



# BERLINER RECHTSZEITSCHRIFT

JURISTISCHE FACHZEITSCHRIFT AN DER FREIEN UNIVERSITÄT BERLIN

## AUS DER LEHRE

*Prof. Dr. Andreas Engert*  
Empirische Rechtswissenschaft –  
Vorstellung einer Forschungsrichtung

## ZIVILRECHT

*Paul Jakob Suilmann*  
Der gewillkürte Parteiwechsel

*Florian Ziehr*  
Patententeignung und COVID-19 (§ 13 PatG)

## ÖFFENTLICHES RECHT

*Marco Vöhringer*  
Die Militäraktion „Peace Spring“ der Türkei in Syrien:  
eine völkerrechtliche Einordnung

## GRUNDLAGEN DES RECHTS

*Dr. Enno Mensching*  
Der Verfassungsbegriff im Nationalsozialismus

*Johanna Hasenburg*  
Kant: Recht als kategorischer Imperativ

## DIGITALISIERUNG IM RECHT

Siegerbeitrag aus dem BRZ-Schreibwettbewerb

*Hannah Wissler*  
Wie kann der Einsatz von KI / Algorithmen in der  
Strafverfolgung kontrolliert werden?

3. Jahrgang | Seiten 1–88

[www.berlinerrechtszeitschrift.de](http://www.berlinerrechtszeitschrift.de)

ISSN (Print) 2699-948X | ISSN (Online) 2699-2132

# AUSGABE 1/2022

Hannah Wissler\*

## Wie kann der Einsatz von KI / Algorithmen in der Strafverfolgung kontrolliert werden?

Bedarf es spezifischer Verteidigungsrechte, Beweisantragsrechte, Rechtsmittel oder internationaler Sicherheitsstandards bspw. Menschenrechte?

Siegerbeitrag aus dem Schreibwettbewerb „Digitalisierung im Recht“ der BRZ

Algorithmen und künstliche Intelligenz kommen im Strafverfahren bereits vermehrt zum Einsatz. Dadurch verändert sich das Verhältnis zwischen den Grundsätzen der Effizienz und der Fairness des Verfahrens mit erheblichen Auswirkungen für die Beteiligten. Es besteht die Gefahr, dass der oder die Beschuldigte durch den Einsatz von Algorithmen und künstlicher Intelligenz zum bloßen Objekt des Strafverfahrens wird. In dem Beitrag werden verschiedenen prozessuale Maßnahmen diskutiert, mit dem Ziel die Verfahrensfairness bei Einsatz von künstlicher Intelligenz und Algorithmen sicherzustellen. Dazu müssen nicht notwendigerweise neue Regelungen geschaffen werden. Vielmehr können Grundsätze des Strafverfahrens im Lichte der besonderen Umstände automatisierter Prozesse ausgelegt werden. Dazu gehören die Rechte des oder der Beschuldigten und der Verteidigung sowie Beweisverwertungsverbote aus rechtsstaatlichen oder datenschutzrechtlichen Überlegungen.

### Inhaltsübersicht

A. Einleitung .....	77
B. Algorithmus und künstliche Intelligenz .....	78
C. Effizienz oder Fairness? .....	78
D. Der mögliche Einsatz von KI im Strafverfahren .....	78
I. Predictive Policing .....	78
II. Intelligente Auswertung von Beweismitteln .....	79
III. KI als Ersatz von menschlichen Richtern und Richterinnen .....	80
IV. Strafzumessung .....	80
V. Zwischenergebnis .....	81
E. Kontrolle .....	81
I. Ethische Leitlinien .....	81
II. Gewährleistung der tatsächlichen Mitwirkung des oder der Beschuldigten .....	81
III. Verteidigungsrechte .....	82
1. Erweiterte Akteneinsichtsrechte .....	82
2. Rahmenbedingungen .....	83

3. Rechtsstaatliches Beweisverwertungsverbot .....	84
IV. Datenschutz im Strafverfahren .....	85
1. Grundsatz der Zweckbindung und der Erforderlichkeit .....	86
2. Datenschutzrechtliches Beweisverwertungsverbot .....	86
V. Sicherstellung eines fairen Urteils .....	87
1. Urteilsbegründungspflicht .....	87
2. Rechtsmittel .....	88
3. Richtige Anwendung der Ergebnisse einer KI ...	88
F. Fazit .....	88

### A. Einleitung

Die stetig zunehmende Digitalisierung hat nicht nur Einfluss auf die Gesellschaft, sondern wirkt auch auf das materielle und prozessuale Strafrecht ein. Die Digitalisierung hat dazu geführt, dass es mehr Daten und somit mehr Informationen gibt. Gleichzeitig haben sich die technischen Möglichkeiten vervielfacht, was zu einer erhöhten und schnelleren Auswertung der Sachverhalte entscheidend beiträgt.<sup>1</sup> Auf der prozessualen Seite bewirkt das einen vermehrten Einsatz von Algorithmen und künstlicher Intelligenz (kurz: KI) im Strafverfahren. Dabei reicht die Spanne von unterstützenden Tätigkeiten, zum Beispiel der Auswertung von Beweismitteln,<sup>2</sup> bis hin zu tatsächlicher richterlicher Entscheidungsgewalt<sup>3</sup>. Während sich dadurch die Effizienz des Strafverfahrens und möglicherweise auch die objektive Gerechtigkeit von Urteilen erhöht, kann der Einsatz automatisierter Prozesse auch mit Grundrechten, wie dem Recht auf rechtliches Gehör oder dem Recht auf informationelle Selbstbestimmung, kollidieren.<sup>4</sup> Diese Grundrechtskollisionen schaffen ein Bedürfnis nach (menschlicher) Kontrolle über den Einsatz von Algorithmen oder KI in der Strafverfolgung.<sup>5</sup>

Die Arbeit geht der Frage nach, wie eine entsprechende Kontrolle ausgestaltet werden könnte. Zunächst werden die Begriffe *Algorithmus* und *künstliche Intelligenz* erklärt (B.)

\* Die Autorin studiert im 10. Semester Rechtswissenschaft an der Freien Universität Berlin. Mit dem an dieser Stelle abgedruckten Beitrag hat sie den Schreibwettbewerb „Digitalisierung im Recht“ der BRZ gewonnen (siehe dazu das Vorwort zu diesem Heft). Er beruht auf einer Seminararbeit, die im Rahmen eines von der Freien Universität Berlin und der Universität Zürich gemeinsam angebotenen Seminars über das Strafrecht im Zeitalter von Digitalisierung und Datafizierung (II) bei Prof. Dr. Carsten Momsen und Prof. Dr. Frank Meyer, LL.M., entstanden ist.

<sup>1</sup> Vgl. Schneider, ZIS 2020, 79 (80).

<sup>2</sup> Bowcott/Devlin, Police trial AI software to help process mobile evidence, <https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence>, zuletzt abgerufen am 1.4.2022.

<sup>3</sup> Vgl. in zivilrechtlichen Verfahren Niiler, Can AI Be a Fair Judge in Court? Estonia Thinks So, <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/>, zuletzt abgerufen am 1.4.2022.

<sup>4</sup> Vertiefend siehe Lentz, KriPoZ 2020, 57.

<sup>5</sup> So auch Zweig, Algorithmische Entscheidungen: Transparenz und Kontrolle, 2019, S. 5.

und die Anforderungen an eine wirksame Kontrolle herausgearbeitet (C.). Weitergehend wird untersucht, welche KI-Systeme im Strafverfahren eingesetzt werden oder mit Blick auf ihren Entwicklungsstand in absehbarer Zukunft eingesetzt werden könnten (D.). Anschließend werden verschiedene Möglichkeiten beleuchtet, wie solche KI-Systeme im deutschen Strafverfahren kontrolliert werden können (E.). Abschließend werden die Ergebnisse zusammengefasst (F.).

## B. Algorithmus und künstliche Intelligenz

Ein Algorithmus ist ein schrittweises Verfahren, um Probleme zu lösen oder ein Ziel zu erreichen.<sup>6</sup> In der gängigen Praxis und auch in dieser Arbeit bezeichnet der Begriff Algorithmus mathematische Objekte, die mithilfe von Gleichungen, Arithmetik, Algebra, Analysis, Logik und Wahrscheinlichkeiten eine Folge mathematischer Operationen in Computercode umwandeln. Vereinfacht gesagt: Der Algorithmus bekommt ein Ziel gesetzt, wird mit Daten aus der realen Welt versorgt und arbeitet Rechenschritte ab, bis er das Ziel erreicht.<sup>7</sup> In der Art und Weise der Zielerreichung wird zwischen regelbasierten und selbstlernenden Algorithmen unterschieden.<sup>8</sup> Bei einem regelbasierten Algorithmus werden direkte und eindeutige Anweisungen von einem Menschen erstellt: *Schritt eins: Tu dies / Schritt zwei: Wenn dies, dann das.*<sup>9</sup> Bei selbstlernenden Algorithmen wird hingegen keine präzise Liste an Anweisungen vorgegeben. Es werden ein klares Ziel benannt und Daten eingegeben. Wenn der Algorithmus zu einem richtigen Ergebnis kommt, gibt man eine positive Rückmeldung. Man überlässt es dem Algorithmus, selbst den besten Weg zu dem vorgegebenen Ziel zu finden.<sup>10</sup> Selbstlernende Algorithmen fallen unter den Überbegriff *künstliche Intelligenz*.<sup>11</sup> Die von der Europäischen Kommission eingesetzte *hochrangige Expertengruppe für künstliche Intelligenz* verwendet dabei folgende Definition: KI-Systeme „sind vom Menschen entwickelte Softwaresysteme [...], die in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene handeln, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten [...] Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten, und über das bestmögliche Handeln zur Erreichung des vorgegebenen Zieles entscheiden [...]“<sup>12</sup>

<sup>6</sup> Zweig (Fn. 5), S. 3.

<sup>7</sup> Zweig (Fn. 5), S. 3.

<sup>8</sup> Fry, Hello World – Was Algorithmen können und wie sie unser Leben verändern, 2019, S. 23 f.

<sup>9</sup> Fry (Fn. 8), S. 23.

<sup>10</sup> Staffler/Jany, ZIS 2020, 164 (165).

<sup>11</sup> Fry (Fn. 8), S. 23.

<sup>12</sup> *Hochrangige Expertengruppe für KI*, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete, 2019, S. 6.

## C. Effizienz oder Fairness?

Der Einsatz automatisierter Prozesse würde die Effizienz in der Strafverfolgung erheblich steigern. Er erlaubt eine schnellere und kostengünstigere Fallbearbeitung, da mehr Fälle mit den gleichen Ressourcen bearbeitet werden könnten.<sup>13</sup> Das führt unter anderem zu einer besseren Durchsetzung des materiellen Strafrechts sowie zur Einhaltung des Beschleunigungsgebotes.<sup>14</sup> Zudem erzielen automatisierte Prozesse in ihrer Analyse grundsätzlich auch eine höhere Genauigkeit.<sup>15</sup> Das Strafverfahren bestimmt sich aber nicht ausschließlich über den Effizienzgedanken. Vielmehr verlangt es aus Gründen der Verfahrensfairness zusätzliche Kontrollmechanismen hinsichtlich Ermittlungsergebnissen und Urteilen. Das dient einerseits der Aufdeckung und Korrektur von Fehlern in der Wahrnehmung und Beurteilung sowie andererseits der Wahrung fundamentaler Grundrechte.<sup>16</sup> Trotz der positiven Auswirkungen auf Fairness und Effektivität kann sich der Einsatz von Algorithmen und KI nachteilig auf den Schutz des Individuums auswirken. Ziel einer wirksamen Kontrolle sollte es sein, die Balance zwischen Fairness und Effizienz im Strafverfahren zu wahren, sodass die Wahrheitsfindung bestmöglich unter Berücksichtigung fundamentaler Grundrechte betrieben werden kann.

Im Folgenden soll anhand praktischer Beispiele herausgearbeitet werden, welche Gefahren sich aus dem Einsatz von Algorithmen und KI im Strafverfahren für den Schutz des Individuums ergeben und durch welche prozessualen Maßnahmen die Balance zwischen Effizienz und Fairness wiederhergestellt oder gewahrt werden kann.

## D. Der mögliche Einsatz von KI im Strafverfahren

### I. Predictive Policing

Im Ermittlungsverfahren werden in mehreren Bundesländern bereits unterschiedliche Programme eingesetzt, die auf Algorithmen und KI basieren. Angewendet werden unter anderem Prognosemodelle, die Wahrscheinlichkeiten für zukünftiges Verhalten oder zukünftige Ereignisse auf Grundlage großer Datenmengen über bisheriges Verhalten berechnen können. Es können keine Aussagen zu möglichen Kausalitäten, Kausalketten, Gründen oder Motiven für ein vorhergesagtes Verhalten getroffen werden.<sup>17</sup> In der Strafverfolgung werden entsprechende Softwareprogramme unter dem Begriff *predictive policing* zusammen-

<sup>13</sup> Vgl. Turner, Fair trial or efficient administration of justice? Trends in modern criminal procedure, in: Hoven/Kubiciel (Hrsg.), Zukunftsperspektiven des Strafrechts – Symposium zum 70. Geburtstag von Thomas Weigend, 2020, S. 187 (191).

<sup>14</sup> Turner (Fn. 13), S. 188.

<sup>15</sup> Vgl. Turner (Fn. 13), S. 193.

<sup>16</sup> Turner (Fn. 13), S. 188 f.

<sup>17</sup> Dreyer, Predictive Analytics aus der Perspektive von Menschenwürde und Autonomie, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big-Data – Regulative Herausforderungen, 2018, S. 135 (135 f.).

gefasst.<sup>18</sup> Ein Beispiel ist das Programm *hessenDATA*. Dieses wurde nicht von der Polizei Hessen, sondern von der US-Firma *Palantir* entwickelt.<sup>19</sup> Hierbei handelt es sich um eine Analysesoftware, die große Datenbestände der Polizei innerhalb eines konkreten Strafverfahrens oder verfahrensübergreifend miteinander verknüpft und auswertet, um leichter Bedrohungslagen erkennen und Gefährder oder Gefährderinnen identifizieren zu können.<sup>20</sup> *HessenDATA* soll bis dato unbekannte Zusammenhänge zwischen verschiedenen Personen oder Ereignissen erkennen, wie zum Beispiel dass Personen nah beieinander wohnen. Dafür werden unter anderem polizeiinterne Informationen über Kriminalfälle und Fahndungen, Verbindungsdaten aus der Telefonüberwachung, Social-Media-Daten oder E-Mails sowie Inhalte ausgelesener Mobiltelefone verarbeitet. Auf diese Weise soll das Softwareprogramm zu einer effizienteren und effektiveren Verbrechensbekämpfung führen.<sup>21</sup> Seit Ende 2017 kommt die Software im Bereich des islamistischen Terrorismus zum Einsatz. Es ist bereits im Gespräch den Einsatz der Software auf schwere und organisierte Kriminalität sowie Ermittlungen zu Kindesentführung und Kindesmissbrauch auszuweiten.<sup>22</sup>

Das Programm *hessenDATA* greift direkt durch die Analyse und dem daraus resultierenden Ergebnis in die Grundrechte des oder der Betroffenen ein.<sup>23</sup> Insbesondere ist hier das vom Bundesverfassungsgericht (BVerfG) aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelte Recht auf informationelle Selbstbestimmung<sup>24</sup> betroffen. Zum Schutz der selbstbestimmten Entwicklung und Entfaltung hat der oder die Einzelne das Recht „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.<sup>25</sup> In die von *hessenDATA* berechnete Wahrscheinlichkeit sich zum Gefährder oder zur Gefährderin zu entwickeln, fließen aber nicht nur aktive Äußerungen ein. So führt z.B. die Verknüpfung mit Social-Media-Daten dazu, dass auch unbewusst preisgegebene Informationen sich auf die Berechnung auswirken können.<sup>26</sup> Zudem wird durch die Verknüpfung der Datenbestände die polizeiliche Eingriffstätigkeit erheblich vorverlagert. Durch die Identifizierung von Gefährdern oder Gefährderinnen – möglicherweise über einen

Zufallsfund – kann die Analysesoftware einen Anfangsverdacht i.S.v. § 152 Abs. 2 StPO begründen.<sup>27</sup>

Zusätzlich können sich aus Fehlern in der Gestaltung der KI-Systeme oder in Bezug auf die der Analyse zugrunde liegenden Daten weitere Risiken ergeben.<sup>28</sup> Die Ergebnisse sind nur so neutral und differenziert, wie die Daten, auf denen sie basieren. Es gibt jedoch keine neutralen Daten. Es besteht die Gefahr, dass Verzerrungen, Vorurteile und Diskriminierungspraktiken, die in den polizeilichen Daten festgeschrieben sind, bei der Analyse reproduziert werden.<sup>29</sup> Die Qualität des Datenbestandes ist demnach entscheidend für die Qualität der errechneten Vorhersage durch die Prognosemodelle.<sup>30</sup>

## II. Intelligente Auswertung von Beweismitteln

Ein weiteres Einsatzgebiet von KI-Software kann die Auswertung von Beweismitteln über die Interpretation von Bildern, den Abgleich von Gesichtern und die Analyse von Kommunikationsmustern sein.<sup>31</sup> Mit diesen Vorgängen sollen bei Ermittlungen sichergestellte digitale Beweismittel schneller untersucht werden können, was wiederum eine Steigerung der Verfahrenseffizienz bedeuten würde.<sup>32</sup> Digitale Beweismittel nehmen in ihrer Bedeutung immer mehr zu. Ermittlungsbehörden müssen exponentiell ansteigende Datenmengen bewältigen, die von Handys und Laptops erzeugt werden.<sup>33</sup> Eingebaute KI-Algorithmen können es ermöglichen, Bilder und Videos danach zu kennzeichnen, ob der Inhalt Waffen, Gesichter, Autos, Nacktheit, Drogen, Flaggen oder andere Kategorien enthält.<sup>34</sup> Auch hier bestehen Bedenken hinsichtlich des Potenzials der Software, Voreingenommenheit in die Verarbeitung von kriminellen Beweisen einzubringen.<sup>35</sup> Es gibt Hinweise auf rassistische Verzerrungen in einigen bestehenden Bilderkennungssystemen, die nachweislich Gesichter von weißen Menschen häufiger korrekt zuordnen als Gesichter von schwarzen Menschen.<sup>36</sup> Zudem kann der oder die Einzelne keine bewusste Kontrolle über die Interpretation der eigens erzeugten digitalen Beweismittel ausüben. Es liegt somit auch ein Eingriff in das Recht auf informationelle Selbstbestimmung vor.

<sup>18</sup> Staffler/Jany, ZIS 2020, 164 (167).

<sup>19</sup> Singelstein, Big Data bei der Polizei – Hessen sucht mit Palantir-Software nach Gefährdern, <https://netzpolitik.org/2019/big-data-bei-der-polizei-hessen-sucht-mit-palantir-software-nach-gefaehrden/>, zuletzt abgerufen am 1.4.2022.

<sup>20</sup> Singelstein (Fn. 19).

<sup>21</sup> Ausführlich dargestellt bei Egbert, Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen, in: Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung – Empirische Polizeiforschung zur polizeipraktischen Ausgestaltung des Rechts, 2020, S. 77 (89 f.).

<sup>22</sup> Singelstein (Fn. 19).

<sup>23</sup> Vgl. Dreyer (Fn. 17), S. 136.

<sup>24</sup> BVerfG NJW 1984, 419 (Volkszählungsurteil).

<sup>25</sup> BVerfG NJW 1984, 419 (422) (Volkszählungsurteil).

<sup>26</sup> Vgl. Dreyer (Fn. 17), S. 142.

<sup>27</sup> Vgl. Egbert (Fn. 21), S. 91.

<sup>28</sup> Vgl. Europäische Kommission, Weißbuch zur künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final, S. 13.

<sup>29</sup> Singelstein (Fn. 19).

<sup>30</sup> Dreyer (Fn. 17), S. 138.

<sup>31</sup> Dieser Vorgang wird aktuell von der britischen Polizei erprobt mit der Software *Analytics Enterprise* von dem Unternehmen *Cellebrite*, siehe Bowcott/Devlin (Fn. 2).

<sup>32</sup> Vgl. Bowcott/Devlin (Fn. 2).

<sup>33</sup> Momsen, Digitale Beweismittel aus der Sicht der Strafverteidigung, in: Beck/Meier/Momsen (Hrsg.), Cybercrime und Cyberinvestigations – Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie, 2015, S. 67 (71).

<sup>34</sup> Bowcott/Devlin (Fn. 2).

<sup>35</sup> Bowcott/Devlin (Fn. 2).

<sup>36</sup> Bowcott/Devlin (Fn. 2).

### III. KI als Ersatz von menschlichen Richtern und Richterinnen

Die Vorstellung von einer KI verurteilt zu werden klingt in Deutschland vielleicht noch nach einer weitentfernten Dystopie (oder Utopie). In Estland ist sie aber bereits Realität. Dort wurde einer KI tatsächliche Entscheidungsgewalt über zivilrechtliche Fälle mit einem Streitwert bis zu 7.000 € übertragen. In dem estländischen Zivilverfahren werden der künstlich intelligenten Richterin per Upload von den beteiligten Zivilparteien alle relevanten Dokumente und Informationen zur Verfügung gestellt. Die KI wertet diese aus und fällt auf Grundlage der bestehenden Gesetze ein Urteil.<sup>37</sup> Eine urteilende KI braucht weder Pausen, Schlaf noch Urlaub und macht grundsätzlich innerhalb des Systems keine Fehler. Zudem ist sie kostengünstiger als die Finanzierung eines breiten Justizapparates.<sup>38</sup> Würde man die KI auf den deutschen Strafprozess übertragen, würden sich potenzielle Konflikte mit dem Recht auf Gewährung rechtlichen Gehörs nach Art. 103 Abs. 1 GG ergeben. Betroffen wäre insbesondere dessen einfachgesetzliche Ausgestaltung in Form des Fragerechtes der Verteidigung und des oder der Angeklagten innerhalb der Hauptverhandlung gem. § 240 Abs. 2 StPO. Zugleich bestünde damit ein Spannungsverhältnis zum Menschenrecht aus Art. 6 Abs. 3 lit. d EMRK.<sup>39</sup> Art. 103 Abs. 1 GG und Art. 6 Abs. 3 lit. d EMRK verlangen grundsätzlich nach einem echten gegenseitigen Austausch zwischen den Parteien im Strafprozess und dem Entscheidungsträger oder der Entscheidungsträgerin.<sup>40</sup> Dahingehend ist der Analyseprozess einer KI nicht transparent. Man kann der Software keine Fragen stellen und sie bietet keine Erklärung ihrer Ergebnisse.<sup>41</sup>

### IV. Strafzumessung

Bei der Bestimmung der Strafe kann eine KI eingesetzt werden. Ein Beispiel ist das sog. *Smart Sentencing*. Hierbei handelt es sich um ein Projekt des *Legal Tech Lab* der Universität Köln. Ziel ist es, eine Datenbank aus Urteilen aufzubauen, damit Richter und Richterinnen bundesweit Strafzumessungsentscheidungen diverser Delikte vergleichen können. Die KI soll die Urteile nach Kriterien filtern, die bei der Strafzumessung eine Rolle gespielt haben und feststellen, ob diese sich strafferhöhend oder mildernd ausge-

wirkt haben.<sup>42</sup> Ein anderes und das wohl bekannteste Beispiel einer KI im Bereich Strafzumessung ist das in den USA eingesetzte Softwareprogramm *COMPAS*. Dieses wurde von dem Unternehmen *Northpointe* (inzwischen *Equivant*) entwickelt und erstellt eine Prognose über das Rückfallrisiko von Straftätern oder Straftäterinnen. Es berechnet auf der Grundlage von Antworten des oder der Angeklagten in einem Fragebogen und seiner oder ihrer Kriminalgeschichte die Wahrscheinlichkeit, dass er oder sie innerhalb der nächsten zwei Jahre wieder straffällig wird.<sup>43</sup> Der zugrundeliegende Beurteilungsmechanismus ist als Geschäftsgeheimnis geschützt, sodass Außenstehende darauf keinen Zugriff haben. Das Gericht erhält nur das Ergebnis der Einschätzung.<sup>44</sup> Obwohl der Algorithmus nur eine Präzisionsrate von rund 70 % erreichte, also bei etwa jedem und jeder Dritten falsch lag, wurde das von dem Algorithmus berechnete Ergebnis von Richtern und Richterinnen bei der Urteilsfindung eingesetzt.<sup>45</sup> So auch in dem Fall „*State v. Loomis*“. *Eric Loomis* wurde 2013 vom Staat Wisconsin in fünf Anklagepunkten angeklagt. Er plädierte in zwei der geringer wiegenden Anklagepunkte auf schuldig. *Loomis* wurde erstinstanzlich zu einer Freiheitsstrafe von sechs Jahren und zu einer fünfjährigen Gemeindeaufsicht verurteilt. Das Gericht bezog sich bei seiner Strafzumessung auf das Ergebnis von *COMPAS*, das im Rahmen der Vorbereitung der Verurteilung erstellt wurde.<sup>46</sup> *Loomis* reichte daraufhin einen Antrag auf Strafmilderung ein, der von dem Gericht abgelehnt wurde. Er argumentierte unter anderem, dass das Vertrauen des Gerichts in *COMPAS* sein Recht auf eine individualisierte Verurteilung verletze. Weiter führte er aus, dass durch die Nicht-Veröffentlichung des Beurteilungsmechanismus sein Recht, auf der Grundlage präziser Informationen verurteilt zu werden, verletzt wurde.<sup>47</sup> Das Berufungsgericht von Wisconsin verwies die Berufung an den Obersten Gerichtshof von Wisconsin, der das Urteil bestätigte. Der Gerichtshof begründete seine Entscheidung unter anderem mit dem Argument, dass das Urteil individualisiert genug sei, da Richter und Richterinnen noch einen Ermessensspielraum hätten und die notwendigen Informationen zur Verfügung ständen, um eine unzulässige Bewertung zu korrigieren.<sup>48</sup>

<sup>37</sup> Niiler (Fn. 3).

<sup>38</sup> Rostalski, Iudex ex machina? Zum Einsatz neuer Technologien in der Rechtsfindung, in: Hoven/Kubiciel (Hrsg.), Digitalisierung und Strafverfahren, 2020, S. 263 (267).

<sup>39</sup> Vgl. Gaede, in: MünchKomm-StPO, Bd. 2, 1. Auflage 2016, § 240 Rn. 1; Gorf, in: BeckOK StPO, 42. Ed. 2022, § 240 Rn. 1.

<sup>40</sup> Vgl. DAV, Stellungnahme des Deutschen Anwaltsverein durch den Ausschuss Europa und den Ausschuss Zivilrecht zur Konsultation der Europäischen Kommission zum Weißbuch Künstlicher Intelligenz COM(2020) 65 final, Nr. 40/2020, Rn. 28; Gaede (Fn. 39), § 240 Rn. 7.

<sup>41</sup> Ernst, JZ 2017, 1026 (1028 f.).

<sup>42</sup> Kaufmann, Mit Legal Tech zur einheitlichen Strafzumessung, <https://www.lto.de/recht/justiz/j/legal-tech-smart-sentencing-strafzumessung-unterschiedlich-hohe-strafen-vergleichen/>, zuletzt abgerufen am 1.4.2022.

<sup>43</sup> Angwin/Larson/Mattu/Kirchner, Machine Bias – There’s software used across the country to predict future criminals. And it’s biased against blacks, <https://www.propublica.org/article/machine-bias-risk-assessment-in-criminal-sentencing>, zuletzt abgerufen am 1.4.2022.

<sup>44</sup> Jiang, Automatisierte Entscheidungsfindung, Strafjustiz und Regulierung von Algorithmen. Ein Kommentar zum Fall „*State v. Loomis*“, in: Beck/Kusche/Valerius (Hrsg.), Digitalisierung, Automatisierung, KI und Recht – Festgabe zum 10-jährigen Bestehen der Forschungsstelle Robot-  
Recht, 2020, S. 557 (560 f.).

<sup>45</sup> Fry (Fn. 8), S. 80.

<sup>46</sup> Jiang (Fn. 44), S. 560 f.

<sup>47</sup> Jiang (Fn. 44), S. 561.

<sup>48</sup> Jiang (Fn. 44), S. 561 f.

Algorithmen wie *COMPAS* können zwei Arten von Fehlern machen. Zum einen können sie das Risiko, das eine Person darstellt, nicht erkennen (Falsch-negatives-Ergebnis) und zum anderen können sie jemanden fälschlicherweise als eine Person mit hohem Risiko einstufen (Falsch-positives-Ergebnis).<sup>49</sup> Falsch-positive Ergebnisse greifen stärker in die Grundrechte des oder der Betroffenen ein, sind aber viel schwerer nachzuweisen. Der Algorithmus stellt für die betroffene Person ein hohes Risiko fest. Auf dieser Grundlage entscheidet sich der oder die zuständige Richter oder Richterin für eine Freiheitsstrafe. Auf Grund der Tatsache, dass die Person sich dann in einem Gefängnis befindet und keine neue Straftat begehen kann, gibt es keine Möglichkeit die Prognose des Algorithmus zu verifizieren. Es ist unmöglich festzustellen, ob der Richter oder die Richterin der Risikobewertung richtigerweise vertraute.<sup>50</sup>

Der Algorithmus *COMPAS* zeigt auch, wie sich Vorurteile in den Daten auswirken können. Die Fehlerquote des Algorithmus ist bei schwarzen und weißen Tätern und Täterinnen insgesamt ungefähr gleich hoch, aber die Art des Fehlers ist je nach Hautfarbe unterschiedlich. Bei schwarzen Angeklagten, die nach ihrer ersten Verhaftung nicht wieder in Schwierigkeiten gerieten, war es doppelt so wahrscheinlich wie bei weißen Straftätern und Straftäterinnen, dass der Algorithmus sie fälschlicherweise als hohes Risiko einstufte. Bei den falsch-positiven Ergebnissen fanden sich folglich unverhältnismäßig viele schwarze Täter und Täterinnen. Umgekehrt fanden sich unter den falsch-negativen Ergebnissen unverhältnismäßig viele weiße Täter und Täterinnen. Das heißt, mit Blick auf einen zweijährigen Zeitraum nach Verurteilung war es doppelt so wahrscheinlich, dass weiße Verurteilte vom Algorithmus fälschlicherweise als geringes Risiko eingeschätzt worden waren als dies bei schwarzen Verurteilten der Fall war.<sup>51</sup>

## V. Zwischenergebnis

Der Einsatz von Algorithmen und KI im Strafverfahren birgt vor allem für den oder die Beschuldigte erhebliche Gefahren. Prognosesoftwares wie *hessenDATA* können dazu führen, dass die Eingriffsschwelle der Ermittlungsbehörden vorverlagert wird. Der notwendige Austausch zwischen Parteien und die Individualisierbarkeit des Strafverfahrens könnten durch den zunehmenden Einfluss künstlich generierter Prognosen auf menschliche Entscheidungen verloren gehen. Verzerrungen, Vorurteile und Diskriminierungspraktiken, die in den polizeilichen Daten festgeschrieben sind, können vermehrt reproduziert werden. Diesen Gefahren kann entgegengewirkt werden. Dazu müssen

nicht notwendigerweise neue Regelungen geschaffen werden. Vielmehr kann auf die bereits bestehenden Grundsätze des Strafverfahrens zurückgegriffen werden. In diesem Rahmen müssen die besonderen Umstände der regelbasierten und der selbstlernenden Algorithmen berücksichtigt werden.

## E. Kontrolle

### I. Ethische Leitlinien

Am 04.12.2018 wurde die *Europäische Ethik-Charta über den Einsatz künstlicher Intelligenz in Justizsystemen und deren Umfeld* von der Europäischen Kommission für die Effizienz der Justiz (CEPEJ)<sup>52</sup> verabschiedet.<sup>53</sup> Darin werden fünf Prinzipien für den Einsatz von KI aufgestellt. Danach sollen (1) Grundrechte bereits in die Entwicklung eines KI-Programmes miteinbezogen werden, (2) besondere Rücksicht auf den Antidiskriminierungsgrundsatz gelegt werden, (3) hinsichtlich der Verarbeitung von gerichtlichen Entscheidungen und Daten zertifizierte Quellen und eine sichere technologische Umgebung zum Einsatz kommen, (4) nach dem Prinzip der Transparenz, Unparteilichkeit und Fairness die Datenverarbeitungsmethoden zugänglich und verständlich gemacht werden und (5) sichergestellt werden, dass die Nutzer und Nutzerinnen informierte Akteure und Akteurinnen sind und die Kontrolle über ihre Entscheidungen haben. Die fünf Prinzipien dienen vorliegend als Orientierung hinsichtlich der einzelnen möglichen Kontrollmaßnahmen.

### II. Gewährleistung der tatsächlichen Mitwirkung des oder der Beschuldigten

Der oder die Beschuldigte soll Teil des Ermittlungsverfahrens sein und kein bloßes Ermittlungsobjekt darstellen. Er oder sie muss sich gegen den Tatvorwurf verteidigen und an der Aufklärung mitwirken können. Aus diesem Grund bestimmt § 136 Abs. 1 S. 1 Hs. 1 StPO, dass dem oder der Beschuldigten bei Beginn der ersten Vernehmung der Tatvorwurf zu eröffnen ist. Der bislang ermittelte Sachverhalt oder Verdachtsmomente sind dem oder der Beschuldigten insoweit und so klar und detailliert mitzuteilen, dass zum einen der Gegenstand des Verfahrens bestimmt und zum anderen die Verteidigung und Mitwirkung im Verfahren tatsächlich möglich wird.<sup>54</sup> Eine Verteidigung und Mitwirkung sind tatsächlich nicht möglich, wenn die beschuldigte Person nicht weiß, wer oder was an der Ermittlung mitgewirkt hat und wo mögliche Fehler passiert sein könnten. Vielmehr muss der oder die Beschuldigte die Umstände der Entstehung des Tatvorwurfes kennen, wenn dieser zum

<sup>49</sup> Fry (Fn. 8), S. 78 f.

<sup>50</sup> Fry (Fn. 8), S. 81; vgl. Zweig (Fn. 5), S. 11.

<sup>51</sup> Angwin/Larson/Mattu/Kirchner (Fn. 43).

<sup>52</sup> Die *European Commission for the Efficiency of Justice (CEPEJ)* ist eine Justizbehörde, die sich 2002 gegründet hat. Sie besteht aus Sachverständigen aller 47 Mitgliedstaaten des Europarates.

<sup>53</sup> CEPEJ, *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 2018.

<sup>54</sup> Vgl. Schuhr, in: MünchKomm-StPO, Bd. 1, 1. Auflage 2014, § 136 Rn. 20 f.

Beispiel durch eine Verknüpfung von Daten durch eine KI wie *hessenDATA* begründet worden ist. Eine Belehrung über an der Ermittlung beteiligte automatisierte Prozesse fördert die Transparenz<sup>55</sup> und wird dem Anspruch des oder der Beschuldigten auf rechtliches Gehör sowie allgemein dem Anspruch auf ein faires Verfahren gerecht.<sup>56</sup>

Man könnte hier noch einen Schritt weiter in Richtung Verfahrensfairness gehen und die Bereitstellung einer Pflichtverteidigung fordern, sobald automatisierte Prozesse an der Fallbearbeitung beteiligt waren oder sind. Die Pflichtverteidigung im Strafverfahren resultiert aus dem Gebot fairer Verfahrensführung und ist somit eine Konkretisierung des Rechtsstaatsprinzips.<sup>57</sup> Eine Pflichtverteidigung kann nach § 140 Abs. 2 StPO bei einer schwierigen Sach- oder Rechtslage geboten sein. Eine schwierige Sachlage kann sich aus dem zu erwartenden Umfang oder der Schwierigkeit der Beweisaufnahme ergeben.<sup>58</sup> Eine schwierige Rechtslage ist gegeben, wenn bei der Anwendung des materiellen oder prozessualen Rechts im konkreten Verfahren Rechtsfragen beantwortet werden müssen, die bislang nicht entschieden wurden.<sup>59</sup> Automatisierte Prozesse schaffen nicht grundsätzlich eine erschwerte tatsächliche und rechtliche Ermittlung, sondern sollen diese im Idealfall effizienter gestalten. Durch eine grundsätzliche Pflichtverteidigung bei automatisierten Prozessen würde die Effizienz durch die zusätzlichen erforderlichen Ressourcen und die damit verbundenen Kosten erheblich verringert werden. In Einzelfällen, zum Beispiel wenn ein Beweisverwertungsverbot in Frage kommt oder eine sachgerechte Verteidigung ohne (erweiterte) Akteneinsicht nicht möglich ist,<sup>60</sup> erscheint es geboten, dass der oder die Vorsitzende auf Antrag oder von Amts wegen nach § 140 Abs. 2 StPO eine Verteidigung bestellt.

In Zukunft sollte die Belehrung des oder der Beschuldigten in der Art und Weise erfolgen, dass die Person weiß, ob und wie eine KI an der Ermittlung beteiligt war. Die beschuldigte Person kann dann selbst entscheiden, ob sie sich verteidigen lassen möchte. Eine grundsätzliche Pflichtverteidigung hingegen führt zu einer erheblichen Minderung der Effizienz, ohne auf der Seite der Verfahrensfairness einen deutlichen Mehrwert im Vergleich zu einer Belehrung zu schaffen. Im Einzelfall kann aber eine schwierige Sach-

oder Rechtslage nach § 140 Abs. 2 StPO vorliegen, sodass ein Antrag auf Pflichtverteidigung gestellt werden kann.

### III. Verteidigungsrechte

#### 1. Erweiterte Akteneinsichtsrechte

Mit dem Recht auf Akteneinsicht gem. § 147 StPO soll die prozessuale Waffengleichheit sichergestellt werden, indem den Parteien die gleichen Informationen zur Verfügung stehen.<sup>61</sup> Insbesondere im Hinblick auf eine effektive Kontrolle automatisierter Prozesse im Strafverfahren erlangt das Recht auf Akteneinsicht immer größere Bedeutung, sodass auch Verteidiger und Verteidigerinnen verstärkt Einsicht in verschiedene Unterlagen und Dateien verlangen.<sup>62</sup> Damit die Verfahrensrechte des oder der Beschuldigten überhaupt Beachtung finden können, muss die Möglichkeit bestehen, den genutzten Algorithmus und die analysierten Daten überprüfen zu können.<sup>63</sup> Nur anhand des Ergebnisses der Analyse der KI selbst kann nicht festgestellt werden, ob dieses zum Beispiel aufgrund eines Vorurteils in den Daten verzerrt ist. Damit eine sachgerechte Überprüfung stattfinden kann, benötigt die Verteidigung zunächst Zugriff auf so viele Details wie (technisch) möglich.<sup>64</sup> Das umfasst die Auswahlprozesse und die in sie eingeschriebenen Theorien und Annahmen, Maßnahmen der Selektion und Aufbereitung von Daten, alle unabhängigen Variablen und ihr Gewicht, den Quellcode des Algorithmus, die Rohdaten sowie den Trainingsdatensatz.<sup>65</sup> § 147 StPO liegt jedoch der formelle Aktenbegriff zugrunde, der Vorbereitungsdokumente von dem Akteneinsichtsrecht ausschließt. Dazu zählt unter anderem der Trainingsdatensatz einer KI.<sup>66</sup> Eine Lösung könnte die Verwendung des weitergehenden materiellen Aktenbegriffes sein, der die Besonderheiten des Einsatzes automatisierter Prozesse besser berücksichtigen kann. Dieser erfasst alle im Zusammenhang mit einer konkreten Tat angefallenen Vorgänge.<sup>67</sup>

Eine andere Lösung könnte sein, den Beweisantrag nach § 244 Abs. 3–4 StPO als eine Art erweiterten Akteneinsichtsanspruch zur Vorbereitung etwaiger folgender Beweisangebote zu qualifizieren. Manche Gerichte leiten aus dem Gebot der Waffengleichheit, dem Grundsatz des fairen Verfahrens und dem Rechtsstaatsgebot ein erweitertes Einsichtsrecht der Verteidigung oder einen Anspruch auf Aktenvervollständigung ab.<sup>68</sup> So auch der Verfassungsge-

<sup>55</sup> Vgl. Prinzip 4 der European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment.

<sup>56</sup> Vgl. *DAV* (Fn. 40), Rn. 98 f.

<sup>57</sup> *Willnow*, in: *Karlsruher Kommentar zur StPO*, 8. Auflage 2019, § 140 Rn. 1.

<sup>58</sup> *Krawczyk*, in: *BeckOK StPO*, 42. Ed. 2022, § 140 Rn. 27.

<sup>59</sup> *Krawczyk* (Fn. 58), § 140 Rn. 32.

<sup>60</sup> *Krawczyk* (Fn. 58), § 140 Rn. 31.

<sup>61</sup> Vgl. *Staffler/Jany*, ZIS 2020, 164 (176); *Wessing* in: *BeckOK StPO*, 42. Ed. 2022, § 147 Rn. 22.

<sup>62</sup> Vgl. *Mysegades*, *Rechtsstaat sticht Software – Wie der Verfassungsgerichtshof des Saarlandes die Beschuldigtenrechte der Zukunft rettete*,

<https://verfassungsblog.de/rechtsstaat-sticht-software/>, zuletzt abgerufen am 1.4.2022.

<sup>63</sup> Vgl. *Martini*, JZ 2017, 1017 (1018); *Staffler/Jany*, ZIS 2020, 164 (176); *Zweig* (Fn. 5), S. 5.

<sup>64</sup> Vgl. *Jiang* (Fn. 44), S. 583, 585.

<sup>65</sup> Vgl. *Jiang* (Fn. 44), S. 585.

<sup>66</sup> Vgl. *Willnow*, in: *Karlsruher Kommentar zur StPO*, 8. Auflage 2019, § 147 Rn. 4.

<sup>67</sup> *Willnow* (Fn. 66), § 147 Rn. 4.

<sup>68</sup> OLG Oldenburg NZV 2017, 392; OLG Brandenburg StraFo 2017, 31; OLG Thüringen NJW 2016, 1457; aA.: OLG Bamberg NZV 2018, 80.



richtshof des Saarlandes (SaarlVerfGH) in seinem Urteil von 2019 über einen maschinell erstellten Bußgeldbescheid.<sup>69</sup> Betroffene erhalten inzwischen einen maschinell erstellten Bußgeldbescheid, ohne dass hinter diesem eine dem Adressaten bekannte Person oder eine für ihn nachvollziehbare menschliche Leistung stünde.<sup>70</sup> Hintergrund der Entscheidung des SaarlVerfGH war eine Verurteilung wegen fahrlässiger Überschreitung der innerorts zulässigen Höchstgeschwindigkeit zu einer Geldbuße i.H.v. 100 €. <sup>71</sup> Die Verteidigung hatte beim Landesverwaltungsamt Antrag auf Herausgabe der Rohmessdaten des Messgerätes in unverschlüsselter Form und der gesamten Messserie des Tattages sowie einer Kopie der Lebensakte des verwendeten Messgerätes gestellt. Die zentrale Bußgeldbehörde genehmigte die Herausgabe der konkreten Messdatei und der Lebensakte, lehnte eine Akteneinsicht jedoch ab. Der Sachverständige der Verteidigung gab daraufhin an, dass anhand der Zusatzdaten zum Falldatensatz eine unabhängige Geschwindigkeitskontrolle nicht annäherungsweise möglich sei. In der Hauptverhandlung stellte die Verteidigung Beweisantrag auf Einholung eines Sachverständigengutachtens zu der Behauptung, dass bei dem eingesetzten Messgerät die Möglichkeit ausgeschlossen sei, die Messung durch ein Sachverständigengutachten überprüfen zu lassen, so dass die Anerkennung als standardisiertes Messverfahren nicht mehr in Betracht komme. Das AG Saarbrücken lehnte den Antrag gem. § 77 Abs. 2 Nr. 1 OWiG ab, da die zum Beweis gestellte Behauptung zur Erforschung der Wahrheit nicht erforderlich sei. Die Zulassung zur Rechtsbeschwerde wurde vom saarländischen OLG durch Beschluss als unbegründet verworfen.<sup>72</sup> Der Beschwerdeführer legte anschließend Verfassungsbeschwerde mit der Begründung ein, dass er durch die Ablehnung seines Beweisantrages in seinem Recht auf ein faires Verfahren verletzt worden sei. Der SaarlVerfGH sah die Verfassungsbeschwerde als begründet an. Bei standardisierten Messverfahren können Gerichte nach der Rechtsprechung des BGH von ihrer Richtigkeit ausgehen und müssen diese nur bei besonderen Anlässen hinterfragen.<sup>73</sup> Liegen dem Gericht zufolge keine besonderen Anlässe vor und entscheidet es sich angesichts der Fülle der zu bearbeitenden Fälle und der typischerweise bestehenden Verlässlichkeit gegen eine Überprüfung, so darf dies der Verteidigung im Lichte des Prinzips der Waffengleichheit nicht deshalb versagt werden.<sup>74</sup> Zu den grundlegenden rechtsstaatlichen Anforderungen an die Verurteilung eines Bürgers oder einer Bürgerin

gehört, dass er oder sie die tatsächlichen Grundlagen seiner oder ihrer Verurteilung kennt, sie in Zweifel ziehen und nachprüfen kann. Gerichte dürfen kein Urteil sprechen, solange der betroffenen Person keine effektive Verteidigung ermöglicht wurde, worunter die Überprüfung der Validität der standardisierten Messungen fällt.<sup>75</sup> Rechtsstaatlichkeit verlangt die Transparenz und Kontrollierbarkeit jeder staatlichen Machtausübung.<sup>76</sup> Routinierte Entscheidungsprozesse dürfen für den oder die Bürgerin nicht undurchschaubar sein. Davon umfasst ist auch die grundsätzliche Nachvollziehbarkeit einer auf technischen Abläufen und Algorithmen beruhenden Entscheidung.<sup>77</sup> Eine Verweisung auf die regelmäßige Richtigkeit standardisierter Messungen würde den oder die Betroffene zum unmündigen Objekt staatlicher Handlungen machen.<sup>78</sup> Der Rechtsprechung des SaarlVerfGH hat sich das BVerfG in seinem Beschluss vom 12.11.2020 weitestgehend angeschlossen. Erhält die Verteidigung nicht bereits Akteneinsicht im Ermittlungsverfahren, muss ihr das Recht eingeräumt werden, einen Beweisantrag stellen zu können, um Kenntnis von solchen Inhalten zu erlangen, die zum Zweck der Ermittlung entstanden sind, aber nicht zur Akte genommen wurden.<sup>79</sup> Es wird der Verteidigung ermöglicht, selbst nach Entlastungsmomenten zu suchen, die zwar fernliegend sein können, aber nicht schlechthin auszuschließen sind.<sup>80</sup> Die dabei gefundenen entlastenden Informationen können dann von der Verteidigung zur fundierten Begründung eines Antrages auf Beiziehung vor Gericht dargelegt werden.<sup>81</sup> Mit dieser Auslegung des Prinzips der Waffengleichheit wird dem Informationsinteresse des oder der Beschuldigten genügt und andererseits gewährleistet, dass der Ablauf des gerichtlichen Verfahrens nicht durch eine sachlich nicht gebotene Ausweitung der Verfahrensakte unverhältnismäßig erschwert wird.<sup>82</sup> Die Balance zwischen Effizienz und Fairness wird durch das erweiterte Akteneinsichtsrecht hergestellt.

## 2. Rahmenbedingungen

### a) Umfang der Transparenz

Problematisch könnte jedoch sein, dass der Quellcode und die inneren Einzelheiten der Programme von privaten Entwicklern und Entwicklerinnen als Geschäftsgeheimnis geschützt sein können. Das ist z.B. bei dem Beurteilungsmechanismus von *COMPAS* der Fall.<sup>83</sup> In bestimmten Fällen muss aus den oben dargelegten Gründen trotz Interesses am

<sup>69</sup> SaarlVerfGH NJW 2019, 2456.

<sup>70</sup> Kubiciel, Die Veränderung des Strafrechts durch die Digitalisierung der Lebenswelt, in: Hoven/Kubicel (Hrsg.), Zukunftsperspektiven des Strafrechts – Symposium zum 70. Geburtstag von Thomas Weigend, 2020, S. 159 (168).

<sup>71</sup> Mysegades (Fn. 62).

<sup>72</sup> OLG Saarbrücken, Beschl. v. 26.06.2017 – Az.: Ss RS 22/2017.

<sup>73</sup> BGH NJW 1993, 3081.

<sup>74</sup> SaarlVerfGH NJW 2019, 2456 Rn. 43.

<sup>75</sup> Vgl. SaarlVerfGH NJW 2019, 2456 Rn. 41, 47.

<sup>76</sup> SaarlVerfGH NJW 2019, 2456 Rn. 47.

<sup>77</sup> SaarlVerfGH NJW 2019, 2456 Rn. 47–49.

<sup>78</sup> SaarlVerfGH NJW 2019, 2456 Rn. 47.

<sup>79</sup> Vgl. BVerfG NJW 2021, 455 Leitsatz Nr. 2.

<sup>80</sup> BVerfG NJW 2021, 455 Rn. 51.

<sup>81</sup> BVerfG NJW 2021, 455 Rn. 52.

<sup>82</sup> Vgl. BVerfG NJW 2021, 455 Rn. 51, 60 f.

<sup>83</sup> Martini, Grundlinien eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse – Gutachten im Auftrag der Verbraucherzentrale des Bundesverbandes, 2019, S. 37 f.



Schutz von Geschäftsgeheimnissen Zugang gewährt werden. Es stellt sich somit die Frage nach dem Umfang der Offenlegungspflicht. Eine vollständige Transparenz ist dabei abzulehnen. Transparenz ist einerseits zwar eine notwendige Grundbedingung, um Vertrauen in algorithmusbasierte Systeme aufbauen zu können.<sup>84</sup> Andererseits birgt eine vollständige Transparenz eine hohe Gefahr der Manipulierbarkeit oder Ausnutzung von Lücken im Schutzsystem der betroffenen Softwareanwendung.<sup>85</sup> Zur Wahrung der Interessen der Entwickler und Entwicklerinnen könnte der Zugang zu dem Algorithmus eingeschränkt werden. So könnte bei einem begründeten Antrag auf erweiterte Akteneinsicht der Algorithmus einer bestimmten Gruppe aus Experten und Expertinnen zugänglich gemacht werden. Diese erstellt daraufhin ein Sachverständigengutachten, das als Beweis dienen kann.<sup>86</sup> Weiter könnte man darüber nachdenken, die Beteiligten vorab eine Vertraulichkeitserklärung unterzeichnen zu lassen.<sup>87</sup> Auf der anderen Seite könnte man dem Interesse auf einen Schutz des Geschäftsgeheimnisses nachkommen, indem man den Entwicklern und Entwicklerinnen das Recht einräumt, zu beantragen, dass der gesamte Fall oder der das Geschäftsgeheimnis betreffende Teil nicht öffentlich verhandelt wird.<sup>88</sup>

#### b) Staatliche Kontrollinstanz

Eine weitere wichtige Voraussetzung betrifft den institutionellen Rahmen in Form der Einrichtung einer staatlichen Kontrollinstanz. Insbesondere wenn eine KI von privaten Entwicklern und Entwicklerinnen programmiert wird, sollte sie, bevor sie in einem Strafverfahren zum Einsatz kommt, einer externen Prüfung unterzogen werden.<sup>89</sup> Die staatliche Kontrollinstanz kann auch als Expertengruppe agieren und ein Sachverständigengutachten erstellen, wenn ein erfolgreicher Beweisantrag auf eine erweiterte Akteneinsicht gestellt wurde und private Entwickler und Entwicklerinnen den Algorithmus offenlegen müssen. Die Offenlegung beschränkt sich in diesem Fall auf die staatliche Expertengruppe.

Eine staatliche Kontrollinstanz könnte entweder als einheitliche Aufsichtsbehörde oder als eine Unterstützungseinheit ausgestaltet sein. Eine einheitliche Aufsichtsbehörde hätte den Vorteil als zentrale Stelle den erforderlich technischen Sachverstand aufzubauen, der erforderlich ist, um die vielfältigen Aufgaben der Algorithmenregulierung

wahrzunehmen und zu bündeln.<sup>90</sup> Aufgrund der Tatsache, dass es sich bei der Kontrolle von Algorithmen um eine Querschnittsmaterie handelt, erscheint die Ausgestaltung als Unterstützungseinheit ebenfalls sinnvoll.<sup>91</sup> Diese könnte als Bundesoberbehörde den erforderlichen technischen Sachverstand aufbauen, um die bereits existierenden Aufsichtsbehörden dahingehend zu unterstützen und mit hochspezialisierten Prüfteams einzelnen Maßnahmen zur Seite stehen.<sup>92</sup>

#### c) Explainable AI

Damit ein erweitertes Akteneinsichtsrecht überhaupt praktisch möglich ist, müsste die KI die erforderlichen Informationen speichern und verständlich zur Verfügung stellen. Problematisch ist hier der Blackbox-Charakter vieler KI-Systeme. Bei manchen KI-Systemen kann es sehr schwierig sein, eine Korrelation zwischen Ergebnis und Ausgangsdaten herzustellen.<sup>93</sup> Die Lösung könnten Dokumentationspflichten oder eine sog. *explainable AI* (deutsch: erklärbare künstliche Intelligenz, kurz: *XAI*) sein. Eine *XAI* soll eindeutig nachvollziehbar machen, wie dynamisch programmierte Systeme zu Ergebnissen kommen.<sup>94</sup> Bisher handelt es sich dabei lediglich um ein Forschungsgebiet und noch nicht um eine tatsächliche Möglichkeit KI-Systeme mit Blackbox-Charakter erklärbar zu machen. Im Bereich der Beurteilungsmechanismen, wie dem Programm *COMPAS*, könnte der Ansatz der sog. *counterfactual explanations* zum Einsatz kommen, wobei ein KI-System nicht nur das Ergebnis liefert, sondern auch die kleinstmögliche Veränderung nennt, die zu einem anderen Ergebnis geführt hätte.<sup>95</sup>

In der Zwischenzeit bestehen Forderungen, dass eine KI mit Blackbox-Charakter in der Justiz aufgrund der unzureichenden Transparenz durch die fehlende Nachvollziehbarkeit nicht zum Einsatz kommen sollte.<sup>96</sup> Im Strafverfahren könnten somit zum aktuellen Zeitpunkt nur regelbasierte KI zum Einsatz kommen, da diese erklärbar sind. Der Entscheidungsweg eines klassischen KI-Algorithmus, zum Beispiel nach dem Muster eines Entscheidungsbaums, ist transparent (sog. *White-Box-Verfahren*).<sup>97</sup>

### 3. Rechtsstaatliches Beweisverwertungsverbot

Wird ein Antrag auf erweiterte Akteneinsicht aus den oben beschriebenen Gründen abgelehnt, liegt ein Verstoß gegen

<sup>84</sup> Martini (Fn. 83), S. 8.

<sup>85</sup> Martini (Fn. 83), S. 41.

<sup>86</sup> Vgl. Jiang (Fn. 44), S. 584.

<sup>87</sup> Jiang (Fn. 44), S. 586.

<sup>88</sup> Jiang (Fn. 44), S. 585 f.

<sup>89</sup> Vgl. allgemein zur Forderung einer externen Kontrolle Martini (Fn. 83), S. 27 ff.

<sup>90</sup> Martini (Fn. 83), S. 31.

<sup>91</sup> Martini (Fn. 83), S. 31.

<sup>92</sup> Martini (Fn. 83), S. 32.

<sup>93</sup> Nassar/Salah/ur Rehman/Svetinovic, Blockchain for explainable and trustworthy artificial intelligence, WIREs Data Mining Knowledge Discovery 2020;10:e1340, S. 1.

<sup>94</sup> DAV (Fn. 40), Rn. 107.

<sup>95</sup> Nassar/Salah/ur Rehman/Svetinovic, Blockchain for explainable and trustworthy artificial intelligence, WIREs Data Mining Knowledge Discovery 2020;10:e1340, S. 5, 2.5.

<sup>96</sup> Campolo/Sanfilippo/Whittaker/Crawford, AI now 2017 Report, S. 1, Nr. 1.

<sup>97</sup> Alsbah, Blick in die Blackbox – Nachvollziehbarkeit von KI-Algorithmen in der Praxis, 2019, S. 7.

den Grundsatz der Waffengleichheit i.S.d. Art. 6 Abs. 1 EMRK vor. Im deutschen Strafprozess stellt sich in einem weiteren Schritt die Frage, wie sich der Verstoß gegen Art. 6 Abs. 1 EMRK auswirkt. Es gilt somit die Frage nach der Verwertbarkeit des Analyseergebnisses zu beantworten. In dem besprochenen Urteil hat der SaarVerfGH entschieden, dass die Verweigerung der Akteneinsicht, ob wegen Unmöglichkeit, der Nichtspeicherung der Rohmessdaten oder aus anderen Gründen, die rechtsstaatliche Unverwertbarkeit der Messung zur Folge hat.<sup>98</sup> Die rechtsstaatliche Unverwertbarkeit folgt hier unabhängig davon, ob die Beweiserhebung rechtmäßig erfolgt ist. Sie folgt aus der Verletzung der Grundrechte des oder der Betroffenen im Ermittlungsverfahren, unter anderem dem Recht auf ein faires Verfahren.<sup>99</sup>

Das Recht auf ein faires Verfahren findet sich unter anderem in Art. 6 EMRK. Der Europäische Gerichtshof für Menschenrechte hat den Fair-Trial-Grundsatz als einen „der Grundwerte der demokratischen Gesellschaft“ bezeichnet.<sup>100</sup> Der Fair-Trial-Grundsatz ist zudem in Art. 47 Abs. 2 GrCh ausdrücklich genannt. Auch nach dem BVerfG gehört das Recht auf ein faires Verfahren zu den „wesentlichen Grundsätzen eines rechtsstaatlichen Strafverfahrens“.<sup>101</sup> Dennoch führt nach der Rechtsprechung der genannten Gerichte ein Verstoß gegen Verfahrensvorschriften nicht zwangsläufig zu einem Beweisverwertungsverbot. Vielmehr muss eine offensichtliche Willkür oder Unfairness des gesamten Verfahrens gegeben sein.<sup>102</sup> Ein Verstoß gegen den Fair-Trial Grundsatz liegt vor, wenn durch die Verwertung die verfahrensrechtliche Stellung des oder der Beschuldigten verletzt wird. Das ist unter anderem der Fall, wenn der oder die Angeklagte zum bloßen Objekt des Verfahrens herabgewürdigt wird.<sup>103</sup> Der SaarVerfGH führt in seinem Urteil aus, dass der oder die Beschuldigte zum unmündigen Objekt staatlicher Verfügbarkeit würde, wenn sein oder ihr Beweisanspruch mit der Begründung abgelehnt würde, dass alles seine Richtigkeit habe. Der oder die Beschuldigte ist in dem Fall angesichts der Undurchschaubarkeit staatlichen Handelns durch den Einsatz automatisierter Prozesse handlungsunfähig.<sup>104</sup> Die Beispiele zeigen, dass die staatliche Wahrheitsforschung beschränkbar sein muss. Sieht man die Funktion der Beweisverwertungsverbote darin, die Fairness des Strafverfahrens zu

bewahren und wiederherzustellen, ist die notwendige Konsequenz bei einem Verstoß gegen den Fair-Trial Grundsatz ein Beweisverwertungsverbot.<sup>105</sup>

#### IV. Datenschutz im Strafverfahren

Durch eine technische Auswertung von digitalen Beweismitteln oder die Verknüpfung von Daten werden unvermeidlich in hohem Umfang personenbezogene Daten der Betroffenen, aber auch unbeteiligter Personen verarbeitet. Deren Integritätsinteresse muss auch im Strafprozess Berücksichtigung finden.<sup>106</sup> Für öffentliche Stellen, die im Rahmen der Strafverfolgung tätig werden, gelten diesbezüglich (ggf. über § 500 Abs. 1 StPO) die allgemeinen Regelungen der §§ 45 ff. BDSG. Daneben sehen die §§ 474 ff. StPO teilweise speziellere Regelungen für das Strafverfahren vor, die dann vorrangig anzuwenden sind.<sup>107</sup> Durch die genannten Normen wurde die Richtlinie (EU) 2016/680 der Europäischen Union zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten umgesetzt.<sup>108</sup> Der Anwendungsbereich der Richtlinie umfasst neben der Datenverarbeitung zur Strafverfolgung auch präventive Tätigkeiten, soweit sie auf Straftaten bezogen sind. Somit sind auch Programme wie *hessenDATA* erfasst.<sup>109</sup> Die berechtigten Stellen sind nach § 483 StPO zur grundsätzlichen Verarbeitung i.S.v. § 46 Nr. 2 BDSG von Daten für Zwecke der Strafrechtspflege befugt. In § 483 StPO wird die Befugnis zur Datenerhebung bereits vorausgesetzt.<sup>110</sup> Die Erhebung personenbezogener Daten ist in zahlreichen Vorschriften über Ermittlungsmaßnahmen der StPO geregelt. Ermittlungsmaßnahmen der StPO müssen als staatliche Grundrechtseingriffe verhältnismäßig sein.<sup>111</sup> In der Angemessenheit müssen die Intensität der Beeinträchtigung und die Anzahl der Betroffenen auf der einen Seite mit den mit der Maßnahme verfolgten Zielen auf der anderen Seite abgewogen werden.<sup>112</sup> Wenn in einer Ermittlung beruhend auf einer Ermittlungsmaßnahme der StPO eine KI eingesetzt wird, müssen in der Angemessenheit auch datenschutzrechtliche Wertungen berücksichtigt werden. Das Softwareprogramm *hessenDATA* und die intelligente Auswertung von Beweismitteln verdeutlichen, dass den Ermittlungsbehörden heute ganz erhebliche Erkenntnisquellen und Befugnisse zur Verfügung stehen, mittels derer sich Informationen aus prak-

<sup>98</sup> SaarVerfGH NJW 2019, 2456 Rn. 73.

<sup>99</sup> Vgl. *Jugl*, Fair Trial als Grundlage der Beweiserhebung und Beweisverwertung im Strafverfahren – Ein Beitrag zu der Lehre von den Beweisverboten am Beispiel des Auskunftsverweigerungsrechts nach § 55 StPO, 2017, S. 25.

<sup>100</sup> EGMR NJW 2009, 2871 (2873).

<sup>101</sup> BVerfG NJW 1969, 1423 (1424).

<sup>102</sup> BVerfGE 57, 250 (274 ff.); EGMR NJW 2010, 213 (215).

<sup>103</sup> BVerfG NJW 1969, 1423 (1424).

<sup>104</sup> SaarVerfGH NJW 2019, 2456 Rn. 47.

<sup>105</sup> *Jugl* (Fn. 99), S. 69.

<sup>106</sup> *Momsen* (Fn. 33), S. 91.

<sup>107</sup> *Singelstein*, NStZ 2020, 639 (639).

<sup>108</sup> Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2000/383/JI des Rates.

<sup>109</sup> Vgl. *Singelstein*, NStZ 2020, 639 (639).

<sup>110</sup> *Singelstein*, in: MünchKomm-StPO, Bd. 3/1, 1. Auflage 2019, § 483 Rn. 1.

<sup>111</sup> *Singelstein*, JZ 2012, 601; siehe auch *Härtling*, NJW 2015, 3284 (3285).

<sup>112</sup> *Singelstein*, JZ 2012, 601 (602).

tisch allen Lebensbereichen einer Person erlangen lassen, und die es ermöglichen, einmal erhobene Daten in stärkerem Maße auch zu anderen Zwecken zu nutzen.<sup>113</sup> Bei der Angemessenheitsprüfung einer entsprechenden Datenverarbeitung sind somit der Zweckbindungsgrundsatz gem. § 47 Nr. 2 BDSG und die Erforderlichkeit als zentrale Voraussetzungen des Datenschutzes zu berücksichtigen.<sup>114</sup>

### 1. Grundsatz der Zweckbindung und der Erforderlichkeit

Der Zweckbindungsgrundsatz folgt bereits aus dem Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Danach dürfen die Daten nur zu einem bestimmten Zweck erhoben werden.<sup>115</sup> Das konkrete Strafverfahren bildet einen einheitlichen Zweck der Datenverarbeitung.<sup>116</sup> Weitergehend dürfen die Daten grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie ursprünglich erhoben wurden.<sup>117</sup> Eine Zweckentfremdung, also die Verarbeitung der Daten zu anderen Zwecken als dem Erhebungszweck, darf nur aufgrund einer entsprechenden Rechtsgrundlage erfolgen, wobei eine erneute Verhältnismäßigkeitsprüfung erfolgen muss.<sup>118</sup> Nach dem Grundsatz der Erforderlichkeit gem. § 47 Nr. 3 BDSG ist die Verarbeitung nur in dem Umfang zulässig, wie sie für das konkrete Strafverfahren auch tatsächlich erforderlich ist.<sup>119</sup> Genauer gesagt muss die Verarbeitung im Einzelfall notwendig sein, um die Aufgabe rechtmäßig, vollständig, mit angemessenem Aufwand und in angemessener Zeit erfüllen zu können.<sup>120</sup> Die Erforderlichkeit begrenzt die Befugnis auf solche Daten, die für die weiteren Ermittlungen oder andere Verfahrenszwecke von Relevanz sind. Somit ist die Grenze der Erforderlichkeit vor allem bei sehr umfangreichen Datenerhebungen von Bedeutung, da hier häufig auch Daten von unbeteiligten Dritten betroffen sind.<sup>121</sup> Durch eine Berücksichtigung des Zweckbindungsgrundsatzes und der Erforderlichkeit könnte der Vorverlagerung der Eingriffsschwelle effektiv vorgebeugt werden. Bei der Vorverlagerung der Eingriffsschwelle wird der Tatverdacht durch die Erhebung und Verknüpfung von Daten erzeugt. Hier fehlt es an einer Zweckbindung sowie an der Erforderlichkeit der Datenerhebung, da der dies begründende Tatverdacht (noch) nicht vorhanden ist. In der Schweiz existiert bereits das Verbot der *fishing expedition*. Bei einer *fishing expedition* wird bewusst nach Beweismitteln gesucht, die mit dem Tatverdacht in keinerlei Zusammenhang stehen. Durch einen absichtlich produzierten Zufallsfund

soll der Tatverdacht dann erst begründet werden.<sup>122</sup> Auch nach der Rechtsprechung des BVerfG hinsichtlich der Erstellung von Persönlichkeitsprofilen gelten zwei absolut geschützte Bereiche. Zum einen ist eine Erstellung durch die Kombination von Daten aus verschiedenen Lebensbereichen mittels einer „Totalausforschung“ generell unzulässig.<sup>123</sup> Zum anderen ist eine Verarbeitung und somit auch die Erhebung von Daten mit Kernbereichsbezug ausnahmslos unzulässig.<sup>124</sup> Je mehr die Eingriffsschwelle durch die Verwendung von *Predictive-Policing*-Systemen vorverlagert wird und einer *fishing expedition* gleicht, desto mehr fehlt der Zweckzusammenhang, was wiederum einen stärkeren Eingriff in die Rechte des oder der Betroffenen bedeutet.<sup>125</sup> In der Verhältnismäßigkeit wäre das Recht auf informationelle Selbstbestimmung dann schwerer zu gewichten als das Aufklärungsinteresse.

Die Intensität des Eingriffes kann auch von der Art der Daten und der Form der Erhebung abhängig sein.<sup>126</sup> Bei der Verarbeitung von sensiblen Daten, zum Beispiel Gesundheitsdaten oder Daten aus denen religiöse Überzeugungen hervorgehen,<sup>127</sup> besteht eine höhere Anforderung an den Zweckzusammenhang und eine stärkere Begrenzung durch die Erforderlichkeit.

### 2. Datenschutzrechtliches Beweisverwertungsverbot

Bereits erhobene Daten werden durch die KI verwertet, unter anderem indem sie miteinander verknüpft werden, um neue Erkenntnisse über neue Verbindungen zu generieren. Ein Beispiel dafür sind die Programme *hessenDATA* und *COMPAS*. Die dadurch entstehenden Ergebnisse sollen als Beweise in der Hauptverhandlung verwertet werden. Der Verwertung könnte ein Eingriff in das Recht auf informationelle Selbstbestimmung durch eine Nichtbeachtung des Zweckbindungsgrundsatzes und der Erforderlichkeit entgegenstehen. In der Richtlinie (EU) 2016/680 war ursprünglich ein umfassendes Verwendungsverbot für rechtswidrig verarbeitete Daten vorgesehen. Das entspräche nicht der deutschen Dogmatik der strafprozessualen Beweisverwertungsverbote, sondern der sog. *fruit of the poisonous tree* Doktrin.<sup>128</sup> Danach erstreckt sich ein Beweisverwertungsverbot auch auf die weiteren Ermittlungsergebnisse, die aufgrund eines unzulässig erworbenen Erstbeweises ermittelt worden sind.<sup>129</sup> Der Beweis aus der Analyse wäre wegen fehlender Zweckbindung unzulässig erworben, wenn im Ermittlungsverfahren ein KI-System, z.B. in Form der Gesichtserkennung, ohne hinreichenden Bezug zum

<sup>113</sup> Vgl. Golla, NJW 2021, 667 (668 f., 671 f.).

<sup>114</sup> Vgl. für den Zweckbindungsgrundsatz Härting, NJW 2015, 3284 (3287).

<sup>115</sup> Härting, NJW 2015, 3284 (3284).

<sup>116</sup> Singelstein, (Fn. 110), § 483 Rn. 5.

<sup>117</sup> Singelstein, NSZ 2020, 639 (640).

<sup>118</sup> Singelstein, in: MünchKomm-StPO, Bd. 3/1, 1. Auflage 2019, Vorb. zu § 474, Rn. 16.

<sup>119</sup> Singelstein (Fn. 118), § 483 Rn. 9.

<sup>120</sup> Singelstein (Fn. 118), § 483 Rn. 9.

<sup>121</sup> Singelstein (Fn. 118), § 483 Rn. 10 f.

<sup>122</sup> Vgl. Bundesgericht (Schweiz), Urteil v. 14.04.2011 – Az.: 6B 849/2010 – E. 2.3.2.

<sup>123</sup> Singelstein (Fn. 118), Vorb. zu § 474 Rn. 14.

<sup>124</sup> BVerfG NJW 2016, 1781 (1787).

<sup>125</sup> Vgl. Egbert (Fn. 21), S. 91.

<sup>126</sup> Vgl. Golla, NJW 2021, 667 (668); Singelstein (Fn. 118), Vorb. zu § 474 Rn. 12.

<sup>127</sup> Vgl. Art. 10 Richtlinie (EU) 2016/680.

<sup>128</sup> Bäcker/Hornung, ZD 2012, 147 (149).

<sup>129</sup> Meyer-Mews, HRRS 2015, 398.

konkreten Strafverfahren zum Einsatz gekommen wäre. Ebenso unzulässig erhoben ist der Beweis, wenn durch das KI-System mehr Daten als erforderlich erhoben werden. Das ist vor allem dann anzunehmen, wenn Daten von unbeteiligten Dritten verarbeitet werden. Weitere Beweise, die nur aufgrund des Analyseergebnisses ermittelt werden konnten, wären dann ebenfalls unverwertbar. Die *fruit of the poisonous tree* Doktrin beinhaltet eine Disziplinierungsfunktion der Ermittlungsbehörden. Diese entspringt einer rechtsstaatlichen Notwendigkeit, da auch bei der Rechtsdurchsetzung das Recht eingehalten werden muss.<sup>130</sup> Weitergehend wird die Schutzfunktion von Beweisverwertungsverboten nicht unterlaufen und somit die Verfahrensfairness sichergestellt. Beweisverwertungsverbote würden leerlaufen, wenn die Ermittlungsbehörden die bewusst oder willkürlich rechtswidrig erlangten Informationen für weitere Ermittlungsmaßnahmen verwenden könnten.<sup>131</sup> In Deutschland wird die Reichweite eines Beweisverwertungsverbotes unter dem Begriff der *Fernwirkung* von Beweisen diskutiert und ist nicht abschließend beantwortet.<sup>132</sup> Dem BGH zufolge soll ein Verfahrensfehler, der ein Verwertungsverbot für ein Beweismittel bewirkt, aus Gründen des Interesses an einer wirksamen Strafverfolgung nicht automatisch das gesamte Strafverfahren stilllegen.<sup>133</sup> Bei einer Verletzung des Kernbereiches privater Lebensgestaltung, der durch das allgemeine Persönlichkeitsrecht geschützt ist, hat das BVerfG aber ein absolutes Beweisverwertungsverbot anerkannt, das Fernwirkung entfaltet.<sup>134</sup> Das BVerfG führte dahingehend aus, dass es der Verpflichtung der staatlichen Gewalt, dem oder der Einzelnen die Entfaltung seiner oder ihrer Persönlichkeit zu ermöglichen, widerspräche, wenn schwere Verletzungen des allgemeinen Persönlichkeitsrechts sanktionslos blieben. „Dies kann insbesondere der Fall sein, wenn unberechtigt gewonnene Daten weitgehend ungehindert verwendet werden dürften oder eine unberechtigte Verwendung der Daten mangels materiellen Schadens regelmäßig ohne einen der Genugtuung der Betroffenen dienenden Ausgleich bliebe.“<sup>135</sup> Betroffene Personen werden weder bei der Auswahl bzw. Generierung des betreffenden Datenpools noch bei der Programmierung der Software-Agenten noch in anderer Weise an der Informationssammlung beteiligt.<sup>136</sup> Um dieser Informationsasymmetrie entgegenzuwirken und dem Anspruch des oder der Beschuldigten auf ein faires Verfahren gerecht zu werden, erscheint ein datenschutzrechtliches Beweisverwertungsverbot in Form der Fernwirkung als eine notwendige Konsequenz.<sup>137</sup>

<sup>130</sup> Meyer-Mews, HRRS 2015, 398.

<sup>131</sup> Meyer-Mews, HRRS 2015, 398.

<sup>132</sup> Meyer-Mews, HRRS 2015, 398.

<sup>133</sup> BGH NJW 1978, 1390 (1390); BGH NJW 1987, 2525 (2526).

<sup>134</sup> Vgl. Meyer-Mews, HRRS 2015, 398 (399).

<sup>135</sup> BVerfG NJW 2010, 833 Rn. 252.

<sup>136</sup> Gless, Predictive Policing und operative Verbrechensbekämpfung, in: Herzog/Schlothauer/Wohlers (Hrsg.), Rechtsstaatlicher Strafprozess und Bürgerrechte – Gedächtnisschrift für Edda Weßlau, 2016, S. 165 (177 f.).

<sup>137</sup> Vgl. Meyer-Mews, HRRS 2015, 398 (406).

## V. Sicherstellung eines fairen Urteils

### 1. Urteilsbegründungspflicht

Bisher und auch in der generellen Debatte werden vor allem mögliche Gefahren beim Einsatz einer KI im Strafverfahren diskutiert. Dadurch kann eine verzerrte Vorstellung dahingehend entstehen, dass der Einsatz einer KI immer zu Nachteilen für den Beschuldigten oder die Beschuldigte führe. Es erscheint einem befremdlich, dass menschliche Richter und Richterinnen sich zum Beispiel bei der Entscheidung über die Strafzumessung auf ein Analyseergebnis einer KI stützen, bei dem nicht immer nachzuvollziehen ist, wie es zustande gekommen ist. Eine gerichtliche Entscheidung muss sowohl individuell getroffen werden, um strafmildernde Umstände oder noch unbekannte Faktoren berücksichtigen zu können als auch objektiv, um in ähnlich gelagerten Fällen im Sinne des Gleichbehandlungsprinzips zu entscheiden.<sup>138</sup> Hier kann ein KI-System, das im Rahmen notwendiger Kontrollmaßnahmen unterstützend eingesetzt wird, jedoch zu einem gerechteren Urteil erheblich beitragen. In den Urteilen menschlicher Richter und Richterinnen bestehen regionale, lokale und richterindividuelle Strafzumessungsunterschiede erheblichen Umfangs.<sup>139</sup> Ein Algorithmus hingegen wird immer die gleiche Antwort geben, wenn er mit den gleichen Umständen konfrontiert wird.<sup>140</sup> Somit könnte der Einsatz von KI-Systemen, die zum Beispiel die Rückfallwahrscheinlichkeit berechnen, zu konstanterer Rechtsprechung beitragen.<sup>141</sup> Damit die Fähigkeit, ein individuelles Urteil sprechen zu können, nicht verloren geht, muss das Gericht trotz Beteiligung automatisierter Prozesse noch eine autonome, unparteiische und unvoreingenommene Entscheidung treffen können.<sup>142</sup> Dazu muss bestimmt werden, ab wann eine Entscheidung ausschließlich auf einer autonomen Verarbeitung basiert, und wie viel Einfluss ein menschlicher Gedankenprozess auf die Entscheidung haben muss.<sup>143</sup> Der *Deutsche Anwaltverein e.V.* fordert, dass aus der Urteilsbegründung hervorgehen muss, dass die Entscheidung des Gerichts auf einer mit nachprüfbaren Argumenten versehenen, von dem KI-basierten System unabhängigen Begründung beruht.<sup>144</sup> In dem Fall *State v. Loomis* ordnete die Richterin an, dass bei der Berücksichtigung einer Risikobewertung von einem Programm wie *COMPAS* in einer gerichtlichen Entscheidung, dem Richter oder der Richterin fünf schriftliche Warnhinweise zukommen müssen und andere Faktoren als die Risikobewertung in der Urteilsbegründung angegeben

<sup>138</sup> Fry (Fn. 8), S. 69 f.; vgl. auch Streng, in: Hoven/Kubiciel (Hrsg.), Digitalisierung und Strafverfahren, 2020, S. 205 (209).

<sup>139</sup> Streng (Fn. 138), S. 205.

<sup>140</sup> Fry (Fn. 8), S. 75.

<sup>141</sup> Vgl. Fry (Fn. 8), S. 69.

<sup>142</sup> DAV (Fn. 40), Rn. 34.

<sup>143</sup> Duve/Zollitsch, Spricht der Mensch oder der Algorithmus Recht, <https://anwaltsblatt.anwaltverein.de/de/anwaeltinnen-anwaelte/anwaltspraxis/kuenstliche-intelligenz-und-recht>, zuletzt abgerufen am 1.4.2022.

<sup>144</sup> DAV (Fn. 40), Rn. 34.

werden muss.<sup>145</sup> Die Verwarnungen sollen darauf hinweisen, dass die Berechnung des Risikos nicht offengelegt wird und dass Zweifel bestehen, ob *COMPAS* eine Gruppe von Tätern oder Täterinnen unverhältnismäßig als Personen mit einem erhöhten Rückfallrisiko identifiziert habe.<sup>146</sup> Auch dies spricht für die Schaffung einer staatlichen Kontrollinstanz.<sup>147</sup> Diese könnte bei der Prüfung der Zulassung ein Sachverständigengutachten erstellen, das die Anwender und Anwenderinnen verständlich über die Gegebenheiten des jeweiligen Algorithmus oder KI-Systems aufklärt.

## 2. Rechtsmittel

Es ist wichtig, dass fehlerhafte automatisierte Entscheidungen korrigiert werden können. Liegt eine Verzerrung in den Daten vor, kann die KI den Bias nicht selbst erkennen und nicht selbst korrigieren. Dem Algorithmus fehlt die Freiheit von klar definierten Vorgaben abzuweichen.<sup>148</sup> Zudem können im menschlichen Bewusstsein noch weitere, bisher unentdeckte Variablen verborgen sein.<sup>149</sup> In Gerichtsverfahren dienen Rechtsmittel der Korrektur einer Entscheidung und sind somit Ausdruck davon, dass eine absolute Sicherheit in Entscheidungen nicht erreicht werden kann.<sup>150</sup> In Estland kann gegen die Entscheidung der künstlichen Richterinnen ein Rechtsmittel eingelegt werden. Das Urteil wird dann von einem menschlichen Richter oder Richterinnen überprüft.<sup>151</sup>

## 3. Richtige Anwendung der Ergebnisse einer KI

Die Warnhinweise, ein grundsätzliches Sachverständigengutachten über das zum Einsatz kommende KI-System oder eine Auseinandersetzung mit der Richtigkeit der Analyse im Rahmen eines Rechtsmittelverfahrens sind nur effektiv, wenn die Anwender und Anwenderinnen diese auch inhaltlich verstehen. Ansonsten würden entsprechende Maßnahmen in ihrer Anwendung obsolet, da Menschen dem Ergebnis eines Computers häufig mehr vertrauen als ihrem eigenen Urteilsvermögen.<sup>152</sup> Neben der Bereitstellung des notwendigen Wissens hinsichtlich des jeweiligen KI-Systems, müssen Anwender und Anwenderinnen die KI-Systeme also auch hinreichend verstehen, mit ihnen interagieren können und in die Lage versetzt werden, das System angemessen zu bewerten, um sich dem Ergebnis entgegenstellen zu können.<sup>153</sup> Es ist daher notwendig, dass Anwender und Anwenderinnen regelmäßig Schulungen darüber erhalten, wie die Resultate der Software zu bewerten sind.<sup>154</sup>

## F. Fazit

Der Einsatz von Algorithmen und KI hat sowohl positive als auch negative Auswirkungen auf das Strafverfahren. Er führt zu einem Effizienzgewinn und kann teilweise zu einer

konstanteren Rechtsprechung beitragen, indem lokale, regionale und richterindividuelle Unterschiede bei Entscheidungen erkannt und durch das Analyseergebnis angeglichen werden können. Auf der anderen Seite kann sich das Machtgleichgewicht zwischen der staatlichen Seite und der beschuldigten Person stark verschieben und die Individualisierbarkeit des Verfahrens verloren gehen. Um wirksam dagegen vorzugehen, müssen nicht notwendigerweise neue Regelungen geschaffen werden. Vielmehr kann man sich auf Grundsätze des Strafverfahrens berufen und diese im Lichte der besonderen Umstände automatisierter Prozesse anwenden. Der oder die Beschuldigte darf nicht bloßes Objekt des Strafverfahrens sein. Ihm oder ihr muss die Möglichkeit geboten werden, aktiv am Verfahren teilzunehmen. Dafür muss es dem oder der Beschuldigten zunächst ermöglicht werden, sich tatsächlich und konkret verteidigen zu können. Er oder sie muss i.S.v. § 136 StPO darüber aufgeklärt werden, ob automatisierte Systeme an der Entstehung des Tatvorwurfes oder der weiteren Ermittlung beteiligt waren. Außerdem muss die Möglichkeit bestehen sowohl den genutzten Algorithmus als auch die zugrundeliegenden Daten überprüfen zu können. Die Verteidigung muss ein erweitertes Akteneinsichtsrecht in Form eines Beweisantrages nach § 244 Abs. 3 StPO geltend machen können, um Zugriff auf die technischen Details, wie den Trainingsdatensatz einer KI, zu erhalten. Es muss diskutiert werden, wie mit den Beweisen, die durch die Analyse eines automatisierten Prozesses entstehen, umgegangen werden soll, wenn dadurch in die Rechte des oder der Beschuldigten eingegriffen wurde. In Betracht kommt eine konsequenter Anwendung eines Beweisverwertungsverbotes aufgrund der Verletzung des Fair-Trial Prinzips oder die Möglichkeit, die Ergebnisse einer KI-Analyse als Beweis in der Hauptverhandlung als nicht verwertbar zu betrachten, wenn bei der Entstehung datenschutzrechtliche Anforderungen verletzt wurden. Sollten Algorithmen oder KI-Systeme in der Hauptverhandlung unterstützend zum Einsatz kommen, muss aus dem Urteil hervorgehen, dass sich das Gericht ernsthaft mit dem Ergebnis der Analyse auseinandergesetzt hat und diese richtig bewerten konnte. Dafür bedarf es verständlicher Informationen über die jeweils zum Einsatz kommende Software. Denkbar sind zum Beispiel Sachverständigengutachten einer noch einzurichtenden staatlichen Kontrollinstanz, sowie regelmäßige Schulungen für Personen, die in ihre Entscheidungen sowohl im Ermittlungsverfahren als auch im Hauptverfahren Analyseergebnisse einer KI einfließen lassen. Gleiche Voraussetzungen müssen auch für die Rechtsmittelinstanz gelten, damit eine wirksame Korrektur über Entscheidungen besteht, die auf einer KI-Analyse beruhen.

<sup>145</sup> Jiang (Fn. 44), S. 562.

<sup>146</sup> Jiang (Fn. 44), S. 562.

<sup>147</sup> Dazu bereits oben unter E. III. 2. b).

<sup>148</sup> Ernst, JZ 2017, 1026 (1028 f.); Jiang (Fn. 44), 582.

<sup>149</sup> Jiang (Fn. 44), 582.

<sup>150</sup> Vgl. Fry (Fn. 8), S. 67.

<sup>151</sup> Niiler (Fn. 3).

<sup>152</sup> Vgl. Fry (Fn. 8), S. 81.

<sup>153</sup> Hochrangige Expertengruppe für KI, Ethik-Leitlinien für eine Vertrauenswürdige KI, 2019, Rn. 64.

<sup>154</sup> Staffler/Jany, ZIS 2020, 164 (175 f.); Zweig (Fn. 5), S. 9 f.