) Nach Abschluss des Telekommunikationsvorgangs

(1) Sicherstellung bzw. Beschlagnahme nach § 94 StPO

Nach Abschluss des Kommunikationsvorgangs könnte ein Zugriff auf die auf einem Endgerät oder Server gespeicherten Daten zunächst über die Sicherstellung bzw. Beschlagnahme nach § 94 Abs. 1, 2 StPO erfolgen. Diese stellt typischerweise eine offene Ermittlungsmaßnahme dar. Dabei wird (bei Fehlen einer Einwilligung) aufgrund einer richterlichen Anordnung (§§ 94 Abs. 2, 98 StPO) ein Gegenstand in Verwahrung genommen oder in anderer Weise sichergestellt. Objekt der Sicherstellung kann dabei jeder Gegenstand sein, der einen Beweiswert haben und für die Untersuchung von Bedeutung sein kann.[16] Die Untersuchung beinhaltet das gesamte Strafverfahren von der Einleitung bis zum rechtskräftigen Abschluss.[17] Der Gegenstand muss als Beweismittel in Frage kommen. Beweismittel ist jeder Gegenstand, der unmittelbar oder mittelbar in der Lage ist, für die Tat oder die Umstände ihrer Begehung Beweis zu erbringen oder für den Straffolgenausspruch Beweisbedeutung hat.[18] Um als potentielles Beweismittel angesehen werden zu können, genügt es, wenn in einer ex ante Betrachtung nicht ausgeschlossen werden kann, dass der Gegenstand im weiteren Verfahren zu Beweiszwecken verwendet wird.[19] Zur Ermächtigung der Strafverfolgungsbehörden genügt ein einfacher Anfangsverdacht i.S.v. § 152 Abs. 2 StPO, d.h. konkrete Tatsachen müssen die Annahme belegen, dass eine verfolgbare Straftat begangen wurde.[20] Zudem muss die Sicherstellung bzw. Beschlagnahme auch verhältnismäßig sein. Die Anordnung einer Beschlagnahme i.S.v. § 94 Abs. 2 StPO bei Fehlen der Freiwilligkeit liegt also grundsätzlich im Ermessen des Ermittlungsrichters.

Der weite Begriff des „Gegenstands" i.S.v. § 94 StPO erlaubt auch die Beschlagnahmefähigkeit nicht körperlicher Gegenstände. Daher sind auch Inhaltsdaten nach Abschluss des Telekommunikationsvorgangs von § 94 StPO erfasst.[21] Der Zugriff auf die Daten kann durch Sicherstellung bzw. Beschlagnahme von Ausdrucken oder Datenträgern selbst erfolgen. Es entspricht jedoch regelmäßig der Verhältnismäßigkeit, nicht den Datenträger selbst zu beschlagnahmen, sondern eine Durchsuchung bzw. Durchsicht i.S.v. §§ 102 i.V.m. 110 Abs. 3 StPO des Datensatzes vorzunehmen, da betroffene Datenträger oft Informationen über unbeteiligte Dritte enthalten.[22] Die Behörden können also eine Spiegelung des Mobiltelefons oder Computers, auf dem die WhatsApp-Nachrichten gespeichert sind, vornehmen und diese auswerten.

Weiterhin können die Nachrichten, sofern sie auf einem Server des Providers zwischen- oder endgespeichert sind, bei dem Provider beschlagnahmt werden.[23] Aufgrund der „End-to-End"-Verschlüsselung liegen die Nachrichten jedoch nicht im Herrschaftsbereich von WhatsApp und das Unternehmen kann diese nicht herausgeben. Anders sieht es aus, wenn der Teilnehmer ein Backup der Nachrichten unverschlüsselt in einer sogenannten „Cloud" gespeichert hat. In diesem Fall könnten die Behörden dieses Backup auch vom jeweiligen Betreiber der Cloud beschlagnahmen.[24]

16 *BVerfG*, NJW 2005, 1917 (1920).
17 *Hauschild*, in: MüKo-StPO, § 94 Rn. 16.
18 *OLG München*, NJW 1978, 601.
19 *BVerfG*, NJW 1988, 890 (894).
20 *Wohlers/Greco*, in: SK-StPO, 5. Aufl. (2016), § 94 Rn. 15.
21 *Gerhold*, in: BeckOK-StPO, § 94 Rn. 4.
22 *Joecks*, in: Radtke/Hohmann, StPO, 2011, § 94 Rn. 25.
23 *BVerfG*, NJW 2009, 2431.
24 *Dalby*, CR 2013, 361 (367).

(2) Erhebung von Bestandsdaten § 100j StPO

Bei Speicherung auf einem Endgerät oder Server kann sich den Ermittlungsbehörden das Hindernis der Zugangssicherungscodes, die sogenannte Bestandsdaten i.S.v. §§ 95, 111 TKG sind, stellen. Zugangssicherungscodes können z.B. PIN, PUK oder Passwörter sein.[25] Daher normiert der 2013 in Kraft getretene § 100j Abs. 1 S. 2 StPO eine Auskunftspflicht über diese Codes für die Telekommunikationsunternehmen. Diese Auskunftspflicht muss gem. § 100j Abs. 3 StPO auf Ersuchen der Staatsanwaltschaft von einem Richter angeordnet werden. Voraussetzung für die Anordnung ist die Erforderlichkeit der Auskunft zur Sachverhaltserforschung.[26] Außerdem müssen auch die gesetzlichen Voraussetzungen für den Zugriff auf die durch die Codes gesicherten Daten vorliegen (z.B. Beschlagnahme nach § 94 StPO), da nur dann die Erforderlichkeit der Auskunft über die Zugangsdaten vorliegen wird.[27] Sind die WhatsApp-Nachrichten demnach auf einem Handy, PC oder in einer Cloud gespeichert, muss entweder der Telefonanbieter, der Anbieter des Betriebssystems oder der Provider der Cloud den zu dem Nutzer gehörigen Zugangscode unverzüglich (Abs. 4) an die Ermittlungsbehörden übermitteln.

(3) Online-Durchsuchung § 100b StPO

Der im August 2017 in Kraft getretene § 100b StPO ermächtigt die Behörden zu einer Online-Durchsuchung. Diese Maßnahme war 10 Jahre lang umstritten. Die Beschlagnahme eines PCs mit komplettem Datenbestand und die anschließende Durchsuchung war zwar schon lange nach §§ 94, 102, 110 Abs. 3 StPO möglich,[28] die heimliche Durchsuchung eines solchen war jedoch nicht von diesen Vorschriften umfasst.[29] § 100b StPO ermöglicht nun den heimlichen Zugriff auf sämtliche informationstechnische Systeme und die auf ihnen gespeicherten Inhalte.[30] Die Online-Durchsuchung erfolgt über einen Remote-Zugriff über die Datenleitung durch eine unbemerkt installierte Software, mit der das Gerät ohne das Wissen des Benutzers kontrolliert werden kann und auf darauf gespeicherte Inhalte (wie z.B. WhatsApp-Nachrichten) zugegriffen werden kann.[31] Die Voraussetzungen für die Anordnung decken sich mit denen des § 100a StPO, bloß der Anlasstatenkatalog bezieht sich bei § 100b StPO auf besonders schwere Straftaten.

c) Hauptverhandlung und Revision

Wie oben bereits ausgeführt, ist es nach § 244 Abs. 2 StPO dem Gericht überlassen, wie es Erkenntnisse in die Hauptverhandlung einführt, verwertet und würdigt. Hauptsächlich können die Daten durch Augenscheinsbeweis in die Verhandlung eingeführt werden, indem sie für die Beteiligten sichtbar gemacht werden.[32] Weiterhin können die (ausgedruckten) Nachrichten aber auch durch Urkundenbeweis eingeführt bzw. einem der Kommunikationspartner bei seiner Aussage vorgehalten werden. Urkunden- und Augenscheinsbeweis können aber nur als authentisches Beweismittel in Betracht kommen, wenn der Prozess der Sichtbarmachung technisch einwandfrei ablief, was eventuell durch Heranziehung der dafür zuständigen Person zu beweisen ist.[33] Es kommt auch die Zeugenvernehmung des zuständigen Auswertungsbeamten über die festgestellten Erkenntnisse in Betracht, was aber den

25 *Graf*, in: BeckOK-StPO, § 100j Rn. 8.
26 *Bär*, MMR 2013, 700 (702).
27 *BVerfG*, NJW 2012, 1419.
28 *BVerfG*, NJW 2006, 976.
29 *BGH*, NJW 2007, 930.
30 *Graf*, in: BeckOK-StPO, § 100b Rn. 1.
31 *Graf*, in: BeckOK-StPO, § 100b Rn. 7-10.
32 *BGH*, NStZ 2001, 493.
33 *Momsen*, in: FS Beulke, 2015, S. 871 (878).

Beweiswert verringert.[34] Grundsätzlich kann eine Revision auf Grundlage von §§ 94, 100a, 100b, 100g StPO darauf gestützt werden, dass das Urteil auf unverwertbaren Erkenntnissen beruht, wenn auf die WhatsApp-Nachrichten nicht hätte zugegriffen werden dürfen.

2. Beispiel

In einem vor dem *Landgericht Frankfurt am Main* verhandelten Fall[35] war der Beschuldigte wegen Mordes an seiner Ehefrau angeklagt. Der Angeklagte war angeklagt, mehrfach mit einem Hammerbeil auf den Kopf seiner Ehefrau eingeschlagen und sie anschließend bis zur Bewusstlosigkeit gewürgt zu haben. Die Verletzungen und der anschließende Blutverlust führten schließlich zum Tod der Frau. In der Hauptverhandlung war vor allem umstritten, ob es sich hierbei um eine Affekthandlung handelte oder ob der Angeklagte die Tat schon länger geplant hatte, um sich am Opfer für die Trennung zu rächen. Im Zentrum der Hauptverhandlung stand daher ein forensisch-psychiatrisches Sachverständigengutachten, das zu dem Ergebnis gelangte, dass der Angeklagte zum Tatzeitpunkt zum einen unter einer schweren seelischen Störung litt, zum anderen, dass für das unmittelbare Tatgeschehen ein höchstgradiger Affekt wahrscheinlich ist. Damit lägen die Voraussetzungen der Anwendung des § 21 StGB aufgrund einer erheblich verminderten Steuerungsfähigkeit bei erhaltender Einsicht vor. In der Beweismittelliste sowie der Anklageschrift befanden sich unter anderem Ausdrucke von vier WhatsApp-Nachrichten des Angeklagten, die er vier Tage vor der Tat an verschiedene Freunde sendete. In diesen äußerte er sich positiv zu Fällen bei denen Familienväter ihre Frauen und Kinder töteten/ermordeten.

Die Beweisrelevanz dieser Nachrichten ergibt sich wie folgt. Sie zeigen, dass die Rachegedanken des Angeklagten, die er schon in einem „Abschiedsbrief" zwei Monate vor der Tat beschrieb, bereits vier Tage vor der Tat wieder aufflammten und er die Tötung als Form zum Ausleben dieser auch in Betracht zog bzw. bei anderen Männern in seiner Position bewunderte. In seiner Einlassung hatte er ausgesagt, die Gedanken seien wieder verschwunden. Die Nachrichten tauchen nicht im Verhandlungsprotokoll auf, nur eine der vier wurde im Urteil erwähnt. Dies deutet darauf hin, dass die Nachrichten nicht als Urkundenbeweis in die Verhandlung eingeführt wurden, sondern wenn überhaupt, durch Vorhalt Teil der Hauptverhandlung wurden. Problematisch bei der Einführung als Urkundenbeweis könnte gewesen sein, dass die Nachrichten hauptsächlich auf Französisch verfasst wurden und eine Verlesung dieser gegen § 184 GVG (Deutsch als Gerichtssprache) verstoßen würde, sofern kein Sachverständiger als Dolmetscher hinzugezogen würde.[36] Das *Landgericht* entschied zugunsten einer Affekthandlung und verurteilte den Angeklagten wegen Totschlags gem. § 212 StGB zu einer Haftstrafe von sieben Jahren.

3. Bedeutung von WhatsApp-Nachrichten als Beweismittel

Anhand dieses Falles lässt sich erkennen, welchen Wert WhatsApp-Nachrichten für die Beweisführung haben können. Sie weisen hier auf den längerfristig vorhandenen Tatvorsatz des Angeklagten hin und hätten bei ordnungsgemäßer Würdigung das Urteil vom Totschlag zum Mord umschwenken lassen können oder müssen. Als problematisch kann gesehen werden, dass die von WhatsApp Inc. 2016 eingeführte „End-to-End"-Verschlüsse-

34 BGHSt 43, 36 (38).
35 *LG Frankfurt a.M.*, Az 5/21 Ks – 3590 Js 244545/16 (6/17).
36 *BGH*, NJW 1965, 643; NStZ 1985, 466.

lung auch die Möglichkeiten der Strafverfolgungsbehörden beschränkt und daher extrem beweisrelevantes Material zum Beispiel im Falle von Verlust oder Zerstörung der Endgeräte für immer verloren gehen kann. Dies steigert aber gerade das Vertrauen der Teilnehmer in die Vertraulichkeit ihrer Nachrichten. Dass der Angeklagte in diesem Fall solch persönliche Gedankengänge an seine Freunde verschickt, zeigt gerade, wie sicher er sich der Vertraulichkeit der Kommunikation war.

Problematisch ist also insbesondere das Spannungsverhältnis zwischen dem extrem hohen Beweiswert bzw. der Beweisrelevanz in der Hauptverhandlung und dem Eingriff in die Privatsphäre bzw. die Vertraulichkeit der Kommunikation bei Erhebung im Ermittlungsverfahren. Bei der Verwertung von persönlichen Daten und zwischenmenschlichen Kommunikation muss sich immer die Frage stellen, inwiefern der Staat zu einem solchen Eingriff ermächtigt werden kann und welche Grundrechte dabei vielleicht verletzt werden könnten. Bei einer Telekommunikationsüberwachung eines laufenden Vorgangs nach § 100a StPO ist immer das Post- und Fernmeldegeheimnis des Art. 10 Abs. 1 GG betroffen. Dieses umfasst auch das Telekommunikationsgeheimnis, also die „unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs“ unabhängig von der Übermittlungsart oder der Inhalte an sich.[37] Geschützt wird die Vertraulichkeit der Kommunikation, nicht aber das Vertrauen der Teilnehmer untereinander.[38] Bei einer heimlichen Online-Durchsuchung informationstechnischer Systeme nach § 100b StPO hingegen findet stets ein Eingriff in das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme“ als eine eigenständige Ausprägung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG statt.[39] Bei allen anderen oben beschriebenen Maßnahmen ist ebenfalls das Grundrecht auf informationelle Selbstbestimmung betroffen.

Eine Rolle spielt auch der sogenannte Kernbereich privater Lebensgestaltung. Der Kernbereich umfasst Inhalte höchstpersönlichen Charakters, die in einer Einzelfallbetrachtung bewertet werden.[40] Dies beinhaltet auch „innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art“.[41] Dieser wird für §§ 100a – 100c StPO durch § 100d StPO seit August 2017 verstärkt geschützt, der wie § 100a StPO a.F. den verfassungsrechtlichen Vorgaben entspricht.[42] So sind gem. §100d Abs. 1 StPO Maßnahmen unzulässig, durch die allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen werden. Darüber hinaus besteht gem. § 100d Abs. 2 StPO ein Verwertungsverbot für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung. Zudem wird vorgeschrieben, dass solche Erkenntnisse unverzüglich zu löschen sind. § 100d StPO ist also eine wichtige Norm, um den Kernbereich privater Lebensgestaltung und die jeweils betroffenen Grundrechte zu schützen. Die Begrenzungen des § 100d StPO beziehen sich jedoch nur auf die Maßnahmen der §§ 100 a-c StPO. Durch die Speicherung der Kommunikationsdaten auf Endgeräten und die mögliche Sicherstellung bzw. Beschlagnahme nach § 94 StPO kann jedoch in vergleichbarem Maße in den Kernbereich privater Lebensgestaltung eingegriffen werden. Dabei ändert das Wissen des Betroffenen nichts an der Eingriffsintensität. Es kann also mit Recht die Frage aufgeworfen werden, ob zum Schutz der Privatsphäre in diesem Bereich noch Handlungsbedarf für den Gesetzgeber besteht.

37 BVerfGE 67, 157 (172); 100, 313 (358); NJW 2008, 822 (825).
38 BVerfGE 85, 386 (399).
39 BVerfGE 120, 274.
40 BVerfGE 80, 367 (374).
41 *Hegmann*, in: BeckOK-StPO, § 100d Rn 6.
42 *BVerfG*, NJW 2012, 833 ff.

Natürlich sind bei den Maßnahmen richterliche Anordnungen unter Beachtung des Subsidiaritätsprinzips erforderlich (§§ 98, 100e StPO und § 100j Abs. 3 StPO). Diese sind jedoch den unterschiedlichsten Anforderungen unterworfen. So ist bei einer Beschlagnahme nach § 94 Abs. 2 StPO lediglich ein einfacher Anfangsverdacht jeglicher verfolgbaren Straftat erforderlich, während bei einer Telekommunikationsüberwachung nach § 100a StPO ein Tatverdacht auf schwere Straftaten, die im Einzelfall erheblich sein müssen, vorliegen muss. § 100a StPO richtet sich (aufgrund der Unanwendbarkeit auf WhatsApp, s. oben) wohl eher auf Telefongespräche. WhatsApp-Nachrichten haben jedoch mittlerweile für viele Menschen Telefongespräche abgelöst, vor allem in jüngeren Generationen. Es werden tiefste Gefühle und private Erlebnisse mit den Telekommunikationspartnern geteilt, immer in dem Vertrauen darauf, dass niemand diese liest, von dem man dies nicht möchte. Sie genießen diesbezüglich auch einen weitaus persönlicheren Stellenwert als zum Beispiel E-Mails, die mittlerweile hauptsächlich für geschäftliche oder professionelle Zwecke genutzt werden. Deshalb muss sich die Frage stellen, warum die Anordnung einer offenen Beschlagnahme der genauso persönlichen Nachrichten geringere Anforderungen erfüllen muss als das Abhören eines Telefongespräches. Zwar stellt das Unwissen des Betroffenen bei heimlichen Maßnahmen eine gewisse Schutzlosigkeit dar, trotzdem muss meiner Meinung nach eine sensiblere und an die hohe Persönlichkeit der Nachrichten angepasste Lösung möglich sein.

Auf der anderen Seite kann argumentiert werden, dass die Nachrichten einen extrem hohen Beweiswert haben. Bei einer möglichst weitreichenden Ermächtigung der Behörden zum Zugriff könnten offensichtlich Straftaten viel effizienter und möglicherweise korrekter aufgeklärt und mit dem richtigen Strafmaß bemessen werden, was wiederum die verfassungsrechtlichen Grundlagen des Verfahrens (faires Verfahren, Schuldprinzip) absichert. Trotzdem sollte der Staat WhatsApp-Nachrichten mit größter Vorsicht behandeln. Die Informationen über die Person und ihre Kommunikationspartner betreffen in den meisten Fällen den Kernbereich privater Lebensgestaltung oder zumindest das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Problematisch ist darüber hinaus, dass WhatsApp dem Nutzer (und somit auch dem Überwachendem) die Option zur Verfügung stellt, auf Nachrichten zuzugreifen, die weit in der Vergangenheit liegen und somit den Behörden Informationen als Beweismittel vorliegen, die vielleicht nicht mehr dem aktuellen Stand entsprechen. Die Anforderungen an einen Eingriff sollten hoch sein und die Ermittlungsbehörden trotz des hohen Beweiswertes nur in seltenen Fällen dazu ermächtigen auf die Nachrichten zuzugreifen. Möglicherweise kann die technische Durchführungsweise so erweitert werden, dass bloß Nachrichten, die tatsächlich Beweiswert haben, betroffen sind und nicht solche, die andere Menschen oder Sachverhalte betreffen.

III. Fazit

Das Thema ist sowohl technisch als auch rechtlich höchst komplex und betrifft höchstpersönliche Informationen. Daher ist wichtig, dass es stets im öffentlichen und politischen Diskurs bleibt und sensibel damit umgegangen wird. WhatsApp-Nachrichten (sowie die anderer Messenger-Dienste) umfassen mittlerweile nicht mehr lediglich die Gespräche selbst. Sie beinhalten häufig auch die Übersendung von Fotos, Videos, Dokumenten und Standorten, bei WhatsApp ist sogar die Übersendung eines Live-Standorts über mehrere Stunden möglich. Zudem gehört WhatsApp zu einem Unternehmen, welches auch die Social-Media-Dienste wie Facebook und Instagram betreibt. Die Menge an Daten, die mithin über Nutzer angesammelt wird, ist folglich enorm und sollte von staatlicher Seite mit großer Vorsicht behandelt werden. Natürlich ist es möglich, WhatsApp-Nachrichten nicht nur repressiv als

Beweismittel, sondern auch präventiv als Möglichkeit der (häufig vermutlich effektiveren) Gefahrenabwehr zu verwenden. Daten könnten von den Beteiligten oder den Anbietern an die Polizei- und Ordnungsbehörden (freiwillig oder unfreiwillig) übergeben werden, um so Gefahren für die öffentliche Sicherheit & Ordnung abzuwenden.

Ähnliches wird aktuell in der Diskussion um die Eindämmung der COVID-19-Pandemie überlegt. Zum einen geht es dabei um die Übermittlung von Verkehrsdaten und den daraus gezogenen Bewegungsprofilen von den Telekommunikationsanbietern (z.B. die Telekom) an die Gesundheitsämter. Diese kann vor dem Hintergrund des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG aber nur anonymisiert und (von den Anbietern) freiwillig erfolgen. Eine Verpflichtung der Anbieter ist ohne ausdrücklich gesetzliche Grundlage nicht möglich. Zum anderen ist die Entwicklung einer sogenannten „Corona-Tracing-App“ geplant. Diese soll über Bluetooth von Smartphone zu Smartphone den Standort austauschen, sodass Infizierte sich eintragen können und die in dem für die Infektion kritischen Abstand von 1,5 – 2 Metern bekommen eine Benachrichtigung und können so entsprechende Quarantäne-Maßnahmen vornehmen. Eine Eindämmung der Infektionszahlen erscheint auf diesem Wege sehr vielversprechend, ist aber rechtlich nur auf rein anonymer und freiwilliger Basis (auch bezüglich der Installation) akzeptabel, um den Datenschutz und somit Schutz des Allgemeinen Persönlichkeitsrechts zu ermöglichen.

Diese Grundsätze lassen sich aber nur bedingt auf WhatsApp-Nachrichten übertragen. Zunächst handelt es sich bei COVID-19 voraussichtlich um eine zeitlich begrenzte Gefahr für die Allgemeinheit, die es schnell zu bekämpfen gilt, um die Gesundheit selbst, das Gesundheitssystem und mittelbar auch die Wirtschaft zu schützen. Darüber hinaus geht die Gefahr nicht von einer Person aus. WhatsApp-Nachrichten werden wohl kaum „freiwillig“ von Personen, die aus wie auch immer gearteten Gründen eine Gefahr darstellen oder verursachen, herausgegeben werden. Und auch WhatsApp Inc. selbst wird sich wohl nicht dazu überreden lassen, dauerhaft bzw. wiederholt freiwillig Daten über seine User herauszugeben, da sie diese dann vermutlich verlieren würden (zudem sind sie dazu technisch ja auch gar nicht in der Lage, s. oben). Auch das Erheben von anonymen Daten wird wohl bei der „alltäglichen“ Gefahrenabwehr kaum bzw. in wenigen Spezialfällen sinnvoll sein, da meist gerade die Information über eine spezifische Person benötigt wird. Fraglich ist auch, wie anonym etwas noch sein kann, wenn Inhalte von Gesprächen analysiert werden. Eine Verpflichtung zur Übergabe von WhatsApp-Nachrichten kann daher auch im präventiven Bereich nur unter Wahrung des Kernbereichs der Privatsphäre und der Verhältnismäßigkeit erfolgen. Eine richterliche Anordnung und eine dringende Gefahr sollten stets vorliegen, ebenso wie im repressiven Bereich ein zumindest hinreichender, wenn nicht sogar dringender Tatverdacht.

Zusammenfassend kann man sagen, dass das letzte Wort zum Thema WhatsApp-Nachrichten als Beweismittel wohl aufgrund der immer weiterlaufenden technischen Entwicklung und der sich daran anzupassen versuchenden Rechtsentwicklung noch nicht gesprochen ist oder vielleicht nie gesprochen sein wird.