

# KriPoZ

## Kriminalpolitische Zeitschrift

### KONTAKT

schriftleitung@kripoz.de

### Herausgeber

Prof. Dr. Gunnar Duttge  
Prof. Dr. Bernd Heinrich  
Prof. Dr. Anja Schiemann

### Schriftleitung

Ass. iur. Sabine Horn  
Stellv.: Alfredo Franzone

### Redaktion (national)

Prof. Dr. Alexander Baur  
Prof. Dr. Gunnar Duttge  
Prof. Dr. Sabine Gless  
Prof. Dr. Bernd Hecker  
Prof. Dr. Martin Heger  
Prof. Dr. Bernd Heinrich  
Prof. Dr. Gabriele Kett-Straub  
Prof. Dr. Florian Knauer  
Prof. Dr. Michael Kubiciel  
Prof. Dr. Otto Lagodny  
Prof. Dr. Carsten Momsen  
Prof. Dr. Helmut Satzger  
Prof. Dr. Anja Schiemann  
Prof. Dr. Edward Schramm  
Prof. Dr. Dr. Markus Thiel  
Prof. Dr. Mark Zöller

### Redaktion international

Prof. Dr. Dres. h.c. Makoto Ida  
Prof. Neha Jain  
Prof. Dr. Doaqian Liu  
Prof. Dr. Dr. h.c. Francisco  
Munoz-Conde  
Prof. Dr. Konstantina  
Papathanasiou  
Prof. Dr. Wolfgang Schomburg  
Prof. Dr. Sheng-Wei Tsai  
Prof. Dongyi Syn PhD  
Prof. Dr. Davi Tangerino  
Prof. Dr. Dr. h.c. Yener Ünver

### ALLGEMEINE BEITRÄGE | 76 – 136

- 76 | Die politische Debatte über das Strafmündigkeitsalter: diskursive Deutungsmuster und Diskurskoalitionen**  
*von Prof. Dr. Thomas Waldvogel und EPHM Selim Celik*
- 89 | „Mittelbare Täterschaft“ durch kompromittierte Systeme – Grenzen personenbezogener Zurechnung im digitalen Raum**  
*von RA Dr. Dr. Fabian Teichmann, LL.M. (London), EMBA (Oxford)*
- 100 | Die heimliche Verabreichung von K.O.-Tropfen de lege lata und de lege ferenda – Zur Einordnung als Tatmittel und zum Reformbedarf infolge des Beschlusses BGH 5 StR 382/24**  
*von Linda Tiggemann*
- 107 | Die aktuellen Vorschläge zum strafrechtlichen Schutz vor digitaler Gewalt – Ein Debattenbeitrag**  
*von Prof. Dr. Elisa Hoven, Tim Marian Friedrich und Katharina Schooltink*
- 116 | Eingriffe in das Persönlichkeitsrecht – die zwangsweise Entsperrung von Mobiltelefonen**  
*von Leo-Valery Zaruba*
- 124 | Biometric device locks – an invitation to law enforcement? An analysis of EU limitations to the contentious police practice after the „Landeck“-Decision**  
*von Prof. Dr. Carsten Momsen und Miriam Süttmann*
- 129 | Die anwaltliche Äußerungsfreiheit im Lichte der Konvention zum Schutz des Anwaltsberufs – Eine Untersuchung der Rechtsprechung des Bundesverfassungsgerichts**  
*von Akad. Rat a.Z. Damien Nippen*

## BUCHBESPRECHUNGEN | 137 – 142

- 137 | **Manon Heindorf: Kinderpornographie im Ermittlungsverfahren**  
von StA Sebastian Christ
- 139 | **Marc Bauer: Grund und Grenzen der Verfolgungsverjährung im Sexualstrafrecht**  
von Simon Schlicksupp
- 141 | **Ibrahim Yanik: Algorithmenbasierte Systeme in der Strafzumessung**  
von Prof. Dr. Anja Schiemann

## TAGUNGSBERICHT | 143 – 156

- 143 | **Erlanger Cybercrime Tag 2025 – Digitale Beweismittel in der Hauptverhandlung**  
von Franka Härtlein, Dipl.-Jur. Leila Khayati und Ass. iur. Tabea Seum

## ALLGEMEINE BEITRÄGE

## Die politische Debatte über das Strafmündigkeitsalter: diskursive Deutungsmuster und Diskurskoalitionen

von Prof. Dr. Thomas Waldvogel und  
Selim Celik\*

### Abstract

Der Beitrag untersucht die politische Debatte um das Strafmündigkeitsalter am Beispiel der Plenardebatte im Deutschen Bundestag im Juni 2025 aus einer diskursanalytischen Perspektive. Leitende Fragestellung ist, wie Kinder- und Jugendkriminalität politisch problematisiert werden und welche kriminalpolitischen Handlungsoptionen durch diese Deutungen plausibilisiert oder marginalisiert werden. Die Arbeit knüpft damit an zentrale Kontroversen der Kriminalpolitik, der Jugendstrafrechtsforschung sowie der politikwissenschaftlichen Diskursforschung an. Im Mittelpunkt stehen dabei Debatten über Punitivität, Prävention und symbolische Sicherheitspolitik. Methodisch basiert der Beitrag auf einer qualitativen Diskursanalyse in Anlehnung an Maarten Hajer. Analysiert werden ein Gesetzentwurf der AfD sowie ausgewählte Plenarreden verschiedener Fraktionen. Im Fokus stehen diskursive Deutungsmuster, Storylines, Narrative und daraus rekonstruierte Diskurskoalitionen.

Die Analyse identifiziert drei zentrale Diskurskoalitionen: eine punitiv-repressive Sicherheitskoalition, eine präventiv-erzieherische Strukturkoalition sowie eine balanciert-rationalisierende Vermittlungskoalition. Diese Koalitionen strukturieren die Debatte weniger entlang formaler Parteigrenzen als entlang konkurrierender Problemdefinitionen von Sicherheit, Verantwortung und Entwicklung. Repressive Forderungen nach einer Absenkung der Strafmündigkeit erweisen sich dabei primär als diskursiv-symbolische Antworten auf wahrgenommene staatliche Kontrollverluste, weniger als empirisch evidenzbasierte Reformvorschläge. Präventiv-erzieherische Positionen interpretieren Jugendkriminalität überwiegend als strukturell und entwicklungsbedingt und rücken langfristige sozialpolitische sowie institutionelle Interventionen in den Vordergrund. Beide Diskurse bleiben jedoch wechselseitig nur begrenzt anschlussfähig, wodurch balanciert-rationalisierende Deutungen eine zentrale Funktion für die diskursive Vermittlung und politische Mehrheitsbildung einnehmen.

Die Arbeit verdeutlicht die politische Relevanz diskursiver Deutungen und der sie tragenden politischen Akteure für

kriminalpolitische Entscheidungsprozesse und unterstreicht den wissenschaftlichen Mehrwert diskursanalytischer Zugänge. Limitiert ist die Studie durch ihre Fokussierung auf eine einzelne Bundestagsdebatte und parlamentarische Kommunikationsformate. Weiterführende Forschung sollte mediale, institutionelle und professionsbezogene Diskurse stärker einbeziehen.

The article examines the political debate on the age of criminal responsibility through a discourse-analytical investigation of the plenary debate in the German Bundestag in 2025. The guiding research question is how child and juvenile delinquency is politically problematized and which criminal policy options are rendered plausible or marginalized through these interpretations. The study thus contributes to key controversies in criminal policy, youth criminal law research, and political science discourse analysis, particularly debates on punitiveness, prevention, and symbolic security politics. Methodologically, the article is based on a qualitative discourse analysis drawing on the work of Maarten Hajer. The analysis focuses on a legislative proposal submitted by the AfD as well as selected plenary speeches by representatives of different parliamentary factions. Particular attention is paid to discursive interpretive patterns, storylines, narratives, and the discourse coalitions reconstructed from them.

The analysis identifies three central discourse coalitions: a punitive-repressive security coalition, a preventive-educational structural coalition, and a balanced, rationalizing mediating coalition. These coalitions structure the debate less along formal party lines than along competing problem definitions of security, responsibility, and development. Repressive demands to lower the age of criminal responsibility primarily emerge as discursively symbolic responses to perceived losses of state control rather than as empirically evidence-based reform proposals. Preventive-educational positions, by contrast, interpret juvenile delinquency largely as structurally and developmentally conditioned and emphasize long-term social policy and institutional interventions. However, both discourses remain only weakly mutually compatible, highlighting the central role of balanced, rationalizing interpretations in

\* Dr. Thomas Waldvogel ist Professor für Politikwissenschaft, politische Bildung und Methodik des wissenschaftlichen Arbeitens an der Hochschule für Polizei in Baden-Württemberg. Selim Celik ist EPHM bei der Polizei Baden-Württemberg.

*enabling discursive mediation and political majority-building.*

*The study highlights the political relevance of discursive interpretations and the political actors who build them for criminal policy decision-making processes and underscores the scholarly value of discourse-analytical approaches. The analysis is limited by its focus on a single Bundestag debate and parliamentary communication formats. Future research should more strongly incorporate media, institutional, and professional discourses.*

## I. Einleitung

„Sie klauen. Sie rauben. Sie morden. Die Zahl der Straftaten von Minderjährigen steigt alarmierend an“ – mit dieser Schlagzeile titelte der „Stern“ bereits im Jahr 1996.<sup>1</sup> Sie macht einerseits deutlich, dass die Diskussion um die Strafmündigkeit von Kindern und Jugendlichen kein neues Phänomen ist. Gleichzeitig zeigt sich in der stark emotional aufgeladenen Formulierung, wie stark die öffentliche Debatte darüber von Sprache geprägt ist.<sup>2</sup>

Ob 1996 oder 2026: Immer wieder wird über eine mögliche Herabsetzung des Strafmündigkeitsalters in Deutschland diskutiert.<sup>3</sup> Auslöser dieser wiederkehrenden Debatten sind oftmals einzelne, medial präsente und besonders schwere Straftaten von Kindern,<sup>4</sup> die den Forderungen auf politischer Ebene vorausgehen.<sup>5</sup> Ein Beispiel aus dem Januar 2025: Der Tod eines zwölfjährigen Jungen in Stuttgart brachte Forderungen nach schärferen Gesetzen wieder auf die politische Agenda.<sup>6</sup> Innerhalb weniger Wochen griffen Medien, Ministerien und Parteien das Thema auf, bis es schließlich in einem Gesetzesentwurf der AfD im Deutschen Bundestag gipfelte, in welchem die Partei die Herabsetzung des Strafmündigkeitsalters von 14 auf 12 Jahre vorsieht.<sup>7</sup> Dieses Vorhaben löste bundesweite Diskurse in Politik und Gesellschaft aus.<sup>8</sup>

Die Analyse dieser (gesellschafts-)politischen Diskurse über das Strafmündigkeitsalter steht im Zentrum dieses Beitrags. Sie knüpft an unterschiedliche Forschungsstränge an, in welchen kriminologische, rechtswissenschaftliche und (entwicklungs-)psychologische Perspektiven dominieren.<sup>9</sup> Der Artikel ergänzt diese um einen ei-

genständigen Beitrag aus der politikwissenschaftlichen Kommunikationsforschung, indem er die Redebeiträge der Plenardebatte im deutschen Bundestag über den AfD Gesetzesentwurf vom Juni 2025 systematisch analysiert, in welchen sich, wie unter einem Brennglas, die politischen Diskurse über die Strafmündigkeit exemplarisch bündeln. Im Zentrum der Analyse stehen dabei die beiden folgenden Fragestellungen:

1. Welche diskursiven Deutungsmuster lassen sich in den politischen Diskursen über die Strafmündigkeit feststellen?
2. Welche Diskurskoalitionen lassen sich in der politischen Auseinandersetzung über die Strafmündigkeit identifizieren?

Ziel der Analyse ist es folglich, diskursive Deutungsmuster und Diskurskoalitionen herauszuarbeiten und einen politikwissenschaftlichen Forschungsstrang in der wissenschaftlichen Diskussion über das Strafmündigkeitsalter zu etablieren, auf dessen Befunden basierend Ableitungen für aktuelle Reformdebatten sowie für zukünftige kriminal- und rechtspolitische Entscheidungsprozesse vorgenommen werden können.

Aus politikwissenschaftlicher Sicht ist die Beantwortung dieser Fragestellungen dahingehend von Bedeutung, da sie exemplarisch verdeutlichen, wie politische Deutungskämpfe um Moral, Sicherheit und Verantwortung geführt werden. Sie offenbart die Aushandlungsprozesse zwischen präventiv-erzieherischen und punitiv-repressiven Leitbildern. Auch für die Polizei ist das Thema von Relevanz, da es um die öffentliche Wahrnehmung von Jugendkriminalität, Prävention und die Legitimation staatlicher Eingriffe in das Leben und die Grundrechte Minderjähriger geht. Wie über Kinder bzw. Jugendliche als Täter oder Opfer gesprochen wird, beeinflusst nicht nur politische Entscheidungsprozesse, sondern auch die gesellschaftliche Erwartung an polizeiliches Handeln.

Zur Beantwortung der Forschungsfragen wird im theoretischen Teil zunächst der aktuelle Forschungsstand dargestellt. Anschließend wird die Diskurstheorie nach *Maarten Hajer* eingeführt,<sup>10</sup> die als theoretisches Grundgerüst für das methodische Vorgehen der Analyse dient. In der

<sup>1</sup> Mathes/Metzner, Kriminelle Kinder: Was tun mit ihnen?, Stern 5 (96), S. 56–68.

<sup>2</sup> Hajer, in: Keller/Hiersland/Schneider/Viehöver (Hrsg.), Handbuch Sozialwissenschaftliche Diskursanalyse, 2004, S. 271–298.; ders., in: Janning/Toens (Hrsg.), Die Zukunft der Policy-Forschung, 2008, S. 211–222.

<sup>3</sup> Mathes/Metzner, Stern 5 (96), S. 56–68; Magoley, Tod von Yosef in Dormagen: Müssen Kinder früher strafmündig werden?, wdr.de v. 6.2.2026, online abrufbar unter: <https://bit.ly/3OY7Ex8> (zuletzt abgerufen am 12.2.2026); Gewalt unter Kindern – Strobl stellt Strafalter infrage, Stuttgarter Zeitung v. 17.2.2026, online abrufbar unter: <https://bit.ly/4s1X5Yj> (zuletzt abgerufen am 20.2.2026).

<sup>4</sup> Weuster/Detsch, Freudenberg: Eltern von Luise verklagen Täterinnen auf Schmerzensgeld, BILD v. 24.7.2025, online abrufbar unter: <https://bit.ly/4sGrxHI> (zuletzt abgerufen am 2.2.2026).

<sup>5</sup> Horten/Steffan/Weinand, Forens Psychiatr Psychol Kriminol 2023, 17 (4), 460–462, DOI: 10.1007/s11757-023-00799-z.; Baur/Rueß/Schaffeld/Fegert, KriPoZ 2024, 245–250.

<sup>6</sup> Karstedt/Stegmüller/Rosar, Stuttgart: 13-Jähriger schubst Junge (12) vor Straßenbahn – tot, BILD v. 31.1.2025, online abrufbar unter: <https://bit.ly/4rGEvEt> (zuletzt abgerufen am 2.2.2026).

<sup>7</sup> Bt-Drs. 21/333.

<sup>8</sup> Schupelius, Mehr Kinder werden Täter, aber sie werden nicht bestraft, BILD v. 6.9.2025, online abrufbar unter: <https://bit.ly/4cEcolm> (zuletzt abgerufen am 2.2.2026).

<sup>9</sup> Bannenberg, APuZ 2025, 32 (36, 37), online abrufbar unter: <https://bit.ly/4rpaRDp> (zuletzt abgerufen am 2.2.2026); Baur/Rueß/Schaffeld/Fegert, KriPoZ 2024, 245–250; Heitlinger, Die Altersgrenze der Strafmündigkeit. Eine Untersuchung entwicklungspsychologischer und kriminalpolitischer Aspekte unter Berücksichtigung der neueren Rechtsentwicklung in Europa, 2004; Horten/Steffan/Weinand, Forens Psychiatr Psychol Kriminol 2023, 17 (4), 460–462; Schmoe, Die Rolle des Alters im Jugendstrafrecht, 2004.

<sup>10</sup> Hajer, in: Keller/Hiersland/Schneider/Viehöver (Hrsg.), Handbuch Sozialwissenschaftliche Diskursanalyse, 2004, S. 271–298.; ders., in: Janning/Toens (Hrsg.), Die Zukunft der Policy-Forschung, 2008, S. 211–222.

anschließenden Untersuchung werden politische Redebeiträge aus der Bundestagsdebatte ausgewertet, um die zentralen Deutungsmuster und Diskurskoalitionen herauszuarbeiten. Im Schlusskapitel werden im Teilabschnitt „Diskussion“ die Ergebnisse zusammengeführt und im bestehenden Forschungsstand verortet. Die Schlussbetrachtung am Ende des letzten Kapitels reflektiert vorhandene Limitationen sowie mögliche Implikationen, die aus dem Artikel für Politik, Gesellschaft, Wissenschaft und Polizei erwachsen.

## II. Forschungsstand

Die wissenschaftliche Diskussion über das Alter, ab dem staatliche Straf- und Sanktionsgewalt gegenüber Heranwachsenden legitim ist, bildet ein Forschungsfeld, das nicht einer einzigen Fachdisziplin zugeordnet werden kann, sondern sich an der Schnittstelle mehrerer wissenschaftlicher Forschungsperspektiven entfaltet. Zentrale Fragestellungen betreffen dabei nicht nur die Formulierung normativer Altersgrenzen, sondern ebenso die juristische Begründung, empirische Fundierung und praktische Wirksamkeit solcher Grenzen. Während im deutschen Strafrecht die strafrechtliche Verantwortlichkeit seit dem Inkrafttreten der Reichsstrafgesetzzordnung und in späterer Ausdifferenzierung des Jugendgerichtsgesetzes bei 14 Jahren liegt (§ 19 StGB), wird diese Grenze in der wissenschaftlichen und politischen Diskussion regelmäßig hinterfragt und mit Blick auf normativ-politische sowie empirische Argumente evaluiert.<sup>11</sup>

Der bestehende Literaturkorpus lässt sich dabei grob in drei dominierende Forschungsperspektiven unterteilen, die unterschiedliche epistemologische Grundlagen, argumentative Schwerpunkte und empirische Zugänge haben. Sie lassen sich jeweils als juristisch-dogmatischer, entwicklungs- bzw. rechtspsychologischer und kriminologischer Strang identifizieren.<sup>12</sup> Dieser dreiteilige Forschungszugang reflektiert zugleich unterschiedliche wissenschaftliche Problemhorizonte: Erstens die systematische Einordnung und normative Legitimation gesetzlicher Altersgrenzen, zweitens die Beurteilung individueller Reife- und Verantwortungsfähigkeit und drittens die Wirkung und Effizienz strafrechtlicher Eingriffe im jugendlichen Lebensverlauf.

Im *juristischen Forschungsstrang* liegt der Fokus auf der normativen Fundierung und systematischen Einbettung des Strafmündigkeitsalters im Strafrecht. Die Frage, ab welchem Alter Personen für rechtswidriges Verhalten verantwortlich gemacht werden können, wird hier vornehmlich als dogmatische Frage diskutiert, die Elemente wie

Schuld- und Verantwortlichkeitslehre, rechtliche Systemkohärenz und verfassungsrechtliche Konsistenz umfasst. Neuere Beiträge thematisieren dabei auch die stark politisierte Debatte um das Strafmündigkeitsalter und zeigen auf, dass die (Rechts-)Dogmatik nicht losgelöst von kriminalpolitischen Erwartungen und gesellschaftlichen Debatten zu verstehen ist.<sup>13</sup>

*Entwicklungs- und rechtspsychologische Forschung* wirkt dabei als verbindendes Argumentationsfeld zwischen empirischer Evidenz und normativer Gesetzgebung, indem sie kognitive, moralische und neurobiologische Reifeprozesse heranzieht, um die Frage des strafrechtlichen Verantwortungsalters evidenzbasiert zu begründen.<sup>14</sup> Die empirische Entwicklungspsychologie liefert beispielsweise evidenzbasierte Einsichten in neurokognitive und psychosoziale Reifungsprozesse,<sup>15</sup> die für juristische Konzepte der Verantwortlichkeit relevant sind und thematisiert die Variabilität individueller Entwicklung. Entwicklungsprozesse werden durch soziale, familiäre, kulturelle und bildungsbezogene Faktoren beeinflusst, die sich nicht allein über das Lebensalter abbilden lassen.<sup>16</sup> Aus Sicht der rechtspsychologischen Literatur führt diese Befundlage zu einer Kritik an der Annahme fester Altersgrenzen als alleiniger Indikator für Verantwortungsreife. Nach dieser Perspektive ist nicht das chronologische Alter selbst das Kriterium für Reife, sondern ein Bündel von psychologischen Fähigkeiten, die sich heterogen entwickeln.<sup>17</sup> Dies zeigt sich auch darin, dass die wissenschaftliche Diskussion über die richtige Altersgrenze für strafrechtliche Verantwortlichkeit im internationalen Vergleich sehr unterschiedlich verläuft und in der Rechtswissenschaft mit neuropsychologischen Argumenten konfrontiert wird, die eine dispositive Herangehensweise an Reifefragen nahelegen.<sup>18</sup>

Die *kriminologische Forschung* zum Strafmündigkeitsalter nähert sich der Fragestellung nicht primär normativ oder entwicklungspsychologisch, sondern über die Analyse von Delinquenzverläufen, Alters-Kriminalitäts-Zusammenhängen und den Wirkungen formeller sozialer Kontrolle.<sup>19</sup> Im Zentrum steht damit weniger die individuelle Reifefähigkeit als vielmehr die Frage, welche kriminalpolitischen Effekte Altersgrenzen der Strafbarkeit entfalten und wie sich frühe oder späte strafrechtliche Interventionen auf kriminelle Karrieren auswirken.<sup>20</sup> Die kriminologische Forschung problematisiert beispielsweise die Annahme, dass eine frühere strafrechtliche Verantwortlichkeit automatisch präventive Effekte entfaltet. Vielmehr zeigt die empirische Forschung, dass frühe formelle Sanktionierung häufig mit Labeling-Effekten, Stigmatisierung und erhöhtem Rückfallrisiko verbunden ist.

<sup>11</sup> *Trips-Hebert*, Aktueller Begriff: Strafmündigkeitsgrenze, Deutscher Bundestag Wissenschaftliche Dienste Nr. 14/24, online abrufbar unter: <https://bit.ly/40HzwIB> (zuletzt abgerufen am 2.2.2026).

<sup>12</sup> *Bannenberg*, APuZ 2025, 32-39; *Baur/Rueß/Schaffeld/Fegert*, KriPoZ 2024, 245-250; *Schmöe*, Die Rolle des Alters im Jugendstrafrecht; *Heitlinger*, Die Altersgrenze der Strafmündigkeit.

<sup>13</sup> *Schmöe*, Die Rolle des Alters im Jugendstrafrecht.

<sup>14</sup> *Heitlinger*, Die Altersgrenze der Strafmündigkeit.

<sup>15</sup> *Icenogle/Steinberg/Duell/Chein/Chang/Chaudhary et al.*, Law and human behavior 2019, 43 (1), 69-85. DOI: 10.1037/lhb0000315; *Steinberg*, Developmental review 2008, 28 (1), 78-106. DOI: 10.1016/j.dr.2007.08.002.

<sup>16</sup> *Leschied*, Canadian journal of criminology 1988, (1), 17-31.

<sup>17</sup> *Horten/Steffan/Weinand*, Forens Psychiatr Psychol Kriminol 2023, 17 (4), 460-462.

<sup>18</sup> *Pillay*, Journal of child and adolescent mental health 2019, 31 (3), 224-234. DOI: 10.2989/17280583.2019.1692851.

<sup>19</sup> *Bannenberg*, APuZ 2025, 32-39; *Cohen*, American Sociological Review 1983, 48 (5), 728, DOI: 10.2307/2094931; *Moffitt*, Psychological Review 1993, 100 (4), 674-701. DOI: 10.1037/0033-295X.100.4.674.

<sup>20</sup> *Bannenberg*, APuZ 2025, 32-39.

Studien zur Wirkung formeller Interventionen gegenüber informellen oder sozialpädagogischen Reaktionen legen nahe, dass gerade bei Jugendlichen und Heranwachsenden strafrechtliche Reaktionen die Wahrscheinlichkeit erneuter Delinquenz eher erhöhen als senken können.<sup>21</sup> Vor diesem Hintergrund wird das Strafmündigkeitsalter in der Kriminologie häufig nicht als Ausdruck moralischer Verantwortungszuschreibung, sondern als Steuerungsinstrument staatlicher Sozialkontrolle analysiert. Die kriminal- und rechtspolitische Forschung fragt danach, ob eine Absenkung der Strafmündigkeitsgrenze tatsächlich zu einer Reduktion von Jugendkriminalität führt oder ob sie lediglich zu einer Vorverlagerung formeller Sanktionierung ohne nachhaltige Präventionswirkung beiträgt. Vergleichende Studien legen nahe, dass niedrigere Strafmündigkeitsgrenzen nicht mit niedrigeren Jugendkriminalitätsraten korrelieren, während wohlfahrts- und interventionsorientierte Jugendhilfesysteme tendenziell günstigere Langzeitverläufe aufweisen.<sup>22</sup>

Die wissenschaftliche Diskussion zum Strafmündigkeitsalter ist bislang deutlich von juristischen, (entwicklungs-)psychologischen und kriminologischen Forschungssträngen geprägt.<sup>23</sup> Diese Perspektiven liefern wichtige Erkenntnisse über normative Anforderungen, individuelle Reifefähigkeit und kriminalpräventive Effekte unterschiedlicher Altersgrenzen. Gemein ist ihnen jedoch, dass sie das Strafmündigkeitsalter primär als Sachproblem behandeln, das entweder rechtlich zu begründen, empirisch zu evaluieren oder entwicklungsbezogen zu bestimmen ist. Der politische Diskurs, in dem Forderungen nach einer Absenkung oder Beibehaltung der Strafmündigkeitsgrenze artikuliert, legitimiert und konflikтуalisiert werden, bleibt demgegenüber bislang weitgehend unberücksichtigt.

Gerade hier eröffnet sich eine zentrale politik- und kommunikationswissenschaftliche Leerstelle. Debatten über das Strafmündigkeitsalter sind nicht lediglich fachwissenschaftliche Auseinandersetzungen über empirische Evidenz oder normative Kohärenz, sondern hochgradig diskursiv strukturierte politische Konflikte, in denen unterschiedliche Deutungen von Jugend, Verantwortung, Schuld, Sicherheit und Staatlichkeit aufeinandertreffen. Ob eine Absenkung der Strafmündigkeit als notwendiger Beitrag zur inneren Sicherheit, als symbolische Strafverschärfung oder als Bruch mit dem Schutzgedanken des Jugendstrafrechts interpretiert wird, ist weniger Ergebnis wissenschaftlicher Konsensbildung als Ausdruck konkurrierender politischer Deutungsmuster.

An dieser Stelle setzt der vorliegende Beitrag an. Er ergänzt die bestehende Forschung um eine politikwissenschaftliche Perspektive aus der Kommunikations- und Diskursforschung, indem er die politischen Aushandlungsprozesse selbst in den Mittelpunkt rückt. Anders als juristische, (entwicklungs-)psychologische oder kriminologische Arbeiten fragt der Artikel nicht danach, welches Strafmündigkeitsalter normativ geboten oder empirisch wirksam ist, sondern danach, wie über Strafmündigkeit politisch gesprochen wird, welche Bedeutungen ihr zugeschrieben werden und welche Akteurskonstellationen diese Deutungen tragen.

### III. Methodisches Vorgehen

Als theoretische Grundlage für das methodische Vorgehen der Analyse dient der diskurstheoretische Ansatz nach *Hajer*,<sup>24</sup> der diskursive Deutungsmuster in Form von Metaphern, Storylines und Narrative sowie Akteurskonstellationen, verstanden als Diskurskoalitionen, in den Mittelpunkt des Erkenntnisinteresses rückt. Ziel seiner Analysen ist es, jene Narrative, Storylines und Metaphern offenzulegen, durch die politische Probleme gedeutet, strukturiert und kommunizierbar gemacht werden sowie die Identifikation von denjenigen Akteurskonstellationen, die diese Deutungsmuster politisch tragen.

*Metaphern* übernehmen in der Diskursanalyse eine zentrale Funktion, da sie als kognitive Deutungsrahmen fungieren, die komplexe politische Sachverhalte vereinfachen und strukturieren. Sie lenken Wahrnehmungen, indem sie bestimmte Aspekte eines Problems hervorheben und andere ausblenden, und präfigurieren auf diese Weise, welche politischen Lösungsoptionen als plausibel oder legitim erscheinen.<sup>25</sup> *Storylines* (Erzählverläufe) sind verdichtete, leicht anschlussfähige Kurz-Erzählungen, die komplexe politische Konflikte in prägnanter Form interpretierbar machen.<sup>26</sup> Sie reduzieren Komplexität, erzeugen Sinnkohärenz und ermöglichen Verständigung zwischen Akteuren mit unterschiedlichen Interessen, Wissensbeständen und normativen Orientierungen, ohne dass hierfür ein vollständiger inhaltlicher Konsens erforderlich ist.<sup>27</sup> *Narrative* konzeptualisiert *Hajer* implizit als übergreifende Erzählmuster eines politischen Diskurses.<sup>28</sup> Sie bilden umfassendere Sinn- und Deutungszusammenhänge, in denen einzelne Elemente wie Metaphern und Storylines miteinander verknüpft werden, sodass eine kohärente „Geschichte“ über ein politisches Problem oder eine gesellschaftliche Entwicklung entsteht.<sup>29</sup> In diesem Verständnis strukturieren Narrative politische Wirklichkeitsdeutungen, indem sie Ereignisse kausal, moralisch und zeitlich ordnen, Verantwortlichkeiten zuschreiben,

<sup>21</sup> Bernburg/Krohn/Rivera, *Journal of Research in Crime and Delinquency* 2006, 43 (1), 67–88, DOI: 10.1177/0022427805280068.

<sup>22</sup> Baur/Rueß/Schaffeld/Fegert, *KriPoZ* 2024, 245–250; Cavadino/Dignan, *Criminology & Criminal Justice* 2006, 6 (4), 435–456, DOI: 10.1177/1748895806068581; Junger-Tas/Gruszczyńska/Steckee/Killias/Enzmann/Haen Marshall (Hrsg.), *Juvenile Delinquency in Europe and Beyond: Results of the Second International Self-Report Delinquency Study*, 2010.

<sup>23</sup> Baur/Rueß/Schaffeld/Fegert, *KriPoZ* 2024, 245–250; Heitlinger, *Die Altersgrenze der Strafmündigkeit*; Schmoe, *Die Rolle des Alters im Jugendstrafrecht*.

<sup>24</sup> Hajer, in: Keller/Hiersland/Schneider/Viehöver (Hrsg.), *Handbuch Sozialwissenschaftliche Diskursanalyse*, 2004, S. 271–298; ders., in: Janning/Toens (Hrsg.), *Die Zukunft der Policy-Forschung*, 2008, S. 211–222.

<sup>25</sup> Hajer, in: Janning/Toens (Hrsg.), *Die Zukunft der Policy-Forschung*, 2008, S. 211–222.

<sup>26</sup> Vgl. Fn. 25.

<sup>27</sup> Vgl. Fn. 25.

<sup>28</sup> Vgl. Fn. 25.

<sup>29</sup> Vgl. Fn. 25.

Problemlagen definieren und politische Handlungsnotwendigkeiten plausibilisieren.

Als *Diskurskoalition* beschreibt *Hajer* eine Gruppe von (politischen) Akteuren, die in einem bestimmten Zeitraum auf ähnliche diskursive Praktiken zurückgreifen und dabei eine begrenzte Auswahl an Storylines und Metaphern verwenden.<sup>30</sup> Unter Praktiken versteht er „verankerte Routinen und gegenseitig verstandene Regeln und Normen, die im gesellschaftlichen Leben für Stimmigkeit sorgen“.<sup>31</sup> Diskurskoalitionen entstehen demnach nicht zwingend aus einem gemeinsamen inhaltlichen Verständnis oder identischen Interessenlagen, sondern bereits aus Überschneidungen in den verwendeten Deutungsmustern, Argumentationslogiken und kommunikativen Routinen. Konkret definiert er Diskurskoalitionen als „ein Zusammenspiel einer Reihe von Erzählverläufen, von Akteuren, die diese Erzählverläufe äußern, und von Vorgehensweisen, durch die diese Erzählverläufe zum Ausdruck kommen“.<sup>32</sup> Politik erscheint in diesem Verständnis als ein Prozess, in dem Akteure mit unterschiedlichen Hintergründen und Argumentationsgrundlagen um bestimmte Metaphern, Storylines und Narrative herum Koalitionen bilden. Der Begriff der Diskurskoalition ist daher eng mit den Konzepten des Narrativs, der Storyline und der Metapher verknüpft. Konsens oder zumindest Anschlussfähigkeit innerhalb eines Diskurses entsteht, indem sich Akteure auf kompatible Narrative, Metaphern und Storylines beziehen, über die politische Problemdeutungen kommunikativ vermittelt, stabilisiert und legitimiert werden.<sup>33</sup>

Diese methodische Herangehensweise auf theoretischer Grundlage von *Hajer* bietet sich für die im Rahmen dieses Artikels zu untersuchenden Fragestellungen nach den diskursiven Deutungsmustern und Diskurskoalitionen in besonderer Weise an, da sie es erlaubt, politische Konflikte nicht allein als Ausdruck divergierender Interessen oder normativer Positionen zu analysieren, sondern als diskursive Aushandlungsprozesse, in denen Bedeutungen, Problemdefinitionen und Handlungsspielräume konstruiert und stabilisiert werden.<sup>34</sup>

Aufbauend auf diesem diskurstheoretischen Ansatz wird der politische Diskurs über das Strafmündigkeitsalter als ein konflikthafte Feld konkurrierender Deutungen analysiert, in dem politische Akteure durch sprachliche Muster, verdichtete Storylines und koalitionsbildende Sinnangebote um Deutungshoheit ringen. Ziel ist es, die zentralen diskursiven Deutungsmuster sowie die sich herausbildenden Diskurskoalitionen systematisch zu rekonstruieren. Die Analyse stützt sich auf eine qualitative Auswertung der Redebeiträge in der 11. Sitzung des Deutschen Bundestags, die für die aktuelle parlamentarische Debatte um das Strafmündigkeitsalter konstitutiv sind. Hierzu zählen der Gesetzentwurf der AfD-Fraktion zur Herabsetzung der Strafmündigkeit sowie das Plenarprotokoll der Bundestagsdebatte vom 6. Juni 2025.<sup>35</sup> Die ausgewählten Debattenbeiträge decken den Diskurs um die Herabsetzung des Strafmündigkeitsalters zwar nicht vollständig ab, da im Rahmen dieser Arbeit der Fokus auf den am 3. Juni 2025 eingereichten Gesetzentwurf und die Reaktionen gelegt wurde. Gleichzeitig ermöglicht diese Materialbasis eine diskurstheoretische Analyse parlamentarischer Aushandlungsprozesse und Akteurspositionen. Sie bietet somit eine konzentrierte Analyse der zentralen diskursiven Ausdrucksformen, Metaphern, Storylines und Narrative und ersucht bestehende Diskurskoalitionen in den Akteurskonstellationen offenzulegen.

Methodisch erfolgte die Auswertung in einem mehrstufigen Vorgehen, das sich eng an *Hajers* diskurstheoretischen Kategorien orientiert.<sup>36</sup> In einem ersten Schritt wurden sprachliche Elemente identifiziert, insbesondere Metaphern und wiederkehrende diskursive Ausdrucksformen, durch die politische Problemdeutungen artikuliert werden. Darauf aufbauend wurden prägende Storylines rekonstruiert, die diese sprachlichen Elemente zu verdichteten Deutungsangeboten bündeln. In einem dritten Schritt wurden diese Storylines zu übergeordneten narrativen Problemdefinitionen zusammengeführt, in denen Jugendkriminalität kausal, moralisch und politisch eingeordnet wird. Abschließend wurden Diskurskoalitionen rekonstruiert, die sich über die gemeinsame Nutzung dieser Narrative, Storylines und Metaphern konstituieren (siehe Tabelle 1).

<sup>30</sup> Vgl. Fn. 24.

<sup>31</sup> Vgl. Fn. 25.

<sup>32</sup> *Hajer*, in: Janning/Toens (Hrsg.), *Die Zukunft der Policy-Forschung*, 2008, S. 211–222.

<sup>33</sup> *Hajer*, in: Keller/Hierselund/Schneider/Viehöver (Hrsg.), *Handbuch Sozialwissenschaftliche Diskursanalyse*, 2004, S. 271–298.

<sup>34</sup> Vgl. Fn. 32.

<sup>35</sup> BT-Drs. 217333 sowie BT-Plenarprotokoll 21/11.

<sup>36</sup> *Hajer*, in: Keller/Hierselund/Schneider/Viehöver (Hrsg.), *Handbuch Sozialwissenschaftliche Diskursanalyse*, 2004, S. 271–298; *ders.*, in: Janning/Toens (Hrsg.), *Die Zukunft der Policy-Forschung*, 2008, S. 211–222.

Tabelle 1: Diskursanalytische Konzepte.

| Theoretisches Konzept / Kategorie             | Beschreibung / Funktion                                                                                                                                                                                                                                                                                     | Beispiele                                                                                                                                                                                                                                                                                |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Metaphern / diskursive Ausdrucksformen</b> | Identifikation zentraler sprachlicher Muster (z.B. <u>alarmistische</u> Bedrohungszuschreibungen, Emotionalisierungen, Entwicklungs- und Verantwortungszuschreibungen, Legitimationsverweise), durch die politische Problemdeutungen artikuliert und plausibilisiert werden.                                | Alarmismus: „immer rücksichtsloser“;<br>Entwicklungszuschreibung: „Kinder sind keine kleinen Erwachsenen“;<br>Legitimationsstrategie: Verweise auf Studien, Statistiken, internationale Vergleiche                                                                                       |
| <b>Storylines</b>                             | Rekonstruktion verdichteter, anschlussfähiger Kurz-Erzählungen, die wiederkehrende Argumentationsmuster bündeln und komplexe politische Konflikte interpretierbar machen (z.B. punitiv-repressiv, präventiv-erzieherisch, balanciert, polarisierend).                                                       | punitiv-repressiv: „Härtere Strafen schützen die Gesellschaft“;<br>präventiv-erzieherisch: „Kinder brauchen Unterstützung statt Strafe“;<br>balanciert: „Entscheidungen müssen auf Daten und Studien beruhen“;<br>polarisierend: „Die politische Gegenseite verharmlost Gewalt“          |
| <b>Narrative</b>                              | Zusammenführung mehrerer Storylines und Metaphern zu übergeordneten Deutungsmustern, in denen Jugendkriminalität kausal, moralisch und politisch eingeordnet wird (z.B. als Sicherheitsproblem, strukturelles Problem, Erziehungsproblem oder Einzelfall).                                                  | Sicherheitsnarrativ: Jugendkriminalität als Bedrohung und Kontrollverlust;<br>Strukturnarrativ: Ursachen in Armut, Schule, sozialem Umfeld;<br>Erziehungsnarrativ: Versagen von Eltern und Erziehungsinstanzen;<br>Einzelfallnarrativ: Ablehnung generalisierender Problemzuschreibungen |
| <b>Diskurskoalitionen</b>                     | Rekonstruktion von Akteurskonstellationen, die durch die gemeinsame Nutzung ähnlicher Narrative, Storylines und Metaphern verbunden sind, ohne notwendigerweise identische Interessen oder ideologische Positionen zu teilen (z.B. punitiv-repressiv, präventiv-erzieherisch, balanciert-rationalisierend). | Punitiv-repressive Koalition: sicherheitspolitische Argumentationsmuster;<br>präventiv-erzieherische Koalition: sozialpolitisch Argumentationsmuster;<br>balanciert-rationalisierend: evidenzbasierte Argumentationsmuster                                                               |

#### IV. Analyse

Die nachfolgende Analyse ersucht, diskursive Deutungsmuster und Diskurskoalitionen in der parlamentarischen Debatte über das Strafmündigkeitsalter herauszuarbeiten.

##### 1. Diskursive Deutungsmuster

Den Ausgangspunkt bildet der von der AfD im Juni 2025 eingebrachte Gesetzesentwurf (BT-Drs. 21/333), der den aktuellen politischen Diskurs um die Strafmündigkeit wie unter einem parlamentarischen Brennglas konzentriert und als aktueller Referenzpunkt für die weitere politische Auseinandersetzung dient.

##### a) Gesetzesentwurf der AfD 2025

Der Gesetzesentwurf der AfD-Fraktion zur Absenkung der Strafmündigkeit ist diskursiv geprägt durch eine stark sicherheitsorientierte Problemkonstruktion, in der Kinder- und Jugendkriminalität als eskalierendes gesellschaftliches Risiko dargestellt wird. Bereits zu Beginn wird darauf verwiesen, dass in den letzten Jahren eine „deutliche Zunahme im Bereich der Kinderdelinquenz“ zu verzeichnen sei, verbunden mit dem Hinweis auf einen „erneuten Höchststand“ der registrierten Straftaten von Kindern unter 14 Jahren. Diese Formulierungen rahmen Jugendkriminalität als dynamisches und sich verschärfendes Problem, das unmittelbares politisches Handeln erforderlich mache.

Zur Dramatisierung dieser Entwicklung werden einzelne Gewaltverbrechen exemplarisch herangezogen. So heißt es, im März 2023 habe „die Ermordung der zwölfjährigen Schülerin Luise aus Nordrhein-Westfalen die Öffentlichkeit“ erschüttert. Dieses Ereignis wird nicht als Ausnahme, sondern als Symptom einer übergreifenden Problemlage präsentiert. Entsprechend wird betont, es handle sich „mitnichten um einen Einzelfall“, sondern um einen Ausdruck einer allgemeinen Entwicklung. Die alarmistische Rahmung wird durch explizite Emotionalisierungen ergänzt. So wird festgestellt: „Besonders erschreckend ist,

dass in den letzten Jahren eine deutliche Zunahme im Bereich der Kinderdelinquenz zu verzeichnen ist.“ Die Kombination aus statistischer Entwicklung und emotionaler Bewertung verstärkt den Eindruck eines eskalierenden Sicherheitsproblems und erhöht den politischen Handlungsdruck. Neben diesen Bedrohungszuschreibungen enthält der Gesetzentwurf klare Verantwortungszuschreibungen. Minderjährige Täterinnen und Täter werden als Akteure adressiert, die strafrechtlich „zur Verantwortung gezogen“ werden müssten. Das bestehende Jugendstrafrecht wird dabei als unzureichend dargestellt, da es „nicht geeignet“ sei, „die steigende Kriminalität von Kindern, Jugendlichen und Heranwachsenden einzudämmen“. Entwicklungspsychologische und erzieherische Leitgedanken des Jugendstrafrechts werden zwar erwähnt, jedoch implizit relativiert, indem ihre Effektivität zur Prävention schwerer Straftaten infrage gestellt wird. Darüber hinaus werden auch elterliche Verantwortlichkeiten problematisiert. So wird ausgeführt, dass Eltern notwendige Maßnahmen teilweise „ablehnen [...] und verweigern“, wodurch staatliches Eingreifen als erforderlich dargestellt wird. Auf diese Weise wird delinquentes Verhalten nicht nur individualisiert, sondern zugleich familial kontextualisiert. Zur Legitimation der vorgeschlagenen Absenkung der Strafmündigkeit greift der Gesetzesentwurf wiederholt auf objektivierend wirkende Verweise zurück. Neben kriminalstatistischen Daten werden internationale Vergleiche herangezogen. So wird darauf hingewiesen, dass die Strafmündigkeit in Staaten wie „England“, „den Niederlanden“ oder „der Schweiz“ bereits unter 14 Jahren liege. Diese Bezugnahmen dienen dazu, die vorgeschlagene Reform als international anschlussfähig und sachlich begründet erscheinen zu lassen.

Diese sprachlichen Elemente verdichten sich zu einer dominanten punitiv-repressiven Storyline, in der härtere strafrechtliche Instrumente als notwendige Voraussetzung für die Wiederherstellung von Sicherheit und Ordnung erscheinen. Strafrecht wird in dieser Erzählung als zentrales

Steuerungsinstrument konstruiert, das sowohl abschreckend wirken als auch den Schutz der Allgemeinheit gewährleisten soll. Präventiv-erzieherische Argumente – etwa der Verweis auf das Kindeswohl oder auf therapeutische Interventionen – treten zwar ebenfalls auf, bleiben jedoch funktional untergeordnet. Sie dienen vor allem dazu, repressivere Maßnahmen zu legitimieren, indem diese als zugleich fürsorglich und verantwortungsbewusst gerahmt werden. Eine genuine Alternative zum strafrechtlichen Zugriff wird auf diese Weise nicht entfaltet.

Auf der narrativen Ebene dominiert im Gesetzesentwurf eindeutig ein Sicherheitsnarrativ. Jugend- und Kinderkriminalität wird als strukturelle Bedrohung für die öffentliche Sicherheit und das Vertrauen in den Rechtsstaat interpretiert, der nur durch entschiedenes staatliches Handeln begegnet werden könne. Dieses Narrativ wird durch ein sekundäres Erziehungsnarrativ ergänzt, in dem Defizite familiärer Verantwortung als mitursächlich für delinquentes Verhalten identifiziert werden. Beide Narrative stützen sich gegenseitig: Während das Sicherheitsnarrativ den Handlungsdruck erzeugt, legitimiert das Erziehungsnarrativ staatliche Eingriffe in familiäre Autonomie. Narrative, die Jugendkriminalität als strukturelles Problem sozialer Ungleichheit oder als Ergebnis individueller Einzelfälle deuten, bleiben hingegen weitgehend ausgeblendet oder werden explizit zurückgewiesen.

#### b) Tobias Matthias Peterka (AfD)

Den Auftakt in der Plenardebatte machte *Tobias Matthias Peterka*, Abgeordneter der AfD. Sein Redebeitrag ist diskursiv durch eine stark zugespitzte sicherheitspolitische Problemkonstruktion geprägt, in der Kinder- und Jugendkriminalität als eskalierendes gesellschaftliches Risiko dargestellt wird. Bereits einleitend wird zwar anerkannt, dass Kinder und Jugendliche sich in einem Prozess des „Heranreifens“ befinden und „noch nicht im Vollbesitz der Erkenntnisfähigkeit“ seien. Diese entwicklungsbezogene Perspektive wird jedoch unmittelbar relativiert, indem betont wird, dass Nachsicht „im Strafrecht irgendwann an eine Grenze“ stoße. Damit wird früh eine argumentative Verschiebung vorgenommen: Entwicklungspsychologische Erwägungen gelten nur bis zu einem Punkt, ab dem strafrechtliche Sanktionen als zwingend notwendig erscheinen.

Zentrale sprachliche Elemente des Beitrags sind alarmistische Bedrohungszuschreibungen, die Jugendkriminalität als außer Kontrolle geratenes Phänomen rahmen. Formulierungen wie die „überhandnehmende Kriminalität Jugendlicher“ oder der Verweis auf „zweistellige Wachstumsraten bei der Kinder- und Jugendkriminalität“ erzeugen den Eindruck einer sich zuspitzenden Lage. Diese Eskalationsdiagnose wird durch eine umfassendere Niedergangserzählung verstärkt, wenn konstatiert wird: „Dieses Land ist nicht mehr, wie es einmal war.“ Jugendkriminalität wird damit nicht nur als isoliertes Problem, sondern als Symptom eines allgemeinen gesellschaftlichen Verfalls interpretiert. Der Redebeitrag arbeitet zudem stark mit Emotionalisierungen und drastischen Gewaltbeschreibungen. Gewalthandlungen werden explizit benannt –

„zusammenschlagen“, „vor Züge stoßen“, „abstechen“ oder „berauben“ –, um moralische Eindeutigkeit herzustellen und die Legitimität repressiver Maßnahmen zu unterstreichen. Metaphorische Bilder wie der Untergang von „Bullerbü an unseren Schulen und Spielplätzen“ kontrastieren eine idealisierte, vermeintlich sichere Vergangenheit mit einer als bedrohlich dargestellten Gegenwart. Diese Emotionalisierung wird durch appellative Zuspitzungen („Hören Sie um Gottes willen endlich auf“) weiter intensiviert. In Bezug auf Verantwortungszuschreibungen weist der Redebeitrag eine deutliche Verschiebung hin zu individueller und kollektiver Schuldzuweisung auf. *Peterka* argumentiert, dass selbst Zwölfjährige in der Lage seien, das Unrecht schwerer Gewalttaten zu erkennen, womit die Fähigkeit zur moralischen Einsicht bereits im Kindesalter behauptet wird. Gleichzeitig werden Eltern als zentrale Verantwortliche problematisiert, die ihre Kinder nicht mit den „Werten und Regeln in diesem Land“ vertraut machten, weil sie diese selbst „kaum kennen oder sie sogar offen verachten“. Kriminalität wird so in einen Kontext defizitärer Erziehung und staatsablehnender Milieus gestellt, während sozialstrukturelle Erklärungen explizit delegitimiert werden. Zur Legitimation seiner Argumentation greift der Redner wiederholt auf scheinbar objektivierende Verweise zurück. Polizeiliche Kriminalstatistiken werden ausführlich zitiert, um das Ausmaß der Jugendkriminalität zu quantifizieren, und zugleich wird ein noch größeres Dunkelfeld suggeriert. Ergänzend beruft sich *Peterka* auf externe Autoritäten wie die Deutsche Polizeigewerkschaft sowie auf internationale Vergleiche mit Ländern wie den Niederlanden, Irland, Großbritannien oder Griechenland, in denen die Strafmündigkeit teilweise deutlich niedriger angesetzt ist. Diese Verweise dienen dazu, die Forderung nach einer Absenkung der Strafmündigkeit als sachlich begründet und international anschlussfähig erscheinen zu lassen.

Diese sprachlichen Elemente verdichten sich zu einer klar dominanten punitiv-repressiven Storyline. Strafrechtliche Verschärfungen werden als einzig wirksames Mittel gegen Jugendkriminalität präsentiert, während präventiv-erzieherische oder sozialpolitische Ansätze explizit abgewertet werden. Verweise auf „sozialarbeiterische Selbstregulierung“ in Familien erscheinen in der Rede als realitätsfern und unzureichend. Zwar wird formal betont, dass weiterhin das Jugendstrafrecht angewendet werden solle, diese Relativierung bleibt jedoch rhetorisch und ändert nichts an der grundsätzlich repressiven Stoßrichtung. Gleichzeitig ist der Beitrag stark polarisierend angelegt. Politische Gegner werden beschuldigt, Probleme zu verdrängen, zu beschwichtigen oder bewusst zu zerreden. Es wird ein implizites Zusammenwirken „über Parteigrenzen hinweg“ suggeriert, das zulasten der öffentlichen Sicherheit gehe. Demgegenüber inszeniert sich die AfD als einzige politische Kraft, die Missstände offen benenne und konsequent adressiere.

Auf der narrativen Ebene dominiert eindeutig ein Sicherheitsnarrativ. Jugend- und Kinderkriminalität werden als Bedrohung für öffentliche Ordnung, Schulen und Spielplätze konstruiert, der nur durch entschlossenes staatli-

ches Handeln begegnet werden könne. Dieses Sicherheitsnarrativ wird durch ein Erziehungsnarrativ flankiert, in dem elterliches Versagen und defizitäre Wertevermittlung als zentrale Ursachen benannt werden. Narrative, die Jugendkriminalität als strukturelles Problem sozialer Ungleichheit oder als Folge einzelner Ausnahmefälle deuten, bleiben hingegen marginalisiert oder werden explizit zurückgewiesen.

#### c) Axel Müller (CDU/CSU)

Der zweite Redebeitrag der Plenardebatte von *Axel Müller* (CDU) ist insgesamt durch eine de-emotionalisierende und rationalisierende Sprache geprägt. Alarmistische Bedrohungszuschreibungen werden explizit zurückgewiesen. So warnt *Müller* davor, „den Eindruck [zu erwecken], dass die Jugend heute schlechter wäre als früher“, und setzt dieser Problematisierung positive Gegenbilder entgegen („Viele junge Menschen engagieren sich ehrenamtlich [...]. Sie sind unsere Zukunft“). Diese Form der Normalisierung und Relativierung fungiert als Gegenstrategie zu alarmistischen Deutungen. Zugleich nutzt *Müller* Legitimationsverweise auf fachliche Expertise und institutionelle Erfahrung. Besonders zentral ist die biografische Autorisierung seiner Argumentation: Er verweist auf „25 Jahre“ Tätigkeit in der Justiz, davon „15 Jahre lang Mitglied einer Jugendstrafkammer“. Diese Selbstverortung dient der diskursiven Absicherung seiner Position gegenüber als populistisch markierten Forderungen. Metaphorisch markant ist die Abwertung des AfD-Gesetzentwurfs als „Dublette“ sowie die Gegenüberstellung von „martialischen Inhalten“ und der realen Entscheidungssituation eines Richters, der „einen 14-Jährigen [...] für zehn Jahre ins Gefängnis schickt“. Hier wird eine Kontrastmetapher zwischen abstrakter, aggressiver Politik und konkreter menschlicher Verantwortung aufgebaut. Entwicklungs- und Verantwortungszuschreibungen stehen im Zentrum der Argumentation. *Müller* betont den „Erziehungsgedanken“ des Jugendstrafrechts, die Notwendigkeit „passgenauer Sanktionen“ und die Bedeutung von „Einsichtsfähigkeit“ als Voraussetzung von Schuld. Verantwortung wird dabei nicht primär repressiv, sondern entwicklungsbezogen verstanden.

Der Redebeitrag folgt überwiegend einer präventiv-erzieherischen Storyline, die jedoch um rational-abgewogene Elemente ergänzt wird und damit stellenweise einen balancierten Charakter annimmt. Die präventiv-erzieherische Storyline zeigt sich in der Betonung des Jugendstrafrechts als erzieherisches Instrumentarium („großer Instrumentenkasten“, „passgenaue Sanktion“, „Erziehungsgedanke“) sowie in der Ablehnung einfacher strafrechtlicher Verschärfungen. Strafrechtliche Interventionen erscheinen als Mittel zur Entwicklungssteuerung, nicht als primäres Sanktions- oder Abschreckungsinstrument. Balancierende Elemente treten dort auf, wo *Müller* empirische Kriminalitätsentwicklungen anerkennt („höchster Stand seit 2011“), diese jedoch in einen breiteren gesellschaftlichen Kontext einordnet („kein auf diese Altersgruppe beschränktes Phänomen“, „multikausal“). Die Gewaltkriminalität wird weder negiert noch dramatisiert, sondern als komplexes Problem mit vielfältigen Ursachen dargestellt.

Explizit grenzt sich *Müller* von polarisierenden und punitiv-repressiven Storylines ab, indem er der AfD vorwirft, „auf komplexe Fragen [...] simple Antworten“ zu geben und sich dem Thema „populistisch“ zu nähern.

Das dominierende Narrativ des Beitrags ist das eines strukturellen Problems. Gewaltkriminalität von Kindern und Jugendlichen wird als Ausdruck gesamtgesellschaftlicher Entwicklungen beschrieben, die durch „wirtschaftliche Unsicherheit, soziale Belastungen, eigene Gewalterfahrungen und gescheiterte Integration“ bedingt sind. Dieses Narrativ widerspricht ausdrücklich einer Engführung auf individuelle Schuld oder moralisches Versagen einzelner Gruppen. Ergänzend tritt ein Erziehungsnarrativ hinzu, welches das Jugendstrafrecht als Instrument der sozialen und moralischen Entwicklung versteht. Die Tat eines Jugendlichen wird als Ausdruck eines „erzieherischen Defizits“ interpretiert, dem mit abgestuften, entwicklungsadäquaten Sanktionen zu begegnen sei. Ein Sicherheitsnarrativ ist zwar implizit präsent – etwa durch die Anerkennung steigender Gewaltzahlen –, bleibt jedoch deutlich nachgeordnet und wird nicht zur zentralen Problemdefinition erhoben. Ebenso wird das Einzelfallnarrativ nur illustrativ genutzt (z.B. der Mord durch einen 14-Jährigen), ohne daraus generalisierende Schlussfolgerungen abzuleiten.

#### d) Lena Gumnior (Bündnis 90/Die Grünen)

*Gumnior* (Bündnis 90/Die Grünen) verwendet zu Beginn ihres Beitrags alarmistische Formulierungen, um auf die steigende rechte Jugendkriminalität aufmerksam zu machen: „Die rechte Kriminalität unter Jugendlichen steigt massiv; sie radikalisiert sich, schließen sich zusammen, um schwere rechtsextreme Straftaten zu begehen.“ Diese Ausdrucksweise signalisiert Dringlichkeit und betont eine akute Bedrohung, die jedoch unmittelbar durch positive Fakten relativiert wird („Insgesamt aber geht die Jugendkriminalität zurück“), was eine balancierte Darstellung unterstützt. Emotionalisierende Elemente dominieren vor allem im Plädoyer für Prävention und Unterstützung: *Gumnior* appelliert an Mitgefühl für Jugendliche, etwa wenn sie auf Perspektivlosigkeit nach der Pandemie verweist („ohne Perspektive alleingelassen werden“) oder die Bedeutung von Anerkennung, Wertschätzung und einem liebevollen Umfeld betont. Zugleich setzt sie Entwicklungszuschreibungen ein, um die Lern- und Reifungspotenziale von Jugendlichen hervorzuheben („aus den meisten ist dann doch noch was ganz Ordentliches geworden“). Legitimationsverweise stützen ihre Argumentation auf bestehende Rechtsnormen und wissenschaftliche Evidenz, insbesondere auf das SGB VIII sowie zeithistorische Erkenntnisse zur Wirksamkeit sozialpolitischer Maßnahmen.

Der Redebeitrag folgt primär einer präventiv-erzieherischen Storyline. *Gumnior* argumentiert, dass die Reduktion von Jugendkriminalität vorrangig durch soziale Unterstützung, Perspektivangebote und psychosoziale Betreuung erreicht wird, während strafrechtliche Verschärfungen nur begrenzte Wirkung entfalten. Gleichzeitig

wird der Beitrag durch Elemente balancierter Argumentation geprägt: Die anfängliche Alarmierung über rechte Jugendkriminalität wird durch statistische Relativierung der Gesamtjugendkriminalität gemildert. Leicht polarisierende Elemente treten in der kritischen Auseinandersetzung mit der Union auf, etwa bei der Abwertung abschreckungsbasierter Strafansätze als „fahlen Atem aus den 50ern“.

Inhaltlich dominiert das strukturelle Narrativ. Kriminalität wird als Folge von Defiziten in sozialen und politischen Strukturen verstanden, insbesondere durch Einsparungen in Jugendämtern, fehlende psychosoziale Unterstützung und mangelnde Perspektiven für junge Menschen. Ergänzend tritt ein erziehungsbezogenes Narrativ auf, dass die Verantwortung der Gesellschaft und Politik für die Begleitung und Förderung Jugendlicher betont. Ein Sicherheits- oder Bedrohungsnarrativ wird lediglich zu Beginn angelegt und dient vornehmlich als rhetorischer Aufhänger. Einzelfallnarrative spielen praktisch keine Rolle; der Fokus liegt auf generellen Strukturen und sozialen Ursachen.

#### e) Mahmut Özdemir (SPD)

Im vierten Redebeitrag der Plenardebatte verwendet Özdemir (SPD) zu Beginn alarmistische, aber gezielt illustrative Formulierungen, etwa wenn er konkrete Vorfälle von „Jugendbanden, die marodierend über eine Einkaufsstraße herziehen“ beschreibt. Diese Darstellungen erzeugen ein emotionales Bild der Gefährdung, dienen jedoch vor allem der Illustration. Emotionalisierungen werden eingesetzt, um Mitgefühl für junge Menschen zu erzeugen und deren gesellschaftliche Prägung zu betonen („Kinder und Jugendliche sind Spiegelbilder ihres Umfelds“) sowie um das normative Unrecht von pauschalen Strafverschärfungen hervorzuheben („...die Jüngsten, die 14-, die 12-Jährigen, die keine Schuld tragen...“). Entwicklungs- und Verantwortungszuschreibungen adressieren sowohl politische Entscheidungsträger als auch Eltern, Schulen und Nachbarschaften als Akteure, die präventiv auf Jugendkriminalität einwirken können. Legitimationsverweise beziehen sich auf bestehende Gesetze (StGB, JGG, BGB, FamFG, SGB) sowie auf wissenschaftliche Evidenz und praxisnahe Programme wie das „Haus des Jugendrechts“, das die interinstitutionelle Prävention betont.

Die präventiv-erzieherische Storyline dominiert den Redebeitrag. Özdemir argumentiert, dass Kriminalprävention vorrangig durch soziale Unterstützung, Jugendhilfe, koordinierte Polizeiarbeit und familien- sowie gemeinschaftsbasierte Maßnahmen erreicht werden kann. Punitiv-repressive Ansätze, wie eine Senkung des Strafmündigkeitsalters, werden explizit abgelehnt. Ergänzend wird eine balancierte Argumentation verwendet, indem statistische Daten überprüft und medial dargestellte Trends relativiert werden. Polarisierende Elemente treten rhetorisch moderat auf, etwa wenn Özdemir das „Stammtischniveau“ der politischen Debatte kritisiert.

Das strukturelle Narrativ dominiert den Beitrag: Kriminalität wird als Ergebnis gesellschaftlicher, kommunaler und familiärer Rahmenbedingungen verstanden. Özdemir verdeutlicht, dass Kinder und Jugendliche stark von ihrem Umfeld geprägt sind und dass Prävention daher auf allen Ebenen – von Schule, Jugendhilfe und Polizei bis zu Eltern und Nachbarschaft – erfolgen muss. Parallel dazu ist das erziehungsbezogene Präventionsnarrativ präsent, welches die Bedeutung koordinierter, frühzeitiger Interventionen und sozialer Unterstützung betont. Sicherheits- und Einzelfallnarrative werden nur ergänzend eingesetzt, um die Relevanz der Maßnahmen zu illustrieren und die Notwendigkeit eines strukturierten, evidenzbasierten Ansatzes zu unterstreichen.

#### f) Luke Hoß (Die Linke)

Bildhafte und dramatisierende Metaphern prägen den Redebeitrag von Hoß (Linke), mit welchen er die vorgeschlagenen repressiven Maßnahmen der AfD grundlegend kritisiert. So kontrastiert er etwa „Besucherzelle statt Badegewand, U-Haft statt U-Bahn-Surfen in Subway Surfers“, um die – aus seiner Sicht – eklatante Absurdität und unverhältnismäßig große Härte des Gesetzentwurfes zu verdeutlichen. Alarmistische Bedrohungszuschreibungen, beispielsweise über den Schusswaffengebrauch gegen Kinder an deutschen Grenzen – verfolgen das Ziel der Entlarvung von Widersprüchlichkeit und Zynismus. Die Rede ist insgesamt stark emotionalisiert: moralische Appelle und Abwertungen der politischen Gegenseite („Schämen sollten Sie sich, und zwar alle!“, „primitiv; meine Güte“) erzeugen Empathie für die betroffenen Kinder und kritisieren zugleich das Vorgehen der AfD. Entwicklungs- und Verantwortungszuschreibungen adressieren Politik, Jugendhilfe und Eltern als zentrale Akteure für Prävention („Wer solche Taten wirklich verhindern will, muss [...] mit pädagogischen Angeboten Hilfe leisten“). Legitimationsverweise stützen sich auf bestehende Instrumente der Jugendhilfe und Familiengerichte sowie auf historische Bezüge zur Strafmündigkeit.

Die präventiv-erzieherische Storyline dominiert den Redebeitrag. Hoß (Linke) argumentiert, dass wirksame Prävention und Rückfallvermeidung durch pädagogische Maßnahmen, Unterstützung von Eltern und Kindern sowie die Stärkung der Jugendhilfe erreicht werden können. Punitiv-repressive Ansätze werden ausdrücklich abgelehnt und als sinnlose Demonstration von Macht dargestellt („Seien Sie doch ehrlich: Sie wollen immer nur Strafe, Strafe, Strafe“). Polarisierende Elemente sind stark ausgeprägt: Hoß richtet seine rhetorische Kritik direkt gegen die AfD, verwendet Übertreibungen, moralische Verurteilungen und emotional aufgeladene Formulierungen, um die politische Gegenseite zu delegitimieren. Eine balancierte, sachlich neutrale Argumentation ist nur marginal vorhanden.

Inhaltlich dominiert das pädagogisch-erziehungsbezogene Narrativ. Kriminalität von Kindern und Jugendlichen wird als spontan und unüberlegt dargestellt, wodurch erzieherische und pädagogische Interventionen als zielführender hervorgehoben werden als repressives Handeln.

Strukturelle Probleme werden sekundär thematisiert, etwa wenn *Hoß* darauf verweist, dass es anderen politischen Akteuren nicht um die Verbesserung der gesellschaftlichen Rahmenbedingungen geht. Sicherheits- und Einzelfallnarrative treten lediglich implizit bzw. nicht auf.

g) *Christian Moser (CDU/CSU)*

CSU-Mann *Moser* verwendet bildhafte und rhetorisch wirkungsvolle Formulierungen, um die Risiken von Schnellschüssen im Strafrecht für Kinder zu verdeutlichen. So spricht er etwa von „billigem Populismus auf dem Rücken unserer Kinder“, um die AfD-Vorschläge kritisch zu kennzeichnen. Emotionale Appelle betonen die Verantwortung der Politik und Gesellschaft gegenüber jungen Menschen („Das sind wir unseren Kindern schuldig.“). Entwicklungs- und Verantwortungszuschreibungen sind zentral: Kinder und Jugendliche werden als eigenständige Persönlichkeiten beschrieben, deren psychologische Reife berücksichtigt werden muss. Legitimationsverweise stützen sich auf das bestehende Jugendstrafrecht (§ 105 JGG), auf wissenschaftliche Studien zur psychologischen Reife von 12- bis 13-Jährigen sowie auf die praktische Belastung der Staatsanwaltschaften.

Die präventiv-erzieherische Storyline dominiert den Redebeitrag. *Moser* betont, dass (Jugend-)Strafrecht primär der positiven Beeinflussung des Täters dient, Wiederholungstaten zu verhindern und Resozialisierung zu ermöglichen. Punitiv-repressive Ansätze werden ausdrücklich kritisiert und als Schnellschüsse dargestellt. Eine balancierte Argumentation ist ebenfalls ausgeprägt: *Moser* fordert evidenzbasierte Entscheidungen und differenzierte Gesetzesdiskussionen, die wissenschaftliche Erkenntnisse berücksichtigen. Polarisierende Elemente sind nur schwach ausgeprägt und sachlich gehalten; die Kritik an der AfD bleibt argumentativ fokussiert.

Das erziehungsbezogene Narrativ ist dominant. Kriminalität von Jugendlichen wird als Ausdruck unreifer Persönlichkeiten verstanden, die gezielt durch pädagogisch fundierte Maßnahmen beeinflusst werden sollen. Strukturelle Aspekte, wie die Kapazität der Staatsanwaltschaften und gesetzliche Rahmenbedingungen, werden unterstützend thematisiert. Sicherheitsprobleme dienen lediglich als Ausgangspunkt der Debatte, während Einzelfallbetrachtungen durch die Diskussion über bedingte Strafmündigkeit und Handlungsspielräume des Jugendrichters integriert werden.

h) *Rainer Galla (AfD)*

*Galla* verwendet überwiegend sachlich-rationale Formulierungen, wobei bildhafte oder stark emotionalisierte Metaphern nur moderat auftreten. So wird etwa das Verhalten von Jugendlichen, das „die Gesellschaft nicht tolerieren

kann“, als Anlass für staatliches Eingreifen beschrieben. Emotionalisierungen finden sich hauptsächlich in Appellen an die elterliche Verantwortung („Die Erziehung von Kindern und Jugendlichen ist zuallererst Aufgabe und Sache der Eltern“). Entwicklungs- und Verantwortungszuschreibungen betonen die primäre Verantwortung der Eltern für die Erziehung von mündigen, kritischen und sozialen Persönlichkeiten, während der Staat nur ausnahmsweise und in begründeten Fällen eingreifen soll. Legitimationsverweise stützen sich auf internationale Vergleichspraktiken niedrigerer Strafmündigkeitsalter, auf die Wahrung der nationalen Werteordnung und auf die logische Argumentation im Hinblick auf Widersprüche zwischen Wahlalter und Strafmündigkeit.

Die dominante Storyline ist punitiv-repressiv: *Galla* spricht sich für eine Senkung der Strafmündigkeit von 14 auf 12 Jahre aus und betont, dass bei erkennbaren Fehlentwicklungen angemessene strafrechtliche Mittel angewandt werden müssen. Balancierende Elemente treten auf, indem betont wird, dass Eingriffe nur ausnahmsweise erfolgen und die Grundprinzipien der Werteordnung gewahrt bleiben. Präventiv-erzieherische Argumentationen spielen nur eine untergeordnete Rolle und werden vor allem über die Verantwortung der Eltern thematisiert. Polarisierende Elemente sind dezent vorhanden, etwa in ironischen Spitzen gegenüber politischen Gegnern.

Zentral ist das erziehungsbezogene Narrativ: Kinder und Jugendliche sind primär durch elterliche Erziehung zu verantwortungsvollen Persönlichkeiten zu entwickeln, staatliche Eingriffe dienen nur der Korrektur bei erkennbaren Fehlentwicklungen. Das Strafrecht wird hier als erzieherisches Instrument gedeutet. Einzelfallbetrachtungen werden implizit berücksichtigt, indem die Notwendigkeit individueller staatlicher Interventionen betont wird. Sicherheits- und strukturelle Probleme werden lediglich sekundär angesprochen; strukturelle Reformbedarfe werden nur durch den Hinweis auf eine nicht mehr zeitgemäße Systematik angedeutet.

## 2. Diskurskoalitionen

Die parlamentarische Debatte um das Strafmündigkeitsalter lässt sich im Sinne der diskurstheoretischen Arbeiten von *Hajer* nicht vornehmlich als Auseinandersetzung zwischen parteipolitischen Positionen verstehen, sondern als Konfrontation unterschiedlicher diskursiver Koalitionen.<sup>37</sup> Diese Koalitionen konstituieren sich weniger über identische politische Interessen als vielmehr über geteilte Problemdeutungen, Storylines und Narrative, die den Akteuren eine gemeinsame argumentative Grundlage bieten. Auf Basis der vorangegangenen Analyse über die diskursiven Deutungsmuster lassen sich drei zentrale Diskurskoalitionen rekonstruieren und ihnen konkrete politische Akteure zuordnen.

<sup>37</sup> *Hajer*, in: Keller/Hiersland/Schneider/Viehöver (Hrsg.), Handbuch Sozialwissenschaftliche Diskursanalyse, 2004, S. 271–298; *ders.*, in: Janning/Toens (Hrsg.), Die Zukunft der Policy-Forschung, 2008, S. 211–222.

Die erste Diskurskoalition ist durch eine punitiv-repressive Sicherheitslogik geprägt und wird maßgeblich von Akteuren der AfD getragen, insbesondere durch den eingebrachten Gesetzesentwurf sowie die Redebeiträge von *Tobias Matthias Peterka* und *Rainer Galla*. Gemeinsamer Kern dieser Koalition ist eine sicherheitszentrierte Problemkonstruktion, in der Kinder- und Jugendkriminalität als eskalierende Bedrohung der öffentlichen Ordnung und des gesellschaftlichen Zusammenhalts dargestellt wird. Diese Kriminalitätsform erscheint hier nicht als punktuelles oder strukturell erklärbares Phänomen, sondern als Ausdruck eines umfassenderen Kontrollverlustes des Staates. Die Absenkung des Strafmündigkeitsalters wird in dieser Perspektive als notwendige Reaktion auf eine als dramatisch beschriebene Entwicklung gerahmt. Zentral ist dabei eine punitiv-repressive Storyline, in der strafrechtliche Verschärfungen als einzig wirksames Mittel zur Wiederherstellung von Sicherheit und Ordnung präsentiert werden. Strafrecht fungiert nicht nur als Sanktions-, sondern zugleich als Erziehungs- und Abschreckungsinstrument. Zwar werden entwicklungspsychologische Argumente punktuell anerkannt, sie werden jedoch konsequent relativiert, indem bereits bei Kindern im Alter von zwölf Jahren eine hinreichende Einsichtsfähigkeit unterstellt wird. Ergänzt wird diese Argumentation durch ein Erziehungsnarrativ, das elterliches Versagen und defizitäre Wertevermittlung als zentrale Ursachen von Jugendkriminalität identifiziert. Dieses Narrativ legitimiert staatliches Eingreifen, indem es familiäre Verantwortung problematisiert und zugleich soziale oder strukturelle Erklärungen delegitimiert. Trotz unterschiedlicher rhetorischer Stile – von stark emotionalisierend bei *Peterka* bis vergleichsweise moderat bei *Galla* – stabilisieren diese Akteure gemeinsam einen diskursiven Rahmen, in dem Sicherheit und Strafverschärfung untrennbar miteinander verknüpft sind.

Der punitiv-repressiven Sicherheitskoalition steht eine präventiv-erzieherische Strukturkoalition gegenüber, der Redebeiträge von Bündnis 90/Die Grünen, der SPD und der Linken zuzuordnen sind. Trotz parteipolitischer Unterschiede verbindet diese Akteure eine grundlegende Problemdefinition, in der Jugendkriminalität primär als Ergebnis sozialer, institutioneller und biografischer Rahmenbedingungen verstanden wird. Kinder- und Jugendkriminalität erscheinen hier nicht als Ausdruck individueller moralischer Defizite, sondern als Symptom struktureller Belastungen, etwa durch soziale Ungleichheit, fehlende Perspektiven oder unzureichende staatliche Unterstützungsangebote. Die dominante Storyline dieser Koalition ist somit präventiv-erzieherisch. Kriminalitätsbekämpfung wird vorrangig als Aufgabe sozialer Prävention, früher pädagogischer Intervention und institutioneller Unterstützung interpretiert. Strafrechtliche Maßnahmen gelten allenfalls als nachgeordnetes Mittel und werden explizit als ungeeignet dargestellt, um nachhaltige Verhaltensänderungen bei Kindern und Jugendlichen zu bewirken. Entsprechend dominieren strukturelle Narrative, in denen politische Verantwortung, Jugendhilfe, Schulen und kommunale Strukturen als zentrale Handlungsebenen identifiziert werden. Ergänzend tritt ein Ent-

wicklungsnarrativ hinzu, welches die Lern- und Reifungsfähigkeit junger Menschen betont und pauschale Zuschreibungen von Schuld zurückweist. Unterschiede innerhalb dieser Koalition zeigen sich vor allem im Stil der Auseinandersetzung: Während etwa *Luke Hoß* (Linke) stark moralisch und polarisierend argumentiert, verfolgen *Mahmut Özdemir* (SPD) und *Lena Gumnior* (Bündnis 90/Die Grünen) eine moderatere, stärker institutionell und sozialpolitisch ausgerichtete Argumentation. Gleichwohl stabilisieren auch diese Akteure einen gemeinsamen diskursiven Deutungsrahmen, der präventive und erzieherische Ansätze ins Zentrum stellt.

Zwischen diesen beiden Polen lässt sich eine dritte Diskurskoalition verorten, die als balanciert-rationalisierend beschrieben werden kann und insbesondere durch Redebeiträge von *Axel Müller* (CDU) und *Christian Moser* (CSU) getragen wird. Diese Koalition zeichnet sich dadurch aus, dass sie sicherheitsbezogene Problemlagen grundsätzlich anerkennt, alarmistische Eskalationen jedoch ausdrücklich zurückweist. Jugendkriminalität wird als reales, aber komplexes Phänomen beschrieben, das differenzierte und evidenzbasierte Antworten erfordert. Die zentrale Storyline dieses Diskursstranges ist von Rationalisierung und Abwägung geprägt. Das bestehende Jugendstrafrecht wird als leistungsfähiges und differenziertes Instrument verteidigt, das bereits heute hinreichende Handlungsspielräume bietet. Strafrechtliche Interventionen werden nicht grundsätzlich abgelehnt, jedoch klar in einen entwicklungsbezogenen und professionellen Rahmen eingebettet. Charakteristisch ist dabei die Berufung auf fachliche Expertise, institutionelle Erfahrung und wissenschaftliche Erkenntnisse, die als Gegenpol zu populistischen Vereinfachungen fungieren. Diese Akteure teilen zwar zentrale Annahmen der präventiv-erzieherischen Koalition, grenzen sich jedoch von deren teilweise normativ zugespitzter Argumentation ab und nehmen eine vermittelnde Position zwischen punitiven Sicherheitserwartungen und pädagogischen Sozialisationslogiken ein.

## V. Diskussion und Schlussbetrachtung

Ziel des vorliegenden Beitrags war es, die parlamentarische Debatte um das Strafmündigkeitsalter im Deutschen Bundestag im Juni 2025 diskursanalytisch zu untersuchen und die darin wirksamen Deutungsmuster sowie Diskurskoalitionen herauszuarbeiten. Ausgehend von der übergeordneten Fragestellung, wie Jugend- und Kinderkriminalität politisch problematisiert und welche kriminalpolitischen Handlungsoptionen dadurch plausibilisiert werden, leistet die Analyse einen eigenständigen Beitrag zur politikwissenschaftlichen Kommunikations- und Diskursforschung. Der Mehrwert der Arbeit liegt insbesondere darin die bestehenden Forschungsperspektiven um eine explizit diskursive Sichtweise zu ergänzen und aufzuzeigen, wie politische Akteure kriminalpolitische Positionen sprachlich legitimieren, emotionalisieren oder rationalisieren.

Die Ergebnisse der Analyse zeigen, dass die parlamentarische Auseinandersetzung weniger entlang klassischer

parteipolitischer Trennlinien verläuft als entlang konkurrierender diskursiver Problemdefinitionen. Im Zentrum stehen drei Diskurskoalitionen, die sich durch jeweils spezifische diskursive Deutungsmuster mit eigenen Storylines und Narrativen konstituieren: eine punitiv-repressive Sicherheitskoalition, eine präventiv-erzieherische Strukturkoalition sowie eine balanciert-rationalisierende Vermittlungskoalition. Diese Koalitionen strukturieren nicht nur die politische Debatte, sondern begrenzen zugleich den Raum dessen, was als legitime kriminalpolitische Antwort auf Jugendkriminalität gilt.

Vor dem Hintergrund der Forschungsfragen lässt sich festhalten, dass insbesondere die punitiv-repressive Koalition Jugendkriminalität als eskalierendes Sicherheitsproblem konstruiert, das entschlossenes staatliches Eingreifen erfordert. Diese Problemdefinition steht in einem Spannungsverhältnis zum bestehenden Forschungsstand, insbesondere zur kriminologischen und entwicklungspsychologischen Literatur.<sup>38</sup> Während im politischen Diskurs der AfD Kriminalstatistiken, Einzelfälle extremer Gewalt und internationale Vergleiche als objektivierende Belege herangezogen werden, weist die kriminologische Forschung seit Langem darauf hin, dass frühe formelle Sanktionierung mit erheblichen Risiken verbunden ist. Studien zu Delinquenzverläufen und Labeling-Effekten zeigen,<sup>39</sup> dass strafrechtliche Interventionen im Kindes- und Jugendalter eher zu Stigmatisierung und erhöhtem Rückfallrisiko beitragen können, anstatt präventive Effekte zu entfalten.<sup>40</sup> Die diskursive Reduktion komplexer Entwicklungs- und Sozialisationserfahrungen auf individuelle Schuldzuschreibungen steht damit in deutlichem Kontrast zu empirisch fundierten Erkenntnissen der Kriminologie.<sup>41</sup> Auch die entwicklungs- und rechtspsychologische Forschung widerspricht der impliziten Annahme, strafrechtliche Verantwortungsfähigkeit lasse sich eindeutig an einem fixen Lebensalter festmachen.<sup>42</sup> Die im Forschungsstand referenzierten Befunde zu neurokognitiven und psychosozialen Reifungsprozessen betonen die Heterogenität individueller Entwicklung und problematisieren starre Altersgrenzen als alleinige Kriterien für Verantwortlichkeit.<sup>43</sup> Vor diesem Hintergrund erscheint es diskursiv aufschlussreich, dass entwicklungspsychologische Argumente im punitiven Diskurs zwar aufgegriffen, jedoch funktionalisiert werden: Sie dienen weniger der ernsthaften Abwägung von Reifefähigkeit als vielmehr der Legitimation repressiver Maßnahmen.

Demgegenüber knüpft die präventiv-erzieherische Strukturkoalition deutlich stärker an die im Forschungsstand beschriebenen kriminologischen und sozialwissenschaftlichen Befunde an.<sup>44</sup> Die Betonung sozialer Ursachen, struktureller Belastungen und präventiver Interventionen korrespondiert mit empirischen Erkenntnissen, wonach Jugendkriminalität eng mit sozialen Ungleichheiten, biografischen Krisen und institutionellen Defiziten verknüpft ist.<sup>45</sup> Allerdings zeigt die Analyse zugleich, dass diese Koalition im parlamentarischen Kontext häufig in eine normative Abwehrhaltung gegenüber sicherheitspolitischen Argumenten gerät. Die starke Moralisierung einzelner Beiträge birgt die Gefahr, den diskursiven Konflikt zu polarisieren und damit die Anschlussfähigkeit präventiver Argumente für sicherheitsorientierte Akteursgruppen zu verringern.

Eine besondere Rolle kommt der balanciert-rationalisierenden Vermittlungskoalition zu, die sich insbesondere in den Beiträgen der CDU/CSU-Abgeordneten zeigt. Diese Koalition erkennt sowohl sicherheitsbezogene Problemlagen als auch entwicklungspsychologische und kriminologische Erkenntnisse an und positioniert sich damit näher an der Mehrdimensionalität des Forschungsstandes.<sup>46</sup> Die Verteidigung des bestehenden Jugendstrafrechts als differenziertes Instrumentarium verweist auf eine kriminalpolitische Logik, die weder reine Abschreckung noch reine Sozialpolitik verfolgt, sondern auf professionelle Abwägung und evidenzbasierte Praxis setzt. In diesem Sinne fungiert diese Koalition diskursiv als Stabilisierung des Status quo.

In der Gesamtschau lässt sich die übergeordnete Fragestellung dahingehend beantworten, dass die politische Debatte um das Strafmündigkeitsalter maßgeblich durch diskursive Konstruktionen von Sicherheit, Verantwortung und Entwicklung geprägt ist, die jeweils unterschiedliche kriminalpolitische Lösungsoptionen plausibilisieren. Die Analyse zeigt, dass politische Forderungen nach einer Absenkung der Strafmündigkeit weniger aus empirischer Evidenz resultieren als aus spezifischen sicherheitspolitischen Narrativen, die auf Emotionalisierung, Einzelfallgeneralisierung und symbolische Politik setzen.

Aus den Ergebnissen ergeben sich mehrere Implikationen. Gesellschaftlich und politisch verdeutlicht die Analyse die Bedeutung diskursiver Rahmungen für kriminalpolitische Entscheidungsprozesse. Für die wissenschaftliche Debatte unterstreicht sie den Mehrwert diskursanalytischer

<sup>38</sup> Bannenberg, APuZ 2025, 32-39; Baur/Rueß/Schaffeld/Fegert, KriPoZ 2024, 245-250.

<sup>39</sup> Cohen, American Sociological Review 1983, 48 (5), 728, DOI: 10.2307/2094931; Moffitt, Psychological Review 1993, 100 (4), 674-701, DOI: 10.1037/0033-295X.100.4.674.

<sup>40</sup> Bernburg/Krohn/Rivera, Journal of Research in Crime and Delinquency 2006, 43 (1), 67-88, DOI: 10.1177/0022427805280068.

<sup>41</sup> Bannenberg, APuZ 2025, 32-39; Cohen, American Sociological Review 1983, 48 (5), 728, DOI: 10.2307/2094931; Moffitt, Psychological Review 1993, 100 (4), 674-701, DOI: 10.1037/0033-295X.100.4.674.

<sup>42</sup> Pillay, Journal of child and adolescent mental health 2019, 31 (3), 224-234, DOI: 10.2989/17280583.2019.1692851.

<sup>43</sup> Horten/Steffan/Weinand, Forens Psychiatr Psychol Kriminol 2023, 17 (4), 460-462.

<sup>44</sup> Baur/Rueß/Schaffeld/Fegert, KriPoZ 2024, 245-250; Cavadino/Dignan, Criminology & Criminal Justice 2006, 6 (4), 435-456, DOI: 10.1177/1748895806068581; Junger-Tas/Gruszczynska/Stekete/Killias/Enzmann/Haen Marshall (Hrsg.), Juvenile Delinquency in Europe and Beyond: Results of the Second International Self-Report Delinquency Study, 2010.

<sup>45</sup> Icenogle/Steinberg/Duell/Chein/Chang/Chaudhary et al., Law and human behavior 2019, 43 (1), 69-85, DOI: 10.1037/lhb0000315; Steinberg, Developmental review 2008, 28 (1), 78-106, DOI: 10.1016/j.dr.2007.08.002.

<sup>46</sup> Bannenberg, APuZ 2025, 32-39; Baur/Rueß/Schaffeld/Fegert, KriPoZ 2024, 245-250; Heilinger, Die Altersgrenze der Strafmündigkeit; Schmöe, Die Rolle des Alters im Jugendstrafrecht.

Zugänge, die normative und empirische Argumente nicht isoliert betrachten, sondern deren politische Übersetzung analysieren. Für die polizeiliche und kriminalpolitische Praxis legt die Arbeit nahe, sicherheitsorientierte Forderungen stärker mit empirischen Erkenntnissen zu konfrontieren und präventive Ansätze diskursiv besser anschlussfähig zu gestalten.

Gleichzeitig weist die Arbeit klare Limitationen auf. Die Analyse beschränkt sich auf eine einzelne Bundestagsdebatte und erhebt keinen Anspruch auf Generalisierbarkeit für den gesamten politischen oder gar gesellschaftlichen Diskurs. Zudem basiert sie auf parlamentarischen Redebeiträgen, die durch strategische Kommunikation und parteipolitische Logiken geprägt sind. Weitere Forschung

könnte diese Perspektive erweitern, indem mediale Diskurse, polizeiliche Fachdebatten oder öffentliche Stellungnahmen von zivilgesellschaftlichen Akteuren und berufsfachlichen Verbänden einbezogen werden.

Abschließend lässt sich festhalten, dass die politische Debatte um das Strafmündigkeitsalter exemplarisch zeigt, wie kriminalpolitische Fragen zu symbolisch aufgeladenen Aushandlungsarenen werden, in denen wissenschaftliche Evidenz, politische Interessen und moralische Deutungen miteinander konkurrieren.<sup>47</sup> Der vorliegende Artikel leistet einen reflektierten Beitrag zu diesem Diskurs, indem er die diskursiven Mechanismen sichtbar macht, die kriminalpolitische Entscheidungen vorbereiten, legitimieren oder verhindern.

<sup>47</sup> *Schupelius*, Mehr Kinder werden Täter, aber sie werden nicht bestraft, BILD v. 6.9.2025, online abrufbar unter: <https://bit.ly/4cEcolm> (zuletzt abgerufen am 2.2.2026); Gewalt unter Kindern – Strobl stellt Straf-Alter infrage, Stuttgarter Zeitung v. 17.2.2026, online abrufbar unter: <https://bit.ly/4s1X5Yj> (zuletzt abgerufen am 20.2.2026); *Magoley*, Tod von Yosef in Dormagen: Müssen Kinder früher strafmündig werden?, wdr.de v. 6.2.2026, online abrufbar unter: <https://bit.ly/3OY7Ex8> (zuletzt abgerufen am 12.2.2026).

## „Mittelbare Täterschaft“ durch kompromittierte Systeme Grenzen personenbezogener Zurechnung im digitalen Raum

von RA Dr. Dr. Fabian Teichmann, LL.M.  
(London), EMBA (Oxford)\*

### Abstract

Digitale Angriffe werden häufig nicht durch einen menschlichen Tatmittler, sondern über kompromittierte Endgeräte, Botnetze und automatisierte Skripte ausgeführt. Dogmatisch liegt deshalb nahe, die Figur der mittelbaren Täterschaft gemäß § 25 Abs. 1 Alt. 2 StGB als Zurechnungsinstrument zu bemühen: Der Hintermann handelt „durch“ infizierte Systeme, ohne selbst am Zielsystem präsent zu sein. Der Beitrag zeigt jedoch, dass eine solche Ausweitung die personenbezogene Struktur der mittelbaren Täterschaft verfehlt. § 25 Abs. 1 Alt. 2 StGB setzt einen Tatmittler als Person voraus. Nicht-personale Durchführungsmittel sind, dogmatisch präzise, Werkzeuge der unmittelbaren Täterschaft. Im digitalen Raum ist daher zwischen Werkzeuggebrauch (unmittelbare Täterschaft), objektiver Zurechnung automatisierter Erfolgsverläufe und echten Konstellationen mittelbarer Täterschaft über menschliche Intermediäre (etwa bei Social Engineering, Irrtums- oder Zwangslagen) zu differenzieren. Nur wo organisationsbezogene Rahmenbedingungen regelhaft, vom Hintermann beherrschte Abläufe auslösen, kann – jenseits klassischer Defektlagen – ein Rückgriff auf Organisationsherrschaft in Betracht kommen. Die vorgeschlagenen Kriterien werden anhand der Delikte der Datenveränderung gemäß § 303a StGB<sup>1</sup> und Computersabotage gemäß § 303b StGB<sup>2</sup> sowie typischer Botnet<sup>3</sup>- und Ransomware-Abläufe<sup>4</sup> dargestellt. Kriminalpolitisch folgt daraus, dass einer Ausweitung des § 25 Abs. 1 Alt. 2 StGB auf technische Durchführungsmittel nicht nur dogmatische, sondern auch rechtsstaatliche Bedenken entgegenstehen: Eine solche Ausdehnung würde das Bestimmtheitsgebot (Art. 103 Abs. 2 GG) strapazieren und die ordnende Funktion des Beteiligungssystems schwächen. Zugleich zeigt die Untersuchung, dass der Gesetzgeber mit den bestehenden Instrumenten - unmittelbare Täterschaft, Vorbereitungstatbestände und objektive Zurechnung - über ein hinreichendes und ausdifferenziertes Regelungsarsenal verfügt, das einer unkontrollierten Vorverlagerung der Täterstrafbarkeit nicht bedarf.

Digital attacks are frequently carried out not by a human intermediary but through compromised end devices, botnets, and automated scripts. From a doctrinal perspective, this raises the question of whether the concept of indirect perpetration (mittelbare Täterschaft) under § 25(1) alternative 2 of the German Criminal Code (StGB) can serve as a basis for attribution: the principal acts "through" infected systems without being physically present at the target. This article demonstrates, however, that such an extension would misconceive the person-based structure of indirect perpetration. Section 25(1) alternative 2 presupposes an intermediary who is a person. Non-personal means of execution are, in doctrinally precise terms, tools of direct perpetration (unmittelbare Täterschaft). In the digital context, it is therefore necessary to distinguish between the use of tools (direct perpetration under § 25(1) alternative 1), the objective attribution (objektive Zurechnung) of automated causal processes, and genuine instances of indirect perpetration through human intermediaries, in particular in cases of social engineering, mistake, or coercion. Only where organisational frameworks produce regular, principal-controlled sequences of conduct can organisational control (Organisationsherrschaft) - itself a contested doctrine - be considered, and even then only with respect to human organisational structures, not technical systems. The proposed criteria are illustrated by reference to the offences of data manipulation (§ 303a StGB), computer sabotage (§ 303b StGB), and typical botnet and ransomware attack scenarios. From a criminal policy perspective, the analysis demonstrates that an extension of § 25(1) alternative 2 to technical means of execution would not only strain the principle of legal certainty (Bestimmtheitsgebot, Article 103(2) of the Basic Law) but would also undermine the ordering function of the participation system. The legislature has already provided targeted instruments for the anticipatory criminalisation of preparatory conduct in the digital sphere (§§ 202c, 303a(3), 303b(5) StGB). There is accordingly no criminal policy need to expand the concept of perpetration; the existing doctrinal framework - direct

\* RA Dr. Dr. Fabian Teichmann, LL.M. (London), EMBA (Oxford) ist Lehrbeauftragter an der Universität zu Köln, der Universität Kassel und der Universität Trier sowie Managing Partner der Teichmann International (Schweiz) AG.

<sup>1</sup> Hecker, in: TK-StGB, 31. Aufl. (2025), § 303a Rn. 4–8; Bär, in: Handbuch des Wirtschaftsstrafrechts, 6. Aufl. (2025), 15. Kap. Rn. 114–118; Altenhain, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 303a Rn. 6–10; Wengenroth, in: Handbuch der Datenschutzsanktionen, 2023, § 21 Rn. 17.

<sup>2</sup> Mahn, in: Wirtschaftsstrafrecht, 3. Aufl. (2023), Kap. 11 Rn. 196, 197; Hecker, in: TK-StGB, 31. Aufl. (2025), § 303b Rn. 5–8; Wieck-Noodt, in: MüKo-StGB, 4. Aufl. (2022), § 303b Rn. 10; Mansdörfer, in: BeckOK IT-Recht, 20. Ed. (1.7.2025), § 303b Rn. 10–21.

<sup>3</sup> BSI, Botnetze, Auswirkungen und Schutzmaßnahmen, abrufbar unter: <http://bit.ly/4bmLdKE> (zuletzt abgerufen am 29.1.2026); Schmidt/Pruß, in: Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, 3. Aufl. (2019), § 3 Rn. 270; Maihold, in: Bankrechts-Handbuch, 6. Aufl. (2022), § 33 Rn. 64, 6; Graf, in: MüKo-StGB, 5. Aufl. (2025), § 202a Rn. 8.

<sup>4</sup> Polizeiliche Kriminalprävention, Ransomware ist Tor zur digitalen Erpressung, abrufbar unter: <https://bit.ly/4r7wRC0> (zuletzt abgerufen am 29.1.2026); BSI, Ransomware – Fakten und Abwehrstrategien, abrufbar unter: <https://bit.ly/3P0i7YN> (zuletzt abgerufen am 29.1.2026); Spiecker gen. Döhm/Bretthauer, Dokumentation zum Datenschutz, 2025, Rn. 16; Sohr/Kemmerich, in: Kipker, Cybersecurity-Handbuch, 2. Aufl. (2023), Kap. 3 Rn. 177.

*perpetration through the use of tools, objective attribution, and delict-specific preparatory offences - is sufficient to capture digital attack scenarios comprehensively and with the precision that the rule of law demands.*

## I. Problemstellung und Gang der Untersuchung

Angriffe auf informationstechnische Systeme sind heute regelmäßig arbeitsteilig, skalierbar und technisch vermittelt organisiert. Typische Modelle – Botnet-Betrieb, Ransomware-as-a-Service, DDoS-Erpressung – zeichnen sich dadurch aus, dass der eigentliche Eingriff am Zielsystem nicht als körperliche Handlung des Angreifers erscheint, sondern als Systemreaktion: Pakete werden automatisiert versandt, Befehle als „Command-and-Control“-Nachrichten verteilt, Skripte ohne weitere menschliche Zwischenschritte ausgeführt. Der Angreifer ist räumlich abwesend; die Ausführung „passiert“ an vielen Orten zugleich.<sup>5</sup>

Diese Struktur verschiebt den dogmatischen Fokus. Während im klassischen Deliktssbild das Tatgeschehen an eine menschliche Ausführungshandlung am Tatort anknüpft, treten im digitalen Raum Fernsteuerung, Automatisierung und Delegation an technische Mittel in den Vordergrund. Für die Zurechnung stellt sich daher wiederkehrend die Frage, ob das Strafrecht eine personelle Vermittlung voraussetzt oder ob technische Durchführungsmittel als „Tatmittler“ im Sinne der Beteiligungsdogmatik verstanden werden können.

Das Problem konzentriert sich auf § 25 Abs. 1 Alt. 2 StGB. Mittelbare Täterschaft ist das klassische Instrument, um Tatbegehung „über Dritte“ zu erfassen.<sup>6</sup> Der Hintermann beherrscht den Tatablauf, weil er einen anderen als Werkzeug einsetzt.<sup>7</sup> Im digitalen Raum scheint diese Figur auf den ersten Blick anschlussfähig: Der Täter bedient sich kompromittierter Systeme<sup>8</sup> und lässt sie „für sich“ handeln. Zugleich fehlt in den typischen Fällen jeder menschliche Tatmittler als Defizitträger. § 25 Abs. 1 Alt. 2 StGB beschreibt aber „durch einen anderen begehrt“, womit ein Mensch gemeint ist, auch wenn dieser als Werkzeug verwendet wird.<sup>9</sup> Die Systeme sind aber keine Personen; sie können weder irren noch vorsätzlich handeln. Die Leitfrage lautet deshalb: Kann (und soll) § 25 Abs. 1 Alt. 2 StGB dort tragen, wo der Täter über Botnetze oder autonome Skripte agiert, obwohl kein menschlicher Tatmittler vorliegt?

Die Antwort ist nicht bloß terminologisch. Eine, auch nur stillschweigende, „Digitalisierung“ der mittelbaren Täterschaft hätte Folgewirkungen für die Abgrenzung zu unmittelbarer Täterschaft, Versuch und Rücktritt sowie für die Anschlussfähigkeit organisationsbezogener Herrschaftsmodelle. Zugleich würde sie die dogmatische Begrenzungsfunktion des Beteiligungssystems schwächen. Wo technische Wichtigkeit genügt, droht eine Zurechnungsentgrenzung, die das Tatbestandsprinzip und die Differenzierung zwischen Täterschaft und Teilnahme verwässert.

Der Beitrag folgt daher einem dreistufigen Programm, bei dem zunächst Struktur und Begrenzungsfunktion der mittelbaren Täterschaft als personenbezogene Zurechnungsfigur herausgearbeitet werden (II). Sodann wird geprüft, ob und mit welchen Argumenten Botnetze und Skripte als „Tatmittler“ verstanden werden könnten – und warum dies dogmatisch nicht trägt (III). Abschließend werden Alternativmodelle entwickelt, die digitale Angriffe ohne dogmatische Verwerfungen erfassen: unmittelbare Täterschaft durch Werkzeuggebrauch, objektive Zurechnung automatisierter Verläufe sowie – in engen Grenzen – Organisationsherrschaft und echte mittelbare Täterschaft über menschliche Intermediäre (IV/V).

Die Fragestellung hat dabei nicht nur dogmatische, sondern auch kriminalpolitische Tragweite. Der zunehmende Verfolgungsdruck im Bereich der Cyberkriminalität begünstigt die Versuchung, über expansive Zurechnungskonstruktionen – etwa die Gleichsetzung technischer Systeme mit Tatmittlern – Beweisschwierigkeiten dogmatisch zu kompensieren. Demgegenüber steht das rechtsstaatliche Gebot, die Grenzen des Beteiligungssystems nicht aus kriminalpolitischer Opportunität zu verschieben. Die nachfolgende Untersuchung versteht sich daher auch als Beitrag zur kriminalpolitischen Debatte um die Reichweite und Begrenzung strafrechtlicher Zurechnungsfiguren im digitalen Raum.

## II. Personenbezogenheit der mittelbaren Täterschaft: Funktion, Struktur und Tatmittlerdefizit

### 1. Ausgangspunkt ist der Gesetzestext

§ 25 StGB unterscheidet drei Grundformen der Täterschaft: unmittelbare Täterschaft („wer die Tat selbst

<sup>5</sup> IDW, Cyberrisk, Ziff. 2, abrufbar unter: <https://bit.ly/4r9RM7Y> (zuletzt abgerufen am 29.1.2026); LDI, Hilfe, ein Cyberangriff, abrufbar unter: <https://www.ldi.nrw.de/cyberangriff> (zuletzt abgerufen am 29.1.2026); Lapp in: Kipker Cybersecurity-HdB, 2. Aufl. (2023), Kap. 10 Rn. 140, 141; Marly/Hessel, Softwarerecht, 8. Aufl. (2024), § 14 Rn. 6–8; Schildbach/Groothuis, DSRI Herbstakademie 2025, 2025; Teichmann, Polizei 2025, 401; Teichmann, NZI 2025, 809.

<sup>6</sup> Haas, in: Matt/Renzikowski, StGB, § 25 Rn. 5–7; Pohlreich, in: Lackner/Kühl/Heger, StGB, 31. Aufl. (2025), § 25 Rn. 2; Weißer, in: TK-StGB, 31. Aufl. (2025), § 25 Rn. 3, 4; Kindhäuser/Hilgen-dorf, LPK-StGB, 10. Aufl. (2025), § 25 Rn. 7–8; Kudlich, in: BeckOK-StGB, 67. Ed. (1.11.2025), § 25 Rn. 19; Scheinfeld, in: MüKo-StGB, 5. Aufl. (2024), § 25 Rn. 60–62.

<sup>7</sup> Ingelfinger, in: Dölling/Duttge/Rössner, StGB, 5. Aufl. (2022), § 25 Rn. 17–20; Schild/Kretschmer, in: NK-StGB, 6. Aufl. (2023), § 25 Rn. 26–28; Scheinfeld, in: MüKo-StGB, § 25 Rn. 61–64; Rüben-stahl, in: Böttger, Wirtschaftsstrafrecht, 3. Aufl. (2023), Kap. 18 Rn. 31–35.

<sup>8</sup> IT-Business, Definition: Was ist kompromittieren, abrufbar unter: <https://bit.ly/3OXEP3K> (zuletzt abgerufen am 29.1.2026); BSI, Prävention und Erste Hilfe bei Webseiten Kompromittierung oder Defacement, Ziff. 2, abrufbar unter: <https://bit.ly/3Ni3nnF> (zuletzt abgerufen am 29.1.2026).

<sup>9</sup> Schild/Kretschmer, in: NK-StGB, § 25 Rn. 73–79; Weißer, in: TK-StGB, § 25 Rn. 5; Kudlich, in: BeckOK-StGB, § 25 Rn. 20.

begeht“, Abs. 1 Alt. 1)<sup>10</sup>, mittelbare Täterschaft („wer die Tat ... durch einen anderen begeht“, Abs. 1 Alt. 2)<sup>11</sup> und Mittäterschaft (Abs. 2)<sup>12</sup>. Der Wortlaut „durch einen anderen“ ist dabei nicht austauschbar. Er meint nach verbreiteter Auffassung einen „anderen“ als Person: „Begehen ‚durch einen anderen‘ bedeutet eines Menschen, also dem Ausführungstäter.“<sup>13</sup>

Damit ist die mittelbare Täterschaft begrifflich als personale Vermittlung konstruiert. Das ist dogmatisch plausibel, weil § 25 Abs. 1 Alt. 2 StGB nicht (nur) eine Kausalitätsfigur ist, sondern eine Verantwortungsfigur. Der Hintermann wird Täter, obwohl er die tatbestandliche Handlung nicht selbst ausführt, weil ihm die Ausführungshandlung des Tatmittlers zugerechnet wird.<sup>14</sup> Zurechnungsgrund ist die Herrschaft über einen defizitären oder strukturell unterlegenen Mittler. Der Hintermann „steht“ im Zentrum, weil er die entscheidende Disposition über das Ob und Wie der Tatbestandsverwirklichung innehat – und zwar mittels einer anderen Person.

## 2. Das Tatmittlerdefizit ist der Kern

Klassische Fallgruppen beruhen darauf, dass der Mittler entweder (i) ohne Vorsatz handelt (Irrtum), (ii) schuldunfähig oder entschuldigt ist, (iii) unter Zwang steht oder (iv) aufgrund normativer Defizite nicht als Täter erfasst wird wie z.B. fehlende Sonderpflichten oder Absichten. In all diesen Konstellationen ist entscheidend, dass der Mittler als Person handelt und sein Handeln (oder Unterlassen) tatbestandsrelevant ist.<sup>15</sup>

## 3. Historische und systematische Einbettung

Die Personenbezogenheit ist auch vor dem Hintergrund der Täterschaftstheorien zu verstehen. Das Gesetz spricht nicht von Tatherrschaft, sondern formuliert die Täterschaftsformen offen. Die dogmatische Debatte über formal-objektive Theorie, subjektive Theorie, Tatherrschaftslehre und Einheitstäterschaft ist dadurch nicht obsolet, sondern in die Aufgabe übersetzt, die in § 25 StGB angelegten Formen mit trennscharfen Kriterien zu füllen. Die Vorbemerkungen zu § 25 StGB zeichnen nach, dass das Kriterium der Tatherrschaft in der Lehre dominiert und in der Rechtsprechung jedenfalls als Indiz im Rahmen

einer Gesamtwürdigung anerkannt ist, während zugleich betont wird, dass im Gesetz von Tatherrschaft nicht die Rede ist und „Zentralgestalt“ ohne Konkretisierung inhaltsleer bleibt.<sup>16</sup> Diese Einbettung ist für digitale Konstellationen bedeutsam, weil sie zeigt, dass „Herrschaft“ nicht mit „Techniknähe“ gleichgesetzt werden darf. Die Gefahr einer dogmatischen Abkürzung ist im Digitalen besonders hoch, denn wer die Infrastruktur kontrolliert, wirkt faktisch zentral; daraus folgt aber nicht automatisch, dass die Tat „durch einen anderen“ begangen wird. Die Formenlehre verlangt eine normative Zurechnungsentscheidung, die an den gesetzlichen Formen festhält.

## 4. Begrenzungsfunktion

Die Personenbezogenheit verhindert, dass § 25 Abs. 1 Alt. 2 StGB zur bloßen Formel für Fernwirkung oder technisches „Outsourcing“ wird. Wäre jede mittelbare Erfolgsherbeiführung zugleich „Begehen durch einen anderen“, verlöre die Abgrenzung zu § 25 Abs. 1 Alt. 1 StGB ihre Konturen; Alt. 2 würde die Werkzeugkategorie absorbieren. Die Beteiligungsformenlehre würde damit ihre ordnende und begrenzende Funktion einbüßen.

## 5. Der digitale Kontext als Stresstest

Technische Beiträge sind oft hochwirksam, ohne dass daraus eine personale Herrschaftsrelation folgt. Ein Bot „führt“ Befehle aus, aber er „entscheidet“ nicht;<sup>17</sup> er unterliegt keinem Irrtum und keinem Zwang; er ist kein Normadressat. Die Zurechnungsfrage ist daher nicht, ob ein Defekt vorliegt, sondern ob der Täter einen tatbestandspezifischen Gefahrenverlauf in Gang gesetzt hat, der sich im Erfolg realisiert.

## 6. Der Grenzfall

„Tatmittler gegen sich selbst“. Wenn ein Täter eine Falle stellt und das Opfer durch eigenes Verhalten, etwa das Öffnen einer präparierten Sendung, den Erfolg auslöst, wird das Opfer bisweilen als Tatmittler verstanden.<sup>18</sup> Der Streit dreht sich dann um Versuchsbeginn und die Frage, wann der Täter „angesetzt“ hat.<sup>19</sup> Der Tatmittler bleibt aber eine Person; die Diskussion setzt ein voluntatives

<sup>10</sup> Weißer, in: TK-StGB, § 25 Rn. 2; Haas, in: Matt/Renzikowski, StGB, § 25 Rn. 2-4; Kudlich, in: BeckOK-StGB, § 25 Rn. 18, 18.1; Pohlreich, in: Lackner/Kühl/Heger, StGB, § 25 Rn. 1-1a; Scheinfeld, in: MüKo-StGB, § 25 Rn. 39-40.

<sup>11</sup> Haas, in: Matt/Renzikowski, StGB, § 25 Rn. 5-7; Scheinfeld, in: MüKo-StGB, § 25 Rn. 61-64; Weißer, in: TK-StGB, § 25 Rn. 3, 4; Kudlich, in: BeckOK-StGB, § 25 Rn. 19; Pohlreich, in: Lackner/Kühl/Heger, StGB, § 25 Rn. 2-6a.

<sup>12</sup> Kudlich, in: BeckOK-StGB, § 25 Rn. 44-45.2; Weißer, in: TK-StGB, § 25 Rn. 79-82; Scheinfeld, in: MüKo-StGB, § 25 Rn. 188; Kindhäuser/Hilgendorf, LPK-StGB, 10. Aufl. (2025), § 25 Rn. 47-50.

<sup>13</sup> Weißer, in: TK-StGB, § 25 Rn. 5; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 73; Scheinfeld, in: MüKo-StGB, § 25 Rn. 61; Kudlich, in: BeckOK-StGB, § 25 Rn. 19; Pohlreich, in: Lackner/Kühl/Heger, StGB, § 25 Rn. 2.

<sup>14</sup> Kudlich, in: BeckOK-StGB, § 25 Rn. 20; Scheinfeld, in: MüKo-StGB, § 25 Rn. 62; Haas, in: Matt/Renzikowski, StGB, § 25 Rn. 5; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 73-77.

<sup>15</sup> Kudlich, in: BeckOK-StGB, § 25 Rn. 20-31.2; Weißer, in: TK-StGB, § 25 Rn. 7; Scheinfeld, in: MüKo-StGB, § 25 Rn. 65-66; Pohlreich, in: Lackner/Kühl/Heger, StGB, § 25 Rn. 4; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 86.

<sup>16</sup> Weißer, in: TK-StGB, Vorb. § 25 Rn. 53-56; Schild/Kretschmer, in: NK-StGB, Vorb. § 25 Rn. 5-7; Pohlreich, in: Lackner/Kühl/Heger, StGB, Vorb. § 25 Rn. 4-6; Kindhäuser/Hilgendorf, LPK-StGB, Vorb. § 25 Rn. 20-39; Scheinfeld, in: MüKo-StGB, Vorb. § 25 Rn. 4-5, 10.

<sup>17</sup> Degen/Emmert, Elektronischer Rechtsverkehr, 3. Aufl. (2025), Rn. 2.

<sup>18</sup> BGH, Beschl. v. 25.10.2023 – 4 StR 81/23, Rn. 20-21; Weißer, in: TK-StGB, § 25 Rn. 8-17; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 73-79, 91-94; Scheinfeld, in: MüKo-StGB, § 25 Rn. 70-80; Kudlich, in: BeckOK-StGB, § 25 Rn. 21-27.1.

<sup>19</sup> Engländer, in: NK-StGB, § 22 Rn. 36-38; Bosch, in: TK-StGB, § 22 Rn. 37-38; Hoffmann-Holland, in: MüKo-StGB, § 22 Rn. 112; Petzsche/Heger, in: Matt/Renzikowski, StGB, § 22 Rn. 27-31.

Verhalten voraus, das tatbestandsrelevant wird. Technische Systeme bieten hierfür kein Äquivalent. Wo ein System lediglich ausführt, steht nicht eine fremde Person zwischen Täter und Erfolg, sondern nur ein technischer Ablauf.

### III. Botnetze und Skripte als „Tatmittler“? – dogmatische Grenzen einer funktionalen Übersetzung

#### 1. Das funktionale Argument

Die Rede von der „Tat durch kompromittierte Systeme“ drängt zu einer Parallelisierung. Wie der Hintermann den schuldunfähigen Vordermann lenkt<sup>20</sup>, lenkt er das Botnetz; wie der Tatmittler die tatbestandliche Handlung ausführt, versenden die Bots die Pakete oder führen den Schadcode aus.<sup>21</sup> Aus dieser Perspektive soll § 25 Abs. 1 Alt. 2 StGB nicht als personale, sondern als instrumentale Zurechnungsfigur verstanden werden.

Diese Intuition beruht auf einer richtigen Beobachtung (Fernsteuerung), übersetzt sie aber in ein dogmatisch falsches Raster. Denn Fernsteuerung ist kein Spezifikum der mittelbaren Täterschaft. Auch der unmittelbare Täter kann aus der Ferne handeln, etwa, indem er ein System über Netzwerkbefehle manipuliert. Der Unterschied liegt nicht im Abstand, sondern darin, ob ein anderer Mensch als tatbestandsrelevantes Zwischenglied instrumentalisiert wird.<sup>22</sup>

#### 2. Auslegung vs. Analogie

Die Gleichsetzung technischer Mittel mit „anderen“ im Sinne des § 25 Abs. 1 Alt. 2 StGB lässt sich nicht ohne Weiteres als teleologische Auslegung legitimieren. Der Normtext differenziert bewusst zwischen „selbst begehen“ und „durch einen anderen begehen“ und stellt eine Legaldefinition dar.<sup>23</sup> Eine Ausdehnung auf Maschinen würde die Grenze zwischen Auslegung und Analogie überschreiten. Gerade weil § 25 Abs. 1 Alt. 2 StGB keine bloße Beschreibung eines Kausalverlaufs ist, sondern eine Zurechnungsformel, wäre eine solche Analogie mit Blick auf Art. 103 Abs. 2 GG besonders problematisch.<sup>24</sup>

#### 3. Nicht-personale Mittel sind keine Tatmittler

In der Kommentarliteratur wird für Grenzkonstellationen, in denen der vermeintliche Tatmittler kein „intentionales Werkzeug“ ist, herausgestellt, dass dann eine unmittelbare Täterschaft naheliegt und eine Behandlung als mittelbare Täterschaft begrifflich überdehnt wäre.<sup>25</sup> Der „Tatmittler“ wäre sonst ein bloßer „blinder Kausalfaktor“, wie ein mechanisches Werkzeug. Diese Beschreibung trifft die digitale Realität genauer: Der Bot ist nicht Adressat einer Willensherrschaft, sondern ein programmiertes/kompromittiertes Ausführungsmittel.<sup>26</sup>

#### 4. Versuchsbeginn als Lackmustest

Gerade bei automatisierten Prozessen zeigt sich die Gefahr dogmatischer Verschiebungen. Wird der Bot als „Tatmittler“ begriffen, liegt es nahe, den Versuchsbeginn an der „Entlassung“ dieses Mittlers in die Ausführung zu knüpfen. Für technische Systeme fehlt jedoch ein entsprechendes Konzept. Die Ausführung ist kein menschlicher Entscheidungsakt, sondern ein programmgemäßes Abarbeiten.<sup>27</sup> Der Versuchsbeginn muss daher an der vom Täter gesetzten Gefährdungsnähe orientiert werden<sup>28</sup>, wie z.B. Ausführung des Payloads oder Beginn der Paketflut, nicht an einer fiktiven „Mittlerhandlung“.

Die Literatur zu Fallenstellungen zeigt, wie sensibel die Anknüpfung ist: diskutiert werden u.a. die Entlassung des Mittlers, der Abschluss der Vorbereitung und die Vornahme einer konkret gefährdenden Handlung. Diese Modelle setzen jedoch eine Person als Mittler voraus und sind nicht ohne Weiteres auf Software übertragbar.<sup>29</sup>

#### 5. Die Gefahr der „Software-Mittäterschaft“

Eine „Digitalisierung“ der mittelbaren Täterschaft würde außerdem den Weg in eine Metaphorik öffnen, die das Beteiligungssystem überlädt. Wenn Software als Tatmittler gilt, wird die Tatbeherrschung des Hintermannes nicht mehr über personale Defektlagen, sondern über reine Steuerungsfähigkeit definiert. Dann ist jedoch nicht erkennbar, warum § 25 Abs. 1 Alt. 1 StGB nicht ausreichen sollte, da Steuerungsfähigkeit gerade ein Kernargument

<sup>20</sup> Schild/Kretschmer, in: NK-StGB, § 25 Rn. 74, 100; Weißer, in: TK-StGB, § 25 Rn. 17; Kudlich, in: BeckOK-StGB, § 25 Rn. 27-27.1; Scheinfeld, in: MüKo-StGB, § 25 Rn. 64; ZJS, Entscheidungsbesprechung zu BGH, Beschl. v. 13.9.2023 – 5 StR 200/23, abrufbar unter: <https://bit.ly/4bm94dj> (zuletzt abgerufen am 29.1.2026).

<sup>21</sup> Degen/Emmert, Elektronischer Rechtsverkehr, Rn. 2 (Stichwort: Bot); BSI, Exkurs: Social Bots und Chatbots, abrufbar unter: <https://bit.ly/4cogVbv> (zuletzt abgerufen am 29.1.2026); SRF, User oder Maschine? KI-Bots fluten das Internet – was das für uns bedeutet, abrufbar unter: <https://bit.ly/415012q> (zuletzt abgerufen am 29.1.2026); Polizeiliche Kriminalprävention, Botnetze – wenn der Computer zum Zombie wird, abrufbar unter: <https://bit.ly/3Nhqyyr> (zuletzt abgerufen am 29.1.2026).

<sup>22</sup> Merkur, Experten warnen: Diese harmlos wirkende Handlung installiert unbemerkt Schadsoftware auf jedem Gerät, abrufbar unter: <https://bit.ly/4b1yBY2> (zuletzt abgerufen am 29.1.2026); Presetext, aktuelle Warnung: Microsoft-signierte Malware ermöglicht gezielte Manipulation des Datenverkehrs, abrufbar unter: <https://bit.ly/46IG6ls> (zuletzt abgerufen am 29.1.2026).

<sup>23</sup> Weißer, in: TK-StGB, § 25 Rn. 1; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 29; Scheinfeld, in: MüKo-StGB, § 25 Rn. 243.

<sup>24</sup> Remmert, in: Dürig/Herzog/Scholz, GG, 108. EL (08/2025), Art. 103 Abs. 2 Rn. 82–86; Aust, in: Huber/Voßkuhle, GG, 8. Aufl. (2024), Art. 103 Rn. 171-172; Sodan, in: Sodan, GG, 5. Aufl. (2024), Art. 103 Rn. 20, 21; Radtke, in: BeckOK-GG, 64. Ed. (15.6.2025), Art. 103 Rn. 40-41.

<sup>25</sup> Scheinfeld, in: MüKo-StGB, § 25 Rn. 90-91; Weißer, in: TK-StGB, § 25 Rn. 26; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 87-90; Kudlich, in: BeckOK-StGB, § 25 Rn. 28-30.

<sup>26</sup> Maihold, in: Ellenberger/Bunte, BankR-HdB, 6. Aufl. (2022), § 33 Rn. 64; Degen/Emmert, Elektronischer Rechtsverkehr, Rn. 2.

<sup>27</sup> Degen/Emmert, Elektronischer Rechtsverkehr, Rn. 2; Wiebe, in: Leupold/Wiebe/Glossner, IT-Recht, 4. Aufl. (2021), Rn. 93.

<sup>28</sup> BGH, Beschl. v. 14.1.2020 – 4 StR 397/19, Rn. 8 ff.; Bosch, in: TK-StGB, § 22 Rn. 39-42; Hoffmann-Holland, in: MüKo-StGB, § 22 Rn. 112-114.

<sup>29</sup> Schild/Kretschmer, in: NK-StGB, § 25 Rn. 73-79; Scheinfeld, in: MüKo-StGB, § 25 Rn. 179-185; Ingelfinger, in: Dölling/Duttge/Rösner, StGB, § 25 Rn. 53-54.

der unmittelbaren Täterschaft im technischen Kontext ist.<sup>30</sup>

Zudem verschiebt sich der Blick von der tatbestandlichen Handlung auf die Projektarchitektur. Wer die Infrastruktur bereitstellt oder die Malware entwickelt, könnte leichter als „mittelbarer Täter“ etikettiert werden, obwohl ihm die konkrete Tatbestandsverwirklichung nicht als eigenes Handeln zugeordnet werden kann. Das ist dogmatisch riskant, weil es die Zurechnung vom Tatbestand löst und in eine allgemeine Verantwortlichkeit für „Cybercrime-Ökosysteme“ umkippen lässt.

## 6. Zwischenfazit

Botnetze und autonome Skripte sind keine „anderen“ im Sinne des § 25 Abs. 1 Alt. 2 StGB. Sie sind Ausführungsmittel. Die Zurechnung muss daher über unmittelbare Täterschaft und objektive Zurechnung laufen; mittelbare Täterschaft bleibt den personenbezogenen Konstellationen vorbehalten.

## IV. Alternativmodelle: unmittelbare Täterschaft, objektive Zurechnung und (begrenzte) Organisationsherrschaft

### 1. Unmittelbare Täterschaft durch Werkzeuggebrauch: Fernsteuerung als eigene Tathandlung

Wer Malware deployt, Befehle an kompromittierte Systeme sendet oder einen DDoS-Flood startet, „begeht“ die Tat selbst, da er mit dem Versenden der Befehle und dem Start der Aktion die Handlungsherrschaft innehat.<sup>31</sup> Die Handlung liegt in der tatplangemäßen Setzung und Aktivierung des technischen Prozesses. Die Ausführung auf dem Zielsystem ist Teil des beherrschten Kausalverlaufs. Dogmatisch entspricht dies dem Einsatz eines Werkzeugs, das den tatbestandlichen Erfolg herbeiführt.

Diese Einordnung ist nicht nur formal. Sie zwingt dazu, die Täterhandlung konkret zu benennen wie z.B. Übermittlung des Command-Befehls, Ausbringen des Schadcodes oder Konfiguration der Paketflut und den Erfolg als Realisierung eines dadurch geschaffenen Risikos zu prüfen. Der Täter wird nicht „über“ eine technische Zwischeninstanz strafbar, sondern wegen seines eigenen, tatbestandsbezogenen Handelns.

### 2. Autonomer Code und „Set-and-Forget“

Ein möglicher Einwand lautet, dass der Angreifer nach dem Inverkehrbringen des Schadcodes nicht mehr steuert. Der Code läuft autonom, etwa nach Zeitplan oder ereignisgesteuert. Auch hier ist die Personalisierung des Systems fehl am Platz. Die fehlende Live-Steuerung spricht nicht für mittelbare Täterschaft, sondern ist im Rahmen der objektiven Zurechnung und des Vorsatzes zu bewer-

ten. Maßgeblich ist, ob der Täter die tatbestandliche Gefahr tatplangemäß gesetzt und den Eintritt des Erfolgs zumindest billigend in Kauf genommen hat.

Im digitalen Raum ist daher zwischen zwei Steuerungsdimensionen zu unterscheiden: (i) ex ante Steuerung (Setzen des Prozesses, Parametrisierung) und (ii) ex post Steuerung (Abbruch-/Modulationsmöglichkeiten). Fehlt die ex post Steuerung vollständig, kann dies für die Reichweite des Vorsatzes und die Zurechnung von Exzessen relevant sein; es macht den Täter aber nicht zum mittelbaren Täter.

### 3. Objektive Zurechnung als Korrektiv

Die objektive Zurechnung ermöglicht es, automatisierte Verläufe normativ zu strukturieren. Sie fragt nach erlaubtem Risiko, Risikoverwirklichung und dem Schutzzweck der Norm. Gerade bei Botnet-Angriffen können Kausalverläufe exzessiv sein, da ein Flood auch Drittsysteme beeinträchtigen kann oder ein Wurm sich schneller ausbreiten kann als geplant. Die Zurechnungsentscheidung darf dann nicht von einer fiktiven „Tatmittlerhandlung“ abhängen, sondern davon, ob sich die vom Täter geschaffene tatbestandspezifische Gefahr realisiert oder ob ein atypischer Verlauf vorliegt.

### 4. Eine Zurechnungsmatrix

Für die dogmatische Einordnung digitaler Angriffskonstellationen kann folgende Prüfungslogik als Arbeitsinstrument dienen:

- Liegt ein menschlicher Intermediär vor, der tatbestandsrelevant handelt? → Wenn ja: Prüfung von § 25 Abs. 1 Alt. 2 StGB (Defektlage/Unterordnung) oder Teilnahme.
- Fehlt ein menschlicher Intermediär und wird der tatbestandsrelevante Prozess technisch ausgelöst? → Regel: § 25 Abs. 1 Alt. 1 StGB (Werkzeuggebrauch) mit objektiver Zurechnung.
- Besteht ein arbeitsteiliger menschlicher Organisationsapparat (Austauschbarkeit/regelhaftes Auslösen von Abläufen) und wird die Tat trotz vollverantwortlicher Ausführender „nahezu automatisch“ bewirkt? → Nur dann (und unter Kritikvorbehalt) Diskussion Organisationsherrschaft.
- Sind exzessive, nicht beherrschte Folgeeffekte eingetreten? → Korrektur über objektive Zurechnung und Vorsatzreichweite, nicht über Umdeutung der Täterform.

Diese Matrix ist bewusst restriktiv gegenüber § 25 Abs. 1 Alt. 2 StGB. Sie schützt die Personenbezogenheit der mittelbaren Täterschaft und verschiebt die normative Arbeit dorthin, wo sie hingehört, und zwar in die Zurechnung des tatbestandsrelevanten Risikos und in die Bestimmung des tatbestandlichen Kerngeschehens.

<sup>30</sup> Schild/Kretschmer, in: NK-StGB, § 25 Rn. 23-25, 37; Scheinfeld, in: MüKo-StGB, § 25 Rn. 65-66; Weißer, in: TK-StGB, § 25 Rn. 22-24; Haas, in: Matt/Renzikowski, StGB, § 25 Rn. 33-36; Ingelfinger, in: Dölling/Duttge/Rösner, StGB, § 25 Rn. 8.

<sup>31</sup> Weißer, in: TK-StGB, § 25 Rn. 2; Scheinfeld, in: MüKo-StGB, § 25 Rn. 39-41; Pohlreich, in: Lackner/Kühl/Heger, StGB, § 25 Rn. 1a; Kudlich, in: BeckOK-StGB, § 25 Rn. 18.

### 5. Organisationsherrschaft: menschliche Apparate vs. technische Regelhaftigkeit

In digitalen Angriffsketten existieren Konstellationen, in denen der Hintermann nicht primär technische Mittel, sondern menschliche Organisationsstrukturen nutzt wie etwa bei arbeitsteiligen „Service“-Modellen (RaaS), in denen Affiliate-Operatoren austauschbar agieren und die Zentrale über Infrastruktur, Schlüsselmaterial oder Auszahlungsmechanismen dispositiv verfügt.

Die Rechtsprechung hat für solche Fälle die Figur der Organisationsherrschaft entwickelt.<sup>32</sup> Trotz vollverantwortlich handelnder Ausführer soll mittelbare Täterschaft möglich sein, wenn der Beitrag des Hintermannes innerhalb bestimmter organisatorischer Rahmenbedingungen regelhafte Abläufe auslöst und nahezu automatisch zur Tatbestandsverwirklichung führt.<sup>33</sup> Diese Konstruktion ist umstritten; kritisiert werden insbesondere Unbestimmtheit und die Gefahr, Beweiserleichterung über Dogmatik zu erzielen.

Auch wenn man Organisationsherrschaft für bestimmte digitale Organisationsmodelle für anschlussfähig hält, muss sie strikt von technischer Automatisierung getrennt werden. Die Regelhaftigkeit eines Programms ist keine Organisationsstruktur im Sinne der Rechtsprechung. Wer technische Regelhaftigkeit mit Organisationsherrschaft gleichsetzt, entkernt den ohnehin umstrittenen Ansatz und macht ihn inhaltsleer.

### 6. Echte mittelbare Täterschaft über menschliche Intermediäre

Schließlich gibt es digitale Konstellationen, in denen mittelbare Täterschaft klassisch einschlägig ist: Social-Engineering-Angriffe, in denen Menschen als unwissende Ausführende agieren wie z.B. Administratoren, die auf Täuschung hin privilegierte Befehle ausführen, oder Angestellte, die Zugangsdaten preisgeben. Hier ist der Tatmittler als Person vorhanden; sein Defekt (Irrtum, fehlender Vorsatz) kann die Tatbeherrschung des Hintermannes begründen.<sup>34</sup> Die digitale Besonderheit liegt dann nicht in

der Abwesenheit des Tatmittlers, sondern im Kommunikationsmedium.

## V. Tatbestandliche Implikationen und Fallkonstellationen (insb. §§ 303a, 303b StGB)

### 1. Datenveränderung (§ 303a StGB)

§ 303a StGB schützt Daten als nicht unmittelbar wahrnehmbare Informationen, an denen ein fremdes Nutzungsrecht besteht; geschützt sind auch Programme und Programmteile.<sup>35</sup> Die Tathandlungen wie Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern bilden den tatbestandlichen Kern und können auch durch Unterlassen verwirklicht werden, wenn ein Garant die drohende Datenveränderung nicht abwendet.<sup>36</sup>

Botnet- oder Malware-Angriffe realisieren § 303a StGB typischerweise durch automatisierte Manipulationen, indem Dateien verschlüsselt (Unbrauchbarmachen)<sup>37</sup>, Logfiles überschrieben (Verändern/Löschen)<sup>38</sup> oder Zugriffe blockiert (Unterdrücken)<sup>39</sup> werden. Dogmatisch ist dabei die Zurechnung nicht deshalb problematisch, weil die Ausführung technisch vermittelt ist, sondern weil sie automatisiert erfolgt. Die Lösung liegt darin, die Programmausführung als vom Täter gesetzten Prozess zu behandeln. Die „Tat“ wird nicht von einem anderen Menschen ausgeführt, sondern vom Täter selbst, indem er den Code zur Ausführung bringt.

Dass dies keine bloße Theorie ist, zeigt bereits die Beschreibung der Tathandlungen. Das vorsätzliche Installieren eines Killer- oder Virusprogramms wird als Beispiel für tatbestandliches Löschen genannt; Unbrauchbarmachen kann durch Programmsperren, Einfügungen oder Überschreiben erfolgen.<sup>40</sup>

### 2. Vorbereitung und Vorfeld: gesetzgeberische Signale

Bemerkenswert ist, dass der Gesetzgeber für digitale Delikte teilweise eigene Vorfelddelikte bzw. Vorbereitungstatbestände geschaffen hat. § 303a Abs. 3 StGB wurde eingefügt, um besonders gefährliche Vorbereitungshandlungen im Hinblick auf Eingriffe in Daten unter Strafe zu

<sup>32</sup> BGH, Beschl. v. 2.11.2007 – 2 StR 384/07, Rn. 6.; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 38-44; Weißer, in: TK-StGB, § 25 Rn. 29-30; Kudlich, in: BeckOK-StGB, § 25 Rn. 28-30, 34-35.1; Scheinfeld, in: MüKo-StGB, § 25 Rn. 199-207.

<sup>33</sup> Weißer, in: TK-StGB, § 25 Rn. 36-40; Scheinfeld, in: MüKo-StGB, § 25 Rn. 147-154; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 106-109.

<sup>34</sup> Haas, in: Matt/Renzikowski, StGB, § 25 Rn. 49-52; Scheinfeld, in: MüKo-StGB, § 25 Rn. 65-66; Kindhäuser/Hilgendorf, in: LPK-StGB, § 25 Rn. 7-10; Schild/Kretschmer, in: NK-StGB, § 25 Rn. 87-90; Kudlich, in: BeckOK-StGB, § 25 Rn. 13-16.

<sup>35</sup> Hecker, in: TK-StGB, § 303a Rn. 1; Wieck-Noodt, in: MüKo-StGB, § 303a Rn. 1-4; Basar/Heinelt, in: ComputerR-HdB, 40. EL (März 2025), Teil 10. 100. Rn. 125; Weidemann, in: BeckOK-StGB, § 303a Rn. 2-2.2; Heger, in: Lackner/Kühl/Heger, StGB, § 303a Rn. 1; Schallbruch, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. (2024), Rn. 15-23.

<sup>36</sup> Weidemann, in: BeckOK-StGB, § 303a Rn. 8-15.1; Wieck-Noodt, in: MüKo-StGB, § 303a Rn. 11; Hecker, in: TK-StGB, § 303a Rn. 4-8; Bär, in: WirtschaftsStrafR-HdB, 6. Aufl. (2025), 15. Kap. Rn. 114-118; Wengenroth, in: DatenschutzsanktionenR-HdB, 2023, § 20 Rn. 15-17.

<sup>37</sup> Hecker, in: TK-StGB, § 303a Rn. 7; Weidemann, in: BeckOK-StGB, § 303a Rn. 13-14; Wieck-Noodt, in: MüKo-StGB, § 303a Rn. 14; Heger, in: Lackner/Kühl/Heger, StGB, § 303a Rn. 3; Kargl, in: NK-StGB, § 303a Rn. 11.

<sup>38</sup> Weidemann, in: BeckOK-StGB, § 303a Rn. 9-10, 15-15.1; Basar/Heinelt, in: ComputerR-HdB, Teil 10. 100. Rn. 134; Wieck-Noodt, in: MüKo-StGB, § 303a Rn. 12, 15; Hecker, in: TK-StGB, § 303a Rn. 5, 8.

<sup>39</sup> Hecker, in: TK-StGB, § 303a Rn. 6; Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 116; Weidemann, in: BeckOK-StGB, § 303a Rn. 11-12.2; Wengenroth, in: Klaas/Momsen/Wybitul, DatenschutzsanktionenR-HdB, § 20 Rn. 19-20.

<sup>40</sup> Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 115; Wieck-Noodt, in: MüKo-StGB, § 303a Rn. 12; Reinbacher, in: NK-WSS, 2. Aufl. (2022), § 303a Rn. 27; Kargl, in: NK-StGB, § 303a Rn. 9; Weidemann, in: BeckOK-StGB, § 303a Rn. 10.

stellen.<sup>41</sup> Gerade diese gesetzgeberische Entscheidung spricht gegen ein Bedürfnis, Vorfeldprobleme über eine Ausdehnung von § 25 Abs. 1 Alt. 2 StGB zu lösen. Wo der Gesetzgeber Vorverlagerung will, normiert er sie – und begrenzt sie zugleich.

### 3. Computersabotage (§ 303b StGB)

§ 303b StGB schützt als Sondertatbestand das Interesse der Betreiber und Nutzer an der ordnungsgemäßen Funktionsweise von Datenverarbeitungen;<sup>42</sup> das Delikt ist ein Erfolgsdelikt, weshalb eine bloße Gefährdung nicht genügt.<sup>43</sup> Tatobjekt ist eine Datenverarbeitung, deren Begriff weit zu verstehen ist und auch den weiteren Umgang mit Daten und deren Verwertung umfasst; das Merkmal der „wesentlichen Bedeutung“ dient als Filter gegen Bagatellen.<sup>44</sup> Der Erfolg liegt in der erheblichen Störung, die den reibungslosen Ablauf nicht unerheblich beeinträchtigt; eine bloße Gefährdung reicht nicht.<sup>45</sup>

DDoS-Angriffe über Botnetze illustrieren, dass die Erfolgsherbeiführung häufig ein Systemeffekt ist. Es genügt bereits, wenn ein konkreter Datenverarbeitungsvorgang infolge der Tat nicht in bisheriger Form durchgeführt werden kann, sofern die Wiederherstellung nicht ohne großen Aufwand gelingt. Der Angreifer setzt die Paketflut in Gang, wählt das Ziel und moduliert die Last.<sup>46</sup> Das spricht nicht für mittelbare Täterschaft, sondern für unmittelbare Täterschaft (Werkzeuggebrauch) mit erfolgsbezogener objektiver Zurechnung.

Für Versuch und Vollendung ist § 303b StGB besonders instruktiv. Nicht jedes unmittelbare Ansetzen zur Sabotagehandlung stellt schon den Versuch der Computersabotage dar, weil der tatbestandliche Erfolg, also die Störung eines konkreten Datenverarbeitungsvorgangs, erforderlich bleibt. Die Versuchsschwelle ist daher stärker erfolgshaft.

Hinzu tritt, dass § 303b Abs. 5 StGB in Verbindung mit § 202c StGB Vorbereitungshandlungen selbständig unter Strafe stellt und sogar ein tätige-Reue-ähnliches Korrektiv

vorsieht.<sup>47</sup> Auch dies ist ein Signal, da die Vorverlagerung normiert wird, aber in einem eigenen, systematisch abgegrenzten Instrument. Eine dogmatische Umgehung über § 25 Abs. 1 Alt. 2 StGB würde diese Systementscheidung unterlaufen.

### 4. Ransomware als Herrschaftsindikator ohne Tatmittlerfiktion

Ransomware-Angriffe zeigen, dass die dogmatisch zentrale Herrschaft nicht im „Ausführen“ (Verschlüsseln) liegt, sondern in der Kontrolle des Fortbestands der Beeinträchtigung. Der Angreifer kann, durch Schlüsselmaterial oder Kill-Switch, über Aufrechterhaltung und Beendigung disponieren.<sup>48</sup> Diese Steuerungsposition ist dogmatisch anschlussfähig, ohne dass das Zielsystem als Tatmittler personalisiert werden müsste.

Technisch ist dies durch hybride Verschlüsselungsarchitekturen begünstigt: Dateien werden lokal symmetrisch verschlüsselt; der Schlüssel wird asymmetrisch gesichert, wobei der private Schlüssel typischerweise auf Angreifer-Infrastruktur verbleibt.<sup>49</sup>

### 5. Fallbeispiele (schematisch)

Zur Illustration lassen sich drei Konstellationen unterscheiden:

#### a) Botnet-DDoS

Der Täter mietet Botnet-Kapazität, setzt Ziel und Dauer und startet den Flood. Tatbegehung ist unmittelbar (§ 25 Abs. 1 Alt. 1 StGB); die Bots sind Werkzeuge. Versuch/Vollendung richten sich nach § 303b-Erfolg.

#### b) Ransomware-Affiliate

Ein Developer stellt Code, ein Affiliate deployt, die Zentrale verwaltet Schlüssel und Zahlungsabwicklung. Hier können neben unmittelbarer Täterschaft der Deployenden

<sup>41</sup> Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 122, 123; Wieck-Noodt, in: MüKo-StGB, § 303a Rn. 7; Hecker, in: TK-StGB, § 303a Rn. 12; Weidemann, in: BeckOK-StGB, § 303a Rn. 16; Kargl, in: NK-StGB, § 303a Rn. 18.

<sup>42</sup> BGH, Beschl. v. 11.1.2017 – 5 StR 164/16, Rn. 19; Weidemann, in: BeckOK-StGB, § 303b Rn. 4, 4.1; Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 128-130a; Wieck-Noodt, in: MüKo-StGB, § 303b Rn. 7-9; Hecker, in: TK-StGB, § 303b Rn. 2, 3; Kargl, in: NK-StGB, § 303b Rn. 4; Gercke, in: Spindler/Schuster/Kaesling, StGB, 5. Aufl. (2026), § 303b Rn. 2-4.

<sup>43</sup> Hecker, in: TK-StGB, § 303b Rn. 1; Wieck-Noodt, in: MüKo-StGB, § 303b Rn. 2; Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 125; Brodowski, in: Kipker Cybersecurity-HdB, 2. Aufl. (2023), Kap. 17 Rn. 36; Basar/Heine, in: ComputerR-HdB, Teil 10. 100. Rn. 142.

<sup>44</sup> Basar/Heinelt, in: ComputerR-HdB, Teil 10. 100. Rn. 146-148; Weidemann, in: BeckOK-StGB, § 303b Rn. 5-9; Wieck-Noodt, in: MüKo-StGB, § 303b Rn. 23; Gercke, in: Spindler/Schuster/Kaesling, StGB, § 303b Rn. 5; Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 126, 127; Altenhain, in: Matt/Renzikowski, StGB, § 303b Rn. 14.

<sup>45</sup> Weidemann, in: BeckOK-StGB, § 303b Rn. 15, 16; Wieck-Noodt, in: MüKo-StGB, § 303b Rn. 19; Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 32; Altenhain, in: Matt/Renzikowski, StGB, § 303b Rn. 4, 5; Hecker, in: TK-StGB, § 303b Rn. 9.

<sup>46</sup> Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 130-130a; Weidemann, in: BeckOK-StGB, § 303b Rn. 15; Hecker, in: TK-StGB, § 303b Rn. 9; Altenhain, in: Matt/Renzikowski, StGB, § 303b Rn. 7, 8; Heger, in: Lackner/Kühl/Heger, StGB, § 303b Rn. 5.

<sup>47</sup> Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 140; Grözing, in: MAH Strafverteidigung, 3. Aufl. (2022), § 50 Rn. 77; Heger, in: Lackner/Kühl/Heger, StGB, § 303b Rn. 9; Weidemann, in: BeckOK-StGB, § 303b Rn. 20; Hecker, in: TK-StGB, § 303b Rn. 21; Altenhain, in: Matt/Renzikowski, StGB, § 303b Rn. 13; Gercke, in: Spindler/Schuster/Kaesling, StGB, § 303b Rn. 12.

<sup>48</sup> BGH, Beschl. v. 8.4.2021 – 1 StR 78/21, Rn. 19; BSI, Ransomware – Fakten und Abwehrstrategien, abrufbar unter: <https://bit.ly/4bjBO6B> (zuletzt abgerufen am 29.1.2026), Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 116, 140.

<sup>49</sup> Beaman/Barkworth, Computers & Security 111 (2021) 102490, insb. S. 2-3; BORN CITY vom 25.1.2026, Osiris-Ransomware nutzt gefährliche BYOVD-Methode, abrufbar unter: <https://bit.ly/3N2OwGP> (zuletzt abgerufen am 29.1.2026); BSI vom 16.2.2025, Cyberaggression: Hybride Bedrohungen des 21. Jahrhunderts und wie wir uns vor ihnen schützen, abrufbar unter: <https://bit.ly/4d1zsl> (zuletzt abgerufen am 29.1.2026).

mittäterschaftliche oder organisationsbezogene Zurechnungsfragen auftreten; mittelbare Täterschaft „durch Systeme“ ist jedoch nicht notwendig.

### c) Social Engineering

Ein Mitarbeiter wird getäuscht und führt ein Skript aus, das Daten löscht. Hier kann mittelbare Täterschaft über einen menschlichen Tatmittler einschlägig sein.

### 6. Kurzer Ausblick auf § 263a StGB (Computerbetrug)

Auch bei § 263a StGB werden Eingaben und Datenverarbeitungen oft skriptgesteuert manipuliert wie z.B. automatisierte Transaktionen oder Credential-Stuffing.<sup>50</sup> Die Zurechnung ist auch hier primär eine Frage der unmittelbaren Täterschaft und objektiven Zurechnung. Der Täter bewirkt durch Eingaben oder Programmsteuerung die unrichtige bzw. unvollständige Datenverarbeitung. Mittelbare Täterschaft ist nur dort erforderlich, wo menschliche Zwischenakte wie etwa unwissende Kontoinhaber oder Mitarbeiter tatbestandsrelevante Handlungen ausführen.

### 7. Ausblick: Autonome Angriffsroutinen

(1) Die Diskussion gewinnt zusätzliche Schärfe, wenn Angriffsroutinen nicht nur automatisiert, sondern adaptiv sind wie z.B. dynamische Zielauswahl oder selbständige Privilegieneskalation. Gerade dann ist Zurückhaltung gegenüber einer Personalisierung technischer Systeme angezeigt. Die Zurechnung muss über Vorsatz, objektive Zurechnung und ggf. Fahrlässigkeitsdelikte gesteuert werden. Eine Erweiterung des § 25 Abs. 1 Alt. 2 StGB würde hingegen die dogmatischen Probleme nur verschieben, nicht lösen.

(2) Täterhandlung ist die tatplangemäße Setzung bzw. Steuerung des technischen Prozesses; die tatbestandliche Erfolgszurechnung erfolgt über objektive Zurechnung (Risikoverwirklichung, Schutzzweck).

(3) Mittelbare Täterschaft kommt nur dort in Betracht, wo Menschen defizitär oder strukturell untergeordnet handeln (insbesondere Social Engineering).

(4) Organisationsherrschaft kann, sofern anerkannt, nur gegenüber menschlichen Organisationsapparaten und unter strengen Voraussetzungen diskutiert werden; technische Regelmäßigkeit genügt nicht.

### 8. Organisationsstrukturen in Cybercrime-Modellen: Abgrenzungslinien zur Organisationsherrschaft

Ein eigener Grenzbereich entsteht bei arbeitsteiligen Geschäftsmodellen (etwa Ransomware-as-a-Service), in denen menschliche Operatoren austauschbar agieren, während zentrale Akteure Infrastruktur, Schlüsselmaterial und

Auszahlungsmechanismen kontrollieren. In solchen Konstellationen kann die Diskussion um organisationsbezogene Zurechnungsmodelle zwar naheliegen. Gleichwohl ist strikt zu trennen: Die Frage, ob eine Tat „durch einen anderen“ begangen wird, ist eine Frage personenbezogener Vermittlung; die Frage, ob eine Organisation tatbestandsrelevante Abläufe regelhaft auslöst, betrifft ein spezifisches Herrschaftsmodell gegenüber Menschen, nicht gegenüber Maschinen.<sup>51</sup> Für die dogmatische Einordnung empfiehlt es sich, zunächst die tatbestandliche Kernhandlung zu identifizieren, also bei § 303a StGB die Datenbeeinträchtigung und bei § 303b StGB die erhebliche Störung, und sodann zu prüfen, wer im konkreten Tatprogramm darüber disponiert: Wer bestimmt Ziel, Zeitpunkt, Intensität, Abbruch? Wer hält technische Schlüsselpositionen wie Schlüsselverwaltung, C2-Kontrolle oder Kill-Switch? Diese Kriterien können innerhalb einer Mittäter- oder (eng begrenzten) organisationsbezogenen Zurechnung relevant sein. Sie sprechen aber gerade nicht dafür, die kompromittierten Systeme als Tatmittler zu behandeln. Das System bleibt Werkzeug; die Zurechnung spielt sich auf der Ebene menschlicher Rollen und Verantwortungsbeziehungen ab. Gerade im digitalen Raum ist zudem zu beachten, dass arbeitsteilige Strukturen häufig modular und marktartig organisiert sind. Wo lediglich standardisierte Leistungen „eingekauft“ werden (Botnet-Miete, Exploit-Pakete, Hosting), fehlt es häufig an der reziproken Bindung, die täterschaftliche Zurechnung im engeren Sinne rechtfertigt. Nach ständiger Rechtsprechung des BGH ist die Frage der Handlungseinheit oder -mehrheit nach dem individuellen Tatbeitrag eines jeden Beteiligten zu beurteilen.<sup>52</sup> Auch insoweit ist der Versuchung zu widerstehen, über § 25 Abs. 1 Alt. 2 StGB eine projektbezogene Gesamtverantwortung zu konstruieren.

Zurechnungsdruck, Attribution und die Versuchung dogmatischer Abkürzungen Digitale Angriffe sind häufig gerade deshalb erfolgreich, weil sie Zurechnung und Nachweis erschweren. Der Angreifer bedient sich kompromittierter Geräte als Verkehrsträger, verschleiert Kommunikationswege und trennt Infrastruktur, Ausführung und Monetarisierung organisatorisch. Für die Strafrechtsdogmatik besteht hier ein doppelter Druck. Einerseits besteht das legitime Bedürfnis, den „Hintermann“ als Täter zu erfassen, auch wenn die Ausführung nicht sichtbar „von Hand“ erfolgt. Andererseits darf die Dogmatik nicht zum Ersatz für technische Attribution werden. Die Einordnung kompromittierter Systeme als „Tatmittler“ hätte (scheinbar) den Vorteil einer einfachen Beschreibung. Die „Tat-handlung“ geschieht durch die Bots, der Hintermann sei deshalb mittelbarer Täter. Damit würde jedoch das Kernproblem nur sprachlich umetikettiert.

Dogmatisch ist die Zurechnung nicht deshalb schwierig, weil der Tatmittler fehlt, sondern weil täterseitige Steuerungshandlungen, wie etwa das Ausbringen der Malware, die Parametrisierung des Floods, die Verwaltung von

<sup>50</sup> Noll, in: MüKo-StGB, § 263a Rn. 1, 2; Schmidt, in: BeckOK-StGB, § 263a Rn. 2, 6-9, 37-40; Bär, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 11; Heger, in: Lackner/Kühl/Heger, StGB, § 263a Rn. 5-15; Noll, in: MüKo-StGB, § 263a Rn. 41-42; Kindhäuser/Hoven, in: NK-StGB, § 263a Rn. 10-12.

<sup>51</sup> Schild/Kretschmer, in: NK-StGB, § 25 Rn. 38; Weißer, in: TK-StGB, § 25 Rn. 29-30, 43-45; Scheinfeld, in: MüKo-StGB, § 25 Rn. 147-149; Kudlich, in: BeckOK-StGB, § 25 Rn. 28-30.

<sup>52</sup> BGH, Beschl. v. 8.4.2021 – 1 StR 78/21, Rn. 20 ff.

Schlüsseln oder das Betreiben der Command-and-Control-Infrastruktur, in den Ermittlungen häufig nur indirekt rekonstruierbar sind. Die richtige Antwort liegt daher in einer Normierung der Zurechnungskriterien (Werkzeuggebrauch und objektive Zurechnung) und in einer forensischen Rekonstruktion dieser Steuerungsakte, nicht in einer „Software-Mittäterschaft“.

Dies gilt umso mehr, als expansive Täterkonstruktionen die Differenzierung zwischen Täterschaft und Teilnahme unterlaufen können. Wer lediglich Zugang zu einem Botnetz bereitstellt, wird nicht dadurch Täter der späteren Computersabotage, dass Bots Pakete versenden. Ob ein solcher Akteur Täter, Mittäter oder Teilnehmer ist, hängt vielmehr von Tatplanbindung, Beitragsherrschaft und Vorsatz ab. Die dogmatische Trennung schützt deshalb nicht nur das Bestimmtheitsgebot, sondern auch die schuldangemessene Individualisierung strafrechtlicher Verantwortung.

#### 9. Versuchsbeginn und Rücktritt im automatisierten Geschehen

Die bislang skizzierte Versuchsdogmatik lässt sich durch zwei Beobachtungen präzisieren. Erstens verschiebt Automatisierung das Gewicht von „Handlungsnähe“ zu „Gefährdungsnähe“. Bei DDoS-Angriffen ist das unmittelbare Ansetzen nicht die vorherige Inbetriebnahme des Botnetzes, sondern der tatplangemäße Start eines Floods gegen ein konkret adressiertes Zielsystem. Das Auslösen der Paketflut ist funktional dem Betätigen eines Auslösers vergleichbar; der nachfolgende Datenverkehr ist – strafrechtlich – der beherrschte Kausalverlauf. Ähnliches gilt bei Ransomware: Das bloße Bereithalten von Schadsoftware ist noch Vorbereitung; das unmittelbare Ansetzen beginnt mit der Ausführung der Verschlüsselungsroutine oder mit dem Schritt, der nach dem Tatplan ohne weitere Zwischenschritte zur Datenunbrauchbarkeit führt.

Zweitens wird die Rücktrittsdogmatik im Digitalen häufig an Abbruch- und Steuerungspositionen konkretisiert. Wer über ein Botnetz verfügt, kann – jedenfalls typischerweise – Stop-Kommandos erteilen oder C2-Knoten abschalten; wer im Ransomware-Kontext Schlüsselmaterial kontrolliert, kann die tatbestandliche Beeinträchtigung beenden oder zumindest abmildern. Diese Möglichkeiten sind rechtlich relevant, weil sie zeigen, dass das Tatgeschehen auch nach Beginn der Ausführung noch steuerbar ist. Im Rücktritt ist dann zu fragen, ob der Täter den Erfolg verhindert oder sich ernsthaft darum bemüht; bei fortdauernden Beeinträchtigungen wie z.B. anhaltender DDoS kann das Abbruchverhalten auch für die Dauer- und Schadensdimension der Tat von Bedeutung sein.

Die zentrale Pointe für die hier diskutierte Täterform ist: Weder Versuchsbeginn noch Rücktritt benötigen einen „Tatmittler“ als Adressaten. Sie lassen sich – systemkonform – als Steuerungsfragen gegenüber dem vom Täter

selbst gesetzten technischen Prozess behandeln. Damit wird zugleich die unproduktive Alternative vermieden, entweder § 25 Abs. 1 Alt. 2 StGB auf Systeme auszudehnen oder aber digitale Angriffsszenarien dogmatisch als „handlungsfern“ zu behandeln. Das Werkzeugmodell erlaubt eine präzise, tatbestandliche Anknüpfung.

#### 10. Systematische Einordnung: Vorverlagerung und Deliktsspezifika statt Täterausweitung

Die Diskussion um mittelbare Täterschaft durch Systeme ist häufig auch Ausdruck eines kriminalpolitischen Bedürfnisses. Digitale Angriffe entstehen aus Vorbereitungshandlungen<sup>53</sup> wie Scans, Exploit-Entwicklung oder Botnet-Aufbau, deren Gefährlichkeit offensichtlich ist, während eine Teilnahme an der späteren Haupttat nicht immer nachweisbar oder – wegen fehlender Tatplanbindung – dogmatisch begründbar ist. Diese Lücke darf jedoch nicht durch eine Ausweitung des Täterbegriffs geschlossen werden. Zum einen würden dadurch die Zurechnungsgrenzen zwischen Täter- und Teilnehmerverantwortlichkeit verwischt. Zum anderen hat der Gesetzgeber gerade im digitalen Bereich gezeigt, dass er die Vorfeldstrafbarkeit punktuell und begrenzt normiert.

Das spricht dafür, systematische Probleme auf der Ebene von Deliktsspezifika wie Vorbereitungstatbestände, Erfolgsstruktur und Versuchsschwelle zu lösen, nicht durch eine Umdeutung des § 25 StGB. Für die Praxis bedeutet dies, dass in Botnet-Konstellationen zunächst sauber zu bestimmen ist, welches Delikt tatbestandlich im Raum steht (z.B. § 303b StGB bei DDoS-Störung, § 303a StGB bei Datenmanipulation). Sodann ist zu klären, welche Steuerungshandlungen dem Beschuldigten zurechenbar sind (Befehle, Parametrisierung, Schlüsselverwaltung). Erst im dritten Schritt sind Zurechnungsformen zu prüfen wie unmittelbare Täterschaft, Mittäterschaft, Teilnahme und ggf. vorbereitende Delikte. Eine Abkürzung über „mittelbare Täterschaft durch Systeme“ ist demgegenüber dogmatisch unpräzise und birgt, gerade bei neutralen oder marktartigen Beiträgen, erhebliche Überdehnungsrisiken.

#### 11. Ausblick: Autonomiegrade und „KI-gestützte“ Angriffsroutinen

Die hier vertretene Begrenzung der mittelbaren Täterschaft wird in Zukunft eher an Bedeutung gewinnen. Mit zunehmender Automatisierung und adaptiven Angriffsroutinen wie z.B. dynamische Ausbreitung, automatisiertes Privilegien-Management oder selbständige Wahl von Angriffspfaden steigt die Versuchung, technische Prozesse als „quasi-personale“ Mittler zu behandeln. Strafrechtsdogmatisch ist hiervor zu warnen, denn je mehr ein System adaptiv reagiert, desto weniger trägt eine Anthropomorphisierung zur Klarheit bei. Die entscheidenden Zurechnungsfragen werden vielmehr verschoben – nämlich auf Vorsatz und objektive Zurechnung.

<sup>53</sup> Hecker, in: TK-StGB, § 303a Rn. 12; Heger, in: Lackner/Kühl/Heger, § 303a Rn. 1-7; Graf, in: MüKo-StGB, § 202c Rn. 1-3a; Eisele, in: TK-StGB, § 202c Rn. 5.

So ist bei hochautonomen Routinen besonders sorgfältig zu prüfen, ob sich noch die vom Täter geschaffene tatbestandspezifische Gefahr realisiert oder ob ein atypischer Verlauf vorliegt, der außerhalb des tatplangemäß beherrschten Risikos liegt. Gleiches gilt für die Reichweite des Vorsatzes. Die Tatsache, dass ein Programm unter bestimmten Bedingungen „selbständig“ eskaliert, kann die Annahme eines Vorsatzexzesses oder, je nach Delikt, die Relevanz fahrlässiger Begehungsformen nahelegen. Das ist dogmatisch anspruchsvoll, aber systematisch sauber. Eine Ausdehnung des § 25 Abs. 1 Alt. 2 StGB würde diese Fragen nicht lösen, sondern verdecken. Die Unschärfe würde in die Täterform verlagert, statt die normativen Kriterien dort anzuwenden, wo sie hingehören. Gerade im digitalen Raum ist jedoch Transparenz der Zurechnung zentral – nicht zuletzt, weil sich strafrechtliche Verantwortung häufig an der Schnittstelle zwischen deliktischer Nutzung und neutraler Technik entfaltet. Das Strafrecht sollte deshalb an der Personenbezogenheit der mittelbaren Täterschaft festhalten und technische Autonomie als Problem von Risiko, Vorsatz und Tatbestandsbezug behandeln.

### 12. Kriminalpolitische Implikationen

Die vorstehende Analyse lässt drei kriminalpolitische Schlussfolgerungen zu. Erstens wäre eine – auch nur stillschweigende – Ausdehnung des § 25 Abs. 1 Alt. 2 StGB auf technische Durchführungsmittel kriminalpolitisch kontraproduktiv. Sie würde die Bestimmtheit des Beteiligungssystems untergraben und den Weg zu einer diffusen „Projektverantwortlichkeit“ für Cybercrime-Infrastrukturen ebnen, die mit dem Schuldprinzip schwer vereinbar ist. Der rechtsstaatliche Preis einer solchen Abkürzung stünde in keinem Verhältnis zum kriminalpolitischen Ertrag, zumal die bestehenden dogmatischen Instrumente – unmittelbare Täterschaft durch Werkzeuggebrauch, Mittäterschaft bei arbeitsteiligen Modellen, Teilnahme und punktuelle Vorbereitungstatbestände – eine lückenlose und differenzierte Erfassung digitaler Angriffsszenarien ermöglichen.

Zweitens bestätigt die Untersuchung, dass der Gesetzgeber im Bereich der Cyberkriminalität eine bewusste Systementscheidung getroffen hat: Wo Vorverlagerung kriminalpolitisch geboten erscheint, normiert er sie in eigenständigen, tatbestandlich begrenzten Instrumenten (§§ 202c, 303a Abs. 3, 303b Abs. 5 StGB). Dieses legislatorische Signal spricht dagegen, Vorfeldprobleme über eine Überdehnung der Täterfigur zu lösen.

Drittens verdient die forensisch-ermittlungspraktische Dimension Beachtung. Die Attraktivität expansiver Täterkonstruktionen erklärt sich häufig daraus, dass die technische Attribution – also die Zuordnung konkreter Steuerungshandlungen zu identifizierbaren Personen – bei digitalen Angriffen besonders schwierig ist. Die Dogmatik darf jedoch nicht zum Ersatz für forensische Aufklärung werden. Kriminalpolitisch wäre es daher vorzugswürdig, in den Ausbau technischer Ermittlungskapazitäten und in die Konkretisierung der Zurechnungskriterien (Werkzeuggebrauch, objektive Zurechnung) zu investieren, statt

die Zurechnungsgrenzen des Beteiligungssystems aufzuweichen. Auch die europäische Dimension ist in den Blick zu nehmen: Da Botnet-Infrastrukturen regelmässig grenzüberschreitend operieren, stellt sich die Frage, ob eine Harmonisierung der beteiligungsrechtlichen Zurechnungsmassstäbe im europäischen Strafrecht – etwa im Rahmen der Cybercrime-Konvention oder künftiger EU-Richtlinien – kriminalpolitisch geboten ist.

### 13. Schlussbemerkung: Dogmatische Ökonomie und Begriffsdisziplin

Die vorgeschlagene Begrenzung ist nicht „dogmatischer Formalismus“, sondern Ausdruck dogmatischer Ökonomie. § 25 Abs. 1 Alt. 2 StGB erfüllt eine spezifische Funktion: die Täterzurechnung über eine Person als defizitäres oder untergeordnetes Ausführungs-Zwischenglied. Wird diese Funktion auf technische Prozesse ausgedehnt, verschiebt sich die Zurechnungsarbeit in eine begriffliche Zone, in der die klassischen Konturen wie Defekt, Herrschaft über eine Person oder Verantwortungsgefälle fehlen. Die Folge ist nicht mehr „Modernität“, sondern Unschärfe. Umgekehrt zeigt der digitale Kontext, dass das Strafrecht über hinreichende Instrumente verfügt: unmittelbare Täterschaft über Werkzeuggebrauch, objektive Zurechnung, Mittäterschaft/Teilnahme für arbeitsteilige Rollenbeiträge sowie punktuelle Vorbereitungstatbestände. Die Aufgabe der Dogmatik besteht darin, diese Instrumente konsequent am tatbestandlichen Kerngeschehen auszurichten und Zurechnung transparent zu begründen. Genau darin liegt der rechtsstaatliche Mehrwert einer begriffsdisziplinierten Lösung.

## VI. Ergebnis: Kriterien und Grenzen

Die Untersuchung hat gezeigt, dass § 25 Abs. 1 Alt. 2 StGB eine personenbezogene Zurechnungsfigur ist und bleibt. Der Wortlaut „durch einen anderen“ meint einen menschlichen Tatmittler, dessen Defektlage oder strukturelle Unterordnung die Tatherrschaft des Hintermannes begründet. Kompromittierte Systeme – Botnetze, Skripte, autonome Routinen – erfüllen diese Voraussetzung nicht. Ihnen fehlt die Eigenschaft, Adressat einer Willensherrschaft zu sein; sie irren nicht, handeln nicht vorsätzlich und tragen kein normatives Defizit. Die Gleichsetzung technischer Ausführungsmittel mit Tatmittlern würde daher die Grenze zwischen Auslegung und Analogie überschreiten und die Begrenzungsfunktion des Beteiligungssystems preisgeben.

Digitale Angriffe über automatisierte Prozesse sind vielmehr als unmittelbare Täterschaft gemäß § 25 Abs. 1 Alt. 1 StGB einzuordnen. Der Täter begeht die Tat selbst, indem er den tatbestandsrelevanten technischen Prozess in Gang setzt und steuert – sei es durch das Ausbringen von Schadcode, das Konfigurieren einer Paketflut oder das Aktivieren einer Verschlüsselungsroutine. Dass die Ausführung sodann automatisiert erfolgt, ändert an der Täterqualität nichts; es verlagert die normative Arbeit lediglich in die objektive Zurechnung, die abweichende oder exzessive Verläufe als Frage der Risikoverwirklichung und des

Schutzzwecks der Norm behandelt. Echte mittelbare Täterschaft bleibt hingegen den Konstellationen vorbehalten, in denen ein menschlicher Intermediär tatbestandsrelevant handelt – etwa beim Social Engineering, bei irrtumsbedingter Ausführung oder unter Zwangslagen. Nur dort ist das Zurechnungsmodell des § 25 Abs. 1 Alt. 2 StGB funktional einschlägig.

Auch die Figur der Organisationsherrschaft bietet keinen Anknüpfungspunkt für eine Personalisierung technischer Systeme. Soweit man ihr folgt, setzt sie einen menschlichen Organisationsapparat voraus, in dem der Hintermann organisationsbezogene Rahmenbedingungen ausnutzt und die Tatbestandsverwirklichung durch austauschbare Ausführende regelhaft auslöst. Ein Botnetz aus kompromittierten Endgeräten ist kein solcher Apparat; die Regelmäßigkeit eines Programms ist keine organisatorische Struktur im Sinne der Rechtsprechung. Für die §§ 303a, 303b StGB bestätigt sich dieser Befund in besonderer Weise: Die automatisierte Ausführung einer Datenveränderung oder Computersabotage spricht nicht für mittelbare Täterschaft, sondern für eine präzise Bestimmung des tatbestandlichen Kerngeschehens und eine daran ausgerichtete Versuchsschwelle. Der Gesetzgeber hat im digitalen Bereich bewusst eigenständige Vorbereitungstatbestände geschaffen (§§ 202c, 303a Abs. 3, 303b Abs. 5 StGB); eine

Umgehung dieser Systementscheidung über § 25 Abs. 1 Alt. 2 StGB wäre dogmatisch nicht zu rechtfertigen.

Im Ergebnis ist eine „Software-Mittäterschaft“ oder „mittelbare Täterschaft durch Systeme“ dogmatisch verzichtbar und systematisch riskant. Das Strafrecht verfügt mit der unmittelbaren Täterschaft über Werkzeuggebrauch, der objektiven Zurechnung, der Mittäterschaft und Teilnahme für arbeitsteilige Rollenbeiträge sowie den punktuellen Vorbereitungstatbeständen über ein hinreichend differenziertes Instrumentarium, das digitale Angriffsszenarien erfasst, ohne die personenbezogene Struktur des Beteiligungssystems aufzugeben.

Kriminalpolitisch ergibt sich aus der Untersuchung, dass das Beteiligungssystem des StGB auch im Zeitalter automatisierter Angriffstechniken keiner strukturellen Erweiterung bedarf. Die Begrenzung der mittelbaren Täterschaft auf personale Vermittlung ist kein dogmatischer Formalismus, sondern rechtsstaatliche Notwendigkeit, die das Bestimmtheitsgebot und die schuldangemessene Individualisierung strafrechtlicher Verantwortung sichert. Wo kriminalpolitischer Handlungsbedarf besteht, ist er auf der Ebene deliktsspezifischer Vorbereitungstatbestände und forensischer Ermittlungskapazitäten – nicht aber durch eine Ausdehnung des Täterbegriffs – zu adressieren.

# Die heimliche Verabreichung von K.O.-Tropfen de lege lata und de lege ferenda – Zur Einordnung als Tatmittel und zum Reformbedarf infolge des Beschlusses BGH 5 StR 382/24

von Linda Tiggemann\*

## Abstract

Die heimliche Verabreichung von K.O.-Tropfen zur Begehung von Sexual- und Raubdelikten ist eine besonders gefährliche und schwer nachweisbare Form der Straftat. Der Beschluss des BGH vom 8. Oktober 2024 (5 StR 382/24) grenzt K.O.-Tropfen restriktiv vom Begriff des „gefährlichen Werkzeugs“ i.S.d. §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB aus und führt begründend insbesondere den Wortlaut an. Der Aufsatz prüft die dogmatische Überzeugungskraft des Beschlusses, erörtert den Reformbedarf und setzt sich kritisch mit den Gesetzentwürfen von Bundesrat sowie BMJV auseinander. Erforderlich erscheint eine kohärente Neubestimmung des Tatmittelbegriffs im StGB, flankiert durch effektive Präventions- und Aufklärungsmaßnahmen.

*The secret administration of knockout drops to commit sexual and robbery offences is a particularly dangerous and difficult-to-prove way of committing a crime. The decision of the German Federal Court of Justice ruled on 8 October 2024 (5 StR 382/24) categorically excludes knockout drops from the definition of “dangerous tool” within the meaning of Sections 177 (8) No. 1 and 250 (2) No. 1 of the German Criminal Code, mainly based on the legislative language. This article explores the doctrinal strength of the decision, discusses the need for reform, and critically assesses the draft bills proposed by the Federal Council and the Federal Ministry of Justice and Consumer Protection. A clear redefinition of the concept of “instrument of crime” in the German Criminal Code seems necessary, along with more effective prevention and awareness-raising measures.*

## I. Einleitung

„Chemische Unterwerfung“ – dieses besonders perfide Phänomen ist spätestens durch das aufsehenerregende Strafverfahren um *Gisèle Pelicot* im französischen Avignon in das Bewusstsein der Öffentlichkeit gerückt.<sup>1</sup> Der

Begriff der chemischen Unterwerfung bezeichnet die gezielte und heimliche Verabreichung sedierender Substanzen, sog. K.O.-Tropfen,<sup>2</sup> mit dem Ziel, das Opfer für die Begehung darauffolgender Straftaten (i.d.R. Sexualdelikte, aber auch Raubdelikte)<sup>3</sup> handlungsunfähig zu machen und dessen Bewusstsein zu beeinträchtigen oder sogar auszuschalten.<sup>4</sup>

Der Begriff „K.O.-Tropfen“ umfasst sämtliche flüssigen oder in Flüssigkeit gelösten Substanzen, die das Bewusstsein beeinträchtigen können.<sup>5</sup> Da das Opfer nicht argwöhnisch werden soll, sind farb-, geruch- und geschmacklose Substanzen für Täter besonders attraktiv.<sup>6</sup> Obwohl dieses Phänomen keineswegs neu ist,<sup>7</sup> verliert es nicht an Aktualität. Die Methoden sind ebenso vielfältig wie heimtückisch: Substanzen wie Gamma-Hydroxybuttersäure (GHB) oder Benzodiazepine werden unbemerkt Getränken oder Speisen beigemischt oder auch per Infusion verabreicht.<sup>8</sup> Nur wenige Milliliter können zu Bewusstlosigkeit, Atemdepression, Gedächtnisverlust oder gar zum Tod führen.<sup>9</sup>

Zugleich entzieht sich das Ausmaß des Problems weitgehend einer verlässlichen quantitativen Erfassung. Die heimliche Verabreichung von K.O.-Tropfen wird in der Polizeilichen Kriminalstatistik nicht erfasst, da von einer derart hohen Dunkelziffer ausgegangen wird, dass die Zahlen eine verzerrte und wenig aufschlussreiche Darstellung liefern würden.<sup>10</sup> Neben der kurzen Nachweisbarkeit der Stoffe verfälscht der typische Begleitkonsum von Alkohol oder Drogen eine Erfassung zusätzlich.<sup>11</sup> Zudem bleibt ein erheblicher Teil der Vorfälle ungemeldet. Dennoch zeigt sich ein Trend zunehmender Fallzahlen auf Bundesebene.<sup>12</sup> In Anbetracht steigender Gewalt gegen Frauen sind dies ernstzunehmende Entwicklungen.<sup>13</sup>

Vor diesem Hintergrund stellt sich die Frage, ob das geltende Strafrecht die heimliche Verabreichung von K.O.-Tropfen tatbestandlich angemessen erfasst. Insbesondere

\* Linda Tiggemann ist Wissenschaftliche Mitarbeiterin am Lehrstuhl für Strafrecht und Strafprozessrecht von Prof. Dr. Dr. h.c. (UG Tiflis) Martin Waßmer.

<sup>1</sup> Vgl. Schläfer, Hat die Scham die Seite gewechselt?, FAZ, online abrufbar unter: <https://bit.ly/41lgQOP> (zuletzt abgerufen am 17.3.2026).

<sup>2</sup> K.O. von engl. „knock out“, dt. etwa: „außer Gefecht setzen“, „kampfunfähig machen“, vgl. Duden Wörterbuch, Stichwort „k.o.“, online abrufbar unter: [https://www.duden.de/rechtschreibung/k\\_o](https://www.duden.de/rechtschreibung/k_o) (zuletzt abgerufen am 17.3.2026).

<sup>3</sup> Neuhaus/Artkämper/Weise, Kriminaltechnik und Beweisführung im Strafverfahren, 2. Aufl. (2024), Rn. 449.

<sup>4</sup> Bicker, SIAK-Journal 3/2015, 13 (13).

<sup>5</sup> Köhler, Kriminalistik 2017, 564 (564).

<sup>6</sup> Köhler, Kriminalistik 2017, 564 (564).

<sup>7</sup> Siehe bspw. BGH, NStZ-RR 1996, 100.

<sup>8</sup> Siehe bspw. BGH, NStZ-RR 2019, 43; BGH, NJW 2024, 3735.

<sup>9</sup> Bicker, SIAK-Journal 3/2015, 13 (19); Neuhaus/Artkämper/Weise, Kriminaltechnik und Beweisführung im Strafverfahren, Rn. 450.

<sup>10</sup> Jahn, JuS 2025, 276 (277).

<sup>11</sup> Jahn, JuS 2025, 276 (277).

<sup>12</sup> SWR, Polizei in BW erfasst mehr Straftaten mit K.O.-Tropfen, online abrufbar unter: <https://bit.ly/4rZ0sic> (zuletzt abgerufen am 17.3.2026); Süddeutsche, Zahl der Straftaten mit Einsatz von K.-o.-Tropfen gestiegen, online abrufbar unter: <https://bit.ly/3PhOD98> (zuletzt abgerufen am 17.3.2026).

<sup>13</sup> BKA, Bundeslagebilder – Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024, online abrufbar unter: <https://bit.ly/4tuiPwD> (zuletzt abgerufen am 17.3.2026); LT-Drs. BaWü 17/7535, S. 5: in Baden-Württemberg sind etwa 80 % der Opfer Frauen.

der Beschluss des *BGH* vom 8. Oktober 2024 (5 StR 382/24), der K.O.-Tropfen nicht als „gefährliches Werkzeug“ i.S.d. §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB einordnet, hat diese Diskussion neu entfacht. Der vorliegende Beitrag untersucht die dogmatische Tragfähigkeit dieser Rechtsprechung, analysiert den daraus resultierenden Reformbedarf und bewertet aktuelle gesetzgeberische Lösungsansätze.

## II. Bedarf einer Gesetzesänderung

### 1. Analyse des Beschlusses des *BGH* (5 StR 382/24)

#### a) Inhalt des Beschlusses

Die heimliche Verabreichung von K.O.-Tropfen im Rahmen von Sexual- und Raubdelikten ist im aktuellen Strafrecht insbesondere von §§ 177, 250 StGB erfasst. In dem Beschluss vom 8. Oktober 2024 (5 StR 382/24) entschied der *BGH*, dass K.O.-Tropfen nicht unter das „gefährliche Werkzeug“ i.S.d. §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB fallen, sodass ein Verwenden von K.O.-Tropfen lediglich die §§ 177 Abs. 7 Nr. 2, 250 Abs. 1 Nr. 1 lit. b StGB erfüllt. Diese stellen das Beisichführen eines Mittels unter Strafe, das der Verhinderung oder Überwindung des Widerstandes einer anderen Person durch Gewalt oder Drohung mit Gewalt dient.

Begründend führte der *BGH* insbesondere den Wortlaut der Normen an. Würde der Werkzeugbegriff auch auf Flüssigkeiten ausgedehnt, überschreite dies die Wortlautgrenze und verletze den Bestimmtheitsgrundsatz aus Art. 103 Abs. 2 GG.<sup>14</sup> Teleologische Erwägungen des *LG Dresden* (Vorinstanz) dahingehend, dass GBL bspw. dem Schlag mit einem Holzknüppel<sup>15</sup> in der Gefährlichkeit in nichts nachstehe und daher beide Mittel als gefährliche Werkzeuge zu qualifizieren seien, könnten nicht die Wortlautgrenze und damit den Bestimmtheitsgrundsatz umgehen.<sup>16</sup> Eine teleologische Erweiterung des Werkzeugbegriffs entgegen dem Wortlaut auch auf Flüssigkeiten verbiete sich daher.<sup>17</sup>

In vergangenen Entscheidungen zu § 250 Abs. 2 Nr. 1 StGB lehnte der *BGH* die Einordnung von K.O.-Tropfen als gefährliches Werkzeug zwar ab, schloss jedoch nicht aus, diese dennoch als gefährliches Werkzeug einzuordnen, sofern sie in höherer Dosierung verwendet werden

und daher zu erheblichen Gesundheitsrisiken für das Opfer führen.<sup>18</sup> Auf die Kriterien der Körperlichkeit oder äußeren Wirkweise ging der *BGH* in diesem Fall nicht ein, sondern erwähnte als maßgebliches Kriterium die Dosierung und die damit einhergehende Gefährlichkeit.<sup>19</sup> Davon wendet sich der Senat nun ausdrücklich ab.<sup>20</sup> Die Gefährlichkeit der Substanz könne eine Einordnung als gefährliches Werkzeug nicht begründen, denn sie scheide bereits aufgrund ihrer fehlenden Festigkeit als potenzielles „Werkzeug“ aus.<sup>21</sup>

Auch die Pipette, mithilfe derer die Tropfen in die Gläser der Opfer gegeben wurden, ist nach Ansicht des *BGH* kein gefährliches Werkzeug.<sup>22</sup> Zur Begründung zieht er eine Parallele zu § 224 Abs. 1 Nr. 2 StGB. § 177 Abs. 8 Nr. 1 StGB sei an § 224 Abs. 1 Nr. 2 StGB angelehnt, sodass die Auslegung gleich erfolgen müsse.<sup>23</sup> In § 224 Abs. 1 Nr. 2 StGB muss die Körperverletzung „mittels“ des gefährlichen Werkzeugs begangen werden.<sup>24</sup> Dies ist nach st. Rspr. der Fall, wenn die Körperverletzung durch ein Tatmittel herbeigeführt wird, das äußerlich unmittelbar auf den Körper des Opfers einwirkt.<sup>25</sup> Ein Gegenstand ist gefährlich, wenn er im konkreten Fall dazu geeignet ist, erhebliche körperliche Schäden unmittelbar zu verursachen.<sup>26</sup> Bei Flüssigkeiten komme eine Einordnung als gefährliches Werkzeug lediglich dann in Betracht, wenn die Flüssigkeit durch einen Gegenstand auf den Körper gerichtet und auf diese Weise mit ihm in Verbindung gebracht werde.<sup>27</sup> Es brauche eine unmittelbare Einwirkung von außen.<sup>28</sup> Die Pipette sei allerdings lediglich Dosierungshilfe, mithilfe derer die Substanz mittelbar mit dem Körper der Opfer in Verbindung gebracht werde.<sup>29</sup> Ihre gesundheitsschädigende Wirkung entfalte die Substanz erst nach Konsum und Verstoffwechselung.<sup>30</sup>

Der *Senat* verneint ein Spezialitätsverhältnis zwischen § 224 Abs. 1 Nr. 1 und Nr. 2 StGB.<sup>31</sup> Dementsprechend könne eine Einordnung von K.O.-Tropfen als gefährliches Werkzeug nicht mit der Begründung erfolgen, ein gesundheitsschädlicher Stoff sei stets auch ein gefährliches Werkzeug, wobei § 224 Abs. 1 Nr. 1 StGB lex specialis zu § 224 Abs. 1 Nr. 2 StGB sei.<sup>32</sup> Diese Trennung zwischen gesundheitsschädlichen Stoffen und gefährlichen Werkzeugen gelte ebenfalls für die an § 224 Abs. 1 Nr. 2 StGB angelehnten §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB,<sup>33</sup> auch wenn die Beibringung gesundheitsschädlicher Stoffe in §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 S. 1 StGB nicht erfasst ist.

<sup>14</sup> Vgl. *Hardtung*, in: MüKo-StGB, 5. Aufl. (2025), § 224 Rn. 15 m.w.N.; ebenso *Grünwald*, in: LK-StGB, 13. Aufl. (2023), § 224 Rn. 20.

<sup>15</sup> Das *LG Dresden* verweist auf BGHSt 1, 1, in dem sowohl Salzsäure als auch ein Holzknüppel als gefährliche Werkzeuge eingeordnet worden seien. Der *Senat* stellt in *BGH*, NJW 2024, 3735 (3737) jedoch klar, dass im damaligen Fall die Salzsäure mit einem Topf ins Gesicht geschüttet wurde, der in dem Fall maßgeblich gewesen sei.

<sup>16</sup> *BGH*, NJW 2024, 3735 (3737).

<sup>17</sup> *BGH*, NJW 2024, 3735 (3737).

<sup>18</sup> Vgl. *BGH*, BeckRS 1998, 30019351; *BGH*, NStZ-RR 2018, 141 (141).

<sup>19</sup> Vgl. *BGH*, BeckRS 1998, 30019351; *BGH*, NStZ-RR 2018, 141 (141).

<sup>20</sup> *BGH*, NJW 2024, 3735 (3735).

<sup>21</sup> *BGH*, NJW 2024, 3735 (3735).

<sup>22</sup> *BGH*, NJW 2024, 3735 (3736 f.).

<sup>23</sup> *BGH*, NJW 2024, 3735 (3736 f.).

<sup>24</sup> St. Rspr.; vgl. zuletzt etwa BGHSt 63, 138 (153); *BGH*, BeckRS 2023, 23529 Rn. 17, jew. m.w.N.

<sup>25</sup> St. Rspr.; vgl. zuletzt etwa BGHSt 63, 138 (153); *BGH*, BeckRS 2023, 23529 Rn. 17, jew. m.w.N.

<sup>26</sup> St. Rspr.; vgl. zuletzt etwa BGHSt 63, 138 (153); *BGH*, BeckRS 2023, 23529 Rn. 17, jew. m.w.N.

<sup>27</sup> *BGH*, NJW 2024, 3735 (3736).

<sup>28</sup> Vgl. *BGH*, NStZ-RR 2011, 275 (276); *BGH*, NStZ-RR 2012, 308; *Grünwald*, in: LK-StGB, § 224 Rn. 20; *Hardtung*, in: MüKo-StGB, § 224 Rn. 15; *Sternberg-Lieben*, in: TK-StGB, 31. Aufl. (2025), § 224 Rn. 6 m.w.N.

<sup>29</sup> *BGH*, NJW 2024, 3735 (3736).

<sup>30</sup> *BGH*, NJW 2024, 3735 (3736).

<sup>31</sup> *BGH*, NJW 2024, 3735 (3736).

<sup>32</sup> *BGH*, NJW 2024, 3735 (3736).

<sup>33</sup> *BGH*, NJW 2024, 3735 (3736 f.).

Die restriktive Auslegung des Werkzeugbegriffs stehe einer angemessenen Sanktionierung nicht entgegen.<sup>34</sup> Im Fall einer heimlichen Verabreichung sedierender Substanzen sei § 177 Abs. 7 Nr. 2 StGB (bzw. § 250 Abs. 1 Nr. 1 lit. b StGB) erfüllt, der bereits das Beisichführen solcher Mittel erfasse.<sup>35</sup> Dies hat zwar lediglich ein Mindeststrafmaß von drei Jahren statt wie bei § 177 Abs. 8 Nr. 1 StGB fünf Jahren zur Folge. Der Gesetzgeber habe jedoch bzgl. der Strafobergrenze zwischen den Absätzen 7 und 8 nicht differenziert.<sup>36</sup> Für die Verwirklichung beider Tatmodalitäten könne eine Höchststrafe von 15 Jahren Freiheitsstrafe verhängt werden (vgl. § 38 Abs. 2 StGB). Dem Rechtsanwender bleibe somit trotz restriktiver Auslegung des Werkzeugbegriffs die Möglichkeit, den erhöhten Unrechtsgehalt einer tatsächlichen Verwendung solcher Substanzen sowie ggf. erschwerender Umstände wie einer bestehenden Alkoholisierung des Opfers durch Ausschöpfung des Strafrahmens zu berücksichtigen.<sup>37</sup>

#### b) Kritische Würdigung des Beschlusses

Das Erfordernis einer unmittelbaren Einwirkung der Flüssigkeit mittels eines Gegenstandes von außen auf den Körper<sup>38</sup> stößt in der Literatur auf Kritik. Es wird zutreffend darauf hingewiesen, dass sich aus naturwissenschaftlicher Sicht die Wirkung einer Flüssigkeit auf den menschlichen Körper nicht stets in eine Wirkung auf das Körperäußere und -innere aufteilen lässt.<sup>39</sup> Als Beispiel kann Pfefferspray angeführt werden, das sowohl äußerlich auf die Augen als auch innerlich auf die Atemwege wirkt.<sup>40</sup> Teile der Literatur regen daher an, eine Unterscheidung derart vorzunehmen, dass gesundheitsschädliche Stoffe jene seien, die einen selbstständigen gesundheitsschädigenden Vorgang im Körper in Gang setzten, unabhängig davon, wie der Stoff in den Organismus gelangt sei.<sup>41</sup> Dies könne auf biologischem, chemischem, thermischem oder elektrischem Wege erfolgen.<sup>42</sup> Wenn das Mittel hingegen mechanisch-kinetisch wirke, ohne dass es auf weitere körperliche Mechanismen oder eine Reaktion mit körpereigenen Stoffen ankomme, liege keine Beibringung eines gesundheitsschädlichen Stoffes vor.<sup>43</sup> Auch wenn diese Herangehensweise nicht frei von Abgrenzungsschwierigkeiten ist,<sup>44</sup> erscheint sie im Vergleich zu einer pauschalen Unterscheidung nach äußerer und innerer Wirkung überzeugend, da sie die tatsächlichen Auswirkungen des Stoffes

in den Blick nimmt und sich nicht lediglich am Wirkort orientiert.

Der BGH ließ in der Vergangenheit ausdrücklich offen, ob Flüssigkeiten als gefährliche Werkzeuge eingestuft werden können.<sup>45</sup> So wurde das Vorliegen eines gefährlichen Werkzeugs bejaht, wobei unerheblich sei, ob die Reini-  
gerflüssigkeit oder die Sprühflasche<sup>46</sup> bzw. das Narkotikum oder der Katheter<sup>47</sup> dem Werkzeugbegriff unterfielen. Auf letztere Entscheidung nimmt der Senat ausdrücklich Bezug und stimmt dem Vorliegen eines gefährlichen Werkzeugs bei der Gabe einer Infusion mit einem Narkotikum durch einen Krankenpfleger zu, da der Katheter dabei (wie für das Vorliegen der Unmittelbarkeit gefordert) direkten Kontakt zum Körper des Opfers hatte.<sup>48</sup> Ob bei einer Infusion mit einem Narkotikum das Vorliegen einer unmittelbaren Einwirkung von außen mit der Verwendung eines Katheters begründet werden kann, während das Mittel im Körper vollständig das Bewusstsein ausschaltet, kann jedenfalls angezweifelt werden. Aus einer Verneinung der Werkzeugeigenschaft ergäbe sich das missliche Ergebnis, dass das anzuwendende Mindeststrafmaß letztlich von Zufälligkeiten abhänge, etwa davon, ob der Pfleger den Katheter selbst gelegt hat und damit Unmittelbarkeit i.S.d. § 177 Abs. 8 Nr. 1 StGB gegeben ist oder ob er den Umstand ausnutzte, dass dem Opfer bereits ein Verweilkatheter gelegt war, an den er die Infusion anschließen konnte.<sup>49</sup> In letzterem Fall wäre dann lediglich eine Strafbarkeit nach § 177 Abs. 7 Nr. 2 StGB mit einem Mindeststrafmaß von drei Jahren gegeben.

Gerade in den Fällen, in denen der Gegenstand bloßes Mittel zur Verbringung des Stoffes in (oder auf)<sup>50</sup> den Körper des Opfers ist, so wie es bei einem Träufeln in den Mund und einer Gabe per Infusion der Fall ist, leuchtet nicht ein, weshalb auf den Gegenstand als gefährliches Werkzeug abzustellen sein sollte.<sup>51</sup> Ob das Opfer das Mittel gespritzt, in sein Getränk oder unmittelbar aus der Pipette in den Mund geträufelt bekommt, kann keinen Unterschied machen.<sup>52</sup> Es handelt sich dabei lediglich um unterschiedliche Arten der Verabreichung des Stoffes.<sup>53</sup> Ein Abstellen auf das Gefäß ist zu unterlassen, wenn die gefährliche Wirkung eindeutig von der Substanz selbst ausgeht.<sup>54</sup> Eine Abgrenzung anhand der Körperlichkeit des Tatmittels erscheint dann wenig sinnvoll, da sich für na-

<sup>34</sup> BGH, NJW 2024, 3735 (3737).

<sup>35</sup> BGH, NJW 2024, 3735 (3737).

<sup>36</sup> BGH, NJW 2024, 3735 (3737).

<sup>37</sup> BGH, NJW 2024, 3735 (3737).

<sup>38</sup> BGH, NJW 2024, 3735 (3736).

<sup>39</sup> Bosch, JURA 2025, 225.

<sup>40</sup> Jesse, NStZ 2009, 364 (365 f.), der Pfefferspray i.E. wegen des Einsatzes des Geräts und dessen Gefährlichkeit dennoch als gefährliches Werkzeug einordnet.

<sup>41</sup> Pschorr/Gmelin, ZfStw 2024, 318 (321); dieses Kriterium stellen die Autoren allerdings nur für die Abgrenzung zwischen § 224 Abs. 1 Nr. 1 und Nr. 2 StGB auf, da aus ihrer Sicht der Werkzeugbegriff in § 177 Abs. 8 Nr. 1 StGB unabhängig von § 224 Abs. 1 StGB auszulegen sei.

<sup>42</sup> Krüger, NStZ, 2019, 273 (275); vgl. näher Krüger/Maurer, JA 2018, 321, (323).

<sup>43</sup> Pschorr/Gmelin, ZfStw 2024, 318 (322); so etwa auch Krüger, NStZ 2019, 273 (275); vgl. näher Krüger/Maurer, JA 2018, 321 (323).

<sup>44</sup> Der BGH selbst führte in BGH, NJW 2008, 2861 (2863) aus, dass „mit den Mitteln herkömmlicher Auslegungstechnik eine umfassende, sachgerechte Lösung für alle denkbaren Einzelfälle nicht zu erreichen ist“.

<sup>45</sup> Siehe bspw. BGH, BeckRS 2004, 1729 Rn. 13; 2018, 4886 Rn. 4.

<sup>46</sup> BGH, NStZ-RR 2011, 275 (276).

<sup>47</sup> BGH, NStZ-RR 2019, 43.

<sup>48</sup> BGH, NJW 2024, 3735 (3736) unter Verweis auf BGH, NStZ 2019, 273.

<sup>49</sup> Krüger, NStZ 2019, 273 (274).

<sup>50</sup> Siehe bspw. BGHSt 1, 1.

<sup>51</sup> Ruppert, JR 2025, 193 (195).

<sup>52</sup> Pschorr/Gmelin, ZfStw 2024, 318 (321).

<sup>53</sup> Ruppert, JR 2025, 193 (195).

<sup>54</sup> Ruppert, JR 2025, 193 (195).

hezu jede Flüssigkeit ein entsprechendes Werkzeug finden lässt.<sup>55</sup> Die Flüssigkeit selbst ist die relevante Substanz, unabhängig davon, wie sie dem Körper des Opfers beigebracht wird, sodass auf diese als maßgebliches Tatmittel abzustellen ist.

Zwar ist der Wortlaut nicht das allein maßgebliche Auslegungskriterium; er markiert allerdings die äußerste Grenze jeder zulässigen Interpretation.<sup>56</sup> Obwohl der Begriff „Werkzeug“ meist für Gegenstände verwendet wird, die im Werkzeugkasten zu finden sind, hat das Wort im allgemeinen Sprachgebrauch auch andere Verwendung. So können bspw. Menschen, die von Dritten instrumentalisiert werden, als Werkzeuge bezeichnet werden („Sie wurde zum Werkzeug einer politischen Agenda.“).<sup>57</sup> Eine etymologische Zerlegung des Wortes in seine Bestandteile „Werk“ und „Zeug“ legt nahe, dass lediglich feste Gegenstände unter den Begriff fallen. Mit dem Begriff „Zeug“ wird eine unbestimmte Vielzahl an Dingen bezeichnet, die es nicht wert sind, genauer benannt zu werden.<sup>58</sup> Unter „Dingen“ werden wiederum körperliche Gegenstände verstanden.<sup>59</sup> Flüssigkeiten sind mangels Körperlichkeit somit gerade nicht als „Zeug“ einzuordnen. Der Wortbestandteil „Werk“ bedeutet so viel wie Arbeit, Tat oder Handlung.<sup>60</sup> Daraus lässt sich schließen, dass ein Werkzeug ein Objekt ist, das einer Handlung dienlich sein kann. Es muss sich somit jedenfalls um einen körperlich greifbaren Gegenstand handeln. Teleologische Erwägungen dahingehend, die Verwendung von K.O.-Tropfen sei für das Opfer gleich oder gar gefährlicher als die Verwendung eines gefährlichen Werkzeugs, können die Wortlautgrenze nicht überwinden. Eine Einordnung sedierender Substanzen als gefährliche Werkzeuge lässt sich auf diese Weise nicht rechtfertigen.

Obwohl bei der Abgrenzung die Orientierung an der Wirkweise und nicht am Wirkort des Stoffes vorzugswürdig erscheint und stets auf das Tatmittel abzustellen ist, von dem maßgeblich die Gefährlichkeit für das Opfer ausgeht, so ist der Entscheidung des BGH dahingehend, dass bei einer Subsumtion von Flüssigkeiten unter den Begriff des gefährlichen Werkzeugs die Wortlautgrenze überschritten ist, i.E. dennoch zuzustimmen.

## 2. Reformbedarf

Ungeachtet der dogmatischen Überzeugungskraft der Entscheidung des BGH wird vereinzelt die Auffassung vertreten, die Verneinung der Werkzeugeigenschaft von K.O.-Tropfen sowie der Pipette wirke im Hinblick auf die steigende öffentliche Sensibilität gegenüber dem Missbrauch sedierender Substanzen nicht zeitgemäß.<sup>61</sup> Die Verweisung des BGH auf dieselbe Strafobergrenze der §§ 177 Abs. 7 Nr. 2, 250 Abs. 1 Nr. 1 lit. b StGB wirkt, als versuche der Senat zu kaschieren, dass die heimliche Sedierung des Opfers auf Tatbestandsebene nicht ausreichend gewürdigt wird. Der BGH scheint sich dieses Missstandes bewusst zu sein. Denn der ausdrückliche Verweis auf eine mögliche hohe Strafzumessung erfolgt direkt im Anschluss an die abschließende Einordnung. Problematisch ist eine niedrige Strafuntergrenze insbesondere, weil sie Richterinnen und Richter i.d.R. als Ausgangspunkt für die Strafzumessung dient.<sup>62</sup> Erschwerend kommt hinzu, dass strafgerichtliche Entscheidungen nicht in hinreichend transparenter Weise veröffentlicht werden, sodass bundesweit eine jedenfalls in etwa einheitliche Strafzumessung für Tatbegehungen mittels K.O.-Tropfen nicht erkennbar ist.<sup>63</sup> Wenn doch die heimliche Sedierung denselben oder jedenfalls einen vergleichbaren Unrechtsgehalt aufweist wie die Tatbegehung mittels eines gefährlichen Werkzeugs, dann wäre die Angleichung der Strafuntergrenze nur folgerichtig. Der Gesetzgeber ist daher gehalten, auf Tatbestandsebene nachzuschärfen, um der besonderen Gefährlichkeit, Unkontrollierbarkeit und Heimtücke solcher Taten Rechnung zu tragen.

Die Möglichkeit der Anordnung eines minder schweren Falls nach §§ 177 Abs. 9, 250 Abs. 3 StGB ermöglicht dabei eine Eingehung auf atypische Einzelfälle, in denen eine Freiheitsstrafe von fünf Jahren unverhältnismäßig erscheint. Dass diese Korrekturfunktion zu einer regelmäßigen Umgehung des erhöhten Mindeststrafrahmens führen könnte,<sup>64</sup> erscheint angesichts des erheblichen Unrechtsgehalts der Tatbegehung fernliegend. Zwar ist ein Mindeststrafmaß von fünf Jahren beachtlich, doch schützen die einschlägigen Normen mit der körperlichen Unversehrtheit und der sexuellen Selbstbestimmung auch bedeutende Rechtsgüter.<sup>65</sup> Dem Einwand, eine Erhöhung des Mindeststrafmaßes sei entbehrlich, da besonders gravierende Fälle bereits von §§ 177 Abs. 8 Nr. 2 lit. b, 250

<sup>55</sup> Pschorr/Gmelin, ZfStw 2024, 318 (321).

<sup>56</sup> Frister, Strafrecht AT, 10. Aufl. (2023), § 4 Rn. 25 f.

<sup>57</sup> Vgl. DWDS, Stichwort „Werkzeug“, online abrufbar unter: <https://www.dwds.de/wb/Werkzeug> (zuletzt abgerufen am 17.3.2026).

<sup>58</sup> PONS, Stichwort „Zeug“, online abrufbar unter: <https://de.pons.com/übersetzung-2/deutsche-rechtschreibung/Zeug> (zuletzt abgerufen am 17.3.2026).

<sup>59</sup> Duden Wörterbuch, Stichwort „Ding“, online abrufbar unter: [https://www.duden.de/rechtschreibung/Ding\\_Gegenstand](https://www.duden.de/rechtschreibung/Ding_Gegenstand) (zuletzt abgerufen am 17.3.2026); DWDS, Stichwort „Ding“, online abrufbar unter: <https://www.dwds.de/wb/Ding#1> (zuletzt abgerufen am 17.3.2026); DWDS, Stichwort „Gegenstand“, online abrufbar unter: <https://www.dwds.de/wb/Gegenstand?o=gegenstand> (zuletzt abgerufen am 17.3.2026).

<sup>60</sup> Duden Wörterbuch, Stichwort „Werk“, online abrufbar unter: <https://www.duden.de/rechtschreibung/Werk> (zuletzt abgerufen am 17.3.2026); DWDS, Stichwort „Werk“, online abrufbar unter: <https://www.dwds.de/wb/Werk> (zuletzt abgerufen am 17.3.2026).

<sup>61</sup> Jahn, JuS 2025, 276 (279); Ruppert, JR 2025, 193 (196).

<sup>62</sup> Ehlen/Hoven/Weigend, KriPoZ 2024, 16 (23).

<sup>63</sup> Vgl. Schäffer, Initiative Offene Urteile: Über eine Million Gerichtsentscheidungen sollen öffentlich werden, online abrufbar unter: <https://rsw.beck.de/aktuell/daily/meldung/detail/initiative-offene-urteile-eine-million-gerichtsentscheidungen-open-jur> (zuletzt abgerufen am 17.3.2026).

<sup>64</sup> Davor warnt Neue Richter\*innenvereinigung, Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.o.-Tropfen, S. 3.

<sup>65</sup> Pschorr, Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.-o.-Tropfen, S. 4.

Abs. 2 Nr. 3 lit. b StGB erfasst würden,<sup>66</sup> ist entgegenzuhalten, dass eine konkrete Todesgefahr bei Verabreichung von K.O.-Tropfen nur selten mit der erforderlichen Sicherheit nachweisbar ist.<sup>67</sup> Da das Vorliegen einer Todesgefahr von Umständen wie der konkreten Dosierung und der körperlichen Verfassung des Opfers abhängt, ist das anzuwendende Mindeststrafmaß bei Verwendung von K.O.-Tropfen im Unterschied zur Verwendung eines gefährlichen Werkzeugs ggf. von Zufälligkeiten abhängig.<sup>68</sup>

Eine Anhebung des Mindeststrafmaßes hätte für Teilnehmer, insbesondere Gehilfen, erhebliche Auswirkungen. Die obligatorische Strafmilderung des Gehilfen nach § 27 Abs. 2 StGB richtet sich nach § 49 Abs. 1 StGB. Danach erhöht sich das Mindestmaß der Strafe des Gehilfen von sechs Monaten auf zwei Jahre Freiheitsstrafe, wenn das Mindestmaß beim Haupttäter von drei auf fünf Jahre steigt. Damit bewegt sich das Mindeststrafmaß des Gehilfen bereits an der gesetzlichen Höchstgrenze für eine Bewährungsaussetzung, die nach § 56 Abs. 2 StGB grundsätzlich nur bis zu zwei Jahre möglich ist. Eine Anhebung des Mindeststrafmaßes des Täters würde somit die Wahrscheinlichkeit vollstreckter Freiheitsstrafen für Teilnehmer deutlich erhöhen und den Strafraum insgesamt verschärfen. Dies könnte zu einer Austrocknung des Schwarzmarktes für K.O.-Tropfen beitragen, da Händler als typische Gehilfen ein deutlich höheres persönliches Risiko eingingen. Insgesamt würde eine Anhebung des Mindeststrafmaßes daher nicht nur eine stärkere Sanktionierung der unmittelbaren Täter ermöglichen, sondern auch das Risiko vollstreckter Freiheitsstrafen für Beteiligte erhöhen und damit präventiv auf die gesamte Tatstruktur wirken.

Damit die Anhebung des Mindeststrafrahmens für Fälle der heimlichen Verabreichung von K.O.-Tropfen nicht bloß symbolische Wirkung entfaltet, ist die Umsetzung effektiver Präventionsmaßnahmen sowie eine verbesserte Aufdeckung der Taten unabdingbar. Straferhöhungen wirken meist wenig abschreckend.<sup>69</sup> Vielmehr wirkt sich insbesondere ein gesteigertes Entdeckungsrisiko tatreduzierend aus.<sup>70</sup> Von herausragender Bedeutung ist dabei die Aufklärung der Bevölkerung über das äußerst kurze Zeitfenster, in dem ein toxikologischer Nachweis überhaupt möglich ist. Es braucht ein Zusammenspiel aus der Anhebung des Mindeststrafmaßes und außerstrafrechtlicher Maßnahmen, um das Unrecht auf tatbestandlicher Ebene ausreichend abzubilden und dies auch in die Praxis zu übermitteln.

### III. Lösungsansätze de lege ferenda

#### 1. Reformvorschläge

In der Diskussion stehen aktuell im Wesentlichen zwei Gesetzentwürfe.

##### a) Gesetzentwurf des Bundesrates

Am 25. März 2025 brachte das Land NRW einen Gesetzentwurf in den Bundesrat ein,<sup>71</sup> der am 23. Mai 2025 beschloss, den Entwurf dem Bundestag zuzuleiten.<sup>72</sup> Der Bundestag nahm die geplante Debatte über den Entwurf allerdings von der Tagesordnung des 16. Oktober 2025.<sup>73</sup> Der Entwurf sieht vor, die Tatbestände der §§ 177 Abs. 8, 250 Abs. 2 StGB um eine Nummer zu ergänzen, die das Beibringen von Gift oder anderen gesundheitsschädlichen Stoffen zur Ausführung der Tat umfasst.<sup>74</sup> Ziel ist es, eine Mindeststrafe von fünf Jahren für Sexual- und Raubstrafaten einzuführen, bei denen der Täter das Opfer zuvor durch die Verabreichung von K.O.-Tropfen wehrlos gemacht hat.<sup>75</sup> Auch der Bundesrat sieht die in dieser Tatbegehung liegende hinterlistige Vorgehensweise und Gefährlichkeit für die Opfer im Mindeststrafmaß nicht ausreichend berücksichtigt.<sup>76</sup> Die Formulierung „zur Ausführung der Tat“ ist §§ 243 Abs. 1 S. 2 Nr. 1, 244 Abs. 1 Nr. 3 StGB entlehnt. Vom Vorsatz des Täters muss umfasst sein, dass die Beibringung gerade die Begehung der Sexual- oder Raubstrafat ermöglicht, was die Beweisführung deutlich erschweren dürfte.<sup>77</sup> Die heimliche Verabreichung von K.O.-Tropfen stelle nach gefestigter Rechtsprechung die Beibringung eines gesundheitsschädlichen Stoffes gem. § 224 Abs. 1 Nr. 1 StGB dar,<sup>78</sup> weshalb durch die geplante Gesetzesänderung gerade diese Tatbegehung erfasst sei.

##### b) Referentenentwurf des Bundesministeriums für Justiz und Verbraucherschutz

Durch einen Referentenentwurf des Bundesministeriums für Justiz und Verbraucherschutz (BMJV) würde das Mindeststrafmaß ebenfalls auf fünf Jahre angehoben, indem „gefährliche Mittel“ in §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB aufgenommen würden.<sup>79</sup> Diese sollen mit dem gefährlichen Werkzeug unter Zugrundelegung eines funktionalen Verständnisses einen einheitlichen Begriff sämtlicher gefährlicher, zur Tatbegehung eingesetzter fester, flüssiger oder gasförmiger Tatmittel bilden. Dadurch soll klargestellt werden, dass insbesondere solche Stoffe, die i.R.d. Körperverletzungsdelikte als „Gift oder andere gesundheitsschädliche Stoffe“ gem. § 224 Abs. 1 Nr. 1 StGB qualifiziert werden, im Bereich der Sexual- und Raubde-

<sup>66</sup> So BGH, BeckRS 2025, 31774, Rn. 23.

<sup>67</sup> Pschorr, Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.-o.-Tropfen, S. 4, 5.

<sup>68</sup> Deutsches Institut für Menschenrechte, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.-o.-Tropfen, S. 7.

<sup>69</sup> Villmow, in: NK-StGB, 6. Aufl. (2023), vor § 38 Rn. 79 m.w.N.

<sup>70</sup> Villmow, in: NK-StGB, vor § 38 Rn. 79 m.w.N.

<sup>71</sup> BR-Drs. 128/25.

<sup>72</sup> BR-Drs. 128/25 (Beschluss).

<sup>73</sup> Deutscher Bundestag, Abgesetzt: Strafverschärfung bei Einsatz von K.O.-Tropfen für Raub- und Sexualdelikte, online abrufbar unter: <https://bit.ly/4rMRSCM> (zuletzt abgerufen am 17.3.2026).

<sup>74</sup> BR-Drs. 128/25 (Beschluss), Anlage, S. 1, 2.

<sup>75</sup> BR-Drs. 128/25 (Beschluss), S. 2.

<sup>76</sup> BR-Drs. 128/25 (Beschluss), S. 4.

<sup>77</sup> Schieman, KriPoZ, 2025, 182 (183).

<sup>78</sup> BR-Drs. 128/25 (Beschluss), Anlage, S. 3.

<sup>79</sup> BMJV, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.o.-Tropfen, S. 4.

likte als qualifikationsbegründende gefährliche Mittel gelten.<sup>80</sup>

Das Erfordernis der Unmittelbarkeit bei Verwendung gefährlicher Werkzeuge aus § 224 Abs. 1 Nr. 2 StGB soll i.R.d. §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB weder für das gefährliche Werkzeug noch das gefährliche Mittel gelten. Der Unrechtsgehalt der Verwendung eines gefährlichen Werkzeugs und der Beibringung eines gesundheitsschädlichen Stoffes seien vergleichbar, weshalb es nicht sachgerecht erscheine, in einem Fall nur unmittelbare, im anderen Fall auch mittelbare Einwirkungen genügen zu lassen. Einer Ausuferung des Tatbestandes werde durch die Anforderungen der objektiven Zurechnung bereits hinreichend begegnet. Das Unmittelbarkeitskriterium sei ohnehin nicht auf §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB zu übertragen, da der Wortlaut anders als bei § 224 Abs. 1 Nr. 2 StGB keine Tatbegehung „mittels“ des gefährlichen Werkzeugs verlange.<sup>81</sup>

## 2. Kritische Würdigung der Reformvorschläge

Die Reformüberlegungen zu §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB sind das Resultat medialer Aufmerksamkeit für das Thema „K.O.-Tropfen“ sowie des Beschlusses des BGH vom 8. Oktober 2024.<sup>82</sup> Ein solcher Anlassbezug ist jedoch keineswegs unüblich<sup>83</sup> und auch nicht zu beanstanden, sofern die Reformideen inhaltlich überzeugen.

Die Einführung eines einheitlichen Tatmittelbegriffs kann grundsätzlich Vorteile bieten. Eine Aufrechterhaltung der bekannten Abgrenzung zwischen gefährlichem Werkzeug und gesundheitsschädlichem Stoff ist nicht zwingend.<sup>84</sup> Eine präzise Zuordnung eines Tatmittels zu einer der Varianten des § 224 Abs. 1 Nr. 1 und 2 StGB bringt regelmäßig keinen entscheidenden Vorteil, da der Qualifikationsstatbestand unabhängig von der konkreten Einordnung ohnehin erfüllt ist.<sup>85</sup> Anders stellt sich die Lage jedoch im Kontext der §§ 177, 250 StGB dar, in denen die Einordnung eines Tatmittels gegenwärtig noch unmittelbare tatbestandliche Auswirkungen hat. Vor diesem Hintergrund erscheint die Überlegung, einen einheitlichen Tatmittelbegriff einzuführen, grundsätzlich nachvollziehbar. Ein solcher Ansatz könnte dazu beitragen, bestehende Abgrenzungsschwierigkeiten zu reduzieren. Angesichts des Bestimmtheitsgebots müsste ein einheitlicher Tatmittelbegriff jedoch klar konturiert sein, um einer uferlosen Ausdehnung des Tatbestands entgegenzuwirken. Insoweit stellt sich die Frage, ob der im Referentenentwurf vorge-

schlagene Begriff der „gefährlichen Mittel“ diesen Anforderungen in gleicher Weise gerecht wird wie die bereits etablierte Kategorie der gesundheitsschädlichen Stoffe. Diese könnte den Einzelnen konkreter über die Strafbarkeit der Verwendung flüssiger oder gasförmiger Stoffe unterrichten als die Verwendung des Begriffes „gefährliche Mittel“. Die Bezugnahme auf „gesundheitsschädliche Stoffe“ hat im Gegensatz zu der Einführung des gänzlich neuen Begriffes des „gefährlichen Mittels“ zudem den Vorteil, an eine im Strafrecht bereits gefestigte Terminologie anzuknüpfen, durch die auf jahrzehntelange Rechtsprechung zurückgegriffen werden kann. Lediglich „sonstige Mittel“ kennt das StGB bisher.

Ob das Unmittelbarkeitserfordernis aus § 224 Abs. 1 Nr. 2 StGB auf §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB zu übertragen ist, ist umstritten. Der BGH legt den Begriff des gefährlichen Werkzeugs parallel zu § 224 Abs. 1 Nr. 2 StGB aus.<sup>86</sup> Aufgrund fehlender Unmittelbarkeit lehnt er die Pipette als gefährliches Werkzeug ab.<sup>87</sup> Bei festen Gegenständen setzt die Unmittelbarkeit einen irgendwie gelagerten Kontakt zum Körper des Opfers voraus, während das Beibringen bei flüssigen und gasförmigen Stoffen diese Aufgabe übernimmt.<sup>88</sup> Die Erfassung auch mittelbarer Einwirkungen lediglich bei gesundheitsschädlichen Stoffen ist damit zu rechtfertigen, dass der Unrechtsgehalt bei unmittelbarer und mittelbarer Beibringung i.d.R. derselbe ist, bspw. wenn dem Opfer die Tropfen unmittelbar in den Mund oder zuvor in ein Getränk geträufelt werden. In beiden Fällen entfaltet der Stoff seine gesundheitsschädigende sedierende Wirkung im Körper des Opfers. Bei festen Gegenständen ist eine unrechtershöhende bloß mittelbare Verwendung seltener, kann dem Opfer u.U. allerdings in gleicher Weise schaden wie ein unmittelbarer Kontakt.<sup>89</sup> Eine Abschaffung des Unmittelbarkeitserfordernisses, sollte, sofern als sinnvoll erachtet, nicht nur punktuell für §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB erfolgen. Vielmehr sollte sich der Gesetzgeber grundsätzlich fragen, ob er dieses Erfordernis aufrechterhalten möchte und dabei alle Tatbestände, die das Tatbestandsmerkmal „Verwenden eines gefährlichen Werkzeuges“ enthalten (insbesondere § 224 Abs. 1 Nr. 2 StGB), in den Blick nehmen.

Der Referentenentwurf verengt seinen Fokus auf die einschlägigen Absätze bzw. Nummern der Norm, statt die Wirkung einer Gesetzesänderung auf sie in Gänze zu betrachten. Pschorr wendet zurecht ein, dass der Referentenentwurf das gefährliche Mittel nicht in §§ 177 Abs. 7 Nr. 1, 250 Abs. 1 Nr. 1 lit. a StGB einzuführen plant.<sup>90</sup> Dies führt dazu, dass i.R.d. §§ 177 Abs. 8 Nr. 1, 250

<sup>80</sup> BMJV, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.O.-Tropfen, S. 7.

<sup>81</sup> BMJV, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.O.-Tropfen, S. 5, 6.

<sup>82</sup> Den Anlassbezug kritisierend: Fischer, (Noch) höhere Strafen für das Verwenden von K.O.-Tropfen oder anderen Substanzen bei sexuellem Übergriff oder Raub?, LTO, online abrufbar unter: <https://bit.ly/4uMP2jV> (zuletzt abgerufen am 17.3.2026).

<sup>83</sup> Die Reform des Sexualstrafrechts („Nein heißt Nein“) war u.a. eine Reaktion auf die Kölner Silvesternacht 2015/2016, vgl. Werthschulte, APuZ Köln 2017, 10.

<sup>84</sup> Vgl. etwa Hilgendorf, ZStW 112 (2000), 811 (824).

<sup>85</sup> Pschorr, Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.O.-Tropfen, S. 3.

<sup>86</sup> BGH, NJW 2024, 3735 (3736 f.).

<sup>87</sup> BGH, NJW 2024, 3735 (3736 f.).

<sup>88</sup> Hardtung, in: MüKo-StGB, § 224 Rn. 10.

<sup>89</sup> Siehe bspw. BGH BeckRS 2016, 05081.

<sup>90</sup> Pschorr, Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.O.-Tropfen, S. 3.

Abs. 2 Nr. 1 StGB eine Gleichstellung von gefährlichen Werkzeugen und Mitteln erfolgt. Für eine Strafbarkeit nach §§ 177 Abs. 7, 250 Abs. 1 Nr. 1 StGB wird zusätzlich zum Beisichführen eines gefährlichen Mittels jedoch weiterhin die Zweckbestimmung des Täters gefordert, einen Widerstand zu überwinden, während das Beisichführen eines gefährlichen Werkzeugs allein für eine Strafbarkeit ausreicht. Auch wenn gefährliche Mittel in den meisten Fällen zur Überwindung eines erwarteten Widerstandes bei sich geführt werden, so entsteht durch die Gesetzesänderung an dieser Stelle eine systematische Diskrepanz.<sup>91</sup> Dies würde erneut eine Abgrenzung von „Werkzeug“ und „Mittel“ i.R.d. §§ 177 Abs. 7, 250 Abs. 1 Nr. 1 StGB erforderlich machen, wenn gefährliche Mittel ohne die entsprechende Zweckbestimmung bei sich geführt werden, der der Referentenentwurf durch Einführung eines einheitlichen Begriffsverständnisses gerade entgegen will.

Dieselbe systematische Diskrepanz ist auch dem Entwurf des Bundesrates vorzuwerfen, indem nur in §§ 177 Abs. 8 Nr. 1, 250 Abs. 2 Nr. 1 StGB „gesundheitsschädliche Stoffe“ eingeführt würden, dies für das bloße Beisichführen in §§ 177 Abs. 7 Nr. 1, 250 Abs. 1 Nr. 1 lit. a StGB aber nicht vorgesehen ist. Zudem führt der Bundesratsentwurf dazu, dass innerhalb derselben Norm gefährliche Werkzeuge und gesundheitsschädliche Stoffe sowie sonstige Werkzeuge und Mittel erfasst würden. Sonstige Werkzeuge und Mittel bilden einen einheitlichen Begriff,<sup>92</sup> während i.R.d. Verwendungsqualifikation weiterhin eine Abgrenzung erforderlich wäre.

Bei der Bewertung der Reformvorschläge ist zudem zu berücksichtigen, dass Änderungen einzelner Tatbestandsmerkmale regelmäßig über den konkreten Regelungsbereich hinaus Wirkungen entfalten. Begriffe wie „gefährliches Werkzeug“, „gesundheitsschädlicher Stoff“ oder „Mittel“ werden im StGB in einer Vielzahl von Delikten verwendet. Ob und inwieweit sich eine Änderung der §§ 177, 250 StGB auf andere Tatbestände auswirken würde, wird in der Gesetzesbegründung nicht behandelt.

### 3. Zwischenergebnis

Die Reformvorschläge des Bundesrates und des BMJV reagieren auf ein reales kriminalpolitisches Problem und verfolgen das legitime Ziel, die heimliche Verabreichung sedierender Substanzen im Zusammenhang mit Sexual- und Raubdelikten strafrechtlich angemessen zu erfassen. In ihrer konkreten Ausgestaltung weisen beide Entwürfe Vorteile und Mängel auf.

Während der Bundesratsentwurf durch Einführung des Begriffs „gesundheitsschädliche Stoffe“ Bestimmtheit

und Rechtssicherheit gewährleistet, birgt der Referentenentwurf mit dem innovativen Begriff „gefährliche Mittel“ Vorteile einer Vereinheitlichung des Tatmittelbegriffs und einer Reduktion von Abgrenzungsschwierigkeiten, riskiert dabei jedoch verfassungsrechtliche Hürden (Art. 103 Abs. 2 GG) durch Ausdehnung des Anwendungsbereichs. Beide Gesetzentwürfe erzeugen systematische Diskrepanzen innerhalb derselben Norm, indem sie nicht den Einfluss einer Gesetzesänderung auf die gesamte Norm mit all ihren Absätzen in den Blick nehmen, sondern ihren Fokus auf die in Rede stehenden Absätze und Nummern verengen. Beide Entwürfe vernachlässigen zudem potenzielle Wechselwirkungen mit anderen Tatbeständen des StGB, die die entsprechenden Tatbestandsmerkmale wortgleich enthalten. Die Gesetzentwürfe laufen daher Gefahr, letztlich mehr Probleme zu schaffen als zu lösen.

### IV. Fazit

Die heimliche Verabreichung von K.O.-Tropfen ist eine besonders gefährliche und hinterlistige Tatbegehung, die einen Angriff auf elementare Rechtsgüter wie die körperliche Unversehrtheit und die sexuelle Selbstbestimmung darstellt. Die Dunkelziffer ist hoch, das Entdeckungsrisiko für Täter bislang gering und die psychischen sowie physischen Folgen für die Betroffenen oft gravierend. Umso wichtiger ist eine präzise strafrechtliche Erfassung dieses Phänomens. Das aktuelle Strafrecht erfasst diese Taten insbesondere über §§ 177, 224, 250 StGB bereits umfassend. Der Ausschluss flüssiger Substanzen vom Werkzeugbegriff, wie ihn der BGH unter Berufung auf Art. 103 Abs. 2 GG vornimmt, ist methodisch überzeugend, offenbart aber zugleich, dass dem Unrechtsgehalt dieser Tatbegehung auf Tatbestandsebene nicht ausreichend Rechnung getragen wird. Eine bloße Kompensation auf Seiten der Strafzumessung greift zu kurz. Eine gesetzliche Reform erscheint daher angezeigt.

Sowohl der Bundesratsentwurf als auch der Referentenentwurf des BMJV bieten hierfür wertvolle Ansatzpunkte, weisen jedoch systematische Diskrepanzen und ggf. terminologische Unschärfen auf. Eine ausgewogene Reform müsste einerseits Rechtssicherheit und Bestimmtheit gewährleisten, andererseits aber auch den Unrechtsgehalt solcher Taten tatbestandlich präzise erfassen. Der Gesetzgeber sollte die aktuelle Debatte daher zum Anlass nehmen, nicht nur punktuelle Anpassungen vorzunehmen, sondern den Begriff des gefährlichen Werkzeugs bzw. Tatmittels sowie das Erfordernis der Unmittelbarkeit im StGB insgesamt grundlegend zu überprüfen und ggf. kohärent neu zu fassen.

<sup>91</sup> Pschorr, Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Stärkung des strafrechtlichen Schutzes vor sogenannten K.o.-Tropfen, S. 3.

<sup>92</sup> Sander, in: MüKo-StGB, § 250 Rn. 38.

# Die aktuellen Vorschläge zum strafrechtlichen Schutz vor digitaler Gewalt – Ein Debattenbeitrag

von Prof. Dr. Elisa Hoven,  
Tim Marian Friedrich und  
Katharina Schooltink\*

## Abstract

Derzeit wird hitzig über digitale Gewalt gegen Frauen diskutiert. Wie so oft ist es ein medial breit rezipierter Einzelfall, der den Ruf nach Erweiterungen des Sexualstrafrechts laut werden lässt. Doch die geplanten Reformen sind tatsächlich überfällig. Das geltende Strafrecht bietet derzeit keine wirksamen Instrumente, um den neuen Risiken von Deepfakes und heimlichen Bildaufnahmen zu begegnen. Der Beitrag analysiert den Entwurf des Bundesjustizministeriums als Grundlage für eine kriminalpolitische Debatte um den strafrechtlichen Schutz vor digitaler Gewalt. Dabei kommen die Verfasser zu einem differenzierten Ergebnis: Während die Vorschläge für eine Ahndung sexualisierter bildbasierter Gewalt überwiegend überzeugen können, erscheint der vorgesehene Tatbestand einer Verletzung von Persönlichkeitsrechten durch täuschende Inhalte in seiner aktuellen Version verbesserungsbedürftig.

Digital violence against women is currently the subject of intense public debate. As is often the case, it is a widely reported individual incident that has sparked calls for an expansion of sexual criminal law. Yet the proposed reforms are in fact long overdue. Existing criminal law does not provide effective instruments to address the new risks posed by deepfakes and covert photography.

The article analyses the draft bill of the Federal Ministry of Justice as a basis for a broader criminal policy debate on the protection against digital violence. It arrives at a nuanced conclusion: while the proposals to sanction sexualised image-based violence are largely convincing, the proposed offence of violating personality rights through deceptive content appears, in its current form, to require further refinement.

## I. Einleitung

Es ist das Schicksal des Strafrechts – und insbesondere des Sexualstrafrechts – erst dann einer kritischen Revision unterzogen zu werden, wenn es gravierende Einzelfälle auf die Titelblätter der Zeitungen und damit in das Bewusstsein der Öffentlichkeit schaffen. Nachdem die Vorwürfe der Schauspielerin und Moderatorin *Collien Fernandes* gegen ihren früheren Ehemann *Christian Ul-*

*men* publik geworden sind, kocht die Stimmung in den sozialen Netzwerken. *Fernandes* wirft *Ulmen* vor, er habe über Jahre hinweg Fake-Profile unter ihrem Namen erstellt und diese genutzt, um mit Dritten sexuelle Kommunikation zu führen. Hierzu soll er Videos versendet haben, die vermeintlich sexuelle Handlungen von *Fernandes* zum Gegenstand hatten. *Christian Ulmen* ließ über seine Anwälte verlautbaren, dass es sich bei den veröffentlichten Vorwürfen zu großen Teilen um unzulässige Verdachtsberichterstattung handele. Die öffentliche Empörung über die mutmaßlichen Taten – denn noch gilt die Unschuldsvermutung, wenn auch eher auf dem Papier – ist jedoch groß. Die Bundesjustizministerin hat nun mit beeindruckendem Tempo einen Gesetzentwurf erarbeitet, der (sexualisierte) Deepfakes ebenso adressiert wie weitere Phänomene bildbasierter sexualisierter Gewalt, die in den vergangenen Monaten Gegenstand kriminalpolitischer Diskussionen waren. Der Entwurf liegt den Verfassern vor und soll zeitnah vorgestellt werden. Wenige Tage später brachte auch die Fraktion Bündnis 90/Die Grünen einen Entwurf in den Bundestag, der unbefugte sexualisierte Bildaufnahmen in den Blick nimmt.<sup>1</sup>

Eile ist bei der Formulierung von (Straf-)Gesetzen meist ein Problem: Es bleibt keine Zeit, um die Folgen der neuen Vorschriften gründlich zu überdenken, weitergehende Entwicklungen zu antizipieren und Unrecht holistisch abzubilden. So entsteht nicht selten ein Flickenteppich aus handwerklich schwachen Normen, die in der Praxis zu erheblichen Auslegungsproblemen führen. Doch das muss nicht sein – der gerade vorgelegte Entwurf des BMJV ist weit in weiten Teilen zu begrüßen. Der Fall *Fernandes* hat hier nur das Momentum für eine grundlegende Reform geschaffen; Bundesjustizministerin *Stefanie Hubig* hatte das bislang unterschätzte Problem bildbasierter sexualisierter Gewalt bereits seit ihrem Amtsantritt im Blick. Damit spielt für die Bewertung des Gesetzesentwurfs auch keine Rolle, welche Vorwürfe sich gegen *Ulmen* letztlich bewahrheiten sollten. Der prominente Fall ist Auslöser für die Reform, nicht deren Maßstab. Die Emotionalität der Debatte mahnt allerdings zur Vorsicht: Gesetzesentwürfe, die von einer aufgeheizten öffentlichen Stimmung getragen werden, sind nicht selten fehleranfällig. An einigen Punkten sollte der Entwurf daher nachgeschärft werden; und hier hat die Strafrechtswissenschaft durchaus noch

\* Prof. Dr. Elisa Hoven ist Inhaberin des Lehrstuhls für deutsches und ausländisches Strafrecht, Strafprozessrecht, Wirtschafts- und Medienstrafrecht an der Universität Leipzig. Tim Marian Friedrich ist Wissenschaftlicher Mitarbeiter und Katharina Schooltink ist wissenschaftliche Mitarbeiterin an ihrem Lehrstuhl.

<sup>1</sup> BT-Drs. 21/4949.

die Möglichkeit, sich kritisch einzubringen. Der vorliegende Beitrag stellt die wesentlichen Neuregelungen knapp vor und skizziert, an welchen Stellen Änderungsbedarf besteht.

## II. Verletzung der Intimsphäre durch Bildaufnahmen: § 184k StGB-E

§ 184k StGB regelt in seiner derzeitigen Fassung das sogenannte Upskirting und Downblousing. Dass die Vorschrift erhebliche Regelungslücken aufweist, hat die Strafrechtswissenschaft schon im Rahmen der damaligen Sachverständigenanhörung deutlich gemacht.<sup>2</sup> Der Gesetzgeber hatte damals allein auf ein konkretes Phänomen reagiert, ohne naheliegende Konstellationen mit vergleichbarem Unrechtsgehalt zu bedenken. Der neue Entwurf unternimmt nun den überfälligen Versuch, diese Regelungsdefizite zu beseitigen und bildbasierte sexualisierte Gewalt umfassender zu pönalisieren.

Die Nummern des § 184k Abs. 1 StGB-E setzen als gemeinsame Tathandlung das unbefugte Herstellen oder Zugänglichmachen einer Bildaufnahme an einen Dritten voraus und unterscheiden sich jeweils durch den abgebildeten Inhalt.<sup>3</sup> Das Merkmal „unbefugt“ soll nach der Entwurfsbegründung parallel zum Verständnis des Begriffs in § 201a Abs. 1 StGB ausgelegt werden; es handelt sich also um einen Hinweis auf die allgemeinen Rechtfertigungsgründe, insbesondere die (mutmaßliche) Einwilligung.<sup>4</sup>

Eine ähnliche Schutzrichtung weisen § 201a Abs. 1 Nrn. 1, 2, 4, 5, Abs. 2 S. 1, Abs. 3 StGB und § 33 Abs. 1 i.V.m. §§ 22, 23 KunstUrhG auf, bieten jedoch mit Blick auf die sexuelle Selbstbestimmung keinen lückenlosen strafrechtlichen Bildnisschutz.

§ 201a StGB pönalisiert die Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen.<sup>5</sup> Daher erfasst die Vorschrift nur solche Bildaufnahmen, auf denen die abgebildete Person identifizierbar ist.<sup>6</sup> In Abs. 1 werden besondere Anforderungen an die Bildaufnahme gestellt. Nach Nr. 1 (ggf. i.V.m. Nr. 4 oder Nr. 5) muss das Opfer sich bei der Bildaufnahme in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befinden; Nr. 2 (ggf. i.V.m.

Nr. 4 oder Nr. 5) fordert die Zurschaustellung der Hilflosigkeit der abgebildeten Person. In beiden Fällen ist eine Verletzung des höchstpersönlichen Lebensbereichs der abgebildeten Person erforderlich.<sup>7</sup> § 201a Abs. 2 StGB hingegen ist ein Eignungsdelikt<sup>8</sup> und erfasst im Gegensatz zu Abs. 1 nur die Tathandlung des unbefugten Zugänglichmachens der Bildaufnahme an einen Dritten. Erforderlich ist zudem, dass die Bildaufnahme geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden. Das Merkmal wird bislang sehr restriktiv ausgelegt, teilweise wird ein erheblicher Ehrangriff oder eine entwürdigende Persönlichkeitsdarstellung verlangt.<sup>9</sup> § 184k StGB-E beschreitet hier einen anderen Weg: Da der Tatbestand die relevanten Inhalte auf ohnehin intime Bereiche beschränkt, bedarf es keiner Eingrenzung der Norm mit Blick auf den räumlichen Kontext oder die Wirkungen der Aufnahme.

§ 33 Abs. 1 i.V.m. §§ 22, 23 KunstUrhG schützt das Recht am eigenen Bild und erfasst daher nur die Verbreitung oder öffentliche Zurschaustellung eines Bildnisses. Eine Schutzlücke verbleibt auch hier im Hinblick auf die Herstellung einer Bildaufnahme.<sup>10</sup> Auch das KunstUrhG setzt die Erkennbarkeit der abgebildeten Person voraus<sup>11</sup> und ist prozessual als absolutes Antrags- (§ 33 Abs. 2 KunstUrhG) und Privatklagedelikt (§ 374 Abs. 1 Nr. 8 StPO) ausgestaltet. Das geltende Recht bietet daher weder materiell- noch prozessrechtlich einen hinreichenden Schutz vor bildbasierter sexualisierter Gewalt.

### 1. § 184k Abs. 1 Nr. 1 StGB-E: Abbildung der sexuellen Handlung einer anderen Person

§ 184k Abs. 1 Nr. 1 StGB-E erfasst Aufnahmen, die eine sexuelle Handlung einer anderen Person abbilden. Über den Schutzbereich des bereits bestehenden § 201a Abs. 1 Nr. 1, Nr. 4 StGB hinaus schützt der § 184k Abs. 1 Nr. 1 StGB-E damit die sexuelle Selbstbestimmung vor unbefugter Herstellung von Bildaufnahmen sexueller Handlungen *ortsunabhängig* und nicht nur in einer Wohnung oder einem gegen Einblick besonders geschützten Raum. § 201a Abs. 1 Nr. 2, Nr. 4 StGB hingegen ist lediglich bei Bildaufnahmen von nicht-einvernehmlichen sexuellen Handlungen, etwa Vergewaltigungen,<sup>12</sup> denkbar. Auch § 201a Abs. 2 S. 1 StGB schützt abgebildete Personen in ihrer sexuellen Selbstbestimmung nur lückenhaft. Dort ist

<sup>2</sup> Deutscher Bundestag: Ausschuss für Recht und Verbraucherschutz, Protokoll-Nr. 19/95, S. 9 ff., online abrufbar unter: <https://bit.ly/4IUCaE0> (zuletzt abgerufen am 25.3.2026); Eisele/Hoven, Die Upskirting-Reform geht nicht weit genug, in: F.A.Z. Einspruch, 4.6.2020, online abrufbar unter: <https://bit.ly/40RhYd0> (zuletzt abgerufen am 25.3.2026).

<sup>3</sup> Einen anderen Weg geht der Entwurf der Fraktion Bündnis 90/Die Grünen: Tatobjekt ist hier eine nicht näher konkretisierte „Bildaufnahme, die eine andere Person sexualbezogen abbildet“. In der Begründung heißt es, gemeint sei eine Darstellung, „in der die Sexualität der abgebildeten Person im Vordergrund steht oder [die] aufgrund von äußeren Merkmalen, Aufnahmeumständen oder sozialer Konnotation eine sexualisierte Wahrnehmung erzeugt“, BT-Drs. 21/4949, S. 7.

<sup>4</sup> Mit der Begründung, dass das Deliktsunrecht nicht in einem Handeln wider Willen des Opfers liege, Eisele, in: TK-StGB, 31. Aufl. (2025), § 201a Rn. 17 m.w.N.; a.A. aber Renzikowski, in: MüKo-StGB, 5. Aufl. (2025), § 184k Rn. 27; Graf, in: MüKo-StGB, § 201a Rn. 85.

<sup>5</sup> BT-Drs. 15/2466, S. 4 ff.; Heger, in: Lackner/Kühl/Heger, StGB, 31. Aufl. (2025), § 201a Rn. 1 m.w.N. auch zu abweichenden Ansichten.

<sup>6</sup> Graf, in: MüKo-StGB, § 201a Rn. 30.

<sup>7</sup> Heger, in: Lackner/Kühl/Heger, StGB, § 201a Rn. 3.

<sup>8</sup> Eisele, in: TK-StGB, § 201a Rn. 37; a.A. Altenhain, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 201a Rn. 3.

<sup>9</sup> BT-Drs. 18/2601, S. 37.

<sup>10</sup> Heuchemer, in: BeckOK-StGB, 68. Ed. (Stand: 1.2.2026), § 201a Rn. 6; zur Schutzlücke in § 33 Abs. 1 i.V.m. §§ 22, 23 KunstUrhG damals schon Ernst, NJW 2004, 1277 (1278 f.).

<sup>11</sup> Valerius, in: BeckOK-StGB, KunstUrhG, § 33 Rn. 9.

<sup>12</sup> LG Essen, BeckRS 2021, 38589; Graf, in: MüKo-StGB, § 201a Rn. 50.

nur die Tathandlung des Zugänglichmachens an einen Dritten und nicht bereits die Herstellung (oder gar der Besitz oder Abruf) der Aufnahme erfasst. Weiter muss die Bildaufnahme geeignet sein, „dem Ansehen der abgebildeten Person *erheblich* zu schaden“. Eine solche Eignung wird bei der Abbildung sexueller Handlungen nicht zwangsläufig angenommen.<sup>13</sup>

Die Entwurfsbegründung („Darunter fällt auch [...] Bildmaterial von nicht-einvernehmlichen, gewalttätigen sexuellen Handlungen (Vergewaltigungsvideos) [...]“) lässt vermuten, dass die Norm eine gesetzgeberische Reaktion auf den Fall *Gisèle Pelicot* in Frankreich oder jüngst durch Recherchen aufgedeckte Chatgruppen ist, in denen Videomaterial von Vergewaltigungen unter Drogen gesetzter Frauen geteilt wurden<sup>14</sup>. Der Tatbestand geht jedoch über die Pönalisierung von Vergewaltigungsvideos hinaus und erfasst auch Bildaufnahmen einvernehmlicher sexueller Handlungen. Damit wird auch das Phänomen von „Revenge Porn“ erfasst; also der Verbreitung ursprünglich einvernehmlicher Aufnahmen nach Beendigung einer Beziehung. Daraus ergeben sich folgende Konstellationen, die sich in ihrem Unrechtsgehalt allerdings unterscheiden: (1) T filmt die Vergewaltigung der O. (2) T filmt heimlich den einvernehmlichen Geschlechtsverkehr mit O. (3) T filmt O, der in der Öffentlichkeit masturbiert.

Mit Blick auf das Schutzgut der sexuellen Selbstbestimmung erschiene eine differenzierte Bewertung der Konstellationen im Strafmaß sinnvoll. Es sprechen gute Gründe dafür, die Dokumentation einer nicht-konsensualen sexuellen Handlung einem höheren Strafrahmen zu unterstellen. Schließlich wird das Unrecht des Übergriffs durch dessen bildliche Perpetuierung für das Opfer massiv erhöht. Bei offensichtlichen Vergewaltigungsvideos sollte zudem über eine Strafbarkeit des Abrufens und Besitzens – parallel etwa zu § 184c Abs. 3 StGB – nachgedacht werden. Wie mediale Recherchen zeigen, schaffen andere Nutzer durch ihre Nachfrage einen erheblichen Anreiz für sexuelle Übergriffe.

In Konstellation (3) hingegen ist der Eingriff in die sexuelle Selbstbestimmung geringer, da O selbst öffentlich sexuelle Handlungen vornimmt. Hier wäre eine Klarstellung in der Entwurfsbegründung notwendig, dass eine Dokumentation exhibitionistischer Handlungen zum Zweck der Beweissicherung nicht als unbefugt gelten darf.<sup>15</sup> Frauen muss es möglich sein, ein solches – strafbares – Verhalten eines Mannes aufzuzeichnen. Die Bildaufnahme kann hier

nicht nur die strafrechtliche Verfolgung ermöglichen, sondern auch eine effektive Verteidigungsstrategie sein, um den Täter von weiteren übergriffigen Handlungen abzuhalten. Die Entwurfsbegründung zu § 184k Abs. 1 Nr. 1 StGB-E statuiert dagegen bislang nur, dass „Bildaufnahmen von sexuellen Handlungen [...] unabhängig davon, wo die sexuellen Handlungen stattfinden, der Intimsphäre und damit dem Schutz des allgemeinen Persönlichkeitsrechts“ unterfallen. Diese Formulierung muss überdacht werden; exhibitionistische Handlungen sollten aufgrund ihres notwendigen Bezugs zur Außenwelt und ihrer Einbindung anderer Personen nicht der Intimsphäre zugeordnet werden.<sup>16</sup>

## 2. § 184k Abs. 1 Nr. 2 StGB-E: Abbildung unbekleideter, intimer Körperteile einer anderen Person

§ 184k Abs. 1 Nr. 2 StGB-E sanktioniert das unbefugte Herstellen oder Zugänglichmachen einer Bildaufnahme, die die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abbildet, und schließt damit eine Strafbarkeitslücke, die der aktuelle § 184k Abs. 1 StGB offengelassen hat. Im vergangenen Jahr wurden verschiedene Fälle bekannt, in denen Männer heimlich die Körper von Frauen in Saunen gefilmt hatten – und straflos blieben.

Die geltende Fassung des § 184k Abs. 1 StGB zielt auf sog. Upskirting- und Downblousing-Aufnahmen ab und schützt Betroffene vor Intimbereichsaufnahmen nur, „so weit diese Bereiche gegen Anblick geschützt sind.“ Nach der Vorstellung des damaligen Gesetzgebers sollte ein strafwürdiger Eingriff in die sexuelle Selbstbestimmung durch Bildaufnahmen intimer Körperteile Erwachsener<sup>17</sup> nur gegeben sein, wenn der Täter die Kleiderbarriere des Opfers als objektive Dokumentation dessen Willens, den Intimbereich vor Anblicken zu schützen, überwindet.<sup>18</sup>

Heimliche Nacktaufnahmen werden daher von § 184k StGB in seiner aktuellen Fassung nicht unter Strafe gestellt. Auch § 201a Abs. 1 StGB bietet in der Regel keinen Schutz, da er Bildaufnahmen allein in besonders geschützten Räumen untersagt. Voyeuristische Bildaufnahmen in Saunen, in FKK-Bereichen, in Sammelduschen und -umkleiden erfüllen diese Voraussetzungen nach herrschender Ansicht nicht.<sup>19</sup>

§ 201a Abs. 2 S. 1 StGB würde nur bei einem Zugänglichmachen der Bildaufnahme an einen Dritten greifen und ist auch sonst nicht einschlägig. Dass Aufnahmen nackter Körper(-teile) Erwachsener von § 201a Abs. 2 S. 1 StGB

<sup>13</sup> So wohl Kargl, in: NK-StGB, 6. Aufl. (2023), § 201a Rn. 23; Eisele, in: TK-StGB, § 201a Rn. 41.

<sup>14</sup> Recherchen des Reportageformats StRG\_F hatten mehrere solcher Chatgruppen aufgedeckt. In den letzten Monaten wurden dann Strafverfahren publik, die Sachverhalte wiederholter chemischer Unterwerfung und Vergewaltigung von Frauen aus dem sozialen Nahbereich und Dokumentation in Chatgruppen betrafen, online abrufbar unter: <https://bit.ly/4bxbHcC> (zuletzt abgerufen am 26.3.2026), <https://bit.ly/4IXOqnS> (zuletzt abgerufen am 26.3.2026).

<sup>15</sup> Anders als in den Beispielen im Begründungstext wird man beim strafbaren Exhibitionisten nicht von einer schlüssigen oder mutmaßlichen Einwilligung in die Bildaufnahme ausgehen können.

<sup>16</sup> Ähnlich in Bezug auf Abbildungen von Straftaten bei § 201a Abs. 1 StGB, Altenhain, in: Matt/Renzikowski, StGB, § 201a Rn. 26.

<sup>17</sup> Bei Abbildungen von unter Achtzehnjährigen gilt zudem § 201a Abs. 3 StGB, der nach dem Entwurf in § 184k Abs. 2 StGB-E überführt werden soll. Zudem stellen die §§ 184b, 184c StGB Tathandlungen im Zusammenhang mit Kinder- und Jugendpornografie unter Strafe.

<sup>18</sup> BT-Drs. 19/17795, S. 14.

<sup>19</sup> OLG Koblenz, NStZ 2009, 268 f.; Graf, in: MüKo-StGB, § 201a Rn. 42; Altenhain, in: Matt/Renzikowski, StGB, § 201a Rn. 8; a.A. Eisele, in: TK-StGB, § 201a Rn. 10; Bosch, NStZ 2021, 370 (371 f.).

nicht ohne hinzutreten weiterer, entwürdigender Umstände erfasst sind, hat der Gesetzgeber bereits bei Schaffung des § 201a Abs. 3 StGB verdeutlicht, der auch nur bei Nacktaufnahmen unter Achtzehnjähriger greift.<sup>20</sup>

§ 33 Abs. 1 i.V.m. §§ 22, 23 KunstUrhG kann bei einer späteren Verbreitung von Bildaufnahmen greifen, setzt allerdings die Erkennbarkeit der Person voraus. Heimliche Aufnahmen des Körpers reichen dazu in aller Regel nicht aus.

§ 184k Abs. 1 Nr. 2 StGB-E stellt damit die notwendige Korrektur einer bisherigen Fehleinschätzung von Strafwürdigkeit und Sanktionsbedürfnis seitens des Gesetzgebers dar. Eine Nichtbedeckung intimer Körperteile mag ein mangelndes Interesse des Opfers vor dem Schutz vor flüchtigen Anblicken Dritter dokumentieren,<sup>21</sup> keinesfalls kann aber darin eine Zustimmung zu einer dauerhaften Bildaufnahme gesehen werden. Das Recht auf sexuelle Selbstbestimmung einer Person beinhaltet auch, „selbst darüber zu befinden, [...] in welcher Form [...] sie Einblick in ihre Intimsphäre [...] gibt.“<sup>22</sup> Dies gilt einmal mehr in einer Zeit, in der Fotos und Videos online in Sekundenschnelle unüberschaubar verbreitet, und aufgrund unkontrollierter Vervielfältigung teils nur schwer vollständig aus dem Netz entfernt werden können.

Ebenfalls begrüßenswert ist, dass die Entwurfsbegründung klarstellt, dass eine Bildaufnahme nach § 184k Abs. 1 Nr. 2 StGB-E keine Erkennbarkeit oder Identifizierbarkeit der abgebildeten Person erfordert. Durch das unbefugte Herstellen oder Verbreiten von Abbildungen intimer Körperteile wird das Recht auf sexuelle Selbstbestimmung einer Person verletzt – unabhängig von einer darüberhinausgehenden, potenziell ehrverletzenden individuellen Zuordnung.

### 3. § 184k Abs. 1 Nr. 3 StGB-E: Abbildung bekleideter, intimer Körperteile einer anderen Person in sexuell bestimmter Weise

§ 184k Abs. 1 Nr. 3 StGB-E bezieht sich auf solche Bildaufnahmen, die „in sexuell bestimmter Weise die bekleideten Genitalien, das bekleidete Gesäß oder die bekleidete weibliche Brust“ einer anderen Person abbilden. Damit zielt der Normenentwurf u.a. auf das vom aktuellen § 184k Abs. 1 StGB adressierte „Upskirting“ und „Downblousing“ ab, sofern nicht bei Nacktheit sogar § 184k Abs. 1 Nr. 2 StGB-E einschlägig ist. Erfasst sind diese Phänomene im Vergleich zur aktuellen Fassung unabhängig von der Überwindung einer etwaigen Kleiderbarriere. § 184k Abs. 1 Nr. 3 StGB-E lässt zudem (objektiv) Bildaufnahmen bekleideter intimer Körperteile – auch abseits der Unterwäsche – sowie (subjektiv) Eventualvorsatz aus-

reichen und geht damit deutlich über den Anwendungsbereich der aktuellen Fassung hinaus. An anderer Stelle ist der Anwendungsbereich des Normenentwurfs im Vergleich zur geltenden Version enger; so verlangt der Entwurf eine Abbildung „in sexuell bestimmter Weise“ (dazu sogleich).

Anlass für § 184k Abs. 1 Nr. 3 StGB-E gab der Fall von *Yanni Gentsch*, die Anfang 2025 beim Joggen heimlich im Bereich ihres bekleideten Gesäßes von einem fremden Mann gefilmt wurde, diesen konfrontierte und das entsprechende Video via Social-Media veröffentlichte. In der Folge wurde die Straflosigkeit derart gelagerter voyeuristischer Aufnahmen zahlreich scharf kritisiert und eine Reform des § 184k StGB g.F. gefordert.<sup>23</sup>

Die Vorschrift ist die schwächste Regelung des geplanten Paragraphen. Die Bildaufnahme erfasst einen bekleideten Körperbereich, der grundsätzlich in dieser Form der öffentlichen Betrachtung – wenn auch nicht der Aufzeichnung – preisgegeben wird. Die Intimsphäre, die § 184k StGB-E schützen möchte, wird durch Aufnahmen des bekleideten Körpers ohne gesonderten Schutz nicht verletzt (anders bei Upskirting-Aufnahmen). Eine Verletzung der sexuellen Selbstbestimmung durch Aufnahmen lässt sich nur damit begründen, dass die Art der Aufnahme die Person gegen ihren Willen sexualisiert. Anknüpfungspunkt hierfür kann die subjektive Motivation des Täters sein (er will durch die Aufnahme die Person zum Objekt seiner sexuellen Befriedigung machen) oder eine objektive (das abgebildete Motiv hat per se einen Sexualbezug). Anders als noch in der Entschließung des Bundesrates<sup>24</sup>, will das BMJV auf das objektive Element „in sexuell bestimmter Weise“ abstellen. In der Begründung wird auf die parallele Formulierung in § 184i StGB und die hierzu entwickelte Rechtsprechung verwiesen. Nun ist die Rechtsprechung zu § 184i StGB allerdings kaum eindeutig<sup>25</sup> und lässt sich auch nicht ohne Weiteres auf den Kontext von Bildaufnahmen übertragen. So heißt es in der Begründung: „Weist die Bildaufnahme nach dem Inhalt dessen, was abgebildet ist, bereits nach dem äußeren Erscheinungsbild einen sexuellen Charakter auf, ist nicht erforderlich, dass der Täter auch von sexuellen Absichten geleitet ist.“ Diese Auslegung mag für § 184i StGB überzeugend sein, der ganz unterschiedliche körperliche Berührungen erfasst.<sup>26</sup> Für § 184k StGB-E macht die Lesart hingegen wenig Sinn. Den „Inhalt dessen, was abgebildet ist“, gibt die Vorschrift bereits konkret vor: bekleidete Genitalien, Gesäß oder weibliche Brust. Das abgebildete Motiv selbst kann daher kaum Auskunft über den Sexualbezug geben. Denkbar wäre allein die Fokussierung einer Aufnahme, etwa auf das Gesäß. Doch auch das erscheint zweifelhaft. Zum einen ließe sich die Strafbarkeit hier leicht umgehen: Der Täter könnte eine Bildaufnahme her-

<sup>20</sup> BT-Drs. 18/2601, S. 36 f.; vgl. zum Umkehrschluss *Eisele*, in: TK-StGB, § 201a Rn. 41.

<sup>21</sup> So damals noch zu § 201a Abs. 1 Nr. 4 StGB-E, BT-Drs. 19/17795, S. 13.

<sup>22</sup> *BVerfG*, NZFam 2016, 400 (405 Rn. 53) m.w.N. (Hervorhebung durch Verf.).

<sup>23</sup> Die Petition der Betroffenen *Yanni Gentsch* zählt bislang 164.083 Stimmen, <https://innn.it/voyeur-aufnahmen#updates> (zuletzt abgerufen am 25.3.2026).

<sup>24</sup> Der Bundesrat fordert den Gesetzgeber dort ausdrücklich auf, „Strafbarkeitslücken bei sexuell motivierten Bildaufnahmen [zu] schließen“, BR-Drs. 26/26.

<sup>25</sup> Kritisch auch *Ziegler*, in: BeckOK-StGB, § 184i Rn. 6.

<sup>26</sup> *BGH*, NJW 2018, 2655 (2657).

stellen und erst beim Betrachten auf das Körperteil zoomen. Zum anderen muss auch eine Großaufnahme nicht zwingend eine Sexualisierung bedeuten. So ließe sich etwa der Fall bilden, dass eine Frau das Gesäß einer anderen Frau in einer engen Sportleggings filmt, um dieselbe Hose erwerben zu können. Letztlich kann sich der Sexualbezug daher bei bekleideten Körperteilen nicht aus objektiven Umständen, sondern allein aus der Tätermotivation ergeben. Diese sicher nachzuweisen, wird die Gerichte vor einige Herausforderungen stellen.

#### 4. § 184k Abs. 1 Nr. 4 StGB-E: Sexualisierte Deepfakes

Mit § 184k Abs. 1 Nr. 4 StGB-E soll Gegenstand der Strafbarkeit auch eine unbefugt hergestellte oder zugänglich gemachte Bildaufnahme sein, „die mittels eines Computerprogramms so verändert, umgestaltet oder mit weiteren Inhalten verbunden wurde, dass der Anschein erweckt wird, dass sexuelle Handlungen oder die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abgebildet seien.“

Damit zielt der Entwurf auf den Schutz vor sexualisierten Deepfakes ab, also Bildaufnahmen, die mithilfe künstlicher Intelligenz erzeugt oder manipuliert werden und dabei den Eindruck von Authentizität vermitteln.<sup>27</sup> Untersuchungen legen dar, dass 96-98 % der online auffindbaren Deepfakes pornografischer Natur seien oder die Nacktheit von Personen darstellten.<sup>28</sup> Mit 99 %, und damit fast ausschließlich betroffen von sexualbezogenen Deepfakes, seien dabei Frauen.<sup>29</sup> Der übliche Fall sexualisierter Deepfake-Inhalte ist der sogenannte „Face-Swap“. Hierbei wird eine generative KI mit Bildern einer (realen) Person „gefüttert“. Die KI zerlegt die eingefügten Gesichter in abstrakte Merkmale, kombiniert Identität und Mimik neu und erzeugt daraus synthetische Gesichter, die anschließend nahtlos in bestehende Bild- oder Videoinhalte integriert werden. So können in kürzester Zeit und mit für jedermann zugänglichen Mitteln,<sup>30</sup> täuschend echte pornografische Inhalte von realen Personen erzeugt werden. Insbesondere Frauen, die in der Öffentlichkeit stehen, zu denen es also leicht zugängliches Ausgangsmaterial gibt, werden so Opfer sexualisierter Deepfakes.

##### a) Bestehende Schutzlücke

Das deutsche Kern- und Nebenstrafrecht enthält zwar bereits Vorschriften, die einzelne Aspekte sexualisierter Deepfakes erfassen können; die Rechtslage erweist sich

jedoch als fragmentarisch und bildet den spezifischen Unrechtsgehalt von Deepfakes nicht hinreichend ab.

Eine Strafbarkeit nach § 201a Abs. 1 StGB scheitert regelmäßig daran, dass hierfür bereits das Ausgangsmaterial selbst tatbestandlich sein muss. Das Foto, mit dem die KI „gefüttert“ wird, müsste somit etwa eine Person in ihrer Wohnung zeigen und bereits für sich genommen eine Verletzung des höchstpersönlichen Lebensbereichs darstellen. Bei öffentlich zugänglichen Inhalten aus Social-Media oder sonstigen Medien, ist das regelmäßig ausgeschlossen.

Ob § 201a Abs. 2 StGB Deepfakes erfasst, ist umstritten.<sup>31</sup> Der Wortlaut der Norm spricht von einer „Bildaufnahme“, die geeignet ist dem Ansehen der abgebildeten Person erheblich zu schaden. Unter den Begriff der „Bildaufnahme“ fallen alle Handlungen, mit denen Abbildungen, sowohl Standbilder als auch Bildsequenzen, auf einem Aufnahmemedium aufgezeichnet werden.<sup>32</sup> Dabei muss es sich aber um reale Bilder einer anderen Person handeln, so dass zwar Fotomontagen bezüglich der verwendeten Einzelbilder tatbestandsmäßig sein können,<sup>33</sup> reine Computeranimationen aber ausscheiden.<sup>34</sup> Im Unterschied zur klassischen Bildmontage wird bei einem Deepfake bzw. einem Face-Swap kein existierendes Bildnis verwendet, sondern ein neues, synthetisches Abbild geschaffen, das die Identität der Person lediglich simuliert. Technisch liegt kein „echtes“ Bild der Person vor, sondern ein durch künstliche Intelligenz neu generiertes Abbild, das auf erlernten Gesichtsdaten basiert und die Identität der Person lediglich imitiert. Es ist also nicht die Bildaufnahme, die die Eignung zur Ansehenschädigung beinhaltet, diese Eignung ergäbe sich vielmehr erst aus dem auf Grundlage der Bildaufnahme neu geschaffenen Inhalts. Nach richtiger Lesart sind Deepfakes damit nicht von § 201a Abs. 2 StGB erfasst. Ohnehin bliebe die Herstellung von Deepfakepornografie nach § 201a Abs. 2 StGB straflos. Auch eine Strafbarkeit nach § 42 Abs. 2 BDSG scheidet aus. Voraussetzung hierfür wäre, dass die verwendeten Ausgangsdaten nicht allgemein zugänglich sind. Bei der Nutzung von Bildern aus öffentlich zugänglichen Social-Media-Profilen oder sonstigen Medien ist diese Voraussetzung regelmäßig nicht erfüllt.

Werden sexualisierte Deepfake-Bilder versendet, können die Ehrschutzdelikte in §§ 185 ff. StGB greifen. Ein gefälschter pornografischer Inhalt kann eine unwahre Tatsachenbehauptung darstellen, die den Tatbestand des § 187 Hs. 1 StGB erfüllt.<sup>35</sup> Die Manipulation darf dabei nicht

<sup>27</sup> Thiel, ZRP, 201 (202).

<sup>28</sup> Ajder/Patrini/Cavalli/Cullen, The State of Deepfakes, Realities, Threats, and Impact, 2019; Godulla, bpb, Fake oder Wirklichkeit: Wieso und wie leicht lassen wir uns täuschen? Warum Bilder uns Täuschen, 2014, online abrufbar unter: <https://bit.ly/4bSLiEZ> (zuletzt abgerufen am 25.3.2026).

<sup>29</sup> Security Hero, 2023, State of Deepfakes, Realities Threats, and Impact, online abrufbar unter: <https://bit.ly/4uPRNB6> (zuletzt abgerufen am 25.3.2026).

<sup>30</sup> „It takes less than 25 minutes and costs 0 \$ to create a 60-second deepfake pornographic video of anyone using just one clear face image“, vgl. Security Hero, 2023, State of Deepfakes, Realities Threats, and Impact, online abrufbar unter: <https://bit.ly/4uPRNB6> (zuletzt abgerufen am 25.3.2026).

<sup>31</sup> Zusammenfassung des Streitstandes m.w.N. bei Kumkar/Rapp ZfDR 2022, 199 (202).

<sup>32</sup> Graf, in: MüKo-StGB, § 201a Rn. 24.

<sup>33</sup> Graf, in: MüKo-StGB, § 201a Rn. 26.

<sup>34</sup> BGH, BeckRS 2024, 8894; Eisele, in: TK-StGB, § 201a Rn. 6; Graf, in: MüKo-StGB, § 201a Rn. 26.

<sup>35</sup> Doerbeck, Cybermobbing, 2019, S. 152; Greif, Strafbarkeit von bildbasierten sexualisierten Belästigungen, 2023, S. 234.

ohne weiteres erkennbar sein.<sup>36</sup> Ist die Bearbeitung etwa dadurch offensichtlich, dass sich das Bild des Opfers nicht synchron mit dem restlichen Video bewegt, kann eine Strafbarkeit nach § 187 StGB ausscheiden.<sup>37</sup> Zudem muss die Darstellung ehrenrührig sein. Das soll bei bloßer Nacktdarstellung nicht zwingend der Fall sein.<sup>38</sup> So ließe sich argumentieren, dass sexuelle Handlungen per se nicht ehrenrührig sind.<sup>39</sup> Problematisch erscheint auch ein weiterer Aspekt: Nach § 187 StGB muss eine Tatsache „in Beziehung auf einen anderen“ behauptet oder verbreitet werden. Handelt der Täter scheinbar im Namen der Betroffenen (sog. Impersonation-Fälle), fehlt es unter Umständen an dem für die Norm erforderlichen Drittbezug.<sup>40</sup>

Eine Möglichkeit zur Bestrafung des Täters bei Verbreitung – nicht bei Herstellung – eines Deepfake-Inhaltes ergibt sich aus § 33 i.V.m. §§ 22, 23 KunstUrhG. Die Vorschrift sieht eine Höchststrafe von einem Jahr Freiheitsstrafe vor und wird in der Praxis weitgehend stiefmütterlich gehandhabt.<sup>41</sup> Sie bildet den spezifischen Unrechtsgehalt sexualbezogener Deepfakes nicht im Ansatz ab.

Der Blick auf das geltende Recht zeigt also Folgendes:

(1) Die Herstellung sexualisierter Deepfakes ist bislang regelmäßig straflos.

(2) Die Weitergabe sexualisierter Deepfakes kann – abhängig von den Umständen des Einzelfalles – von einzelnen Strafvorschriften erfasst werden. Eine Strafbarkeit ergibt sich notwendig aus § 33 i.V.m. §§ 22, 23 KunstUrhG, dem jedoch in der Praxis keine nennenswerte Bedeutung zukommt und der das spezifische Unrecht der Tat nicht zu erfassen vermag.

Um das Phänomen von Deepfake-Pornographie angemessen ahnden zu können, ist eine Reform des Strafrechts notwendig. Die leider noch immer verbreitete Ablehnung jeder Erweiterung von Strafrecht erweist sich hier ein weiteres Mal als unterkomplex.<sup>42</sup> Das Strafrecht muss auf neue technische Entwicklungen und damit auf neue Kriminalitätsphänomene reagieren. Digitale sexuelle Gewalt stellt gerade für betroffene Frauen ein massives Problem und eine erhebliche Beeinträchtigung ihrer Sexualautonomie dar. Diese Phänomene zu ignorieren, würde den Risiken der digitalen Gesellschaft und den berechtigten Belangen der Opfer nicht gerecht. Aufgabe der Strafrechtswissenschaft kann es nicht sein, aus generellen Erwägungen den Einsatz von Strafrecht abzulehnen; vielmehr liegt es an uns, gerade in aufgeheizten politischen Debatten auf eine maßvolle Umsetzung zu achten.

## b) Kritische Würdigung

Der Tatbestand des § 184k Abs. 1 Nr. 4 StGB-E ist angesichts der bestehenden Schutzlücken grundsätzlich zu begrüßen. Deepfake-Pornographie stellt einen erheblichen Eingriff in die sexuelle Selbstbestimmung des Betroffenen dar und sollte strafrechtlich sanktioniert werden. Eine bloße Kennzeichnungspflicht kann hier nicht genügen, da der Inhalt selbst bei Offenlegung der Täuschung eine unzulässige Sexualisierung des anderen darstellt.

Kritik hat die Strafbarkeit bereits des „Herstellens“ eines Deepfakes auf sich gezogen.<sup>43</sup> Das Herstellen selbst stellt einen gegenüber dem Verbreiten des Inhalts deutlich geringeren Rechtsgutsangriff dar. Doch das Recht am eigenen Bild und das Recht auf sexuelle Selbstbestimmung schützen auch davor, dass das Bild einer Person gegen oder ohne ihren Willen zum Gegenstand sexualisierter Manipulation durch einen anderen wird.<sup>44</sup> Das Recht auf sexuelle Selbstbestimmung sichert in subjektiv rechtlicher Hinsicht die autonome Entscheidung darüber, ob und welche sexuellen Handlungen mit welchen Personen vollzogen werden sollen.<sup>45</sup> Darunter fällt auch die freie Verfügungsgewalt über eigene sexualbezogene Abbildungen;<sup>46</sup> es obliegt dem Rechtsgutsträger darüber zu entscheiden, welche sexualbezogenen Inhalte er von sich herstellt oder herstellen lässt und mit wem er diese Inhalte teilt.<sup>47</sup> Das gilt auch, wenn – wie im Fall von Deepfakes – fiktionale Inhalte hergestellt werden, die den Anschein erwecken, dass sie tatsächliche sexuelle Handlungen wiedergeben oder den Körper sexualbezogen darstellen.<sup>48</sup> Eine sexuelle Verobjektivierung der dargestellten Person tritt auch im Falle der Herstellung von Deepfakes ein.<sup>49</sup> Die teilweise empörten Kommentare auf Social-Media-Accounts, die dem Staat ein Moralwächtertum vorhalten, sind vor diesem Hintergrund ebenso unsachlich wie verwunderlich. Zumal dem Recht des Täters, von anderen Menschen sexualisierte Deepfakes herzustellen, in der Abwägung auch kein besonderes Gewicht zukommen dürfte. Für eine Bestrafung bereits des Herstellens spricht zudem, dass in der heutigen Zeit jedes produzierte Deepfake den Weg in die Öffentlichkeit finden kann.

Überarbeitet werden sollte allerdings die Formulierung des Tatbestandes. Sprachlich stimmig ist die Verbindung von Nr. 4 zum Beginn der Vorschrift nicht. So wird bestraft, wer „unbefugt eine Bildaufnahme herstellt [...], die mittels eines Computerprogramms so verändert, umgestaltet oder mit weiteren Inhalten verbunden wurde, dass [...]“ Bei dem hergestellten Deepfake handelt es sich allerdings – wie oben dargestellt – nicht um eine „Bildaufnahme“; es setzt eine Bildaufnahme vielmehr voraus. Da-

<sup>36</sup> Doerbeek, Cybermobbing, S. 152.

<sup>37</sup> Doerbeek, Cybermobbing, S. 152.

<sup>38</sup> Greif, Strafbarkeit von bildbasierten sexualisierten Belästigungen, 2023, S. 237.

<sup>39</sup> Vgl. auch Fn. 13.

<sup>40</sup> Vgl. BGH, NStZ 1984, 216; Doerbeek, Cybermobbing, S. 153; Regge/Pegel, in: MüKo-StGB, § 186 Rn. 17.

<sup>41</sup> Nur 100–200 Verurteilungen pro Jahr in den letzten Jahren, Kaiser, in: Erbs/Kohlhaas, KunstUrhG, 259. EL (Stand: Oktober 2025), § 33 Rn. 3.

<sup>42</sup> Vgl. Hoven, ZStW 136 (2024), 433.

<sup>43</sup> Etwa Meinicke, DSRITB 2020, 981 (999).

<sup>44</sup> Vgl. Völzmann, ZUM 2025, 493 (496 f.).

<sup>45</sup> Valentiner, Das Grundrecht auf sexuelle Selbstbestimmung, 2021, S. 415.

<sup>46</sup> Valentiner, in: Burghardt/Schmidt/Steinl, Sexuelle Selbstbestimmung jenseits des Körperlichen, 2024, S. 58; Schmidt, Pornographie und Sexuelle Selbstbestimmung, 2025, S. 195.

<sup>47</sup> Schmidt, Pornographie und sexuelle Selbstbestimmung, S. 195.

<sup>48</sup> Schmidt, in: Burghardt/Schmidt/Steinl, Sexuelle Selbstbestimmung jenseits des Körperlichen, S. 186.

<sup>49</sup> Schmidt, Pornographie und sexuelle Selbstbestimmung, S. 253.

mit passt die zeitliche Zuordnung sprachlich nicht: der Täter stellt keine Bildaufnahme her, die verändert wurde – er verändert eine Bildaufnahme und stellt damit einen Deepfake-Inhalt her.<sup>50</sup>

Zu Missverständnissen könnte zudem die Formulierung führen, dass der „Anschein“ einer sexuellen Handlung einer anderen Person erweckt werden soll. Hieraus ließe sich ableiten, dass Deepfakes, die etwa durch Wasserzeichen als solche gekennzeichnet wurden, den Tatbestand nicht erfüllen. Eine solche Lesart wäre nach dem Wortlaut nicht zwingend und angesichts der Systematik eher fernliegend (denn anders als in § 201b StGB-E wird gerade nicht der Anschein eines „tatsächlichen Geschehens“ verlangt. Doch um Auslegungsprobleme zu vermeiden, erscheint eine Präzisierung an dieser Stelle ratsam. Der Entwurf der Fraktion Bündnis 90/Die Grünen recurriert hier überzeugend auf eine „sexualbezogene Abbildung“; diesen Wortlaut sollte übernommen werden.

Problematisch erscheint auch die Konstellation, in der ein sexualbezogener Deepfake-Inhalt geschaffen wird, zu dessen Erzeugung die KI ihrerseits ausschließlich mit bereits erzeugten (unverfänglichen) Deepfakes gefüttert wird. § 184k Abs. 1 Nr. 4 StGB-E stellt nach seinem Wortlaut darauf ab, dass eine Bildaufnahme, die entsprechend verändert, umgestaltet oder mit weiteren Inhalten verbunden worden ist, hergestellt werden muss. Die Gesetzesbegründung verweist hier auf die Ausführungen *Eiseles* im Tübinger Kommentar zu § 201a StGB; es kann also davon ausgegangen werden, dass hier dasselbe Begriffsverständnis zugrunde gelegt werden soll. Konsequenterweise wären sexualbezogene Deepfakes von einer Strafbarkeit ausgenommen, wenn sie nicht auf Grundlage einer Bildaufnahme, sondern auf Basis einer – nicht sexualisierten – Deepfake-Abbildung erstellt wurden. Eine mögliche Strafbarkeit käme hingegen nach § 201b StGB-E in Betracht. Wieso diese aber aus dem Bereich der Sexualdelikte herausgelöst normiert werden muss, erschließt sich nicht.

Zur Diskussion gestellt werden sollte zudem, ob bei konsequenter Durchsetzung des Rechts auf sexuelle Selbstbestimmung und der damit einhergehenden Verfügungsgewalt über sexualbezogene Abbildungen nicht auch der Besitz und das Speichern solcher Inhalte strafbar sein sollte.<sup>51</sup> Soweit hingegen bereits das Beschaffen des Ausgangsmaterials mit der Absicht daraus sexualbezogene Deepfakes zu erstellen, eigenständig pönalisiert werden soll,<sup>52</sup> ist dem nicht beizutreten. Eine Verletzung des Rechtsguts der sexuellen Selbstbestimmung liegt in diesem Stadium noch nicht vor; für die Verletzung des Rechts am eigenen Bild sind die bisherigen Straftatbestände hinreichend.<sup>53</sup> Die Kriminalisierung einer solchen

Vorbereitungshandlung erscheint hier als zu weitreichender Eingriff in die Freiheitssphäre des Bürgers.<sup>54</sup>

Sinnvoll ergänzen ließe sich hingegen die Herstellung von simulierten Stimmaufnahmen, die sexuelle Inhalte wiedergeben. Von § 184k Abs. 1 Nr. 4 StGB-E erfasst sind allein Bildaufnahmen, keine Audiodateien. Unter § 201b StGB-E fällt eine solche Versendung anzüglicher Deepfake-Sprachnachrichten entgegen der Entwurfsbegründung nicht, da die Vorschrift einen Drittbezug voraussetzt („ein tatsächliches Geschehen in Bezug auf eine andere Person wiederzugeben“).<sup>55</sup> Wird die Nachricht als vermeintlich eigene versendet, ist diese Voraussetzung jedenfalls zweifelhaft.

§ 184k Abs. 1 StGB sieht eine Freiheitsstrafe bis zwei Jahre oder Geldstrafe vor. Angesichts der Schwere der Taten – insbesondere einer Verbreitung realer Vergewaltigungsvideos – überrascht der niedrige Strafraum. Dies gilt vor allem deshalb, weil ein früherer Entwurf des Bundesrates zu persönlichkeitsrechtsverletzenden Deepfakes noch eine Freiheitsstrafe bis zu fünf Jahre vorgesehen hatte.<sup>56</sup> Das italienische Recht droht in Art. 612-quarter des codice penale für die Weitergabe, Veröffentlichung oder Verbreitung sexualbezogener Deepfakes eine Freiheitsstrafe von einem Jahr bis zu fünf Jahren an.

Es erscheint sinnvoll, dass § 184k StGB-E keine Mindeststrafe androht, da bereits das Herstellen von sexualisierten Deepfakes als vergleichsweise geringes Unrecht erfasst wird. Sinnvoll wäre es dann aber, den Gerichten durch einen weiter gefassten Strafraum mehr Spielraum in der Bewertung der Taten einzuräumen. Qualifikationen – etwa für reale Vergewaltigungsvideos, Revenge Porn oder das Verbreiten an eine breite Öffentlichkeit – könnten die Strafzumessung besser strukturieren.

### III. Verletzung von Persönlichkeitsrechten durch täuschende Inhalte: § 201b StGB-E

#### 1. Hintergrund und Regelungsgehalt

Nach § 201b StGB-E sollen künftig auch Deepfakes unter Strafe gestellt werden, die zu einer Verletzung von Persönlichkeitsrechten führen. Hintergrund waren unter anderem Deepfake-Videos, in denen Prominente als Werbeträger für bestimmte Produkte erschienen. Der erste Absatz der Vorschrift lautet:

*„Wer einer dritten Person einen mittels eines Computerprogramms erstellten oder veränderten Inhalt (§ 11 Absatz 3), der den Anschein erweckt, ein tatsächliches Geschehen in Bezug auf eine andere Person wiederzugeben, und der geeignet ist, dem Ansehen dieser Person erheblich zu schaden, unbefugt zugänglich macht, wird mit*

<sup>50</sup> Anders im Entwurf der Fraktion Bündnis 90/Die Grünen, der (korrekterweise) auf die Veränderung der Bildaufnahme mit technischen Mitteln abstellt, BT-Drs. 21/4949, S. 4.

<sup>51</sup> Schmidt, Pornographie und sexuelle Selbstbestimmung, S. 264.

<sup>52</sup> Hierzu Schmidt, Pornographie und sexuelle Selbstbestimmung, S. 264.

<sup>53</sup> Wenn auch nur selten einschlägig, vgl. Greif, Strafbarkeit von bildbasierten sexualisierten Belästigungen, 2023, S. 230 f.

<sup>54</sup> Vgl. Moeller, Definition und Grenzen der Vorverlagerung von Strafbarkeit: Diskussionsstand, Rechtsgeschichte und kausalitätstheoretische Bezüge, 2018, S. 162; vgl. Puschke, Legitimation, Grenzen und Dogmatik von Vorbereitungstatbeständen, 2017, S. 436.

<sup>55</sup> Zur Parallelproblematik bei §§ 186, 187 StGB siehe: Regge/Pegel, in: MüKo-StGB, § 187 Rn. 7.

<sup>56</sup> BT-Drs. 21/1383.

*Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Dies gilt auch dann, wenn sich die Tat nach Satz 1 auf eine verstorbene Person bezieht.“*

Ziel der Norm soll es sein, das spezifische Tatunrecht des unbefugten Zugänglichmachens ansehensschädigender Deepfakes und vergleichbarer technischer Manipulationen zielgenau zu erfassen. Im Unterschied zu § 184k Abs. 1 Nr. 4 StGB-E ist § 201b Abs. 1 StGB-E nicht auf sexualbezogene Deepfakes beschränkt. Ob sexualisierte Deepfakes stets auch § 201b StGB-E unterfallen, ist zweifelhaft; gerade reine Nacktaufnahmen müssen nicht zwingend ansehensschädigend sein.<sup>57</sup> Strafbare Tathandlung ist das Zugänglichmachen; anders als bei § 184k Abs. 1 Nr. 4 StGB-E soll also die Herstellung des Inhalts von der Strafbarkeit ausgenommen bleiben.

Aufgrund der Abkoppelung vom Ausgangsmaterial der Bildaufnahme können § 201b StGB-E im Gegensatz zu § 184k Abs. 1 Nr. 4 StGB-E auch solche Deepfakes unterfallen, die auf Grundlage eines anderen Deepfakes erstellt worden sind, soweit sie geeignet sind dem Ansehen der abgebildeten Person erheblich zu schaden.

Die Vorschrift ist nicht auf Bildaufnahmen als Grundstoff der technischen Täuschung beschränkt. Daher sollen nach der Vorstellung der Entwurfsbegründung auch fingierte Stimmaufnahmen tatbestandlich sein können. Allerdings weist § 201b StGB-E – in Anlehnung an §§ 186, 187 StGB – einen Drittbezug auf. Suggestiert der Täter, dass das Opfer selbst die Audioaufnahme erstellt und verschickt, erscheint der Drittbezug zweifelhaft.

## 2. Regelungslücke

Das Verbreiten von ansehensschädigenden Deepfakes kann bereits jetzt strafrechtlich sanktioniert werden. Einschlägig ist etwa – erneut – § 33 i.V.m. §§ 22, 23 KunstUrhG. Allerdings wählt § 201b StGB-E hier mit dem Zugänglichmachen an Dritte eine weiter gefasste Tathandlung, da das KunstUrhG nur die Verbreitung<sup>58</sup> und das öffentliche Zurschaustellen unter Strafe stellt. Für das Verbreiten im Sinne des KunstUrhG kommt es gerade darauf an, dass durch die Weitergabe die Verfügungsgewalt über das Bildnis aus der Hand gegeben wird.<sup>59</sup> Dementgegen reicht es für ein Zugänglichmachen aus, dass einem Dritten die Möglichkeit zur Kenntnisnahme gegeben wird. Es reicht also aus, einer anderen Person den etwaigen Inhalt auf dem eigenen Gerät oder Medium zu zeigen.<sup>60</sup> Tatsächliche Verfügungsgewalt muss der Adressat der Zugänglichmachung nie erhalten. Zudem ist die in § 201b StGB-E vorgesehene Höchststrafe mit zwei Jahren höher als im KunstUrhG.

Zweifelhaft ist allerdings, ob über § 187 Hs. 1 StGB hinaus überhaupt ein sinnvoller Anwendungsbereich für die Vorschrift verbleibt. Ein Inhalt, der den Anschein erweckt, ein tatsächliches Geschehen in Bezug auf einen anderen darzustellen, ist eine unwahre Tatsachenbehauptung.<sup>61</sup> Wie der Gesetzesbegründung zu entnehmen ist, soll die Eignung zur erheblichen Ansehensschädigung an §§ 186, 187 StGB angelehnt sein. Sofern ein Inhalt also die Eignung nach § 201b StGB-E aufweist, muss auch eine Eignung im Sinne von § 187 Hs. 1 StGB vorliegen. Tathandlungen im Sinne des § 187 Hs. 1 StGB sind das Behaupten und das Verbreiten. Hierfür genügt es, dass der Täter die Tatsache selbst als richtig hinstellt oder eine fremde Behauptung an einen Dritten gelangen lässt.<sup>62</sup> Wer einem Dritten einen gefälschten Inhalt, der den Anschein erweckt ein tatsächliches Geschehen wiederzugeben, im Sinne von § 201b StGB-E zugänglich macht, stellt diesen – jedenfalls konkludent – als richtig hin. Da auch der Drittbezug identisch gefasst ist, verbleibt für die neue Vorschrift auch in „Impersonation-Fällen“<sup>63</sup> kein relevanter Anwendungsfall, der nicht bereits hinreichend über das geltende Recht erfasst werden kann.

Die §§ 186, 187 StGB setzen allerdings voraus, dass eine tatsächliche Kenntnisnahme stattfindet. Die bloße Möglichkeit zur Kenntnisnahme reicht dagegen nicht aus.<sup>64</sup> Für das Zugänglichmachen genügt hingegen, dass der Inhalt für den Empfänger abrufbar ist; auf eine tatsächliche Kenntnisnahme kommt es nicht an. Ein weiterer minimaler Unterschied ergibt sich aus der für § 187 Hs. 1 StGB geltenden Rechtfertigungsmöglichkeit nach § 193 StGB, die zwar einer ähnlichen Entsprechung in Form der durch § 201b Abs. 2 StGB-E bezuggenommen Sozialadäquanzklausel aus § 201a Abs. 4 StGB entgegensteht, mit dieser aber nicht vollends identisch ist. Diese Nuancen in der strafrechtlichen Würdigung lassen einen eigenen Tatbestand allerdings kaum erforderlich erscheinen.

## 3. Kritische Würdigung

Anders als § 184k StGB-E überzeugt der geplante § 201b StGB-E nicht. Die Vorschrift importiert die Probleme, die bereits den Umgang mit Fake News in §§ 186 und 187 StGB erschweren.<sup>65</sup> Wann ein Inhalt geeignet ist, dem Ansehen dieser Person erheblich zu schaden, ist in hohem Maße interpretationsoffen. Können dafür politische Positionen genügen, die einer Person zugeschrieben werden? Und ob die im Entwurf als Beispiel angeführte vorgebliche Werbung eines bekannten Mediziners für ein bestimmtes Produkt stets eine Ansehensschädigung bedeutet, dürfte zweifelhaft sein. Solange sich das vorge-täuschte Verhalten nicht als rechtswidrig darstellt, bleibt der Ansehensverlust gerade in einer Gesellschaft mit unterschiedlichen Wertesystemen eine komplexe Einschätzungsfrage.

<sup>57</sup> Lantwin, MMR 2020, 78; a.A. Greif, Strafbarkeit von bildbasierten sexualisierten Belästigungen, 2023, S. 236.

<sup>58</sup> Teilweise wird sogar gefordert, dass Ausnahmen zum strafbewehrten Verbreiten im Kreis enger Vertrauensbeziehungen gemacht werden soll, Specht-Riemenschneider, in: Dreier/Schulze, KunstUrhG, 8. Aufl. (2025), § 22 Rn. 9.

<sup>59</sup> Specht-Riemenschneider, in: Dreier/Schulze, KunstUrhG, § 22 Rn. 9.

<sup>60</sup> Woerlein, MMR-Aktuell 2024, 01624; Pfeiffer, MMR 2025, 934.

<sup>61</sup> Doerbeck, Cybermobbing, S. 152.

<sup>62</sup> Regge/Pegel, in: MüKo-StGB, § 186 Rn. 18.

<sup>63</sup> Doerbeck, Cybermobbing, S. 153.

<sup>64</sup> Pfeiffer, MMR 2025, 934 (936).

<sup>65</sup> Vgl. Hoven, ZStW 129 (2017), 718.

Eine vielleicht ungewollte Einschränkung ergibt sich aus dem Wortlaut der Vorschrift, der den Anschein eines „tatsächlichen Geschehens“ verlangt. Ist der Inhalt offensichtlich als KI gekennzeichnet, entfällt der Anschein der Authentizität – mit der Folge, dass der Tatbestand nicht zur Anwendung käme. Dabei sind auch Inhalte denkbar, die trotz Kennzeichnung ansehensverletzend wirken – etwa, weil sie grob entwürdigend erscheinen.

Die vorgeschlagene Regelung greift daher in jeder Hinsicht zu kurz. Der Gesetzgeber sollte hier zunächst differenzieren: Welche Inhalte sind (vergleichbar den sexualisierten Deepfakes) derart persönlichkeitsverletzend, dass sie selbst bei Kennzeichnung untersagt werden müssen. Hier muss eine Strafvorschrift so formuliert sein, dass eine Strafbarkeit nicht durch ein Kennzeichen umgangen werden kann. Darüber hinaus sollten Deepfakes aber nicht allein als Problem individueller Persönlichkeitsrechte adressiert werden, sondern als Grundlage für Desinformation. Man stelle sich vor, dass ein KI-Video von Bundeskanzler *Friedrich Merz* in Umlauf gebracht würde, in dem er Russland den Krieg erklärt und die Bevölkerung dazu aufruft, sich durch Hamsterkäufe auf einen drohenden Krieg vorzubereiten. Eine Ansehensschädigung wäre das wohl nicht – aber eine gefährliche Falschinformation. Gleiches gilt für Deepfake-Videos über fingierte Kriegsverbrechen oder angebliche Experteninterviews zu einem Virus. Anstatt eine Spezialvorschrift für Persönlichkeitsverletzungen zu schaffen – die bereits weitgehend durch das Kunsturhebergesetz oder das Gesetz gegen den unlauteren Wettbewerb erfasst sind – sollte eine holistische Regelung gefunden werden, die das Problem von Desinformationen durch Deepfakes adressiert. Eine straf- oder bußgeldbewehrte Kennzeichnungspflicht erscheint hier als die bessere Alternative.

#### IV. Fazit

Trotz des rasanten Tempos hat das BMJV einen teilweise überzeugenden Entwurf zur strafrechtlichen Ahndung bildbasierter sexualisierter Gewalt vorgelegt. § 184k StGB-E schließt offenkundige Regelungslücken und pönalisiert relevante Kriminalitätsphänomene. Die geplante Neufassung ist auch deshalb zu begrüßen, weil sie dem Recht auf sexuelle Selbstbestimmung weitere Konturen verleiht. Die Sexualautonomie kann nicht nur durch

reale Übergriffe, sondern auch durch Bildaufnahmen und Deepfakes gefährdet werden. Diesen neuen Risiken zu begegnen, ist überfällig. Es bleibt gleichwohl zu hoffen, dass sich der Gesetzgeber die Zeit nimmt, um Kritik an den Details der geplanten Vorschriften aufzunehmen und Formulierungen sowohl im geplanten Gesetzestext als auch in dessen Begründung nachzubessern.

Abstand nehmen sollte der Gesetzgeber hingegen von § 201b StGB-E. Der Entwurf steht in keinem notwendigen Zusammenhang zu den aktuellen Debatten; er wirkt vielmehr wie ein Trittbrettfahrer in der derzeitigen Diskussion um sexualisierte bildbasierte Gewalt. Die Vorschrift bietet in ihrer derzeit vorgesehenen Ausgestaltung auch keinen ernsthaften Mehrwert: Ihr Anwendungsbereich deckt sich weitestgehend mit § 187 StGB. Zugleich erscheint die Beschränkung auf eine Ansehensschädigung wenig nachvollziehbar; so wird über kurz oder lang ein Flickenteppich verschiedener Vorschriften zur Ahndung unterschiedlicher Formen von Deepfakes entstehen. Statt hier einen Schnellschuss vorzunehmen, sollte grundlegend über den rechtlichen Umgang mit Deepfakes gerade als Instrument zur Verbreitung von Desinformation nachgedacht werden.

Im Übrigen bleibt ein zentraler von *Collien Fernandes* erhobener Vorwurf vom Entwurf des BMJV unbeachtet. Das Phänomen des Identitätsdiebstahls, etwa in Gestalt der Erstellung und Nutzung fremder Profile zur Kommunikation unter falscher Identität, wird bislang in seinem Unrechtsgehalt nicht eigenständig adressiert. Das Strafrecht erschöpft sich hier in einem fragmentarischen Regelungsgefüge, das die strukturellen Besonderheiten digitaler Täuschung nur unzureichend erfasst.

Bei alledem sollte nicht vergessen werden, dass Reformen des materiellen Strafrechts nur die Grundlage für einen tatsächlich anderen Umgang mit sexualisierter digitaler Gewalt bilden können. Eine Neuregelung würde ein klares Signal an die Ermittlungsbehörden senden, das Unrecht der Taten ernst zu nehmen und sie konsequent zu verfolgen. Ohne hinreichende Kapazitäten in der Justiz, ohne Schulungen und Spezialisierungen in den Strafverfolgungsbehörden bleibt auch das beste Strafgesetz ein stumpfes Schwert.

## Eingriffe in das Persönlichkeitsrecht – die zwangsweise Entsperrung von Mobiltelefonen

von Leo-Valery Zaruba\*

### Abstract

*Die Entscheidung des BGH vom 13. März 2025 nimmt die zwangsweise Entsperrung von Mobiltelefonen mittels Fingerabdrucks im Rahmen von Wohnungsdurchsuchungen in den Blick. Der Beitrag untersucht die berührten Grundrechte (informationelle Selbstbestimmung, IT-Grundrecht, nemo-tenetur), bewertet einschlägige StPO-Vorschriften und vergleicht obergerichtliche Entscheidungen, um offene Rechtsfragen und Handlungsoptionen zu erläutern.*

*The BGH decision of 13 March 2025 brings compulsory fingerprint unlocking of mobile phones during residential searches into focus. This article analyses the fundamental rights at stake (informational self-determination, IT fundamental right, nemo tenetur), evaluates relevant StPO provisions and higher-court practice, and explain remaining legal questions and policy options.*

### I. Einleitung

Am 13. März 2025 erging ein Beschluss des Zweiten Strafsenats des BGH, wonach die Entsperrung eines Mobiltelefons unter Anwendung von Zwang grundsätzlich zulässig ist.<sup>1</sup> Hierbei handelt es sich um die erste höchstgerichtliche Entscheidung zu dieser Rechtsfrage.<sup>2</sup> Bereits kurze Zeit zuvor hatte das OLG Bremen in einem Beschluss zur Problematik der zwangsweisen Entsperrung von Mobiltelefonen mittels Fingerscans im Rahmen eines Strafverfahrens Stellung genommen und die Maßnahme ebenfalls als rechtmäßig erachtet.

Das Smartphone, inzwischen nicht aus unserer Gesellschaft wegzudenken, ist Wegbegleiter, Tagebuch, Kamera, Computer und vieles mehr in einem, letztlich ein präzedenzloser Datenschatz. Mit jedem Zugriff eines Dritten auf ein fremdes Smartphone wird die Privatsphäre massiv beeinträchtigt. Handelt es sich bei diesem Dritten um den Staat, entsteht unmittelbar eine strafrechtliche, strafprozessuale und grundrechtliche Problematik. Diese ist auch von der Rechtsprechung erkannt worden; gleich-

wohl wurden staatliche Eingriffe teilweise mit fragwürdiger Argumentation gebilligt. Faktisch stellt das Handy inzwischen eine Standardquelle für Beweise dar. Die Unklarheiten hinsichtlich der Eingriffsbefugnisse betreffen jedes Jahr den Beschuldigten, Ermittlungsbeamten und Gerichte gleichermaßen.

### II. Sachverhalt und Lösungsansatz des BGH

Der Entscheidung des BGH ging ein Verdacht auf Verstoß gegen das Berufsverbot gem. § 145c StGB voraus.<sup>3</sup> Während einer Wohnungsdurchsuchung beim Beschuldigten zwangen die Ermittlungsbeamten diesen, sein Handy zu entsperren.<sup>4</sup> Dies erfolgte mit Hilfe eines biometrischen Fingerabdrucks, d.h. mithilfe von menschlichen Messdaten, die die eigene Person identifizieren können.<sup>5</sup> Die Wohnungsdurchsuchung diente u.a. dem Zweck, das Mobiltelefon aufzufinden, da es für die Strafbarkeit relevant sein konnte.<sup>6</sup> Im Revisionsverfahren wurde ein Beweisverwertungsverbot mit dem Hauptargument gerügt, dass keine Rechtsgrundlage für die Entsperrung unter Zwang des Mobiltelefons des Beschuldigten existierte, sodass eine Verletzung nach § 261 StPO vorliege.<sup>7</sup>

Es überrascht nicht, dass der BGH und andere Gerichte mit gewissen Abweichungen<sup>8</sup> Möglichkeiten zu einer Lösung suchten. Zusammengefasst soll eine zwangsweise Entsperrung möglich sein, wenn unter Zugrundelegung des Tatbestandes von § 81 Abs. 1 StPO auch nach einer „nach §§ 102, 105 Abs. 1 StPO richterlich angeordneten Durchsuchung gerade auch dem Auffinden von Mobiltelefonen dient und der beabsichtigte Datenzugriff trotz seiner Eingriffsintensität verhältnismäßig ist.“<sup>9</sup>

### III. Nemo-Tenetur: Wird der besondere Schutz verkannt?

Der nemo-tenetur Grundsatz wurde in den Entscheidungen der Gerichte stets abgelehnt.<sup>10</sup> Die Selbstbelastungsfreiheit, die sich aus Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG aufgrund dessen Nähe zu der Menschenwürde

\* Leo-Valery Zaruba ist Student der Rechtswissenschaften an der Friedrich-Alexander Universität Erlangen-Nürnberg und als studentische Hilfskraft am Lehrstuhl für Bürgerliches Recht, Internat. Privatrecht und Rechtsvergleichung in Erlangen tätig. Der Verfasser beschäftigt sich im Rahmen seiner Seminararbeit mit der zwangsweisen Entsperrung von Mobiltelefonen.

<sup>1</sup> BGH, NStZ 2025, 560.

<sup>2</sup> OLG Bremen, BeckRS 2025, 295.

<sup>3</sup> BGH, BeckRS 2025, 9876 Rn. 1.

<sup>4</sup> BGH, BeckRS 2025, 9876 Rn. 19.

<sup>5</sup> Vgl. BSI, <https://www.bsi.bund.de/dok/6614894>, zuletzt abgerufen am 12.3.2025.

<sup>6</sup> BGH, BeckRS 2025, 9876 Rn. 18.

<sup>7</sup> BGH, BeckRS 2025, 9876 Rn. 23.

<sup>8</sup> OLG Bremen, BeckRS 2025, 295; LG Ravensburg, NStZ 2023, 446.

<sup>9</sup> Amtlicher Leitsatz BGH, BeckRS 2025, 9876.

<sup>10</sup> Anschaulich BGH, BeckRS 2025, 9876 Rn. 32: „da diese lediglich vor der aktiven Mitwirkung an der eigenen Überführung, nicht aber vor dem Dulden von Ermittlungsmaßnahmen schützt.“

ergibt,<sup>11</sup> besagt jedoch, dass „niemand gezwungen werden [kann], sich selbst durch eine Aussage einer Straftat zu bezichtigen und damit zu seiner Überführung beizutragen oder anders als durch Äußerungen zum Untersuchungsgegenstand aktiv an der Aufklärung des Sachverhalts (...) mitzuwirken“.<sup>12</sup> Vordergründig darf der Beschuldigte also nicht zum Instrument des Strafverfahrens werden.<sup>13</sup>

Jedoch muss von einer (aktiven) Mitwirkung Folgendes unterschieden werden. Bei passiven Handlungen, wie der Duldung einer Zwangsmaßnahme, greift der nemo-tenetur Grundsatz nach herrschender Auffassung nicht.<sup>14</sup> Beispielsweise sei der § 81a Abs. 1 StPO genannt. Hiernach kann der Körper des Beschuldigten untersucht werden, wobei der Fokus darauf liegt, dass der Untersuchte einen „objektive[n] Personalbeweis“<sup>15</sup> darstellen soll, der notwendigerweise eine passive Duldung erforderlich macht. Denn schon allein der Untersuchungsvorgang an sich setzt denklingsch voraus, dass der Beschuldigte sich untersuchen lässt. Wie sonst könnte z.B. eine Blutabnahme nach § 81a Abs. 1 S. 2 Alt. 1 StPO erfolgen?

Nach herrschender Meinung ist der Beschuldigte nicht verpflichtet, seine Zugangsdaten aktiv preiszugeben oder selbst einzugeben,<sup>16</sup> da eine entsprechende Mitwirkung regelmäßig nur unter Anwendung von Drohung, Gewalt oder Täuschung erzwungen werden könnte.<sup>17</sup> Er hat jedoch das zwangsweise Führen und Auflegen seines Fingers auf den Sensor zu dulden.<sup>18</sup> Demgegenüber besteht keine Pflicht, die Augen unter Täuschung oder Zwang aktiv zu öffnen;<sup>19</sup> das bloße Heranführen des Mobiltelefons an die Augen kann hingegen zulässig sein, vergleichbar der Abnahme einer Brille zur Ermöglichung der Identitätsfeststellung.<sup>20</sup> Die insoweit vorgenommene Differenzierung zwischen aktiver und passiver Mitwirkung erweist sich als kaum trennscharf, führt zu Rechtsunsicherheit und erscheint dogmatisch konstruiert.<sup>21</sup>

Wenn behauptet wird, es gehe in erster Linie um ein Wissen des Betroffenen (z.B. das Passwort) für die Differenzierung zwischen aktiver und passiver Mithilfe, sodass eine Biometrieingabe als passive Duldungsmaßnahme zu

bewerten sei,<sup>22</sup> so wird verkannt, dass eine starke Nähe zur Menschenwürde beim nemo-tenetur Grundsatz besteht.<sup>23</sup> Mithin würden zu viele Ausnahmen und Differenzierungen letztlich den Beschuldigten als Objekt darstellen lassen.<sup>24</sup> Wo, wenn nicht in der zwangsweisen Führung des Fingers auf seinem eigenen Smartphone, kann eine massive Belastung der eigenen Person durch eine letztlich „aktive“ oder erzwungene Handlung zu sehen sein? Die Rechtsprechung verweist pauschal auf eine passive Duldungspflicht, aber bereits die zwangsweise Führung des Fingers oder ggf. das Aufreißen der Augen darf nicht als „passive Maßnahme“ angesehen werden.<sup>25</sup> Dies lässt schon der Menschenwürdegehalt des Grundsatzes nicht zu, andernfalls wird der Beschuldigte zum bloßen Instrument.<sup>26</sup>

#### IV. Grundrechte: Welche sind stets tangiert?

Durch das zwangsweise Führen des Fingers auf dem Smartphone ist die körperliche Unversehrtheit im Sinne des Art. 2 Abs. 2 S. 1 Alt. 2 GG nicht berührt. In Fällen einer lediglich kurzfristigen, schmerzfreien und unerheblichen<sup>27</sup> Beeinträchtigung kann regelmäßig kein relevanter Grundrechtseingriff vorliegen, sodass der Schutzbereich nur ausnahmsweise eröffnet sein kann. Da zudem nicht der laufende Kommunikationsvorgang, sondern ausschließlich das bereits abgeschlossene Kommunikationsergebnis betroffen ist, ist Art. 10 GG in der Regel ebenfalls nicht einschlägig.<sup>28</sup>

Dagegen ist der Schutzbereich des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG<sup>29</sup> (APR) stets eröffnet. Darunter fällt das Recht auf informationelle Selbstbestimmung (RiS),<sup>30</sup> das „Grundrecht auf Datenschutz“<sup>31</sup>. Dieses erfasst das Recht, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“.<sup>32</sup> Das RiS ist also dann verletzt, wenn über die etwaige Preisgabe von Daten nicht mehr der Betroffene entscheiden kann.<sup>33</sup> Eine Entsperrung durch Biometrie führt zwar nicht zu dem sofortigen Auslesen der Daten, jedoch öffnet sie dem Entsperrenden die Möglichkeit der

<sup>11</sup> BGHSt 58, 301; Dreier, in: Dreier, GG, 4. Aufl. (2023) Art. 1 Abs. 1 Rn. 139; Eichberger, in: Huber/Voßkuhle, GG, 8. Aufl. (2024), Art. 2 Rn. 366.

<sup>12</sup> BGHSt 52, 11 (17).

<sup>13</sup> Vgl. Nicolai, Das Internet der Dinge und das Strafrecht – Herausforderungen vernetzter Geräte für das materielle Strafrecht und das Strafprozessrecht, 2023, S. 366 f.

<sup>14</sup> BVerfGE 56, 37 (42); Nadeborn/Irscheid, StraFO 2019, 274 (275); Meyer, in: Karpenstein/Mayer, Konvention zum Schutz der Menschenrechte und Grundfreiheiten: EMRK, 3. Aufl. (2022), Art. 6 Rn. 142.

<sup>15</sup> Rogall, in: SK-StPO, Bd. 1, 5. Aufl. (2018), § 81b Rn. 37.

<sup>16</sup> Schlothauer, in: Müller/Schlothauer/Knauer, Münchener Anwalts-handbuch Strafverteidigung, 3. Aufl. (2022), § 3 Rn. 111; mit Verweis auf die Menschenwürde: Horn, Kriminalistik 2019, 641 (642); vgl. Rettke, NZWiSt 2020, 45 (52).

<sup>17</sup> OLG Bremen, NSZ 2025, 566 (567); Ladiges, Die Polizei 2014, 70 (71); Kasiske, StraFO 2010, 228 (233).

<sup>18</sup> Vgl. BGHSt 34, 39 (45).

<sup>19</sup> Zur Täuschung: BGHSt 40, 66 (71 f.).

<sup>20</sup> Krause, in: LR-StPO, 27. Aufl. (2017), § 81b Rn. 21.

<sup>21</sup> Vgl. auch Nicolai, StV-S 2023, 148.

<sup>22</sup> BGH, BeckRS 2025, 9876 Rn. 32; Dölker/Müller-Peltzer, DSRITB 2015, 863 (872 ff.); kritisch Satzger/Safraz, NSZ 2025, 560 (566).

<sup>23</sup> BVerfGE 156, 63 (115); BGH, NJW 2018, 1986 (1987); Eschelbach, in: Münchener Anwalts-handbuch Strafverteidigung, § 31 Rn. 106; Horn, Kriminalistik 2019, 641 (642).

<sup>24</sup> Eichberger, in: Huber/Voßkuhle, GG, Art. 2 Rn. 366; vgl. van Ender, in: Heusch/Ullrich/Posser, Handbuch Verfassungsrecht in der Praxis, 2024, § 12 Rn. 3.

<sup>25</sup> Sehr differenzierend: Neuhaus, StV 2020, 489 (491).

<sup>26</sup> Vgl. Nicolai, S. 366 f.; vgl. Meyer, in: SK-StPO, Bd. 10, 5. Aufl. (2019), Art. 6 EMRK Rn. 1.

<sup>27</sup> BVerfGE 56, 54 (75 ff.); vgl. Horn, in: Stern/Becker, GG, 4. Aufl. (2024), Art. 2 Rn. 125.

<sup>28</sup> BVerfGE 67, 157 (172); Wenzel, NZWiSt 2016, 85 (88); M. Martini, in: v. Münch/Kunig, GG, 8. Aufl. (2025), Art. 10 Rn. 12.

<sup>29</sup> BVerfGE 54, 148 (153); Papier/Shirvani, in: Dürig/Herzog/Scholz, GG, 107. EL (2025), Art. 14 Rn. 368.

<sup>30</sup> Barczak, in: Dreier, GG, Art. 2 Abs. 1 Rn. 90; BVerfGE 65, 1 (41 ff.).

<sup>31</sup> Bäumler, JR 1984, 361 (362).

<sup>32</sup> BVerfGE 115, 320 (341).

<sup>33</sup> BVerfGE 65, 1 (43); Lang, in: BeckOK-GG, 62. Ed. Stand: 1.7.2025), Art. 2 Rn. 115.

„schlichte[n] Kenntnisnahme“<sup>34</sup>, was einen Grundrechtseingriff nahelegt. Immerhin gibt der Beschuldigte unter Zwang das Geschehen völlig aus der Hand, seine Daten werden mit seiner Hilfe gänzlich grundsätzlich jedem Dritten zur Verfügung gestellt. Er überlässt es mithin anderen zu entscheiden, welche Lebenssachverhalte offengelegt werden.

Zudem ist das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme<sup>35</sup> (IT-Grundrecht)<sup>36</sup> verletzt. Das Smartphone ist dank seiner Eigenschaft als komplexes, technisches System entsprechend von dem sachlichen Schutzbereich des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG erfasst.<sup>37</sup> Die Rechtsprechung erkannte die besondere Bedeutung des IT-Grundrechts für solche Fälle an.<sup>38</sup>

Mit dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme wurde durch das *BVerfG* auch eine Schutzlücke geschlossen, die das Recht auf informationelle Selbstbestimmung hinterließ. So schützt das RiS vor der Erhebung einzelner Daten,<sup>39</sup> dagegen das IT-Grundrecht schützt sogar davor, dass „auf das informationstechnische System insgesamt zugegriffen wird“.<sup>40</sup> Daraus wird der besondere Schutz des informationstechnischen Systems an sich deutlich, unabhängig davon, ob und wie ein Datenabfluss erfolgt. Denn sobald das Smartphone erfolgreich entsperrt wurde, erübrigen sich alle weiteren Datenverarbeitungen, da so der gesamte Datenbestand geöffnet ist.<sup>41</sup> Hier wird nun mit dem Zwang das Smartphone entsperrt und die Daten dann z.B. für die Ermittlungsbeamten als Dritte zugänglich gemacht. Bereits die Entsperrung durch Biometrie oder durch vergleichbare Handlungen<sup>42</sup> nimmt die wesentliche Hürde hinsichtlich des Schutzes, sodass das IT-Grundrecht hier tangiert ist.<sup>43</sup> Denn der Schutzbereich der *Integrität* des Systems ist dadurch massiv verletzt,<sup>44</sup> das Handy wurde (unter Zwang) geöffnet. Das APR bzw. das RiS wie IT-Grundrecht ist mitunter in jedem erdenklichen Fall tangiert. Nötig ist mithin eine Ermächtigungsgrundlage, Art. 20 Abs. 3 GG.<sup>45</sup>

## V. Derzeitiger Meinungsstand in Literatur und Rechtsprechung

Der *BGH* verneint dies auch nicht<sup>46</sup>; jedoch herrscht Streit, über die Natur einer Ermächtigungsgrundlage hierzu.

### 1. Erster Anhaltspunkt: § 81a Abs. 1 StPO

Gemäß § 81a Abs. 1 StPO können körperliche Untersuchungen vorgenommen werden. Durch das Verwenden des Fingers wird ein Teil des Körpers „genutzt“,<sup>47</sup> was für eine Anwendung spräche.<sup>48</sup> Entscheidend ist jedoch, unabhängig davon, ob überhaupt eine körperliche Untersuchung tatsächlich vorliegt,<sup>49</sup> dass der Körper des Beschuldigten das Beweismittel sein soll.<sup>50</sup> Ein Beispiel wären Tattoos am Körper des Beschuldigten,<sup>51</sup> die zu dessen Identifizierung führen können. § 102 StPO regelt, inwieweit Sachen am Körper oder der Kleidung der Person gesucht werden können.<sup>52</sup> Hieran zeigt sich, dass § 81a Abs. 1 StPO im Umkehrschluss den Beweisgegenstand „Körper“ selbst erfassen muss,<sup>53</sup> sowie das Innere des Körpers durch ggf. körpereigene Öffnungen.<sup>54</sup> Bei der Entsperrungsproblematik sind dagegen die innewohnenden Daten und nicht der Körper entscheidend.<sup>55</sup>

### 2. Der (Irr)Weg der herrschenden Ansicht: § 81b Abs. 1 StPO

Der *BGH* sowie das *OLG Bremen* und Teile der Literatur verweisen auf § 81b Abs. 1 StPO.<sup>56</sup> Entscheidend bei der erkennungsdienstlichen Maßnahme des § 81b Abs. 1 StPO, ist die Trennung zwischen dem Ziel einer Maßnahme und der Maßnahme selbst; nur bei Vorhandensein einer geeigneten Zielrichtung, könnte eine Maßnahme daraus resultieren. Nach § 81b Abs. 1 Alt. 1 StPO sollen etwaige Maßnahmen der Durchführung des Strafverfahrens und nach § 81b Abs. 1 Alt. 2 StPO dem Erkennungsdienst dienen.

Das Wort „Biometrie“ erwähnt der Wortlaut jedoch nicht. Die Überschrift des § 81b StPO könnte dahingehend ausgelegt werden, dass im Vordergrund die Identifizierung liege, vgl. „Erkennungsdienstlich“. Insbesondere werde

<sup>34</sup> *Di Fabio*, in: Dürig/Herzog/Scholz, GG, 105. EL (2024), Art. 2 Abs. 1 Rn. 176.

<sup>35</sup> *BVerfG*, WM 2008, 503; *Lang*, in: BeckOK-GG, Art. 2 Rn. 123b; *Burghart*, in: Leibholz/Rinck, GG, 92. Lf. (2024), Art. 2 Rn. 124.

<sup>36</sup> *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 186; *Luch*, MMR 2011, 75.

<sup>37</sup> *BVerfGE* 120, 274 (314); *Eichberger*, in: Huber/Voßkuhle, GG, Art. 2 Rn. 346.

<sup>38</sup> *OLG Bremen*, BeckRS 2025, 295 Rn. 13; *LG Ravensburg* NStZ 2023, 446.

<sup>39</sup> *Kingreen/Poscher*, Staatsrecht II, 40. Aufl. (2024) Rn. 537; vgl. *Burghart*, in: Leibholz/Rinck, GG, Art. 2 Rn. 124.

<sup>40</sup> So *BVerfGE* 120, 294 (313); kritisch hier zu *Sodan*, in: Sodan, GG, 5. Aufl. (2024), Art. 2 Rn. 6c; *Gurlit*, NJW 2010, 1035 (1037).

<sup>41</sup> *Franzius*, ZJS 2015, 259 (262 ff.).

<sup>42</sup> Vgl. Entsperrung durch den Iris-Scan, oder durch Appel-Watch auf dem Arm, bei dem das „Wischen“ über das Handy reicht.

<sup>43</sup> *BVerfGE* 120, 274 (314).

<sup>44</sup> *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 175; vgl. *Gersdorf*, in: BeckOK-InfoMedienR, 48. Ed. (Stand: 1.11.2024), Art. 2 Rn. 39; *Hortler*, NStZ 2023, 446 (447).

<sup>45</sup> *Leisner*, in: Sodan, GG, Art. 20 Rn. 48 ff.; *Jarass*, in: Jarass/Pieroth, GG, 18. Aufl. (2024) Art. 20 Rn. 69 f.

<sup>46</sup> *BGH*, BeckRS 2025, 9876 Rn. 28, Rn. 33, Rn. 42 mit Verweis auf *BVerfGE* 120, 274 (323) ohne das IT-Grundrecht zu nennen.

<sup>47</sup> Vgl. *AG Wuppertal*, BeckRS 2017, 166377 Rn. 7.

<sup>48</sup> S. Normüberschrift „Zulässigkeit körperlicher Eingriffe“.

<sup>49</sup> Verneinend *Grzesiek/Zühlke*, StV-S 2021, 117 (118).

<sup>50</sup> *Rottmeier/Eckel*, NStZ 2020, 193 (196 f.); *Brauer*, in: Gercke/Temming/Zöller, StPO, 7. Aufl. (2023), § 81a Rn. 6.

<sup>51</sup> *Trück*, in: MüKo-StPO, 2. Aufl. (2023) § 81 Rn. 9.

<sup>52</sup> Vgl. *Krause*, in: LR-StPO, § 81a Rn. 19; *Hausschild*, in: MüKo-StPO, § 102 Rn. 24.

<sup>53</sup> Vgl. *Jäger/Wohlers*, in: SK-StPO, Bd. 2, 6. Aufl. (2025), § 102a Rn. 13; *Soiné*, in: Soiné, StPO, 150. Lf. (2025), § 81a Rn. 7.

<sup>54</sup> *Goers*, in: BeckOK-StPO, 56. Ed. (Stand: 1.7.2025), § 81a Rn. 5; vgl. *Hadamitzky*, in: KK-StPO, 9. Aufl. (2023) § 81a Rn. 6.

<sup>55</sup> *BGH*, BeckRS 2025, 9876 Rn. 25; *Rottmeier/Eckel*, NStZ 2020, 193 (197); vgl. *Momsem*, DRiZ 2018, 140 (141).

<sup>56</sup> *BGH*, BeckRS 2025, 9876 Rn. 37; *OLG Bremen*, MMR 2025, 641 (642).

hierfür die Einschränkung herangezogen, dass alle Maßnahmen erfasst sind, die die körperliche Untersuchung bzw. Feststellung der körperlichen Beschaffenheit betreffen, aber nicht von § 81a Abs. 1 StPO erfasst seien.<sup>57</sup>

Es sollten aber auch anhängige Strafverfahren vorangebracht werden können,<sup>58</sup> wie auch der Wortlaut der Norm selbst „Durchführung des Strafverfahrens“ signalisiere. Daher seien trotz der widersprüchlichen Überschrift zwei verschiedene Zielrichtungen genannt. Somit läge eine Zweckbestimmung vor, die zu weitergehenden Handlungen berechtigt.<sup>59</sup> Anknüpfungspunkt für die zwangsweise Entsperrung ist dann der Zweck der Durchführung des Strafverfahrens, sofern z.B. konkrete Anhaltspunkte bestehen, dass der Beschuldigte in eine Tat involviert war.<sup>60</sup> Knüpft man an diese Zweckrichtung an, erscheint § 81b Abs. 1 Var. 3 a.E. StPO als Befugnis denkbar.

Der Wortlaut „ähnliche Maßnahmen“ nach § 81b Abs. 1 Var. 3 a.E. StPO ist einer weiten Interpretation zugänglich. In Kombination mit § 81b Abs. 1 Var. 1 a.E. „Lichtbild“ oder Var. 2 a.E. StPO „Fingerabdruck“ wäre (auch) eine bloße biometrische Nutzung zur Entsperrung vom Wortlaut erfasst.<sup>61</sup> Dafür könnte sprechen, dass § 81b Abs. 1 StPO bewusst „technikoffen“<sup>62</sup> formuliert ist und mithin auch eben ähnlich gelagerte, neue Fälle in der Zukunft erfassen soll.

Teleologisch gesehen kann angeführt werden, dass § 81b Abs. 1 StPO sogar die dauerhafte Speicherung biometrischer Daten (Fingerabdrücke) ermöglichen könnte, wie der Wortlaut „Aufnahme“ andeutet.<sup>63</sup> Dagegen wäre eine bloße Verwendung des Fingers auf dem Sensor ein „Minus“ zu einer dauerhaften Speicherung,<sup>64</sup> sodass der Grundrechtseingriff in diesem Fall sogar geringer ausfallen würde. Man könnte einen Erst-Recht-Schluss wagen, da eine kurze „Nutzung“ der biometrischen Daten vorliegt und eine dauerhafte Speicherung nicht nötig ist.<sup>65</sup> Ähnlich wie § 81a Abs. 1 StPO auf die Gewinnung und Auswertung einer Blutprobe als Beweismittel gerichtet ist und der damit verbundene körperliche Eingriff lediglich vorbereitenden Charakter hat,<sup>66</sup> verhält es sich auch hinsichtlich der auf dem Mobiltelefon gespeicherten Daten: Die kurzfristige zwangsweise Entsperrung stellt insoweit lediglich eine vorgelagerte Maßnahme dar, die der Erlangung der beweiserheblichen Informationen dient.

Die Vorschrift des § 81b Abs. 1 StPO erfasst bereits ausdrücklich die Aufnahme von Fingerabdrücken, die Verbindung mit dem Smartphone wäre entsprechend nur eine konsequente Fortführung des Zwecks zur „Durchführung des Strafverfahrens“.<sup>67</sup> Außerdem würden die Vorschriften der §§ 94 ff., 102 ff. StPO andere Folgemaßnahmen regeln,<sup>68</sup> sodass auch keine umfassende Generalnorm in § 81b Abs. 1 StPO vorläge. Die Voraussetzungen dieser Vorschriften müssten ebenfalls geprüft werden. Schließlich erfolge auch eine Authentifizierung im Sinne einer Identifizierung nach § 81b StPO, denn der Daumen des Beschuldigten und die Öffnung des Smartphones lassen Rückschlüsse auf dessen Person zu.<sup>69</sup>

#### a) Verfehlt Zweck

Die konkrete Zielsetzung des § 81b Abs. 1 StPO liegt aber darin, bestimmte Merkmale zu erfassen, um entweder Identifizierungen vornehmen zu lassen oder etwaige Taten aufklären zu können, bspw. inwieweit man Fingerabdrücke bestimmten Verdächtigen zuordnen kann. Zentral ist die Erfassung dauerhafter, körperlicher Merkmale.<sup>70</sup>

Die Entsperrung mit der Biometrie geht aber deutlich weiter, denn sie schafft es, Informationen zu beschaffen bzw. zu offenbaren, die der Beschuldigte sonst niemals hätte preisgeben wollen.<sup>71</sup> Das Argument, dass die Biometrie auch eine Authentifizierung (d.h. Identifizierung durch Biometrie) zu Grunde habe,<sup>72</sup> geht ins Leere. Denn häufig teilen sich Personen Zugangsdaten, sodass das Smartphone von einem Dritten, bspw. von der Partnerin oder dem Partner mit dem Daumen genauso wie von dem oder der Eigentümer:in selbst entsperrt werden kann. Aber auch wenn Biometrie in der Regel zu einer konkreten Identifizierung führen sollte, ist und bleibt das Ziel der Entsperrung der Zugriff auf die dort liegenden Daten, was nicht in § 81b Abs. 1 StPO angelegt ist. Daran ändert sich auch nichts, wenn etwaige Folgemaßnahmen von §§ 94 ff. StPO erfasst sein könnten.

Bereits bei der Entsperrung müsste nämlich eine zulässige Zweckverfolgung nach § 81b Abs. 1 StPO vorliegen, wenn sie darauf fußen soll. Auch trotz zweier unterschiedlich klingender Alternativen („Strafverfahren“ und „Erkennungsdienst“) – in *beiden* Fällen steht der Erkennungsdienst im Vordergrund.<sup>73</sup> Das erkennungsdienstliche Ziel gem. Alt. 1 dient insbesondere dem Tatnachweis

<sup>57</sup> BGHSt 34 39 f.; Schmitt, in: Schmitt/Köhler, StPO, 68. Aufl. (2025), § 81b Rn. 8; Bock/Fülscher, StraFO 2023, 386 (387).

<sup>58</sup> Vgl. Brauer, in: Gercke/Temming/Zöller, StPO, § 81b Rn. 2; Schlothauer, in: Müller/Schlothauer/Knauer, Münchener Anwalts-handbuch Strafverteidigung, § 3 Rn. 172.

<sup>59</sup> Deutscher, StRR 2023, 26 (27 f.); vgl. Rogall, in: SK-StPO, § 81b Rn. 13; Trück, in: MüKo-StPO, § 81b Rn. 8.

<sup>60</sup> So Neuhaus, StV 2020, 489 (490).

<sup>61</sup> Im Ergebnis jedoch Anwendung von § 81b StPO verneinend Hor-ter, NStZ 2023, 446 (448).

<sup>62</sup> BGH, ZD 2025, 453 (454); OLG Bremen, BeckRS 2025, 295 Rn. 8; Hadamitzky, in: KK-StPO, § 81b Rn. 3; im Ergebnis aber ablehnend Ziebarth, GSZ 2025, 161 (162).

<sup>63</sup> Vgl. Rottmeier/Eckel, NStZ 2020, 193 (200); LG Ravensburg, GSZ 2024, 252 (256); Bosch, in: KMR-StPO, 133. Aktual. (2025), § 81b Rn. 11.

<sup>64</sup> Am LG Ravensburg dagegen lag eine vorgelagerte Aufnahme vor: LG Ravensburg, NStZ 2023, 446.

<sup>65</sup> Beukelmann/Heim, NJW-Spezial 2025, 154.

<sup>66</sup> Vgl. Trück, in: MüKo-StPO, § 81a Rn. 10; BVerfG, NJW 1996, 771 (772).

<sup>67</sup> Vgl. Bäumerich, NJW 2017, 2718 (2721).

<sup>68</sup> BGH, BeckRS 2025, 9876 Rn. 61; vgl. Mosbacher, JuS 2025, 742 (744); Krause, in: LR-StPO, § 81b Rn. 16.

<sup>69</sup> Ruhs, GSZ 2024, 252 (255); Beukelmann, NJW-Spezial 2024, 696.

<sup>70</sup> Vahle, Kriminalistik 1992, 158; Bosch, in: KMR-StPO, § 81b StPO, Rn. 11; Trück, in: MüKo-StPO, § 81b Rn. 16.

<sup>71</sup> Momsen, DRiZ 2018, 140 (141).

<sup>72</sup> Ruhs, GSZ 2024, 252 (255).

<sup>73</sup> Vgl. Kramer, JR 1994, 224 (225 f.).

bei einem potentiellen Beschuldigten oder dessen Identifizierung.<sup>74</sup> Dagegen ermöglicht das Strafverfahrensziel i.S.d. Alt. 2, dass auch präventiv ein Datenbestand biometrischer Merkmale geschaffen werden kann, um vorsorglich der Straftataufklärung dienen zu können.<sup>75</sup> Die Alternativen ergänzen sich einander, so dient Alt. 2 den Ermittlungsbeamten als Datengrundlage für zukünftige Verfahren.<sup>76</sup>

Weitergehende Zwecke, darunter insbesondere zwanghafte körperliche Eingriffe, sollten nicht pauschal erfasst werden, da im Ergebnis eine ausufernde „Entschlüsselungsnorm“<sup>77</sup> entstehen würde.<sup>78</sup> Mithilfe dieser Vorschrift könnte unter Zugrundelegung der Alt. 2 in Kombination mit den möglichen „ähnlichen“ Maßnahmen stets zurückgegriffen werden,<sup>79</sup> und damit verfassungsrechtliche Vorgaben für staatliches Handeln umgangen werden. Auch im Falle einer Bejahung von der Technikoffenheit der Maßnahmen, gibt dies keinen Rückschluss darauf, ob auch der Zweck entsprechend weit gefasst werden kann.<sup>80</sup> Stattdessen gilt das Identifizierungsziel weiterhin.

Der BGH führt die digitale Speicherung der Fingerabdrücke als Beispiel an,<sup>81</sup> zieht aber keinen Unterschied zu der Entsperrung heran. Er erkennt, dass es eben keine bloße Aufzeichnung von biometrischen Daten ist, sondern eine zwangsweise Entsperrung. Dennoch zieht er daraus ein Argument für die Anwendung von § 81b Abs. 1 StPO.<sup>82</sup> „Technikoffenheit“ meint lediglich, dass die Formulierung „ähnliche Maßnahme“ sich systematisch an den anderen beiden genannten Maßnahmen orientieren muss und neuere Entwicklungen auf diese Weise erfassen darf.<sup>83</sup>

Selbst bei großzügigster Auslegung des Begriffes „ähnliche Maßnahme“ besteht kein zulässiger Zweck. Besonders hervorzuheben ist, dass § 81b Abs. 1 StPO unter keinem Richtervorbehalt<sup>84</sup> steht, sodass der Eingriffstiefe<sup>85</sup> durch eine etwaige Verletzung der *Integrität* insoweit keine Rechnung getragen werden würde.<sup>86</sup> Auch das muss den Anwendungsbereich der Norm entsprechend einschränken.

#### b) Verpasste Chance in der Historie?

Historisch gesehen, hat der Gesetzgeber bei der Schaffung von § 81b StPO die Existenz von biometrischen Daten

und deren Erfassung in § 81b Abs. 1 StPO nicht vorhersehen können.<sup>87</sup> Dies spräche ebenfalls gegen eine Anwendung der Norm, weil es zahlreiche Möglichkeiten gab, die Normen entsprechend zu ergänzen, was aber z.B. bei der letzten Reform der StPO unterlassen wurde.<sup>88</sup> Angebracht wurde bei der Entstehung des § 81b StPO, dass die aufgenommenen Fingerabdrücke für Abgleiche mit vorhandenen biometrischen Daten von den Ermittlungsbeamten genutzt werden könnten. Letztlich diene § 81b Abs. 1 StPO ebenfalls für Identifizierungszwecke.<sup>89</sup> Eine Erfassung von biometrischen Daten, die dann zur Entsperrung von einem gewaltigen Informationsbestand genutzt werden, erscheint eine fernliegende Idee, die nicht erfasst werden konnte und ggf. sogar nicht erfasst werden sollte.<sup>90</sup>

#### c) Systematische Einwände

Neben „ähnliche Maßnahme“ müsste man systematisch stets „an ihm“, d.h. am Beschuldigten lesen, sodass eine Maßnahme an einem mobilen Endgerät (auch durch Führen des Fingers o.ä.) schwer erfasst werden kann.<sup>91</sup> In Bezug auf die Maßnahmen wurden unter dem Wortlaut „ähnlich“ z.B. folgende Fälle erfasst: Sicherung von Geruchsspuren;<sup>92</sup> die Aufzeichnung von Stimmspuren und von Sprachvergleichen;<sup>93</sup> (ggf. mit Zustimmung) sowie auch Fußabdrücke;<sup>94</sup> oder eine etwaige Bartveränderung.<sup>95</sup> Im Ergebnis drehen sich diese Beispiele darum, *Identifizierungsprozesse* mithilfe des Körpers zu erleichtern, und nicht darum, durch eine Beschaffenheit des Körpers oder der Verwendung von Körperteilen mehr Informationen zu generieren.

#### d) Zwischenstand: §§ 102, 105 Abs. 1 StPO sowie Verhältnismäßigkeit als Rettungsanker?

Der BGH verweist außerdem auf die Vorschrift des § 105 Abs. 1 StPO. Im Rahmen des Durchsuchungsverfahrens nach den §§ 102 ff. StPO, die häufig der Entsperrung vorausgehen,<sup>96</sup> soll ein richterlicher Beschluss ergehen.<sup>97</sup> In diesem Durchsuchungsbeschluss sind „die zu suchenden Beweismittel möglichst konkret zu bezeichnen“.<sup>98</sup>

<sup>74</sup> Bosch, in: SSW-StPO, 6. Aufl. (2025), § 81b Rn. 2; Schmitt, in: Schmitt/Köhler, § 81b Rn. 2.

<sup>75</sup> Vgl. BVerwGE 66, 192 (196); Bosch, in: SSW-StPO, § 81b StPO Rn. 3.

<sup>76</sup> Ausführlich, Kramer JR 1994, 224 ff.

<sup>77</sup> Jahn, JuS 2025, 791 (793).

<sup>78</sup> Ruppert, StV 2025, 565 (566); zur Gefahr einer zu starken Praxisorientierung der Norm: Schild, in: BeckOK-Datenschutzrecht, 53. Ed. (Stand: 1.8.2025), § 46 BDSG Rn. 52; den Zweck des Zugriffs dagegen billigend Goers, in: BeckOK-StPO, § 81b Rn. 4.1.

<sup>79</sup> Vgl. Bosch, in: SSW-StPO, § 81b Rn. 7.

<sup>80</sup> So Nicolai, StV-S 2023, 148 (149).

<sup>81</sup> BGH, BeckRS 2025, 9876 Rn. 40.

<sup>82</sup> BGH, BeckRS 2025, 9876 Rn. 40.

<sup>83</sup> Bosch, in: SSW-StPO, § 81b Rn. 7; vgl. BVerfGE 47, 252.

<sup>84</sup> Insoweit der „Königsweg des Grundrechtsschutzes“ für den Beschuldigten: Hüls, ZIS 2009, 160 m.w.N.

<sup>85</sup> Rückert, S. 489.

<sup>86</sup> Horter, NStZ 2023, 446 (448); Grzesiek/Zühlke StV 2021, 117 (119).

<sup>87</sup> Schweckendieck, ZRP 1989, 125 f.; BGBl., 455, 638 (Bundesgesetzblatt 1950 Nr. 40 am 20.9.1950), wo § 81b Abs. 1 StPO wortgleich seit 1950 bereits erwähnt ist.

<sup>88</sup> BGBl. I, S. 3420; Bück/Fülscher, StraFO 2023, 386 (388).

<sup>89</sup> Vgl. Beukelmann/Heim, NJW-Spezial 2023, 218.

<sup>90</sup> Vgl. Kramer, JR 1994, 224 (227 f.).

<sup>91</sup> Hecken/Ziegler, jurisPR-ITR Anm. 5.

<sup>92</sup> Maciejewski, NStZ 1995, 482 (483).

<sup>93</sup> Hadamitzky, in: KK-StPO, § 81b Rn. 3.

<sup>94</sup> Rogall, in: SK-StPO, § 81a Rn. 49.

<sup>95</sup> Kühne, Strafprozessrecht, 9. Aufl. (2015), Rn. 479.

<sup>96</sup> BGH, BeckRS 2025, 9876; OLG Bremen, BeckRS 2025, 295; LG Ravensburg, NStZ 2023, 446.

<sup>97</sup> BGH, BeckRS 2025, 9876 Rn. 52.

<sup>98</sup> BGH, BeckRS 2025, 9876 Rn. 52.

Zwar wird dem Argument des mangelnden Richtervorbehalts in § 81b Abs. 1 StPO Rechnung getragen,<sup>99</sup> an der Anwendbarkeit der Norm selbst ändert der Wohnungsdurchsuchungsbeschluss indes nichts. Grundsätzlich sollen sich die Gerichte an den bestehenden Maßnahmen der StPO orientieren. Dass nicht jeder Sachverhalt unter die StPO subsumiert werden kann, ist dem „Code law“ immanent. Der Richtervorbehalt hilft nicht aus einem etwaigen ermächtigungsfreien Handeln heraus.<sup>100</sup>

Der BGH weist in seinem Urteil ebenso mehrmals auf die Notwendigkeit einer Verhältnismäßigkeit hin.<sup>101</sup> Im Umkehrschluss kann davon ausgegangen werden, dass der BGH von einem massiven Grundrechtseingriff ausgeht. Doch gerade aufgrund der extremen Eingriffstiefe in das IT-Grundrecht wie in das RiS sowie der Instrumentalisierung des Beschuldigten im Widerspruch zum nemo-tenetur-Grundsatz erlaubt es, nicht eine etwaige Verhältnismäßigkeit der Maßnahme anzunehmen.<sup>102</sup> Zwar verfolgt die Entsperrung einen legitimen Zweck<sup>103</sup> (Strafverfolgung) und ist auch durchaus geeignet<sup>104</sup>, den Ermittlungsbeamten mithin einen uneingeschränkten und umfassenden Datenzugriff zu ermöglichen. Andere Ermittlungsmethoden, wie die Zeugenbefragung, das Auffinden von Zugangsdaten oder der externe Zugriff unter den strengen Voraussetzungen der §§ 100b ff. StPO, werden umgangen. Insoweit kann man an der Angemessenheit der Zwangsentsperrung zweifeln.<sup>105</sup> Denn selbst bei schweren Taten wird allein schon aus dem nemo-tenetur Verstoß ein deutlicher Verstoß gegen die Angemessenheit zu sehen sein.<sup>106</sup> Aufgrund der mangelnden Ermächtigungsgrundlage stellt sich die Frage nach der Verhältnismäßigkeit ohnehin nicht, sie ist ebenfalls kein Instrument um über rechtswidriges, *ermächtigungsfreies* Handeln hinwegzukommen.<sup>107</sup>

### 3. Umweg über Annexkompetenzen

Die Heranziehung der §§ 94 ff. StPO<sup>108</sup> oder des § 110 Abs. 3 StPO<sup>109</sup> als „Annexkompetenz“ für die zwangsweise Entsperrung ist auf den ersten Blick naheliegender als der Ansatz des BGH. § 94 Abs. 1 StPO erfasst Gegenstände<sup>110</sup> und damit auch Datenträger,<sup>111</sup> bzw.

inhaltlich relevante digitale Informationen.<sup>112</sup> Die Rechtsfigur der Annexkompetenz dient dazu, solche Maßnahmen zu legitimieren, die eine rechtmäßige Primärmaßnahme notwendigerweise begleiten, ihr funktional zugeordnet sind und ihrerseits den Anforderungen des Verhältnismäßigkeitsgrundsatzes genügen.<sup>113</sup> Bei physischen Behältnissen, wie z.B. bei Kisten, besteht keine dogmatische Barriere gegen ein gewaltsames Öffnen.<sup>114</sup> Überträgt man dieses Modell auf Smartphones, so erscheint es technisch denkbar, auch Schutzvorrichtungen zu überwinden, um an „inhaltlich relevante“ Daten zu gelangen.<sup>115</sup>

Rechtlich problematisch ist daran jedoch zweierlei. Erstens greift die Annexkompetenz nur dort, wo eine klare, bereits zulässige Primärmaßnahme besteht.<sup>116</sup> Sie kann nicht originär neue Eingriffsformen schaffen. Zweitens unterschätzt die Annex-Argumentation die besondere Schutzdimension informationstechnischer Systeme,<sup>117</sup> darunter insbesondere die Verletzung der Integrität des Geräts,<sup>118</sup> die eine spezielle gesetzliche Grundlage erfordert. Ferner ist zu beachten, dass die Annex-Logik bei biometrischer Entsperrung leicht zur Umgehung spezifischer StPO-Regelungen führt und damit den Gesetzesvorbehalt aushebelt.<sup>119</sup> Deshalb ist die bloße Reklamation einer Annexkompetenz keine überzeugende, dauerhaft tragfähige Lösung. Sie bleibt allenfalls „Übergangstechnik“, nicht aber Ersatz für eine klar geregelte Ermächtigungsnorm.

### 4. Entsperrung unter höheren Anforderungen der §§ 100a ff. StPO

Den eher geringen Anforderungen an § 81b Abs. 1 StPO könnten also stattdessen z.B. die Voraussetzungen der Onlinedurchsuchung nach § 100b Abs. 1 StPO entgegenhalten werden.<sup>120</sup> Angeknüpft werden kann an die Formulierung in § 100b Abs. 1 S. 1 StPO: „darf mit technischen Mitteln in ein von dem Betroffenen informationstechnische Systeme eingegriffen werden“. So erscheint eine Entsperrung als Eingriff darunter erfasst, ggf. eine Analogie<sup>121</sup> für die zwangsweise Entsperrung erschiene in Bezug auf den Begriff „technisch“ sinnvoll. Jedenfalls deutet „auch ohne Wissen“ an, dass es mit Wissen geschehen könnte.<sup>122</sup>

<sup>99</sup> Lauer, NJ 2025, 459 (460); El-Ghazi, NJW 2025, 847 (850); Vgl. für den Bundesfinanzhof/Reichsfinanzhof: Sangmeister, DStR 2020, 2705 (2708).

<sup>100</sup> Vgl. BGH, NJW-RR 2024, 1257; am Beispiel der Finanzgerichtsbarkeit: Vgl. Mellinghoff, DStR 2018, 2049 (2050) mit Verweis auf (nicht veröffentlichte) Entscheidung des RFH vom 20.11.1941, Az: IV 47/41.

<sup>101</sup> BGH, BeckRS 2025, 9876 Rn. 46, Rn. 48, Rn. 50, Rn. 51, Rn. 53.

<sup>102</sup> Eine Verhältnismäßigkeit annehmend: BGH, BeckRS 2025, 9876 Rn. 57 f.; LG Ravensburg, BeckRS 2023, 3879 Rn. 14; OLG Bremen, BeckRS 2025, 295 Rn. 14.

<sup>103</sup> Grzeszick, in: Dürig/Herzog/Scholz, GG, Art. 20 Rn. 113; Rux, in: BeckOK-GG, Art. 20 Rn. 193 f.

<sup>104</sup> Grzeszick, in: Dürig/Herzog/Scholz, GG, Art. 20 Rn. 114; Rux, in: BeckOK-GG, Art. 20 Rn. 194.

<sup>105</sup> Grzeszick, in: Dürig/Herzog/Scholz, GG, Art. 20 Rn. 119; Rux, in: BeckOK-GG, Art. 20 Rn. 197.

<sup>106</sup> Vgl. BVerfGE 44, 353 (373).

<sup>107</sup> Vgl. Gropp, JZ 1998, 501 (505).

<sup>108</sup> Vgl. Horn, Kriminalistik 2019, 641 (643).

<sup>109</sup> Im Ergebnis auf § 81b verweisend Rottmeier/Eckel, NSTz 2020, 193 (196).

<sup>110</sup> Köhler, in: Schmitt/Köhler, StPO, § 94 Rn. 4; Greven, in: KK-StPO, § 94 Rn. 1, Rn. 4 ff.

<sup>111</sup> Zerbes/El-Ghazi, NSTz 2015, 425 (427 ff.); Soiné, in: Soiné, StPO, § 94 Rn. 17.

<sup>112</sup> „Gleichbehandlung von körperlichen und nichtkörperlichen Beweismitteln“, BT-Drs. 19/27654, S. 63.

<sup>113</sup> Horn, Kriminalistik 2019, 641 (643); Gercke, in: Gercke/Temming/Zöller, StPO, § 105 Rn. 77; Vgl. BGH, NSTz 2016, 551.

<sup>114</sup> Vgl. Zerbes/El-Ghazi, NSTz 2015, 425 (427).

<sup>115</sup> Rottmeier/Eckel, NSTz 2020, 193 (196); Horn, Kriminalistik 2019, 641 (643); Vgl. Ludewig, KriPoZ 2019, 293 (298).

<sup>116</sup> Zur Kritik an §§ 94 ff. StPO: El-Ghazi, in: Verhandlungen des 74. Deutschen Juristentages Stuttgart 2024, S. 65 ff.

<sup>117</sup> BVerfGE 120, 274 (324).

<sup>118</sup> Vgl. Bock/Fülscher, StraFO 2023, 386 (389).

<sup>119</sup> In die Richtung: Nadeborn/Albrecht, NZWiSt 2021, 420 (421 f.).

<sup>120</sup> Momsen, DRiZ 2018, 140 (142 f.); Vgl. auch Nadeborn/Irscheid, StraFo 2019, 274 (275).

<sup>121</sup> Momsen, DRiZ 2018, 140 (142 f.).

<sup>122</sup> Vgl. BT-Drs. 17/5846, 39.

Die Idee, die Vorschriften der §§ 100b ff. StPO für die *Entsperrung* heranzuziehen, ggf. auch analog, ist aber im Ergebnis abzulehnen. Entscheidend ist zunächst der Begriff „technisch“. Hiernach sind Eingriffe über das Internet, oder mit Trojanern und Ähnlichem erfasst.<sup>123</sup> Eine direkte Anwendung scheidet somit aus. Es verbleibt lediglich eine analoge Anwendung auf z.B. „das Führen des Fingers an den Sensor“.

Neben der planwidrigen Regelungslücke, die hier bereits kritisch gesehen werden kann aufgrund des Wortlauts „Fingerabdrücke“ in § 81b Abs. 1 StPO, müsste aber auch die Interessenslage vergleichbar sein.<sup>124</sup> Jedoch ist in erster Linie das Ziel von § 100b Abs. 1 StPO die „Umgehung“ von etwaigem Schutz und nicht die forcierte „Überwindung“, wie durch das Einscannen-Lassen durch Zwang.<sup>125</sup> Während die genannten Überwachungsmaßnahmen weder PIN-Codes noch biometrische Sicherungen substituieren, setzt die zwangsweise Entsperrung eines Mobiltelefons gerade voraus, dass auf die Finger des Beschuldigten physisch zugegriffen wird, um diese zur Authentifizierung zu verwenden. Diese Argumentationslinie findet Rückhalt in der Gesetzesbegründung, wonach „jeder Zugriff auf ein informationstechnisches System des Betroffenen (...) grundsätzlich nur auf technischem Wege oder mittels kriminalistischer List erfolgen [darf]“,<sup>126</sup> was auf eine Begrenzung unmittelbarer körperlicher Inanspruchnahme hindeutet.

## VI. Gesetzgeber gefragt

Ausgehend von der Diskussion um die verschiedenen Ermächtigungsgrundlagen wird deutlich: keine Norm erfasst den Sachverhalt der zwangsweisen Entsperrung. Auch ihre analoge Anwendung kommt nicht in Betracht,<sup>127</sup> da eine Analogie für *Zwangmaßnahmen* nach der StPO einen schweren Verstoß gegen die legislative Entscheidung,<sup>128</sup> wie bestimmte Taten verfolgt werden dürfen, sowie den Gesetzesvorbehalt<sup>129</sup> darstellt.<sup>130</sup> Schließlich sollen entsprechend zwei Lösungsansätze aufgezeigt werden, wie ein rechtsstaatskonformes und effektives Handeln ermöglicht werden könnte.

### 1. Bewertung der Lösung des BGH

Dem BGH ist beizupflichten, dass laut ihm im Rahmen der Wohnungsdurchsuchung klare Maßnahmen wie die Entsperrung des Handys benannt werden müssen. Weiterhin ist ein (grundsätzlicher) Richtervorbehalt,<sup>131</sup> der bei § 81b Abs. 1 StPO nicht vorgesehen ist, durch den Wohnungsdurchsuchungsbeschluss nach § 105 Abs. 1 StPO jedenfalls nötig. Insbesondere schafft der BGH dadurch höhere Hürden, die Entsperrung auf § 81b Abs. 1 StPO zu

stützen. Neben der (richtigerweise) vom BGH mehrmals erwähnten Verhältnismäßigkeit muss aber explizit der Kernbereichsschutz herangezogen werden, ähnlich wie in § 100d StPO. Dies hat der BGH bereits verkannt.

Am Ende scheitert der Weg des BGH aber auch an der Dogmatik – die Normen, die die Entsperrung selbst betreffen, sind nicht heranziehbar. Der BGH versucht zwar einen rechtstaatlich konformen Weg zu gehen. Sobald jedoch eine Ermächtigungsnorm fehlt, ist der Eingriff rechtswidrig, unabhängig davon wie man die verschiedenen Normen der §§ 81b Abs. 1, 94 Abs. 1 und §§ 102, 105 Abs. 1 StPO mischt und neukombiniert – eine neue Norm so erschaffen darf und kann er nicht. Eine Ermächtigungsnorm ist keine bloße Formalität, sondern in Anlehnung an Art. 20 Abs. 3 GG essenziell. Insbesondere spricht die Systematik gegen eine Kombination aus § 102 StPO mit § 81b Abs. 1 StPO mangels etwaigen Verweises. Aber auch bei Bejahung einer Systematik ist der Tatbestand nicht erfüllt, § 81b Abs. 1 StPO ermöglicht tatbestandlich nicht die Entsperrung von Mobiltelefonen.

Stattdessen kann und muss der Gesetzgeber eingreifen und klare Regeln schaffen, damit es nicht zu einem rechtswidrigen „Normen-Konglomerat“ kommt. Dies hat er bei den §§ 100a ff. StPO bereits getan.

### 2. Vorschlag zu einer Gesetzesänderung

Um der effektiven Strafverfolgung und dem Grundrechtsschutz Rechnung zu tragen könnte an bestehende Normen wie § 100j StPO – Bestandsdatenauskunft angeknüpft werden. So soll § 100j Abs. 1 um einen weiteren Satz (neben Anpassung in den Absätzen 3 und 4 aufgrund der bestehenden Verweise innerhalb der Norm) ergänzt werden.

„(...) Ist eine Auskunft nicht zielführend, ist eine Erhebung und Verwendung der Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, ermöglicht wird (§ 23 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes), auch gegen den Willen des Betroffenen im Sinne des § 81b Absatz 1 StPO insoweit möglich, als das hierbei biometrische oder vergleichbare Daten erhoben werden; § 100j Absatz 2, Satz 1, Satz 2, § 100d Absatz 1, 2 und 3 gelten sinngemäß.“

§ 100j StPO bietet sich insoweit an, als bereits in Abs. 1 S. 2 Passwörter und Codes erfasst werden.<sup>132</sup> Durch die Einschränkung in S. 2, dass die Voraussetzungen für die Nutzung der Daten vorliegen müssen, wird auf die Vorschriften der §§ 94 ff. StPO<sup>133</sup> oder auf

<sup>123</sup> Gercke, in: HK-StPO, 7. Aufl. (2023), § 110a Rn. 38; Gercke/Grözinger, in: Gercke/Temming/Zöller, StPO, § 100b Rn. 8.

<sup>124</sup> Vgl. bei § 81b StPO AG Baden-Baden, BeckRS 2019, 66684 Rn. 9.

<sup>125</sup> Grzesiek/Zühlke, StV-S 2021, 117 (118); vgl. Rückert, in: MüKo-StPO, § 100b Rn. 1.

<sup>126</sup> BT-Drs. 18/12785, S. 52.

<sup>127</sup> Jedenfalls in Betracht ziehend: AG Wuppertal, BeckRS 2017, 166377; Momsen, DRiZ 2018, 140 (142 f.).

<sup>128</sup> BVerfGE 71, 108 (116).

<sup>129</sup> Vgl. BVerfG NJW 2008, 3627.

<sup>130</sup> Kudlich, in: MüKo-StPO, Einl. Rn. 602; vgl. Wohlers/Singelstein, in: SK-StPO, vor § 94 Rn. 7.

<sup>131</sup> Vgl. Hegmann, in: BeckOK-StPO, § 105 Rn. 4; Henrichs/Weingast, in: KK-StPO, § 105 Rn. 1.

<sup>132</sup> BT-Drs. 17/12879, S. 11; Rückert, in: MüKo-BGB, § 100j Rn. 16; Graf, in: BeckOK-StPO, § 100j Rn. 20.

<sup>133</sup> Rückert, in: MüKo-StPO, § 100j Rn. 16.

§ 100a ff. StPO<sup>134</sup> verwiesen. Damit ergibt sich auch ein systematischer Zusammenhang zu dem Kernbereichsschutz und dem Richtervorbehalt, §§ 100j Abs. 2 S. 2, 100d Abs. 1 StPO. Der herrschenden Ansicht folgend, könnte bei § 81b Abs. 1 StPO eine Änderung erfolgen und der Verweis auf die § 100a ff. StPO hergestellt werden. Jedoch müsste nicht nur die Zielrichtung durch entweder eine Änderung der Normüberschrift oder eine konkretere Ausformulierung der Alt. 2 umgestaltet werden. Zudem ist ein systematischer Zusammenhang zwischen den §§ 100a ff. StPO schwerer herzustellen, im Vergleich zu einer Erweiterung des § 100j Abs. 1 StPO.<sup>135</sup>

## VII. Resümee

Das durch die Entscheidung des *BGH* aufgeworfene Problem ist nicht gelöst. Letztlich könnte nur Abhilfe geschaffen werden durch die explizite Erwähnung des Kernbereichsschutzes, die differenzierte Berücksichtigung der Normenkette der §§ 100a ff. StPO sowie eine Einschränkung auf schwere Taten, damit bloße Ordnungswidrigkeiten nicht erfasst werden können. Somit wird die kopflas-

tige und im Ergebnis nur von der freien richterlichen Würdigung abhängige Verhältnismäßigkeit nicht überstrapaziert, sondern von vornerein nur schweren Taten erfasst. Diese sind auch i.d.R. vor den Gerichten verhandelt worden. Nicht für jeden Sachverhalt findet sich eine individuelle Ermächtigungsgrundlage.

Es ist Aufgabe der Justiz zu prüfen, unter welche allgemein gehaltene Normen die Lebenssachverhalte zu subsumieren sind. Dies entbindet jedoch weder vom Grundrechtsschutz noch von dem Erfordernis der Bestimmtheit der Normen. Es muss ersichtlich sein, unter welchen Voraussetzungen Zwangsmaßnahmen durchgeführt werden dürfen. Je invasiver der Eingriff, desto strenger müssen die Tatbestandsvoraussetzungen sein. Annexkompetenzen oder systemwidrige Normketten reichen dann nicht mehr für rechtmäßiges, staatliches Verhalten aus. Möglicherweise kann aber mit diesem Vorschlag ein kleiner Beitrag geleistet werden, um dem Gesetzgeber zusammen mit anderen Stimmen aus Strafverteidigung und Literatur einen Impuls zur (zeitgemäßen) Reform der StPO zu geben.<sup>136</sup>

<sup>134</sup> *BVerfG*, NJW 2012, 1419 (1429); *Henrichs/Weingast*, in: KK-StPO, § 100j Rn. 3a.

<sup>135</sup> *Bosch* dagegen plädiert für die § 94 ff. StPO: *Bosch*, in: KMR-StPO, § 81b Rn. 11.

<sup>136</sup> *Suliak*, <https://www.lto.de/recht/hintergruende/h/cue-kommission-stpo-reform-bmjbv-beschleunigung-straiprozess>, (zuletzt abgerufen am 23.10.2025) mit Verweis auf die anstehenden Reformen zur Effektivitätsverbesserung der StPO.

## Biometric device locks – an invitation to law enforcement? An analysis of EU limitations to the contentious police practice after the “Landeck”-Decision

von Prof. Dr. Carsten Momsen und  
Miriam Süttmann\*

### Abstract

Inzwischen ist es gängige Praxis der deutschen Polizei, Smartphones mithilfe biometrischer Daten zu entsperren. Geschieht dies durch Zwang, sind Rechtsgrundlagen wie Rechtmäßigkeit jedoch umstritten. Die Bedeutung der Law Enforcement Data Protection Directive (EU-RL 2016/680), vom EuGH 2024 in seiner „Landeck“-Entscheidung präzisiert, erlangt in dieser Debatte (zu) wenig Beachtung. Denn auch die Einhaltung europäischer Minimalstandards wird gefährdet, wenn die träge deutsche Gesetzgebung sich fortentwickelnde Polizei-Taktiken in einem sich rasch wandelnden technologischen Umfeld nicht reguliert, insbesondere so lange Gerichte die missachteten Anforderungen nicht durchsetzen. Vor diesem Hintergrund versuchen wir nachfolgend eine Einordnung der kontroversen Entscheidungen des BGH (2 StR 232/24) und des OLG Bremen (1 OR 26/24) aus dem vergangenen Jahr im Lichte europäischer Standards.

Nowadays, biometric data is routinely used by German law enforcement for the purpose of unlocking smartphones. However, when pursued by force, the legal basis and legality are contentious. The Law Enforcement Data Protection Directive (EU Directive 2016/680), which the ECJ clarified in its “Landeck” decision in 2024, provides a legal framework. The reluctance of German legislation to keep pace with rapidly evolving technological environments has the potential to compromise compliance with these standards. This is of particular concern when courts fail to enforce legal requirements, thus jeopardising civil liberties. Two decisions issued by the Federal Court of Justice (BGH, 2 StR 232/24) and the Higher Regional Court of Bremen (OLG Bremen, 1 OR 26/24) in the previous year were met with great controversy. As demonstrated below, these critics find themselves in alignment with the requirements imposed by EU regulations.

### I. Introduction

The central role mobile phones play in everyday life – used to chat, store photos and documents, search the internet, access emails or cloud storages – evidently makes them a target for law enforcement. In the past, accessing the stored information could be difficult, when devices were password protected: Since *Nemo Tenetur* prevents obtaining the password from the user through coercion, police had to hope to find it somewhere in writing. Otherwise, they would have to crack open the device themselves – which would be a lengthy and costly process.<sup>1</sup>

A much easier way opened up with the spread of fingerprint sensors since the launch of the Apple iPhone 5S in 2013: Suddenly law enforcement could bypass the PINs in many cases by placing the user’s finger onto the sensor, often with brute force.

Since then, it has become standard police practice to unlock phones using biometric features, such as fingerprint-, face- or iris-scans: A German Police officer recommends on an independent police journal’s online blog, to “assist [the phone user] in unlocking their phone, if needed by force”, if they are present.<sup>2</sup> Meanwhile, grassroots groups, protest organizers and human rights organizations are warning citizens “to not have face or fingerprint lock on your phone, as the police can use those to unlock your phone without your consent”<sup>3</sup>.

The slow rate at which procedure codes adapt to technological change enables law enforcement to exploit loopholes and a lack of regulation, resulting in serious infringements of sensitive fundamental rights. Therefore, the rulings of high courts such as the *European Court of*

\* Carsten Momsen is Professor for “Comparative Criminal Law, Criminal Procedural Law, Corporate Criminal Law and Environmental Criminal Law” at the Department of Law of the Free University Berlin, Miriam Süttmann is a member of his team. The following analysis was first presented as part of the Webinar “Police Access to Digital Devices: Where Are the Limits? Reflecting on the Landeck case C-548/21 and beyond” by Fair Trials, 3.12.2025, and further develops an expert opinion provided to the German Judges Association (Deutscher Richterbund) in 2018, published in modified form as Momsen, DRiZ 2018, 14.

<sup>1</sup> Through trying out passwords (generally considered admissible, Hegmann, in: BeckOK-StPO, 57. Ed. (updated on 1.1.2026), § 110 Rn. 19; critical Brodowski/Eisenmenger, ZD 2014, 119 (123)), or through technical circumvention, as regulated in § 100b StPO. The latter is not popular, as statistics show, likely because it is too resource-intensive in the majority of cases, Bundesamt für Justiz, Übersicht Telekommunikationsüberwachung für 2022 (Maßnahmen nach 100b StPO), available online: <https://bit.ly/4b7SaxQ> (last accessed 10.1.2026).

<sup>2</sup> Weingarten, KSV Polizeipraxis, available online: <https://bit.ly/46BtbSk> (last accessed 3.12.2025).

<sup>3</sup> Quote from the initiative Gofilmthepolice by KOP (Kampagne für Opfer rassistischer Polizeigewalt), available online: <https://bit.ly/4bncDA2>; other examples are: Bündnis Widersetzen, available online: <https://bit.ly/4r8EubR>; Demo101, available online: <https://bit.ly/4sbbKRn>; Migrantifa Berlin, available online: <https://bit.ly/4uiKnGr> (all accessed on 3.12.2025).

*Justice* (ECJ) are becoming increasingly important in safeguarding citizens' rights.

## II. Fundamental rights and EU minimum standards – the directive 2016/680 and Landeck

Authorities extracting information from devices in the EU are bound by Art. 7 and 8 of the Charter of Fundamental Rights (CFR), which guarantee the right to respect for private life and the protection of personal data. The minimum requirements for the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences are further specified by EU directive 2016/680 – also known as the *Law Enforcement Data Protection Directive*.<sup>4</sup>

In October 2024, the ECJ clarified in its *Landeck*-ruling<sup>5</sup> the limits and requirements the directive imposes on law enforcement's access to personal phones. Due to the sensitive nature of the stored data stored, including biometric information, personal recordings, photographs, cloud keys, health data and business secrets, which can be used to create movement or personality profiles, the court declared that any *attempt* to access phones and bypass locking measures seriously interferes with the fundamental right to privacy and the protection of personal data.

While not entirely precluded, access to mobile phone data is only allowed under high requirements: It must be based on a suitable enabling provision and guided by the principles of data minimization and proportionality. The respect of these principles is to be guaranteed by prior review by a judge or an independent administrative body. The ruling establishes that the severity of the offence under investigation is an essential factor in evaluating the proportionality of a measure. However, the court concluded that the directive should not be interpreted as limiting investigative powers to serious crimes, as this would unduly limit law enforcement authorities and undermine the objective of establishing an area of freedom, security and justice within the EU.<sup>6</sup>

## III. Current (il)legal practice in Germany

As we will see, the German practice clearly falls far short of meeting these standards. Several times since 2017 courts had to position themselves on the admissibility of obtained information.<sup>7</sup> Points of contention are a possible conflict with *Nemo Tenetur*, as well as whether the German Code of Criminal Procedure contains a provision fit to enable the measure. While the practice doesn't necessarily directly violate the *Nemo Tenetur*-Principle, it still interferes with free will: Access to information is gained

against the defendant's manifested will and encroaches therefore upon their freedom to store and provide personal data as they please. A legal basis would need to reflect this dimension.

In Germany, concerns regarding the legal foundation pertain to the fact that the German Code of Criminal Procedure – to this day – has not specifically regulated the forced unlocking of devices through biometric features. In line with *Landeck*, German jurisprudence recognizes that biometric unlocking by force cannot be based on general investigative authority. Does the measure therefore have no legal basis, rendering it illegal? Or could it be based on one of the existing provisions, and if so, what would the application require?

In identifying a legal foundation within the present Code of Criminal Procedure, three different approaches have been considered by the courts: Section 81a, that allows the physical examination of the accused, Section 81b, that allows the collection of photographs and fingerprints of the accused and Sections 94 ff., allowing and regulating infringements of the right to privacy, such as through searches, seizures of digital mediums, phone surveillance etc.

### 1. Section 81a

In 2017 a lower-level court ruled<sup>8</sup> that fingerprint extortion could be based on section 81a, regulating the physical examination of the accused. The application of Section 81a would be attractive to investigative bodies because the measure is subject to relatively lower requirements. Notably, it is not linked to serious offences. However, this understanding is now generally rejected. Rightfully so – measures under that section are reserved for the examination of the physical constitution, not the retrieval of data through physical features.<sup>9</sup>

### 2. Recent judicial practice: Section 81b

The prevailing judicial practice in Germany is such that law enforcement officials are authorized to unlock smartphones through fingerprint scans on the basis of Section 81b, which stipulates the collection of photographs and fingerprints of the accused.

Post-*Landeck*, two decisions by a Higher Regional Court (*OLG Bremen*) and the *Federal Court of Justice* (*BGH*) have upheld this reasoning,<sup>10</sup> that in two aspects seems to severely misinterpret both the law and the *ECJ*'s ruling: First of all, stating that the legality of accessing the phone can be evaluated separately from the search of the phone.

<sup>4</sup> Directive (EU) 2016/680 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

<sup>5</sup> *European Court of Justice*, 4.10.2024 – C-548/21 (*Landeck*), available online: <https://bit.ly/4cvqzsp> (last accessed 4.3.2026).

<sup>6</sup> *ECJ*, *Landeck* (fn. 5), para. 97. In agreement with the "German Jurists' Conference" (Deutscher Juristentag), see *Wahl*, *eu crim* 3, 2024, 189 (191).

<sup>7</sup> *BGH*, *NStZ* 2025, 560; *OLG Bremen*, *NJW* 2025, 847; *LG Ravensburg*, *NStZ* 2023, 446; *AG Baden-Baden*, *Beschl. v.* 13.11.2019 – 9 Gs 982/19 (juris); *AG Verden*, 9a Gs 800 Js 15636/17 (2373/17), *Beschl. v.* 27.6.2017 (not published).

<sup>8</sup> *AG Verden* (fn. 7).

<sup>9</sup> *Momsen*, *DRiZ* 2018, 14 (15).

<sup>10</sup> *OLG Bremen*, 1 OR 26/24 and *BGH*, 2 StR 232/24, fn. 7.

Secondly, concluding that the scope of Section 81b extends to unlocking smartphones by placing the fingerprint on the sensor, thereby disregarding the logic upon which annex powers are predicated.

*a) Two measures – or just a prelude?*

Both the *OLG Bremen* and the *BGH* recognize Landeck as a landmark ruling.<sup>11</sup> Still, both courts concluded that accessing the device and processing/storing the information are two separate measures that can be assessed separately and find their legal basis in different provisions. “Processing the data is a *separate, subsequent measure* to the unlocking and can be assessed independently according to the rules that apply to it.”<sup>12</sup>

This contradicts a key aspect from the *Landeck*-ruling. The *ECJ* was very clear that the directive also applies to operations taking place prior to the processing itself – such as a processing attempt. The objectives of the directive, to ensure a high level of protection of the personal data of natural persons and their right to determine who has access to personal data, would be undermined by a narrow interpretation.<sup>13</sup> The directive does not merely protect the data itself, it also protects the safety mechanisms set in place to guard the data. Even if the intention behind unlocking a phone was merely to identify a person as the owner, the directive would still apply, since breaching the security mechanism is an intermediate goal. Whether or not further processing is intended is inconsequential.

The legal basis permitting access to the device therefore needs to be fit to protect against the extent and intensity of smartphone access *and* impose correspondingly high barriers to intervention. Moving beyond a superficial approach that focusses on the use of biometrics, the actual substance of the investigative measure comes to light: A prelude to the use of and access to data. Unlocking the device is a necessary preparatory or accompanying measure to searches of the device, chats, cloud storage, etc.

It is recognized, that accompanying legal measures – so-called annex-measures – intended to enforce the primary measure, can be based on the provision allowing the primary measure, if they are typically connected and are suitable, necessary and proportional with regards to the purpose of the primary measure.<sup>14</sup> The constitutional requirement of legal reservation is satisfied if the accompanying measure is so typical and subordinate that it corresponds to the objective intent behind the primary measure.<sup>15</sup> This concept results from the circumstance that many (primary) measures will have to be carried out against the will

of the person concerned.

For example, an apartment search may involve breaking down the front door.<sup>16</sup> Now if a police officer uses my finger as a crowbar to break down the digital door to my smartphone – could this be treated as an annex to the subsequent search of my device?<sup>17</sup>

*b) Scope of section 81b*

It might seem obvious that section 81b is not a suitable basis for a device search that needs to overcome security mechanisms. The provision states that “Photographs and fingerprints of the accused may be taken, even against his or her will, and measurements may be made of the accused and other similar measures taken with regard to him or her insofar as is required for the purposes of conducting the criminal proceedings or for the purposes of the police records department.”<sup>18</sup>

Nonetheless, both *BGH* and *OLG Bremen* argue that biometric unlocking can be based on the provision for taking fingerprints *for the purpose of conducting the criminal proceedings*, claiming that the broad wording allows the use of fingerprints for any and every purpose, as long as it suits the investigation.<sup>19</sup> The argument ties to the creation process, during which the scope of the provision was deliberately kept open to encompass technological advancements.<sup>20</sup>

This understanding disregards a key point: While the legislator opted for a technology-unrestricted understanding, this does not absolve it from the necessity to limit the scope to measures that align with the purpose of determining physical characteristics and conducting biometric/dactyloscopic comparisons – which the unlocking of a phone clearly goes beyond.<sup>21</sup> *For the purpose of conducting the criminal proceeding* is not sufficiently limiting.<sup>22</sup> After all, any police measure supposedly serves in some way the purpose of investigating crimes.

Furthermore, such a broad understanding of Section 81b does not adequately consider the impact of unlocking a phone on the right to privacy. While the *OLG Bremen* correctly points out that the German Constitutional Court considered the hidden, secret infiltration of information systems a particularly severe infringement (para. 17), the argument that openly accessing a secured device interferes less with fundamental rights is inaccurate. The Constitutional Court stated that an intense interference, comparable to the surveillance of the home, is given with any access to the data stored on personal devices.<sup>23</sup> Due to its

<sup>11</sup> However, the higher regional court notably does not even recognize the applicability of the Law Enforcement Data Protection Directive on the unlocking of phones, *OLG Bremen* (fn. 7), para. 17.

<sup>12</sup> “Das Auslesen des Mobiltelefons als Ziel der Entsperrung ist eine dem Entsperrn nachfolgende Maßnahme, die selbstständig an den für sie geltenden Regeln gemessen werden kann.“ *BGH* (fn. 7) para. 65, emphasis added.

<sup>13</sup> *Landeck* (fn. 4), para. 74, 75.

<sup>14</sup> *BGH*, NJW 2001, 1658 (1659); *AG Hamburg*, StV 2009, 636.

<sup>15</sup> Extensively *Zieman*, ZStW 2018, 762; *AG Hamburg* (f. 14), 637.

<sup>16</sup> *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. (2023), § 105 para. 14a.

<sup>17</sup> *LG Ravensburg* (fn. 7); critical *Hort*, NSTZ 2023, 446 (448), since forceful biometric unlocking requires the „use“ of the human body.

<sup>18</sup> Translation of the German criminal procedure code by *Duf-fet/Ebinger/Müller-Tostin/Mahdi/Reusch*, published <https://bit.ly/4rbLwfW> (accessed on 30.11.2025).

<sup>19</sup> *OLG Bremen* (fn. 7), para. 13, *BGH* (fn. 7), para. 62.

<sup>20</sup> *Rottmeier/Eckel*, NSTZ 2020, 193 (195).

<sup>21</sup> *Ruppert*, StV 2025, 565 (565), see also *Momsen* (fn. 9), p. 15.

<sup>22</sup> Unless the era of absolutist (investigative) power as seen in the 18<sup>th</sup> and 19<sup>th</sup> century not come to an end after all? *Zieman*, ZStW 2018, 762 (773).

<sup>23</sup> *BVerfG*, NJW 2016, 1781.

intensity and the often highly personal nature of the data stored on an information technology system, it compares the severity of the intrusion to that of a (secret) intrusion into the sanctity of the home. The differentiation between hidden and open measures should be understood as an emphasis on transparency and ensuring access to judicial review in these cases, since this is limited in the case of hidden access. This consideration does *not* suggest that the right to privacy is less affected by other, open access to protected device data, given that this also enables comprehensive monitoring of the system's use and reading of its storage media against the manifested will of the user.

As Cyber-investigations expert *Felix Ruppert* pointed out: Section 81b offers no protection against the extent and intensity of smartphone access, nor does it impose correspondingly high barriers to intervention. This comes as no surprise, as the regulation was never intended to interfere with fundamental IT rights. The fact that it is unsuitable for this purpose is a logical consequence.<sup>24</sup>

Forcing the unlocking of a device can also not be considered an annex to a measure under section 81b, since bypassing the device lock is the focus of the measure, not just enabling or accompanying a biometric (dactyloscopic) examination. Assuming otherwise would be akin to considering an apartment search to be a mere extension of breaking down the front door.

### 3. Scope of section 94 ff., 110 – annex to the examination of electronic storage media?

Now what happens if we switch to an understanding that moves beyond the use of biometrics to the actual intended goal – the securing of the data. Could it be based on Section 94 ff., allowing the searches of objects, including digital documents, of the suspect, and section 110 regulating the examination of documents and electronic storage media and of data stored with cloud providers?

This understanding is implied as an alternative in the *BGHs* decision. Considering the possibility of a judicial review requirement under *Landeck*, the court states that this would be met by the issued warrant allowing the apartment search, since the search was specifically intended to locate mobile phones.<sup>25</sup>

This approach seems plausible at first glance. However, it disregards that there is a significant difference between accessing openly accessible documents and digital storage, as opposed to those *consciously secured* through security measures, such as passwords. The intensity of the measure is not an effect of the use of biometrics, but that the system is “hacked” by brute force – in any form an intense breach to the right of privacy.<sup>26</sup> As the legislators' considerations regarding section 100b show, the key difference lies in the direct impact on the fundamental right

to informational self-determination when accessing a secured device against the *manifested will* of the user.<sup>27</sup>

This dimension is not reflected in the scope of sections 94 ff., 110, because it was not taken into consideration by the legislator. Therefore, accessing and searching a device by unlocking it through biometric measures cannot be seen as a mere negligible annex, and based on these provisions.

## IV. Alternative: Section 100b?

Section 100b on the other hand does allow encroachment on the scope of protection of the fundamental right to integrity and confidentiality of information technology systems as an independent manifestation of the right to privacy. It legitimizes the technical circumvention of device protection without the knowledge of the user to collect stored data. But the requirements are high: The suspicion of a severe crime from a specified catalogue, the gravity of the offence in the individual case, and the heightened significance of the infiltration for the investigations. The search is subject to strict procedural requirements and must be documented.

Of course, the measures we are discussing aren't identical: The circumvention of security measures does not take place by technical means, and not *without the knowledge* – but “just” against the will of the user. However, the objective of the intervention is comparable – and, arguably, so is the intensity of the interference with the right to privacy, since the search also enables comprehensive monitoring of the system's use and reading of its storage media. Therefore, while the wording does not allow direct application in the case of accessing a device through biometric measures, the analogous application of the standard lies at hand.<sup>28</sup>

One might argue that the strict provisions of Section 100b regarding judicial review, documentation, and restriction to a catalogue of severe crimes only serve to mitigate the hidden nature of online searches. However, this distinction is not as clear-cut as it seems, since it is common practice to force biometric unlocking on the spot, thereby also obstructing prior judicial review.

In any case, it is the legislator, not the courts, who must carve out these distinctions. That is the only way to ensure compliance with fundamental laws and the Law Enforcement Data Protection Directive, as set out in *Landeck*.

## V. Conclusion: Regulation, until then inadmissibility

Current practice is shaped by significant uncertainty surrounding the requirements for breaches of security measures designed to protect the data on mobile phones – devices that store the most intimate information. The fact that, despite almost a decade of debates, there have been

<sup>24</sup> Ruppert, LTO, <https://bit.ly/3MNoUVc> (accessed on 30.11.2025).

<sup>25</sup> BGH (fn. 7), para. 73.

<sup>26</sup> This understanding is a continuation of the argument against brute-force-„hacking“ by trying out passwords made by Brodowski/Eisenmenger (fn. 1), p. 123.

<sup>27</sup> Momsen (fn. 8), p. 16.

<sup>28</sup> Momsen (fn. 8), p. 16-17.

no legislative efforts, is concerning.<sup>29</sup> Even more concerning is that German courts keep approving of this, in direct contradiction to ECJ case law and in disregard of the importance of the right to privacy. By abandoning procedure codes and making all means available for the purpose of investigating crime<sup>30</sup> the courts are exceeding their authority and eroding EU standards. The only true solution

to this worrying trajectory is a legislative one: Either the broadening of the scope of section 100b, or the creation of an appropriate provision that takes into consideration fundamental rights as specified by *Landeck*. Until then, until there is clarity on the legal basis and procedure, courts must rule that any evidence obtained through forced biometric unlocking is inadmissible.

---

<sup>29</sup> Hopes that the *ECJ*'s decision would prompt the legislator to act, see *Wahl* (fn. 6), have not been fulfilled.

<sup>30</sup> *Schneider*, *NStZ* 1999, 388 (389), *AG Hamburg*, *StV* 2009, 636 (637), *Ziemann*, *ZStW* 2018, 762 (773).

# Die anwaltliche Äußerungsfreiheit im Lichte der Konvention zum Schutz des Anwaltsberufs – Eine Untersuchung der Rechtsprechung des Bundesverfassungsgerichts

von Akad. Rat a.Z. Damien Nippen\*

## Abstract

*Der Beitrag nimmt die neue Europaratskonvention zum Schutz des Anwaltsberufs zum Anlass, die anwaltliche Äußerungsfreiheit in den Blick zu nehmen. Er stellt die drei wesentlichen anwaltlichen Äußerungsfreiheiten vor, die sich aus der Konvention ergeben. Darauf folgt eine kritische Untersuchung der Rechtsprechung des Bundesverfassungsgerichts zu anwaltlichen Äußerungen, die grundsätzlich geeignete Leitlinien aufstellt, um die Ziele der Konvention zu erfüllen. Nur vereinzelt wären Anpassungen wünschenswert.*

*The article takes the new Council of Europe Convention for the Protection of the Profession of Lawyer as an opportunity to examine lawyers' freedom of expression. It presents the three key dimensions of lawyers' expressive freedoms that follow from the Convention. It then offers a critical analysis of the German Federal Constitutional Court's case law on lawyers' statements, which generally sets sound guidelines for achieving the Convention's objectives. Only few adjustments appear eligible.*

## I. Einleitung

Am 26. Januar 2026 unterzeichnete die Bundesjustizministerin Hubig die Konvention des Europarats zum Schutz des Anwaltsberufs („Anwaltskonvention“).<sup>1</sup> In der Pressemitteilung bezeichnet sie Anwälte als „Kämpferinnen und Kämpfer für Rechtsstaatlichkeit und bürgerliche Freiheit“ und spricht davon, dass sie insbesondere „Anti-Demokraten und Autoritären ein Dorn im Auge“ sind.<sup>2</sup> Auf globaler Ebene stehe die Anwaltschaft unter Druck; ein solches völkerrechtliches Abkommen sei „bitter nötig“.<sup>3</sup> Der nächste Schritt ist die Ratifikation der Konvention durch ein Vertragsgesetz (Art. 59 Abs. 2 GG) und die Umsetzung in nationales Recht. Heinrichs spricht im Interview mit beck-aktuell davon, dass es für den deutschen Gesetzgeber kaum Anpassungsbedarf gebe, da bereits ein

gutes Schutzniveau bestehe.<sup>4</sup> Auch die Justizministerin sieht nur punktuellen Umsetzungsbedarf.<sup>5</sup>

Ein solcher Bedarf könnte bspw. aufgrund von Art. 4 Abs. 3 Anwaltskonvention bestehen, der vorsieht, dass Anwaltsvereinigungen in Gesetzgebungsverfahren anzuhören sind, wenn die geplanten Gesetze sich unmittelbar auf die berufliche Tätigkeit von Rechtsanwälten auswirken können.<sup>6</sup> Anpassungen nationalen Rechts könnten ferner für die Durchsuchungen von Kanzleiräumen erforderlich sein.<sup>7</sup> Art. 9 Abs. 1 Anwaltskonvention sieht für diesen Fall das Recht vor, einen weiteren Anwalt als Zeugen hinzuziehen. Die Konvention wird jedoch nicht nur für den Gesetzgeber, sondern auch für die Gerichte Bedeutung haben, die sie im Wege der völkerrechtsfreundlichen Auslegung<sup>8</sup> zu berücksichtigen haben. Tritt die EU der Konvention bei, würde sie „integraler Bestandteil des Unionsrechts“ und genösse Anwendungsvorrang vor nationalem Recht (Art. 216 Abs. 2 AEUV).<sup>9</sup>

Eine Berücksichtigung bei der Anwendung nationalen Rechts kommt insbesondere in Betracht, wenn anwaltliche Äußerungen Gegenstand von Gerichtsverfahren sind. Denn ein besonderes Anliegen der Konvention ist die anwaltliche Äußerungsfreiheit, die sie gleich in mehreren Artikeln regelt. Sie misst der anwaltlichen Redefreiheit nicht nur eine entscheidende Rolle bei der Vertretung der Interessen der Mandanten zu, sondern sieht sie auch als wichtiges Instrument zur Kritik am Justizsystem an, die der Wahrung rechtsstaatlicher Prinzipien diene. Der folgende Beitrag gibt zunächst einen kurzen Überblick zur Konvention und stellt dann die drei Äußerungsrechte dar, die die Konvention garantiert. Im Lichte dieser drei Äußerungsrechte wird die einschlägige Rechtsprechung des BVerfG untersucht. Die Untersuchung wird zeigen, dass das BVerfG anwaltlicher Äußerungsfreiheit eine große Bedeutung beimisst und seine Maßstäbe zur Bestimmung zulässiger und unzulässiger Äußerungen grundsätzlich

\* Damien Nippen ist Akademischer Rat a.Z. am Lehrstuhl für Strafrecht und Strafprozessrecht von Prof. Dr. Dr. h.c. (UG Tiflis) Martin Waßmer.

<sup>1</sup> [https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26\\_Europarat\\_Schutz\\_Anwaltberuf.html](https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26_Europarat_Schutz_Anwaltberuf.html) (zuletzt abgerufen am 18.3.2026).

<sup>2</sup> [https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26\\_Europarat\\_Schutz\\_Anwaltberuf.html](https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26_Europarat_Schutz_Anwaltberuf.html) (zuletzt abgerufen am 18.3.2026).

<sup>3</sup> [https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26\\_Europarat\\_Schutz\\_Anwaltberuf.html](https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26_Europarat_Schutz_Anwaltberuf.html) (zuletzt abgerufen am 18.3.2026).

<sup>4</sup> Heinrichs, beck-aktuell, Europarat plant staatliche Schutzpflicht für Anwälte, online abrufbar unter: <https://bit.ly/4rSsUlr> (zuletzt abgerufen am 18.3.2026).

<sup>5</sup> [https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26\\_Europarat\\_Schutz\\_Anwaltberuf.html](https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/01/26_Europarat_Schutz_Anwaltberuf.html) (zuletzt aufgerufen am 18.3.2026).

<sup>6</sup> Arconada Valbuena, DSr 2025, 2268 (2270).

<sup>7</sup> Karpenstein, NJW-Editorial, Schutz des Anwaltsberufs, online abrufbar unter: <https://rsw.beck.de/aktuell/daily/magazin/detail/editorial-njw-2026-5-schutz-des-anwaltsberufs> (zuletzt abgerufen am 18.3.2026).

<sup>8</sup> Hierzu Hofmann, JURA 2013, 326 (329 ff.).

<sup>9</sup> Bungenberg/Reinhold, in: von der Groeben/Schwarze/Hatje/Terhechte, Europäisches Unionsrecht, 8. Aufl. (2025), Art. 216 AEUV Rn. 55.

geeignet sind, den Zielen der Konvention zu genügen. Lediglich an einzelnen Stellen wären Konkretisierungen wünschenswert.

## II. Die Regelungen der Konvention

### 1. Die Konvention im Überblick

Auch Staaten, die nicht Mitglieder des Europarats sind, können der Anwaltskonvention beitreten. Sie tritt nach Art. 17 Abs. 3 Anwaltskonvention in Kraft, wenn mindestens acht Staaten sie ratifiziert haben, von denen mindestens sechs Mitglieder des Europarats sein müssen. Zum 18.3.2026 haben bereits 29 Staaten das Abkommen unterzeichnet.<sup>10</sup> Ziel der Konvention ist nach Art. 1 Abs. 1 Anwaltskonvention den Schutz anwaltlicher Tätigkeit zu stärken und ihre Unabhängigkeit zu gewährleisten. Eine Besonderheit stellt der detaillierte Überwachungsmechanismus nach Art. 10 ff. Anwaltskonvention dar.<sup>11</sup> Eine acht- bis zwölköpfige Expertengruppe wird die Einhaltung der Konvention überwachen (Art. 10 Abs. 1 Anwaltskonvention). Sie veröffentlicht ihre Untersuchungsberichte (Art. 12 Abs. 7, 13 Abs. 3 Anwaltskonvention), um politischen Druck auf Staaten auszuüben, die Regelungen der Konvention einzuhalten.<sup>12</sup>

Die konkreten Pflichten der Vertragsstaaten finden sich in den Art. 4–9 Anwaltskonvention. Während Art. 4 Anwaltskonvention die Vertragsparteien verpflichtet, Anwälten zu ermöglichen, sich in unabhängigen und selbstverwalteten Vereinigungen zu organisieren, sieht Art. 5 Anwaltskonvention vor, dass die Zulassung zur Anwaltschaft frei von Diskriminierung und anhand objektiver sowie transparenter Kriterien zu erfolgen hat. Die Art. 8 und 9 Anwaltskonvention legen verfahrensrechtliche Regelungen für Disziplinarverfahren und Zwangsmaßnahmen gegen Anwälte fest. Eine zentrale Norm ist Art. 6 Anwaltskonvention, in der sich einige konkret formulierte Rechte finden,<sup>13</sup> die für die Ausübung anwaltlicher Tätigkeit fundamental sind.<sup>14</sup> Sie sieht bspw. den Zugang zu Ermittlungsakten vor (Art. 6 Abs. 1 lit. e Anwaltskonvention) und garantiert die vertrauliche Kommunikation des Anwalts mit seinem Mandanten (Art. 6 Abs. 3 Anwaltskonvention). Einschränkungen dieser Rechte sind nach Art. 6 Abs. 4 S. 1 Anwaltskonvention nur aufgrund von Gesetzen und unter der Voraussetzung möglich, dass sie in einer demokratischen Gesellschaft notwendig sind. Die Formulierung entspricht dem aus der EMRK bekannten Schrankenvorbehalt, der sich unter anderem auch in Art. 10 Abs. 2 EMRK zur Meinungsfreiheit findet. Eine Einschränkung ist nach der Rechtsprechung des EGMR nur dann „in einer demokratischen Gesellschaft notwendig“, wenn sie „einem dringenden sozialen Bedürfnis“ entspricht.<sup>15</sup>

### 2. Die drei Äußerungsrechte der Konvention

In der Präambel nimmt die Konvention auf andere internationale Regelungen Bezug, wie etwa die „Basic Principles on the Role of Lawyers“ der Vereinten Nationen. Deren Nummern 20 und 23 garantieren ebenfalls die anwaltliche Äußerungsfreiheit: Nummer 20 sieht rechtliche Immunität für prozessuale Äußerungen vor, die der Anwalt in gutem Glauben abgibt, und nach Nummer 23 haben Anwälte insbesondere das Recht, sich zu rechtspolitischen Themen zu äußern. Bei diesen Bestimmungen handelt es sich jedoch um nicht verbindliches *soft law*; mit der Konvention gibt es erstmals ein völkerrechtlich verbindliches Instrument zum Schutz des Anwaltsberufs.<sup>16</sup> Die Konvention regelt in Art. 6 Abs. 2 Anwaltskonvention ein *prozessuales* Äußerungsrecht, in Art. 7 Abs. 1 Anwaltskonvention ein *mediales* Äußerungsrecht und in Art. 7 Abs. 2 Anwaltskonvention ein *rechtspolitisches* Äußerungsrecht.

Nach Art. 6 Abs. 2 Anwaltskonvention haben die Vertragsparteien sicherzustellen, dass Anwälte weder zivil- noch strafrechtlich für mündliche oder schriftliche Äußerungen haftbar sind, die sie für ihre Mandanten in gutem Glauben und sorgfältig im Rahmen eines Verfahrens abgeben. Unzulässig sind auch disziplinarrechtliche Maßnahmen gegen Anwälte, da die Begrenzung auf „straf- und zivilrechtliche“ Haftung nicht eng im Sinne der deutschen Dogmatik zu verstehen ist. Im Einklang mit der Rechtsprechung des EGMR soll der Anwalt nicht aus Angst vor rechtlichen Konsequenzen Äußerungen unterlassen müssen, die er zur Vertretung der Interessen seines Mandanten für erforderlich hält.<sup>17</sup> Nach dem *explanatory report* des Europarats ist der freie und schlagkräftige Austausch von Argumenten wesentlicher Bestandteil eines fairen Verfahrens.<sup>18</sup> Der Wortlaut von Art. 6 Abs. 2 Anwaltskonvention lässt zwar zu, Äußerungen, die der Anwalt nicht in gutem Glauben („*in good faith*“) oder sorgfältig („*diligently*“) abgibt, aus dem Anwendungsbereich herauszunehmen; und der *explanatory report* spricht davon, dass der Schutz nicht für bewusste Lügen und für missbräuchliches oder bedrohliches Verhalten gelten soll.<sup>19</sup> Gegen eine zu weite Auslegung dieser Merkmale spricht jedoch der Zweck der Konvention, eine möglichst freie Berufsausübung zu gewährleisten. Nach dem *explanatory report* soll der Anwalt nicht rechtlich haftbar sein, nur weil er den Standpunkt seines Mandanten vertritt.<sup>20</sup> Und in systematischer Hinsicht machen die weiteren anwaltlichen Äußerungsrechte aus Art. 7 Anwaltskonvention deutlich, dass die Konvention der Meinungsfreiheit eine hervorgehobene Bedeutung beimisst. Das prozessuale Äußerungsrecht steht unter dem Schrankenvorbehalt des Art. 6 Abs. 4 Anwaltskonvention. Die Unzulässigkeit anwaltlicher Äußerungen kann nach dem *explanatory*

<sup>10</sup> <https://www.coe.int/de/web/conventions/full-list?module=signatures-by-treaty&treatyid=226> (zuletzt abgerufen am 18.3.2026).

<sup>11</sup> Arconada Valbuena, DStR 2025, 2268 (2271).

<sup>12</sup> Arconada Valbuena, DStR 2025, 2268 (2272).

<sup>13</sup> Arconada Valbuena, DStR 2025, 2268 (2270).

<sup>14</sup> Vgl. Europarat, CETS No. 226 and explanatory report, Rn. 34.

<sup>15</sup> EGMR, NJOZ 2018, 504 Rn. 56.

<sup>16</sup> Arconada Valbuena, DStR 2025, 2268 (2268).

<sup>17</sup> EGMR, Urt. v. 21.3.2002, 31611/96 (Nikula v. Finland) Rn. 54.

<sup>18</sup> Europarat, CETS No. 226 and explanatory report, Rn. 47.

<sup>19</sup> Europarat, CETS No. 226 and explanatory report, Rn. 47.

<sup>20</sup> Europarat, CETS No. 226 and explanatory report, Rn. 47: „it is not intended that lawyers should incur civil and criminal liability merely for having presented their clients' version“.

tory report nur in Ausnahmefällen als in einer demokratischen Gesellschaft notwendig angesehen werden.<sup>21</sup> Der Regelfall ist damit ihre Zulässigkeit.

Art. 7 Abs. 1 Anwaltskonvention regelt ein Äußerungsrecht, das sich als mediales Äußerungsrecht bezeichnen lässt. In der Regelung befindet sich keine ausdrückliche Bezugnahme auf Medien, aber sie will garantieren, dass Anwälte die Öffentlichkeit über Verfahren ihrer Mandate informieren können. Und hierfür werden sie sich zwangsläufig eines Mediums bedienen müssen; sei es ein klassisches wie Fernsehen oder Zeitung, oder ein neues wie eine Social-Media-Plattform oder eine eigene Webseite. Umfasst ist hiervon insbesondere das Recht, das Verfahren kritisch zu kommentieren.<sup>22</sup> Die Bedeutung dieses Rechts geht über das konkrete Verfahren hinaus, da die Äußerung Probleme allgemeiner Tragweite aufzeigen kann.<sup>23</sup> Es geht im Kern um anlassbezogene Justizkritik. Der Anwalt kann die Rechtsanwendung bestimmter Vorschriften kritisieren und Mängel des Justizsystems aufzeigen.<sup>24</sup> Ein Spannungsverhältnis mit den Beleidigungsvorschriften der §§ 185 ff. StGB ist diesem Äußerungsrecht immanent: Wirft der Anwalt einem Richter eine fehlerhafte Rechtsanwendung vor, bewegt er sich im Dunstkreis des Vorwurfs der Rechtsbeugung, welcher grundsätzlich ehrverletzenden Charakter hat.<sup>25</sup> Da die Kontrolle der Rechtspflege durch die Allgemeinheit in einem Rechtsstaat wesentlich ist,<sup>26</sup> ist die Regelung eines medialen Äußerungsrechts jedoch zu begrüßen. Einschränkungen dieses Äußerungsrechts stehen unter einem Gesetzesvorbehalt und sind nur zulässig, wenn berufliche Pflichten, die Funktionsfähigkeit der Rechtspflege, die Achtung des Privatlebens dies erfordern und sie in einer demokratischen Gesellschaft notwendig sind.

Art. 7 Abs. 2 Anwaltskonvention verleiht Rechtsanwälten und Rechtsanwaltsvereinigungen ein rechtspolitisches Äußerungsrecht. Sie können sich demnach öffentlich äußern zu den Inhalten von Gesetzen und ihrer Anwendung, gerichtlichen Entscheidungen und dem Schutz der Menschenrechte sowie Reformvorschläge machen. Auch zu Gerichtsverfahren, in denen Anwälte nicht selbst involviert sind, dürfen sie sich kritisch äußern.<sup>27</sup> Die Begründung für dieses rechtspolitische Äußerungsrecht erschließt sich aus der beruflichen Stellung und der Expertise von Anwälten, die in besonderer Weise und stärker als juristische Laien dazu in der Lage sind, rechtspolitische Ereignisse kritisch zu kommentieren.<sup>28</sup> Nach dem Wortlaut der Konvention besteht kein Schrankenvorbehalt.

Richtigerweise gestattet auch das rechtspolitische Äußerungsrecht nicht Äußerungen jeder Art. Der Schrankenvorbehalt aus Art. 10 Abs. 2 EMRK ist entsprechend heranzuziehen. Das Fehlen eines Schrankenvorbehalts erklärt sich vermutlich damit, dass Konflikte mit anderen Rechtspositionen bei rechtspolitischen Äußerungen seltener sind als bei den beiden anderen Äußerungsarten (dazu unter III. 6.), sodass redaktionell kein Bedarf für einen ausdrücklichen Schrankenvorbehalt gesehen wurde.

### III. Die Rechtsprechung des Bundesverfassungsgerichts

#### 1. Rechtliche Risiken anwaltlicher Äußerungen

Einen Rechtsanwalt, der für seinen Mandanten am Kampf um das Recht teilnimmt, umgeben einige rechtliche Risiken.<sup>29</sup> Nach der Konvention darf er schlagkräftig argumentieren – und muss das unter Umständen auch, wenn er den Standpunkt seines Mandanten effektiv vertreten will.<sup>30</sup> Die Ausübung seines Berufes kann es demnach mit sich bringen, dass er mit anderen Verfahrensbeteiligten nicht zimperlich umgeht:<sup>31</sup> Er wirft dem Prozessgegner eine Pflichtverletzung vor, unterstellt einem Zeugen zu lügen, oder lehnt das Gericht ab, weil er es für befangen hält. Solche Äußerungen haben stets einen ehrverletzenden Zug, weswegen ein Spannungsverhältnis mit den §§ 185 ff. StGB offenbar ist.<sup>32</sup> Für seinen Mandanten muss ein Anwalt Tatsachen vortragen, deren Richtigkeit er nicht kennt. Sind sie nicht erweislich wahr, könnte es sich um üble Nachrede (§ 186 StGB) handeln. Erweisen sie sich als falsch, kommt unter Umständen ein Prozessbetrug (§ 263 StGB) in Betracht.<sup>33</sup> In zivilrechtlicher Hinsicht besteht das Risiko, auf Unterlassen und Widerruf von Äußerungen verklagt zu werden.<sup>34</sup> Ferner drohen disziplinarrechtliche Folgen.<sup>35</sup>

Die freie, ungehinderte Berufsausübung – die die Konvention garantieren will (Art. 1 Abs. 1 Anwaltskonvention) – wäre stark beeinträchtigt, wenn ein Anwalt stets derartige rechtliche Risiken befürchten müsste, wenn er sich verfahrensbezogen äußert. Nach der Rechtsprechung des EGMR sollen derartige Abschreckungswirkungen („chilling effects“) nicht bestehen.<sup>36</sup> Es wäre auch nicht prozessökonomisch, wenn anwaltliche Äußerungen stets zum Gegenstand neuer Verfahren würden.<sup>37</sup> Das BVerfG zieht daher in ständiger Rechtsprechung die Grenzen anwaltlicher Äußerungsfreiheit zurecht sehr weit. Mit wenigen Präzi-

<sup>21</sup> Europarat, CETS No. 226 and explanatory report, Rn. 47.

<sup>22</sup> Europarat, CETS No. 226 and explanatory report, Rn. 54.

<sup>23</sup> Europarat, CETS No. 226 and explanatory report, Rn. 54.

<sup>24</sup> Europarat, CETS No. 226 and explanatory report, Rn. 54.

<sup>25</sup> Vgl. BayObLG, NStZ-RR 2002, 40 (41): „Der gegen Richter und Staatsanwälte erhobene Vorwurf der Rechtsbeugung hat die Rechtsprechung wiederholt beschäftigt.“

<sup>26</sup> Vgl. BGH, NStZ 2019, 549 (550).

<sup>27</sup> Europarat, CETS No. 226 and explanatory report, Rn. 56.

<sup>28</sup> Europarat, CETS No. 226 and explanatory report, Rn. 56: „Certainly, their professional role means that they are well placed to draw attention to problems posed by particular legal provisions or judicial decisions, as well as by various aspects of the operation of the justice system, which concern or affect the profession of lawyer, and to suggest possible solutions for them.“

<sup>29</sup> Hirtz, AnwBl 2008, 163 (163); Ignor, in: GS Schlüchter, 2002, S. 317 (317).

<sup>30</sup> Europarat, CETS No. 226 and explanatory report, Rn. 47.

<sup>31</sup> BVerfG, NJW 2003, 3263 (3264): „nicht immer schonend“.

<sup>32</sup> Vgl. Ignor, in: GS Schlüchter, 2002, S. 317 (318).

<sup>33</sup> Vgl. Ignor, in: GS Schlüchter, 2002, S. 317 (317).

<sup>34</sup> Hirtz, AnwBl 2008, 163 (163).

<sup>35</sup> Hierzu Peitscher, Anwaltsrecht, 4. Aufl. (2025), § 18 Rn. 52 ff.

<sup>36</sup> EGMR, Urt. v. 21.3.2002, 31611/96 (Nikula v. Finland), Rn. 54.

<sup>37</sup> OLG Hamm, NStZ-RR 2006, 7 (8), das erkennt, dass die Einleitung von Strafverfahren wegen jeder möglichen Ehrverletzung „zu einer erheblichen Belastung der Strafjustiz mit Bagatelldelikten führen würde.“

sierungen sind sie ein guter Maßstab, um die Ziele der Konvention zu verwirklichen.

## 2. Die erste Weichenstellung: Tatsachenbehauptung oder Werturteil?

Nach der Ermittlung des Sinnes einer Äußerung<sup>38</sup> ist die erste wesentliche Weichenstellung des *BVerfG* die Frage, ob die Äußerung ein Werturteil oder eine reine Tatsachenbehauptung ist.<sup>39</sup> Eine Verletzung des Art. 5 Abs. 1 S. 1 GG liegt bereits darin, dass ein Gericht eine Äußerung zu Unrecht als Tatsachenbehauptung einstuft.<sup>40</sup> Nach dem *BVerfG* ist der Begriff der Meinung aus Art. 5 Abs. 1 S. 1 GG weit zu verstehen.<sup>41</sup> Hierunter fallen alle Äußerungen, die durch ein Element der Stellungnahme geprägt sind.<sup>42</sup> Eine Tatsachenbehauptung zeichnet sich hingegen dadurch aus, dass ihre Richtigkeit theoretisch mit den Mitteln des Beweises überprüfbar ist.<sup>43</sup> Bei der Abgrenzung von Werturteil und Tatsachenbehauptung ist der Gesamtkontext zu berücksichtigen.<sup>44</sup> Häufig vermischen sich Werturteile und Tatsachenmitteilungen untrennbar in einer Äußerung.<sup>45</sup> Eine isolierte Betrachtung einzelner Äußerungsteile ist nicht zulässig, weil dies „den Anforderungen an eine zuverlässige Sinnermittlung regelmäßig nicht gerecht“ wird.<sup>46</sup> Nur solange der Sinn einer Äußerung nicht verfälscht wird, ist eine isolierte Betrachtung möglich.<sup>47</sup> Sind Tatsachenbehauptungen Voraussetzungen für eine Meinungsbildung oder fügen sie sich in eine im Schwerpunkt wertende Argumentation ein, so handelt es sich um eine einheitliche Äußerung, die als Werturteil den Schutz des Art. 5 Abs. 1 S. 1 GG genießt.<sup>48</sup>

## 3. Die Zulässigkeit von Tatsachenbehauptungen

Diese erste Weichenstellung ist entscheidend, da die Zulässigkeit von Werturteilen und Tatsachenbehauptungen unterschiedlichen Maßstäben unterliegt. Ein Anwalt darf keine Tatsachen verbreiten, von denen er sicher weiß, dass sie nicht stimmen (§ 43a Abs. 3 BRAO). Behauptet ein Anwalt bewusst falsche Tatsachen, so macht er sich nach § 187 StGB strafbar, wenn es sich um ehrverletzende Tatsachen handelt, und nach § 263 StGB, wenn er sie vorträgt, um seinem Mandanten einen rechtswidrigen Vermögensvorteil zu verschaffen. Erforderlich ist für ein „bewusstes“ Verbreiten von Unwahrheiten (§ 43a Abs. 3 BRAO) direkter Vorsatz in Form der Wissentlichkeit.<sup>49</sup> Es genügt daher grundsätzlich nicht, dass der Anwalt die Unwahrheit einer Tatsachenbehauptung im Sinne eines bedingten Vorsatzes lediglich für möglich hält.<sup>50</sup>

Auf den ersten Blick kommt allerdings nach einigen Normen eine Strafbarkeit in Betracht, wenn der Anwalt die Unrichtigkeit lediglich für möglich hält. Und dieser Wissensstand dürfte der Regelfall sein, denn normalerweise weiß der Anwalt nicht mit Sicherheit, ob der Sachverhalt, den der Mandant ihm mitteilt, richtig oder falsch ist. Trägt er eine Tatsache vor, die nicht erweislich wahr ist, kommt insbesondere eine Strafbarkeit nach § 186 StGB in Betracht.

Es liegt auf der Hand, dass eine Strafbarkeit nur wegen möglicherweise falscher Tatsachenbehauptungen die Ausübung des Anwaltsberufs weitgehend unmöglich machen würde. Zöge man eine Strafbarkeit ernsthaft in Betracht, so müsste der Anwalt zunächst zum Ermittler gegen seinen Mandanten werden, bevor er eine Ansicht seines Mandanten vorträgt, da er nicht auf dessen Aussagen vertrauen dürfte. Dies „würde das Vertrauensverhältnis zwischen Anwalt und Mandant zerstören“.<sup>51</sup> Das *BVerfG* stellt deswegen richtigerweise fest, dass sich ein Anwalt Äußerungen seines Mandanten grundsätzlich nicht zu eigen macht, wenn er sie vorträgt.<sup>52</sup> Diese Rechtsprechung liegt auf Linie mit Art. 6 Abs. 5 Anwaltskonvention, der verlangt, dass ein Anwalt grundsätzlich keine Nachteile dadurch erleiden darf, dass er mit der Sache seines Mandanten identifiziert wird. Das *BVerfG* stellt ferner fest: „Eine regelmäßige Kontrolle der vom Mandanten mitgeteilten Tatsachen kann berufsrechtlich nicht verlangt werden.“<sup>53</sup> Es besteht daher, anders als teilweise in der Literatur gefordert wird,<sup>54</sup> grundsätzlich keine Prüfpflicht des Anwalts. Bloße Zweifel an der Richtigkeit können eine Prüfpflicht nicht begründen; das ist frühestens dann anzunehmen, wenn sich die Unrichtigkeit einer Behauptung aufdrängt.<sup>55</sup> Es besteht keine Strafbarkeitslücke, da der Mandant, der dem Anwalt unrichtige Informationen mitteilt, als mittelbarer Täter strafbar sein kann.<sup>56</sup>

Es ist ferner ein Gebot des Fair-trial-Prinzips, dass ein Verfahrensbeteiligter nicht aus Furcht vor einer Bestrafung davon absieht, eine nicht erweislich wahre Tatsache, die er für rechtserheblich hält, vorzutragen.<sup>57</sup> Nicht erforderlich ist, dass der Verfahrensbeteiligte ausdrücklich offenlegt, dass er für seine Behauptung keinen Beweis hat.<sup>58</sup> Denn das würde die Überzeugungskraft seines Vortrags erheblich verringern.<sup>59</sup> Ein faires Verfahren muss den Verfahrensbeteiligten jedoch genügend Spielraum lassen,

<sup>38</sup> *BVerfG*, NJW 1999, 2262 (2263).

<sup>39</sup> *BVerfG*, NStZ-RR 2024, 168 (169); *BVerfG*, NVwZ 2025, 1338, Rn. 30; vgl. auch *Bethge*, in: Sachs, GG, 10. Aufl. (2024), Art. 5 Rn. 29.

<sup>40</sup> *BVerfG*, NJW 1999, 2262 (2263); *BVerfG*, NJW 2000, 3196 (3197); *BVerfG*, NStZ-RR 2024, 168 (169).

<sup>41</sup> *BVerfG*, NJW 2000, 3196 (3197).

<sup>42</sup> *BVerfG*, NJW 2000, 3196 (3197); *BVerfG*, NStZ-RR 2024, 168 (168).

<sup>43</sup> *BVerfG*, NJW 1996, 1131 (1133).

<sup>44</sup> *BVerfG*, NStZ-RR 2024, 168 (169).

<sup>45</sup> *BVerfG*, NJW 2000, 3196 (3197).

<sup>46</sup> *BVerfG*, NStZ-RR 2024, 168 (169).

<sup>47</sup> *BVerfG*, NStZ-RR 2024, 168 (169).

<sup>48</sup> Vgl. *BVerfG*, NJW 2000, 3196 (3196); BayObLGSt 2001, 92 (97); *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>49</sup> *Bauckmann*, in: Weyland, BRAO, 11. Aufl. (2024), § 43a Rn. 39; *Henssler*, in: Henssler/Prütting, BRAO, 6. Aufl. (2024), § 43a Rn. 188.

<sup>50</sup> *Bauckmann*, in: Weyland, BRAO, § 43a Rn. 39; *Henssler*, in: Henssler/Prütting, BRAO, § 43a Rn. 188.

<sup>51</sup> *BVerfG*, NJW 2003, 3263, 3264.

<sup>52</sup> *BVerfG*, NJW 1996, 3267 (3267); *BVerfG*, NJW 2003, 3263 (3264).

<sup>53</sup> *BVerfG*, NJW 2003, 3263 (3264).

<sup>54</sup> *Eisele/Schittenhelm*, in: TK-StGB, 31. Aufl. (2025), § 193 Rn. 22.

<sup>55</sup> Vgl. bei *Regge/Pegel*, in: MüKo-StGB, 5. Aufl. (2025), § 193 Rn. 69.

<sup>56</sup> Vgl. *Kargl*, in: NK-StGB, 6. Aufl. (2023), § 193 Rn. 28; *Rogall*, in: SK-StGB, 10. Aufl. (2024), § 193 Rn. 8.

<sup>57</sup> Vgl. *BVerfG*, NJW 2000, 3196 (3197).

<sup>58</sup> *BVerfG*, NJW 2000, 3196 (3198).

<sup>59</sup> *BVerfG*, NJW 2000, 3196 (3198).

ihren Standpunkt effektiv vorzutragen.<sup>60</sup> Äußerst sich ein Anwalt verfahrensbezogen für seinen Mandanten, kommt eine Strafbarkeit wegen einer Tatsachenbehauptung daher oftmals nur dann in Betracht, wenn der Anwalt deren Unrichtigkeit kennt.

#### 4. Die Zulässigkeit von Werturteilen

##### a) Erster Prüfungspunkt: Schmähung, Formalbeleidigung oder Verletzung der Menschenwürde?

Im Rahmen der Beleidigungsdelikte finden die Belange der Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 GG über § 193 StGB Berücksichtigung, der aufgrund seiner offenen Formulierungen grundrechtlichen Erwägungen in besonderer Weise offensteht.<sup>61</sup> Durch dieses „Einfallstor“ ebenfalls zu berücksichtigen sind das Rechtsstaatsprinzip, aus dem sich der Grundsatz des fairen Verfahrens ableiten lässt, und der Anspruch auf rechtliches Gehör nach Art. 103 Abs. 1 GG.<sup>62</sup>

Zu einer Abwägung zwischen Meinungsfreiheit und Persönlichkeitsrechten kommt es jedoch nach der Rechtsprechung des *BVerfG* dann nicht, wenn die Äußerung eine Schmähung, eine Formalbeleidigung oder einen Angriff auf die Menschenwürde darstellt.<sup>63</sup> Bei diesen drei Fallgruppen „handelt es sich um Ausnahmekonstellationen, an deren Vorliegen jeweils strenge Kriterien anzulegen sind“. <sup>64</sup> Ein Verstoß gegen Art. 5 Abs. 1 S. 1 GG ist bereits darin zu sehen, dass ein Gericht zu Unrecht eine dieser drei Fallgruppen annimmt und es deswegen nicht mit den Belangen der Meinungsfreiheit abwägt.<sup>65</sup>

In der Rechtsprechung des *BVerfG* finden sich leicht unterschiedliche Definitionen dazu, was eine Schmähung ist. So wiederholt es in vielen Entscheidungen, dass eine Schmähung eine Äußerung ist, bei der „nicht mehr die Auseinandersetzung in der Sache, sondern – jenseits auch polemischer und überspitzter Kritik – die Diffamierung der Person im Vordergrund steht“. <sup>66</sup> An anderer Stelle spricht das *BVerfG* jedoch davon, dass eine Schmähung erst vorliegt, „wenn eine Äußerung keinen irgendwie nachvollziehbaren Bezug mehr zu einer sachlichen Auseinandersetzung hat und es im Grunde nur um das grundlose Verächtlichmachen der betroffenen Person als solcher geht“. <sup>67</sup> Nun kann allerdings etwas, das nur im Hintergrund einer Äußerung mitschwingt, noch einen „irgendwie nachvollziehbaren Bezug“ zur Sache haben. Besonders deutlich wird dieser Sachbezug auf sprachlich-pragmatischer Ebene, wenn ein Anwalt lediglich *vordergründig* etwas sagt, um etwas Anderes auszudrücken. In

einem Plädoyer sprach ein Anwalt davon, dass die Strafverfolgungsbeamten Ermittlungen nach „Gestapo-Methoden“ vorgenommen hätten.<sup>68</sup> Ein Vergleich, der ohne Frage ehrverletzend ist.<sup>69</sup> Aber um eine Schmähung handelt es sich nicht,<sup>70</sup> da bei zutreffender Sinnermittlung deutlich ist, dass der Anwalt letztlich auf sachlicher Ebene die Beweiserhebung kritisierte. Das *LG Hechingen* bewertete die Äußerung als nach § 193 StGB gerechtfertigt, weil der Anwalt zur Verteidigung von Rechten handelte und er „auf drastische Weise die Wertlosigkeit“ der Ermittlungsmaßnahme deutlich machen wollte.<sup>71</sup> Richtigerweise ist eine Äußerung bereits dann keine Schmähung, wenn sie einen – wenn auch noch so geringen – Sachbezug hat. Auch zum Schutz von Persönlichkeitsrechten ist eine Einordnung als Schmähung nicht erforderlich, denn bei der Abwägung von Meinungsfreiheit und Persönlichkeitsrecht kann zugunsten des letzteren berücksichtigt werden, dass eine Äußerung nur einen sehr geringen Sachbezug hat.<sup>72</sup>

Formalbeleidigungen sind nach der Rechtsprechung des *BVerfG* „schwerwiegende Schimpfwörter“. <sup>73</sup> Es geht um „kontextunabhängig gesellschaftlich absolut missbilligte und tabuisierte Begrifflichkeiten“. <sup>74</sup> Begriffe wie „Justizverbrecher“ oder „Rechtsbeuger“ sind keine Formalbeleidigungen, weil mit ihnen „durchaus sachliche Kritik an Personen und deren Verhalten zum Ausdruck gebracht werden könnte“. <sup>75</sup>

Eine Menschenwürdeverletzung setzt voraus, dass „sich eine Äußerung nicht lediglich gegen einzelne Persönlichkeitsrechte richtet, sondern einer konkreten Person den ihre menschliche Würde ausmachenden Kern der Persönlichkeit abspricht“. <sup>76</sup> Stellt eine Äußerung eine Verletzung der Menschenwürde dar, muss die Meinungsfreiheit stets zurücktreten.<sup>77</sup> Denn die Menschenwürde ist „als Wurzel aller Grundrechte mit keinem Einzelgrundrecht abwägungsfähig“. <sup>78</sup> Das *BVerfG* betont, dass es sich um eine Ausnahme handelt, deren Annahme einer besonders sorgfältigen Begründung bedarf.<sup>79</sup> Ein Beispiel für eine Formalbeleidigung und eine Menschenwürdeverletzung ist eine ehrverletzende Äußerung mit dem N-Wort, da es sich bei ihm um eine gesellschaftlich absolut missbilligte Begrifflichkeit und eine Verletzung der Menschenwürde handelt.

##### b) Die Abwägung im engeren Sinn

Liegt keine der drei Ausnahmen vor, ist eine „grundrechtlich angeleitete Abwägung“ zwischen Meinungsfreiheit

<sup>60</sup> Vgl. *BVerfG*, NJW 2000, 3196 (3198).

<sup>61</sup> *BVerfG*, NJW 2000, 199 (200).

<sup>62</sup> *BVerfG*, NJW 1991, 2074 (2075); *BVerfG*, NJW 2000, 3196 (3197); *BVerfG*, NJW 2017, 2606 Rn. 12.

<sup>63</sup> *BVerfG*, NJW 2022, 680 Rn. 29; *BVerfG*, NJW 2024, 745 Rn. 5.

<sup>64</sup> *BVerfG*, NVwZ 2025, 1338 Rn. 21.

<sup>65</sup> Vgl. *BVerfG*, NJW 2022, 1931 Rn. 29 ff.

<sup>66</sup> *BVerfG*, NJW 2009, 3016 (3017); *BVerfG*, NJW 2016, 2870 Rn. 17.

<sup>67</sup> *BVerfG*, NJW 2022, 1931 Rn. 28; *BVerfG*, NJW 2016, 2870 Rn. 18: „außerhalb jedes in einer Sachauseinandersetzung wurzelnden Verwendungskontextes“.

<sup>68</sup> *LG Hechingen*, NJW 1984, 1766 (1766).

<sup>69</sup> *LG Hechingen*, NJW 1984, 1766 (1767).

<sup>70</sup> Vgl. zur Begründung in einem ähnlichen Fall *OLG München*, NJW 2016, 2759.

<sup>71</sup> *LG Hechingen*, NJW 1984, 1766 (1767).

<sup>72</sup> Vgl. *OLG München*, NJW 2016, 2759 (2760): Umfang der Sach- und verfahrensbezogenheit ist „auch bei der Abwägung im engeren Sinne von entscheidender Bedeutung“.

<sup>73</sup> *BVerfG*, NVwZ 2025, 1338 Rn. 32.

<sup>74</sup> *BVerfG*, NJW 2022, 1931 Rn. 29.

<sup>75</sup> *BVerfG*, NJW 2020, 2622 Rn. 37.

<sup>76</sup> *BVerfG*, NJW 2020, 2622 Rn. 22.

<sup>77</sup> *BVerfG*, NJW 2020, 2622 Rn. 22.

<sup>78</sup> *BVerfG*, NJW 2020, 2622 Rn. 22.

<sup>79</sup> *BVerfG*, NJW 2020, 2622 Rn. 22.

und Persönlichkeitsrechten erforderlich, „die an die wertungsoffenen Tatbestandsmerkmale und Strafbarkeitsvoraussetzungen des StGB, insbesondere die Begriffe der ‚Beleidigung‘ und der ‚Wahrnehmung berechtigter Interessen‘, anknüpft“.<sup>80</sup> Dabei bestehe „kein Indiz für einen Vorrang der Meinungsfreiheit.“<sup>81</sup> Das ist in rechtlich-theoretischer Hinsicht zutreffend, in Bezug auf verfahrensbezogene Äußerungen von Anwälten wird sich jedoch praktisch in vielen Fällen ein Vorrang der Meinungsfreiheit ergeben, da die folgenden drei gewichtigen Abwägungssichtspunkte des *BVerfG* für die Meinungsfreiheit streiten: Machtkritik, der Kampf um das Recht und die berufliche Stellung des Anwalts.

Die Meinungsfreiheit gewährleistet insbesondere, die Ausübung staatlicher Macht zu kritisieren.<sup>82</sup> Das *BVerfG* spricht davon, dass die Meinungsfreiheit „gerade aus dem besonderen Schutzbedürfnis der Machtkritik erwachsen“ ist und „darin unverändert ihre Bedeutung“ findet.<sup>83</sup> Von der Meinungsfreiheit ist daher umfasst, dass ein Äußern der „von ihm als verantwortlich angesehene Amtsträger in anklagender und personalisierter Weise für die zu kritisierende Art der Machtausübung angreifen kann“.<sup>84</sup> Es „gehört zum Kernbereich der Meinungsfreiheit“, „Maßnahmen der öffentlichen Gewalt ohne Furcht vor staatlichen Sanktionen auch scharf kritisieren zu können“.<sup>85</sup> In einer Entscheidung, die keine anwaltliche Äußerungen betraf, ging das *BVerfG* davon aus, dass der Gedanke der Machtkritik bei Politikern stärker zu gewichten sei als bei Amtswaltern, „denen ohne ihr besonderes Zutun im Rahmen ihrer Berufsausübung eine Aufgabe mit Bürgerkontakt übertragen wurde“.<sup>86</sup> Bei Äußerungen von Anwälten, die sich gegen die Ehre von Richtern und Staatsanwälten richten, ist jedoch von einer beträchtlichen Bedeutung der Machtkritik im Rahmen der Abwägung auszugehen. Denn sowohl Richter als auch Staatsanwälte haben sich einen Beruf ausgesucht, in dem nicht nur der Bürgerkontakt unausweichlich ist, sondern zu dem zwangsläufig gehört, erheblich in die Rechte von Bürgern einzugreifen.

Ein Aspekt dieser Machtkritik ist, Richter wegen Befangenheit abzulehnen. Dieses Recht wird durch Art. 6 Abs. 1 lit. g Anwaltskonvention garantiert. Der Artikel sieht ferner vor, dass die Ablehnung des Staatsanwalts möglich sein soll – ein Recht, welches das deutsche Strafprozessrecht nicht vorsieht,<sup>87</sup> sodass hier Nachbesserungsbedarf besteht. In einem Fall lehnte ein Anwalt die beisitzenden Richter einer Strafkammer ab, weil sie dem

Vorsitzenden gegenüber „hörig“ seien.<sup>88</sup> Der Gerichtspräsident stellte Strafantrag wegen Beleidigung; das Schöffengericht sprach den angeklagten Anwalt jedoch zurecht frei.<sup>89</sup> Das *KG* bestätigte als Revisionsinstanz den Freispruch, da der Anwalt die Grenzen einer nach § 193 StGB erlaubten Kritik nicht überschritten hat.<sup>90</sup> Tatsächlich wäre die Wahrnehmung des Rechts, Richter wegen Befangenheit abzulehnen (§ 24 StPO, Art. 6 Abs. 1 lit. g Anwaltskonvention), praktisch weitgehend unmöglich, wenn Anwälte stets zu befürchten hätten, wegen Beleidigung angezeigt zu werden. Denn Richtern vorzuwerfen, sie leiteten ein Verfahren, obwohl sie befangen sind, hat stets eine ehrverletzende Tendenz. Die beisitzenden Richter als „hörig“ zu bezeichnen, stellt nicht einmal eine sonderlich unsachliche Ausdrucksweise dar, die die anwaltliche Äußerungsfreiheit ebenfalls zuließe.

Für weite Äußerungsmöglichkeiten spricht zudem der Gesichtspunkt des „Kampfs um das Recht“. Nach dem *BVerfG* „ist es im Kontext rechtlicher Auseinandersetzungen grundsätzlich erlaubt, auch besonders starke und eindringliche Ausdrücke zu benutzen, um Rechtspositionen und Anliegen zu unterstreichen“.<sup>91</sup> Zulässig sind „plastische Darstellungen“ zur Begründung der eigenen Rechtsposition.<sup>92</sup> Nicht entscheidend ist, ob der Äußernde weniger starke Ausdrücke hätte nutzen können.<sup>93</sup> Im Kampf um das Recht ist dem Verfahrensbeteiligten nicht abzuverlangen, „jedes Wort auf die Waagschale“ zu legen.<sup>94</sup>

Das *BVerfG* zählt zu „den wesentlichen Abwägungssichtspunkten“ die Stellung, aus der sich eine Person äußert.<sup>95</sup> Dabei spricht die berufliche Stellung eines Rechtsanwalts für eine weite Äußerungsfreiheit. Im Rahmen seiner Berufsausübung darf er „auch starke, eindringliche Ausdrücke und sinnfällige Schlagworte benutzen und sogar ‚ad personam‘ argumentieren“.<sup>96</sup> Zwar ist der Rechtsanwalt Organ der Rechtspflege (§ 1 BRAO), aber „die anwaltliche Berufsausübung [unterliegt] grundsätzlich der freien und unreglementierten Selbstbestimmung des einzelnen“.<sup>97</sup> Nicht mit der freien Berufsausübung vereinbar wäre, anwaltliche Äußerungen bereits deswegen zu sanktionieren, weil sie von anderen Verfahrensbeteiligten „als stilwidrig, ungehörig oder als Verstoß gegen den guten Ton und das Taktgefühl empfunden“ werden.<sup>98</sup> Denn zu den Aufgaben des Anwalts gehört „gerade das Äußern von Meinungen“ und für ihn sind „Wort und Schrift die wichtigsten ‚Berufswaffen‘“.<sup>99</sup> Äußerungsverbote trafen Anwälte aufgrund ihres Berufs besonders empfindlich.

<sup>80</sup> *BVerfG*, NVwZ 2025, 1338 Rn. 22.

<sup>81</sup> *BVerfG*, NVwZ 2025, 1338 Rn. 22.

<sup>82</sup> *BVerfG*, NJW 2009, 3016 (3019).

<sup>83</sup> *BVerfG*, NJW 2009, 3016 (3019).

<sup>84</sup> *BVerfG*, NJW 2009, 3016 (3019).

<sup>85</sup> *BVerfG*, NJW 2017, 2606 Rn. 12.

<sup>86</sup> *BVerfG*, NJW 2022, 680 Rn. 33.

<sup>87</sup> Vgl. *BGH*, NStZ 2025, 313 Rn. 7, möglich ist nur, beim Vorgesetzten des Staatsanwalts darauf hinzuwirken, „dass dieser ihn auf Grundlage des § 145 GVG durch einen anderen“ ersetzt. Tut der Vorgesetzte dies nicht, obwohl der Staatsanwalt befangen ist, begründet dies die Revision. Prozessökonomischer wäre die Einführung eines Ablehnungsrechts, und nach Ratifikation der Konvention auch rechtlich erforderlich.

<sup>88</sup> *KG*, NStZ-RR 1998, 12 (12).

<sup>89</sup> *KG*, NStZ-RR 1998, 12 (13).

<sup>90</sup> *KG*, NStZ-RR 1998, 12 (13).

<sup>91</sup> *BVerfG*, NJW 2020, 2622 Rn. 33; *BVerfG*, NVwZ 2025, 1338 Rn. 26.

<sup>92</sup> *BVerfG*, NJW-RR 2012, 1002 Rn. 16.

<sup>93</sup> *BVerfG*, NJW-RR 2012, 1002 Rn. 16.

<sup>94</sup> *BVerfG*, NJW-RR 2012, 1002 Rn. 16.

<sup>95</sup> *BVerfG*, NJW 2000, 199 (200); *BVerfG*, NJW 2000, 3196 (3197).

<sup>96</sup> *BVerfG*, NJW 2000, 199 (200).

<sup>97</sup> *BVerfG*, NJW 1988, 191 (193).

<sup>98</sup> Vgl. *BVerfG*, NJW 1988, 191 (193).

<sup>99</sup> Vgl. *BVerfG*, NJW 1988, 191 (193).

### 5. Das „mediale Äußerungsrecht“ in der Rechtsprechung des Bundesverfassungsgerichts

Das *BVerfG* zieht zwar den Kontext einer Äußerung bei der Abwägung heran, unterscheidet jedoch anders als die Konvention nicht ausdrücklich zwischen prozessualen, medialen und rechtspolitischen Äußerungsrechten. Konstellationen eines medialen Äußerungsrechts waren gleichwohl Gegenstand von Entscheidungen des *BVerfG*. Auch hier zeigt sich die – im Lichte der Konvention begrüßenswerte – Tendenz, die Äußerungsgrenzen weit zu ziehen.

In einem Fall kam es im Rahmen einer Haftbefehlsverkündung zwischen einem Anwalt und der mit dem Verfahren betrauten Staatsanwältin zu einer Auseinandersetzung, da der Anwalt seinen Mandanten zu Unrecht verfolgt sah.<sup>100</sup> Am Abend erhielt der Anwalt einen Anruf eines Journalisten, der eine Reportage über den Beschuldigten plante.<sup>101</sup> Auf hartnäckiges Nachfragen des Journalisten und weil er verärgert über den Verlauf der Ermittlungen war, äußerte sich der Anwalt und bezeichnete die Staatsanwältin unter anderen als „widerwärtige, boshafte, dummliche“, „durchgeknallte“ und „geistesranke“ Staatsanwältin.<sup>102</sup> Das Landgericht verurteilte den Anwalt wegen Beleidigung; die Revisionsinstanz bestätigte die Verurteilung.<sup>103</sup> Das *BVerfG* stellte fest, dass die Entscheidungen eine Verletzung des Art. 5 Abs. 1 S. 1 GG darstellen.<sup>104</sup> Das Landgericht habe fälschlicherweise eine Schmähung angenommen und die erforderliche Grundrechtsabwägung unterlassen.<sup>105</sup> Die Urteilsgründe trügen die Annahme einer Schmähung nicht, da sie nicht darlegen, dass die ehrverletzenden Äußerungen „von vornherein außerhalb jedes in einer Sachauseinandersetzung wurzelnden Verwendungskontextes“ standen.<sup>106</sup> Da der Anwalt sich zu einem konkreten Verfahren und aus Ärger über den Verlauf der Ermittlungen äußerte, hatten die Äußerungen fraglos Sachbezug und waren damit keine Schmähungen. Es handelt sich weiter nicht um Formalbeleidigungen, da Formulierungen wie „durchgeknallt“ oder „dummlich“ zwar ehrverletzend sind, mit ihnen aber noch sachliche Kritik zum Ausdruck gebracht werden kann, weil hinter diesen Äußerungen letztlich der Vorwurf steht, eine Vorgehensweise sei unvernünftig. Sie sind demnach keine gesellschaftlich absolut missbilligten Begrifflichkeiten.

Nicht zuzustimmen ist jedoch der Segelanweisung des *BVerfG* für die neue Verhandlung der Sache, dass „ein Anwalt grundsätzlich nicht berechtigt ist, aus Verärgerung über von ihm als falsch angesehene Maßnahmen einer Staatsanwältin oder eines Staatsanwalts diese gerade gegenüber der Presse mit Beschimpfungen zu überziehen.“<sup>107</sup> In diesem Fall müsse sich, so das *BVerfG*, „grundsätzlich das allgemeine Persönlichkeitsrecht der Betroffenen durchsetzen.“<sup>108</sup> In dieser Pauschalität ist dies

nicht mit dem medialen Äußerungsrecht des Art. 7 Abs. 1 Anwaltskonvention in Einklang zu bringen: Anwälte sollen sich über ihre laufenden Verfahren gerade auch kritisch äußern dürfen.<sup>109</sup> Bei der Abwägung im Einzelfall kommt es entscheidend darauf an, inwieweit die Äußerungen des Anwalts in eine sachliche Kritik eingebunden waren. Einem „grundsätzlichen“ Vorrang des Persönlichkeitsrechts, wenn ein Anwalt ehrverletzende Äußerungen „gerade gegenüber der Presse“ tätigt, steht die Konvention entgegen.

In der Abwägung spricht der Gesichtspunkt der Machtkritik für die Meinungsfreiheit. In einem anderen Fall war es kein Anwalt, sondern ein Publizist, der einen Staatsanwalt als „durchgeknallt“ bezeichnete.<sup>110</sup> Er wurde wegen Beleidigung verurteilt. Die hiergegen gerichtete Verfassungsbeschwerde war „offensichtlich begründet“.<sup>111</sup> Zunächst stellt das *BVerfG* fest, dass „durchgeknallt“ keine Schmähung ist.<sup>112</sup> Ferner sei zu berücksichtigen, dass die Meinungsfreiheit „gerade aus dem besonderen Schutzbedürfnis der Machtkritik erwachsen“ ist.<sup>113</sup> Die Vermutung für die freie Rede erlange „umso schwereres Gewicht, als die geübte Kritik die Ausübung staatlicher Gewalt zum Inhalt hatte“.<sup>114</sup>

Im Rahmen des medialen Äußerungsrechts ist außerdem der Abwägungsgesichtspunkt der beruflichen Stellung des Anwalts zu berücksichtigen. Denn auch mit Äußerungen in Medien kann ein Anwalt die Interessen seines Mandanten vertreten.

### 6. Das „rechtspolitische Äußerungsrecht“ in der Rechtsprechung des Bundesverfassungsgerichts

Art. 7 Abs. 2 Anwaltskonvention garantiert Anwälten und Anwaltsvereinigungen ein rechtspolitisches Äußerungsrecht. Aufgrund ihrer beruflichen Stellung und Expertise sind sie besonders dazu geeignet, Gesetze oder Gesetzesvorhaben sowie das Justizsystem zu kritisieren.<sup>115</sup> Rechtspolitische Äußerungen von Anwälten waren noch nicht Gegenstand bundesverfassungsrechtlicher Rechtsprechung. Dies mag daran liegen, dass Anwälte losgelöst von konkreten Verfahren, deren Ausgang über das Schicksal ihrer Mandanten entscheidet, seltener zu eindringlichen Formulierungen greifen und sich solche Formulierungen seltener gegen bestimmte Personen richten. Ein Konflikt mit den Persönlichkeitsrechten anderer Personen sind diesem Äußerungsrecht keineswegs so immanent wie den beiden anderen Äußerungsrechten.

Gleichwohl lassen sich aus der Rechtsprechung des *BVerfG* Maßstäbe gewinnen, die den Zielen des Art. 7 Abs. 2 Anwaltskonvention dienen. Bei rechtspolitischen Äußerungen handelt es sich um Beiträge zur öffentlichen Meinungsbildung, bei denen „eine Vermutung zugunsten

<sup>100</sup> *BVerfG*, NJW 2016, 2870 (2870).

<sup>101</sup> *BVerfG*, NJW 2016, 2870 (2870).

<sup>102</sup> *BVerfG*, NJW 2016, 2870 (2870).

<sup>103</sup> *KG*, BeckRS 2016, 15727.

<sup>104</sup> *BVerfG*, NJW 2016, 2870 Rn. 9 ff.

<sup>105</sup> *BVerfG*, NJW 2016, 2870 Rn. 16.

<sup>106</sup> *BVerfG*, NJW 2016, 2870 Rn. 18.

<sup>107</sup> *BVerfG*, NJW 2016, 2870 Rn. 20.

<sup>108</sup> *BVerfG*, NJW 2016, 2870 Rn. 20.

<sup>109</sup> *Europarat*, CETS No. 226 and explanatory report, Rn. 54.

<sup>110</sup> *BVerfG*, NJW 2009, 3016 (3016).

<sup>111</sup> *BVerfG*, NJW 2009, 3016 Rn. 26.

<sup>112</sup> *BVerfG*, NJW 2009, 3016 Rn. 34 ff.

<sup>113</sup> *BVerfG*, NJW 2009, 3016 Rn. 38.

<sup>114</sup> *BVerfG*, NJW 2009, 3016 Rn. 38.

<sup>115</sup> *Europarat*, CETS No. 226 and explanatory report, Rn. 56.

der Freiheit der Rede“ besteht.<sup>116</sup> Diese Vermutungswirkung für die freie Rede „in einer die Öffentlichkeit wesentlich berührenden Frage“ entwickelte das *BVerfG* bereits 1958 im Lüth-Urteil.<sup>117</sup> Sie ist seitdem ständige Rechtsprechung und „ist von ungeminderter Aktualität und Bedeutung.“<sup>118</sup> Weiterhin spielt der Abwägungsgesichtspunkt der Machtkritik eine entscheidende Rolle, der es gestattet, „Amtsträger in anklagender und personalisierter Weise“ für ihre Machtausübung zu kritisieren.<sup>119</sup>

#### IV. Schlussbemerkungen

Die Grenzen anwaltlicher Äußerungsfreiheit sind weit zu ziehen. Im Kampf um das Recht müssen Verfahrensbeteiligte mitunter Äußerungen aushalten können, die eindeutig ehrverletzend sind. Das gilt freilich auch für anwaltliche Äußerungen gegen andere Anwälte; der einzige Abwägungsgesichtspunkt, der hier nicht zum Tragen kommt, ist der der Machtkritik. Auf einem anderen Blatt steht, dass derartige Äußerungen oftmals taktisch nicht sinnvoll sind. Aber die Entscheidung für oder gegen eine „starke“ Formulierung obliegt den Anwälten; eine staatliche Qualitätskontrolle ist grundsätzlich abzulehnen.<sup>120</sup>

Wie Richter souverän mit ehrverletzenden Äußerungen umgehen können, zeichnet das *OLG Hamm* in einem bemerkenswerten Revisionsbeschluss vor. Der Angeklagte (kein Anwalt) lehnte in einem sozialgerichtlichen Rechtsstreit einen Richter mit der Begründung ab, dieser lüge, inszeniere einen Schauprozess und entferne in Verschleiерungsabsicht Aktenstücke aus der Prozessakte.<sup>121</sup> Der Angeklagte wurde wegen Beleidigung und übler Nachrede verurteilt; das *OLG Hamm* hob diese Entscheidungen auf und sprach den Angeklagten frei.<sup>122</sup> Die Verurteilung wegen übler Nachrede war bereits deshalb nicht haltbar,

weil die Behauptung, der Richter entferne Aktenstücke, zwar isoliert betrachtet eine Tatsachenbehauptung darstellt, aber eine isolierte Betrachtung war nicht statthaft, weil sich diese Äußerung in eine insgesamt wertende Argumentationskette einfügte.<sup>123</sup> Aufgrund des eindeutigen Bezugs zum Verfahren liegt keiner der drei Ausnahmefälle vor, in denen eine Abwägung mit der Meinungsfreiheit entbehrlich ist.<sup>124</sup> Und auch wenn die Äußerungen zweifelsohne ehrverletzend sind, überwiegt die Meinungsfreiheit.<sup>125</sup> Denn an einem unparteiischen Verfahren besteht ein „überragendes öffentliches Interesse“ und es muss Verfahrensbeteiligten daher erlaubt sein, Kritik auszuüben, „ohne sogleich befürchten zu müssen, Strafverfolgung ausgesetzt zu sein.“<sup>126</sup>

Das Bemerkenswerte an der Entscheidung ist, dass das *OLG Hamm* als Revisionsgericht plötzlich ungewöhnlich persönlich wird: Es verhehe „kaum ein Tag, an dem bei den hiesigen Strafsenaten nicht Schreiben mit Äußerungen, die auf oder unter dem Niveau“ der Äußerungen des Angeklagten liegen, eingingen.<sup>127</sup> Es gebe aber „unterhalb der Schwelle der strafrechtlichen Ahndung zahlreiche Möglichkeiten, auf derartige Anwürfe zu reagieren, in der Regel reicht jedoch schon schlichtes Ignorieren aus.“<sup>128</sup> Tatsächlich dürfte schlichtes Ignorieren die Souveränität des Gerichts oftmals besser wahren, als Strafanzeige zu stellen, und damit der Person Gelegenheit zu geben, „über drei Instanzen in ihrem Tun fortzufahren, was wieder neue Strafverfahren zur Folge hätte.“<sup>129</sup> So erspart sich das Gericht auch das wenig schmeichelhafte Attest, „über ein besonders ausgeprägtes Ehrgefühl zu verfügen“, welches *Degenhart* dem ehemaligen Wirtschaftsminister *Habeck* ausstellte, der hunderte Strafanzeigen wegen Beleidigung stellte.<sup>130</sup>

<sup>116</sup> *BVerfG*, NJW 1999, 2262 (2263).

<sup>117</sup> *BVerfGE* 7, 198 (212).

<sup>118</sup> *Heintzen*, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. (2022), § 117 Rn. 80.

<sup>119</sup> *BVerfG*, NJW 2009, 3016 Rn. 38.

<sup>120</sup> Vgl. *Eschelbach*, in: BeckOK StPO, 58. Ed. (1.1.2026), § 258 Rn. 13.

<sup>121</sup> *OLG Hamm*, NStZ-RR 2006, 7 (7).

<sup>122</sup> *OLG Hamm*, NStZ-RR 2006, 7 (7).

<sup>123</sup> Vgl. *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>124</sup> *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>125</sup> *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>126</sup> *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>127</sup> *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>128</sup> *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>129</sup> Vgl. *OLG Hamm*, NStZ-RR 2006, 7 (8).

<sup>130</sup> *Degenhart*, KriPoZ 2025, 4 (7).

## BUCHBESPRECHUNGEN

### ***Manon Heindorf: Kinderpornographie im Ermittlungsverfahren***

von StA Sebastian Christ

2025, Verlag Dr. Kovač, ISBN 978-3-339-14596-3, S. 552, Euro 149,80

#### **I. Einführung**

Dissertationen braucht man für gewöhnlich nicht zu lesen. Die Dissertation von *Manon Heindorf*, die unter dem Titel „Kinderpornographie im Ermittlungsverfahren – Eine Untersuchung materiell-rechtlicher Voraussetzungen und strafprozessualer Ermittlungsmaßnahmen“ erschienen ist, stellt eine seltene Ausnahme dar, weil sie über den „universitären Elfenbeinturm“ hinaus auch praktische Einblicke in typische Ermittlungsmaßnahmen bietet. Die Autorin ist Rechtsanwältin und verteidigt seit Jahren in der gesamten Bundesrepublik auch im Sexualstrafrecht. Ihr gelingt hierdurch die seltene Kombination praktischen Einblicks mit wissenschaftlichem Tiefgang.

#### **II. Aufbau und Inhalt**

In dem 550 seitenstarke Werk untersucht die Autorin in sieben Kapiteln die strafrechtliche Behandlung kinderpornographischer Inhalte im Kontext digitaler Kommunikationsräume mit besonderem Fokus auf den Tatbestand des § 184b StGB und die Herausforderungen der Internetstrafverfolgung. Nach einer einleitenden Darstellung von Problemstellung und Zielsetzung widmet sich die Autorin zunächst den dogmatischen Grundlagen des § 184b StGB. Hierzu werden die historische Entwicklung des Straftatbestands, die geschützten Rechtsgüter sowie die einzelnen Tatbestandsmerkmale systematisch aufgearbeitet. Darauf aufbauend werden die unterschiedlichen Erscheinungsformen kinderpornographischer Inhalte sowie deren Verbreitungswege im Internet dargestellt und kriminologische Aspekte der entsprechenden Delinquenz beleuchtet. Im Anschluss untersucht die Arbeit die strafrechtliche Verantwortlichkeit für entsprechende Inhalte sowohl nach geltendem Recht (*de lege lata*) als auch unter kriminalpolitischen Reformgesichtspunkten (*de lege ferenda*).

Besonderes Gewicht legt die Arbeit auf das fünfte Kapitel, das sich ausführlich den praktischen und rechtlichen Herausforderungen der Strafverfolgung kinderpornographischer Delikte im Internet widmet. Ausgehend von den Grundlagen der Anwendbarkeit deutschen Straf- und Strafprozessrechts bei grenzüberschreitenden Online-Sachverhalten – etwa Fragen des Territorialitätsprinzips, der internationalen Zuständigkeit und der Zusammenarbeit mit ausländischen Strafverfolgungsbehörden – arbeitet die Autorin zunächst die strukturellen Schwierigkeiten digitaler Ermittlungen heraus. Dazu zählen insbesondere

die Anonymisierungsmöglichkeiten im Netz, internationale Serverstrukturen sowie die technische Dynamik moderner Kommunikationsplattformen. Daran anschließend werden die verfügbaren Ermittlungsinstrumente systematisch aufgearbeitet und hinsichtlich ihrer praktischen Einsatzmöglichkeiten bewertet. Neben klassischen Maßnahmen wie Durchsuchung, Beschlagnahme oder Telekommunikationsüberwachung behandelt die Arbeit auch spezifische digitale Ermittlungsformen, etwa den Einsatz verdeckter Ermittler im Internet, Open-Source-Intelligence-Recherchen, den Umgang mit Plattformdaten sowie Darknet-spezifische Ermittlungsansätze wie Honey-pot-Server, Phishing-Seiten oder Korrelationsangriffe. Ebenso werden neuere Entwicklungen wie der Einsatz künstlicher Intelligenz zur Auswertung großer Datenmengen oder technische Verfahren zur Identifizierung von Darstellern und Tätern – etwa über Metadatenanalyse oder Deep-Fake-Erkennung – diskutiert. Ergänzend analysiert die Autorin die rechtlichen Rahmenbedingungen einzelner Ermittlungsmaßnahmen der Strafprozessordnung, darunter insbesondere Maßnahmen zur Verkehrs- und Bestandsdatenerhebung nach §§ 100g, 100j StPO, Online-Durchsuchungen, verdeckte Ermittlungen sowie die Zusammenarbeit mit Telemediendiensten und internationalen Behörden. Insgesamt zeichnet das Kapitel damit ein differenziertes Bild der praktischen Ermittlungsrealität und verbindet die technische Analyse digitaler Ermittlungsinstrumente mit einer rechtlichen Bewertung ihrer Zulässigkeit und Effektivität.

Auf dieser Grundlage entwickelt die Autorin abschließend materiell-rechtliche und strafprozessuale Reformvorschläge, die im Fazit zusammengeführt und im Hinblick auf zukünftige kriminalpolitische Entwicklungen eingeordnet werden.

#### **III. Fazit**

Die Arbeit zeigt insgesamt eindrucklich, dass die strafrechtliche Bekämpfung kinderpornographischer Inhalte im digitalen Raum vor erheblichen tatsächlichen und rechtlichen Herausforderungen steht. Besonders hervorgehoben wird die zentrale Bedeutung des § 184b StGB, dessen wiederholte Ausweitung und insbesondere die Strafrahmensverschärfung der vergangenen Jahre erhebliche praktische Konsequenzen für die Ermittlungs- und Strafverfolgungspraxis entfaltet haben. Die Autorin arbeitet überzeugend heraus, dass die Einordnung des Tatbestands als Verbrechenstatbestand in der Praxis zu erheblichen Belastungen der Strafverfolgungsbehörden geführt hat, da niedrigschwellige Fallkonstellationen häufig nicht

mehr ohne Weiteres durch Einstellungen nach Opportunitätsvorschriften erledigt werden können.

Zugleich verdeutlicht die Untersuchung die zunehmende Bedeutung technischer Ermittlungsinstrumente: Hinweise internationaler Meldestellen wie des National Center for Missing and Exploited Children (NCMEC), automatisierte Bildanalysen über Hashwertvergleiche, datenbankgestützte Analyseprogramme sowie KI-gestützte Auswertungssysteme bilden inzwischen zentrale Bausteine moderner Ermittlungen. Daneben werden klassische kriminalistische Methoden – etwa die detaillierte Bild- und Videoanalyse zur Identifizierung von Tatorten oder Beteiligten – ebenso behandelt wie verdeckte Ermittlungen in Online-Foren und Darknet-Strukturen sowie technische Maßnahmen wie Quellen-TKÜ oder Online-Durchsuchungen. Die Autorin macht dabei deutlich, dass effektive Strafverfolgung zunehmend von technischen Analysefähigkeiten und interdisziplinärer Zusammenarbeit abhängt, zugleich aber auch rechtliche Grenzen – etwa im Hinblick auf Datenanalysen ohne konkreten Tatverdacht oder die verfassungsrechtlichen Anforderungen an neue Ermittlungsinstrumente – sorgfältig zu beachten sind.

Für die kriminalpolitisch interessierte Leserschaft, aber insbesondere auch für mit Sexualstraftaten befasste Kri-

minalbeamte und Staatsanwälte, bietet die Arbeit damit einen instruktiven und praxisnahen Überblick über die tatsächlichen Ermittlungsrealitäten im Bereich der internetbasierten Kinderpornographiedelikte mit wissenschaftlichem Tiefgang.

Besonders der umfangreiche Abschnitt zur Strafverfolgung im Internet vermittelt einen detaillierten Einblick in aktuelle Ermittlungsstrategien, technische Werkzeuge und rechtliche Rahmenbedingungen. Gerade für Praktiker aus Justiz, Polizei und Strafverteidigung dürfte die Untersuchung deshalb von besonderem Interesse sein, da sie die dogmatische Analyse des materiellen Strafrechts mit einer fundierten Darstellung der tatsächlichen Ermittlungsarbeit verbindet und zugleich Reformüberlegungen zur Weiterentwicklung des rechtlichen Instrumentariums formuliert. Die Arbeit stellt damit einen wertvollen Beitrag zur aktuellen kriminalpolitischen Diskussion über den angemessenen rechtlichen und praktischen Umgang mit internetbasierter Sexualdelinquenz dar und ist, um die Eingangsformel aufzugreifen, obwohl es sich um eine Dissertation handelt, auch für Praktiker sehr lesenswert.

# Marc Bauer: Grund und Grenzen der Verfolgungsverjährung im Sexualstrafrecht

von Simon Schlicksupp

2025, Springer Verlag, ISBN 978-3-658-47453-9, S. 332, Euro 99,99

Wie viele Materien des Besonderen Strafrechts, die aus den universitären Lehrplänen ausgeklammert sind und darüber hinaus in der Praxis mangels lukrativer Mandate auch wenig Anreiz zur eingehenden wissenschaftlichen Beschäftigung bieten, leidet auch das Sexualstrafrecht trotz seiner kriminalpolitischen Dynamik und Brisanz an einer deutlichen „Untertheoretisierung“. <sup>1</sup> Umso mehr machen sich Autoren verdient, die sich dennoch mit der notwendigen Sorgfalt und Unvoreingenommenheit mit diesem Gegenstand und seinen vielfältigen Sonderstellungen im System des deutschen Strafrechts befassen. Marc Bauer legt mit seiner Dissertation zu „Grund und Grenzen der Verfolgungsverjährung im Sexualstrafrecht“ ein derartiges Unterfangen vor, das sich einem überaus praxisrelevanten Teilgebiet der Straftaten gegen die sexuelle Selbstbestimmung widmet.

Nach einem einleitenden ersten Abschnitt, in dem der Autor bündig in die Thematik und den diesbezüglichen Stand der Forschung einführt und die Ziele („Erstes Ziel ist es, die verfassungsrechtlichen Grundlagen der Verfolgungsverjährung zu konturieren und Maßstäbe für die Prüfung des einfachen Rechts zu gewinnen. [...] Das zweite Ziel ist es, die Eigenheiten des Sexualstrafrechts in ihrer Ambivalenz herauszuarbeiten.“, S. 5), den Untersuchungsgegenstand und den Gang der Untersuchung vorstellt, widmet sich das erste Kapitel des Hauptteils dem Rechtsinstitut der Verfolgungsverjährung (S. 9ff.). Dabei stellt der Autor das geltende Recht, die Dogmatik und die Gesetzgebungshistorie dar und wagt Seitenblicke in die Rechtsvergleichung und das Disziplinarrecht. Abschließend diagnostiziert der Autor ein „verjährungskritisches Klima“ in der Gegenwart (S. 29).

Das zweite Kapitel untersucht die Gründe für die Verfolgungsverjährung insbesondere im Hinblick auf die tatsächlichen Wirkungen des Zeitablaufs, etwa den faktischen Beweisschwund (S. 31ff.), das „Strafbedürfnis“, wobei insbesondere auf die Strafzwecklehre rekurriert wird (S. 40 ff.), die Verfahrensrechte des Beschuldigten, die Interessen der Strafrechtspflege sowie einige weitere Gesichtspunkte (S. 61 ff.). Im Rahmen der kenntnisreichen Erörterung der Strafzwecklehren hätten – gerade mit Blick auf die insofern besonders „aufwühlende“ Sexualkriminalität – noch Überlegungen zum Zusammenhang zwischen „gerechter Vergeltung“ durch Strafe und dem staatlichen Gewaltmonopol („retributive Generalprävention“<sup>2</sup>) sowie neueren Ansätzen einer auf Genugtuung ausgerichteten Straftheorie im Stil der „restorative justice“ interessiert, die jeweils auch Auswirkungen auf das Institut der Verjährung implizieren könnten – den Aspekt

der Opfergenugtuung spricht der Autor allerdings an späterer Stelle ausführlich an, etwa S. 85 f. Zur „Legitimation und Rechtsnatur der Verjährung“ resümiert er am Ende des Kapitels: „Die rechtliche Unmöglichkeit der Strafverfolgung wegen Zeitablaufs – Verjährung – trägt dem sinkenden Strafbedürfnis Rechnung, schützt den Unschuldigen vor den Nachteilen des Beweisschwundes und veränderter Rahmenbedingungen und damit der Gefährdung eines fairen Verfahrens, stellt Rechtssicherheit her und entlastet als erwünschte Nebenfolge die Justiz.“ (S. 70).

Auf dieser Grundlage prüft der Autor im folgenden Kapitel (S. 72 ff.) die Existenz und den Umfang eines Rechts auf Verjährung, wobei er (überzeugend) hauptsächlich auf verfassungsrechtliche Aspekte abstellt und im Ergebnis ein solches bejaht, dessen Ausgestaltung aber gesetzgeberischem Ermessen unterliege (S. 119).

Nachdem in den ersten drei Kapiteln die Verfolgungsverjährung als der eine Untersuchungsgegenstand der Arbeit somit ausführlich beleuchtet wurde, widmet sich das folgende Kapitel dem zweiten Erkenntnisobjekt, nämlich den Entwicklungslinien des Sexualstrafrechts (S. 121 ff.). Vor dem Hintergrund eines historischen Abrisses und eines fundierten Blicks auf die rechtspolitische Lage werden darin unter anderem einzelne Entwicklungen im materiellen Recht inklusive der Sanktionen (S. 153 ff.) sowie im Bereich des Opferschutzes (S. 175 ff.) dargelegt. Seit den 1990er Jahren sei, so das Fazit des Kapitels, ein „punitive turn“ im Sexualstrafrecht festzustellen (S. 197). Treffend bezeichnet der Autor Sexualdelikte als „die signal crimes unserer Zeit“ und das „homogenisierte Bild“ des Sexualstraftäters als „Problemfigur schlechthin“ (S. 198) und charakterisiert damit griffig die rechtspolitische Entwicklung des Sexualstrafrechts.

Gleichsam als Synthese der zuvor getrennt eingeführten Gegenstände erfolgt sodann der Blick auf die Verfolgungsverjährung im Sexualstrafrecht (S. 202 ff.) als Kernstück der Arbeit. Dabei stellt der Autor zunächst Entwicklungen im Strafrecht sowie zivilrechtliche Sonderregelungen dar. Im Anschluss daran werden verjährungsrelevante Besonderheiten des Sexualstrafrechts beleuchtet. Insbesondere das Ruhen der Verjährung bis zur Vollendung des 30. Lebensjahres des Tatopfers nach § 78b Abs. 1 Nr. 1 StGB wird einer kritischen Prüfung unterzogen, an die sich die Erörterung alternativer Regelungsmodelle und ein konkreter Normvorschlag anschließen (S. 260). Das letzte Kapitel widmet sich den Rückwirkungen im Bereich der Verfolgungsverjährung (S. 266 ff.).

Die Arbeit schließt mit einer knappen Schlussbetrachtung (S. 289 f.), die an dieser Stelle zwar noch von einer systematischen Zusammenfassung der einzelnen Erträge der

<sup>1</sup> Vgl. Hörnle, ZStW 2015, 851 (851f.).

<sup>2</sup> Vgl. etwa Andrissek, Vergeltung als Strafzweck, 2017.

Arbeit profitiert hätte, aber im Plädoyer für eine Achtung der Rechtsstaatlichkeit, zu deren Kernbestand auch die Verjährung zählt, auch und gerade auf politisch überhitzten Rechtsgebieten wie dem Sexualstrafrecht einen schlüssigen und überzeugenden Schlusston findet: „Das Strafrecht ist nicht das Allheilmittel der Gesellschaftspolitik und darf nicht mit der Aufgabe überfordert werden, die individuellen und kollektiven Traumata von Missbrauchsoffern zu überwinden.“ (S. 290).

Der Autor, der selbst mehrere Jahre im Bundestag und im Bundesministerium der Justiz im Referat für Parlaments-

und Kabinettsangelegenheiten tätig war und insofern das „Innenleben“ der Kriminalpolitik aus eigener Anschauung kennt, liefert mit seiner Arbeit somit auch eine gezielt rechtspolitische Betrachtung. Sie stellt insgesamt einen wichtigen Beitrag auf einem der derzeit dynamischsten Bereiche der Strafrechtssetzung und -wissenschaft dar und offenbart hellsichtige Einblicke in eine Thematik, die auch in Zukunft an Brisanz kaum einbüßen wird. Der äußerst umfangreiche Quellenapparat beweist den erheblichen Rechercheaufwand und legt auch für die anknüpfende Forschung zu vielen (angrenzenden) Detailfragen hilfreiche Fährten in die bisherige Literatur.

## ***Ibrahim Yanik: Algorithmenbasierte Systeme in der Strafzumessung***

*von Prof. Dr. Anja Schiemann*

2025, Duncker & Humblot GmbH, ISBN: 978-3-428-19598-5, S. 346, Euro 99,90

Schon in der Einleitung macht der Verfasser deutlich, dass die einzelnen Phasen der Strafzumessung besonders kritisch sind und ein Idealfall, nach dem bei identischen Strafzumessungsumständen auch die zu verhängende Strafe exakt gleich ausfalle, wohl nie eintreten dürfte. Ob dann der Einsatz von algorithmenbasierten Systemen in der Strafzumessung eine gangbare und erfolgsversprechende Lösung ist, ist bereits Kern unterschiedlicher Forschungsschriften geworden. Ziel dieser Arbeit ist es, auf Grundlage zweier denkbarer Entwicklungsansätze eine Einschätzung darüber zu geben, inwiefern der Einsatz algorithmenbasierter Systeme für die Strafzumessung in der Gerichtspraxis aus technischer Sicht realisierbar sein wird. Den Schwerpunkt der Arbeit bildet dabei das Abstecken der rechtlichen Rahmenbedingungen eines solchen Einsatzes.

Einführend werden zunächst die terminologischen Grundlagen gesetzt, der Begriff des Algorithmus<sup>1</sup> greifbar gemacht und die Entwicklung algorithmenbasierter Systeme – wenn auch sehr knapp – nachgezeichnet. Der Begriff der Künstlichen Intelligenz wird aus Art. 3 Nr. 1 der KI-Verordnung übernommen. Differenziert wird im Hinblick auf die Strafzumessung nach zwei Ausgestaltungsvarianten: zum einen, dass das Ergebnis des durch das System generierten Strafmaßes die richterliche Strafmaßentscheidung ersetzt. Zum anderen, dass das Ergebnis lediglich der Unterstützung der richterlichen Entscheidung dient, so dass die Entscheidungshoheit beim Richter verbleibt (S. 30). Hinsichtlich dieser Differenzierung ist schon vielfach betont worden, dass lediglich bei Verbleib der Entscheidungshoheit beim Richter eine algorithmenunterstützte Strafzumessungsentscheidung rechtlich zulässig sei. Insofern bleibt spannend, wie sich hier der Verfasser positioniert.

In Kapitel 2 gibt der Verfasser zunächst einen Überblick über die Grundlagen der Strafzumessung und wendet sich hierzu den Strafzwecken zu. Nachdem diese kurz vorgestellt werden, werden Stärken und Schwächen der Grundpositionen beschrieben und sich für eine „Offenheit gegenüber mehreren Strafzwecken“ (S. 43) ausgesprochen. Dennoch bedürfe es für eine praktikable Umsetzung der Vereinigungstheorien auf den Strafzumessungsvorgang einer Konkretisierung. Hier wird sich an den fünf Schritten des Strafzumessungsvorgangs von *Hans-Jürgen Bruns* orientiert und diese dann in eine Strafzumessungsfolgeentscheidung überführt. Abgerundet wird dies durch einen „Blick auf die Praxis“ und die „Darstellung der Strafzumessungsentscheidung im Urteil“ (S. 96). Der Verfasser kommt zu dem Ergebnis, dass weder die gesetz-

lichen Regelungen den Vorgang der Strafzumessung abstrakt widerspiegeln noch auf Grundlage des konkreten Urteils exakt und in jeder Hinsicht eindeutig die einzelnen Schritte von der individuellen Tat hin zum konkreten Strafmaß konstruiert werden könnten.

Dieses ernüchternde Ergebnis leitet über zu den aktuellen Entwicklungen zur Optimierung der Strafzumessungspraxis. Hintergrund dieser Reformüberlegungen sind empirische Befunde zu regionalen Strafmaßdivergenzen sowie zu der Auswirkung spezifischer Merkmale in der Person des Urteilenden sowie die Fokussierung auf weniger entscheidende Strafzumessungskriterien. Diese Befunde werden überführt in eine Darstellung bislang existierender Optimierungsansätze seitens der Literatur, die sehr knapp aber unter ausführlicher Quellenauswertung referiert werden. Insbesondere sei es für den Verfasser naheliegend, die Idee von der Unterstützung der Strafzumessungspraxis weiter zu denken und das Potenzial computergestützter Technologien für die Strafzumessung nutzbar zu machen (S. 112). Verwiesen wird hier auf ein Forschungsprojekt, dass eine Datenbank erstellt hat und dessen erster Prototyp einzelne Strafzumessungserwägungen in Entscheidungen erkennbar und Urteile danach untersuchbar machen könne. Auch ein Decision-Support-System helfe bereits bei der Bewertung von Eigentums- und Vermögensdelikten. Daher sei es nur konsequent, einen Schritt weiterzudenken und die Möglichkeit einer auf maschinellen Lernverfahren basierende Strafzumessung zu erwägen. Ausblickend wird eine „entwicklungsoffene Grundhaltung mit angemessener Skepsis“ (S. 115) für am zielführendsten gehalten.

Kapitel 3 widmet sich dann der Realisierbarkeit des Einsatzes algorithmenbasierter Systeme in der Strafzumessung aus technischer Sicht. Die erste Herausforderung bestehe an der Schnittstelle zwischen Mensch und Maschine. Hier müsse ein angemessener, praxistauglicher Ausgleich zwischen notwendig detailoffener Benutzeroberfläche und technisch realisierbarer Komplexität gewährleistet werden. Die „Algorithmierbarkeit“ des Strafzumessungsvorgangs sei hier die zentrale technische Voraussetzung. Die Entwicklungsschritte auf dem Weg zu einem algorithmenbasierten System für die Strafzumessung werden in einem weiteren Kapitel nachgezeichnet.

Dabei wird einem die Euphorie völlig zu Recht genommen, was die Tauglichkeit solcher Systeme anbelangt, da diese zumindest nach aktuellem Stand der Technik nicht in der Lage sein werden, den Vorgang der Strafzumessung allumfassend zu übernehmen. Allerdings hätten die algorithmenbasierten Systeme durchaus Potential für einfache Tatbestandskonstellationen, bei denen die Mehrzahl der Fälle verhältnismäßig standardisiert aufträte. Diese identifiziert der Verfasser im Bereich der Alltagskriminalität,

wie einfache Diebstahlsdelikte, Trunkenheit im Verkehr sowie einfache Betäubungsmittel- und Steuerstraftaten. Zielführend sei hier ein deliktsspezifisches datenbasiertes Vorgehen, bei welchem eine Vielzahl an Strafzumessungsentscheidungen mittels maschineller Lernverfahren auf Gesetzmäßigkeiten in den Urteilen analysiert werde. Ergänzend hierzu seien einzelne verbindliche Regeln gezielt einzuprogrammieren, um z.B. überproportionale Berücksichtigung bestimmter Strafzumessungsgesichtspunkte zu vermeiden.

Betont wird zudem, dass eine Realisierung algorithmenbasierter Systeme für die Strafzumessung eine interdisziplinäre Zusammenarbeit erfordere. Der Verfasser plädiert hier für die Einrichtung einer speziellen Kommission bestehend aus Experten des Strafzumessungsrechts sowie der Informatik. Die Problemlösungskapazitäten moderner Systeme künstlicher Intelligenz eröffneten durchaus eine Perspektive für die Realisierung eines solchen Systems, erforderlich sei hierfür aber eine aufwendige, komplexe und willensstarke Grundlagenforschungsarbeit (S. 167).

In Kapitel 4 werden die rechtlichen Anforderungen an den Einsatz algorithmenbasierter Systeme in der Strafzumessung beschrieben. Dazu werden zunächst die Anforderungen des materiellen Strafzumessungsrechts gem. § 46 StGB abgesteckt, bevor die Anforderungen an den gesetzlichen Richter im Sinne des Grundgesetzes beschrieben werden. Interessant sind auch die Überlegungen des Rechts des Angeklagten auf eine „menschliche“ Entscheidung. Übergeleitet wird dann zu dem Anspruch auf rechtliches Gehör sowie den Rechtsschutz und die – nach Auffassung des Verfassers – zu bildende Strafzumessungskommission.

Nicht überraschend und ganz konform mit dem bisherigen Meinungsbild wird ein System, das die generierten Strafmaßegebnisse für den Richter verbindlich festlegt und mithin an die Stelle des menschlichen Entscheidungsträgers tritt, als verfassungswidrig eingestuft. Dies widerspräche nicht nur Art. 92, 97 und 101 Abs. 1 S. 2 GG, sondern auch dem Recht des Angeklagten auf eine Entscheidung durch einen Menschen. Dies folge aus dem aus der Menschenwürdegarantie und der Garantie der Eigenverantwortlichkeit des Menschen sowie dem Rechtsstaatsprinzip hergeleiteten Grundsatz schuldangemessenen Strafs. Dieselbe Wertung sei Art. 22 DSGVO zu entnehmen. Zudem könne bei einer Entscheidung durch das algorithmenbasierte System, Sachinhalt und persönlichen Eindruck nicht ausreichend Rechnung getragen werden.

Dagegen sei die Verwendung eines algorithmenbasierten Systems zur Unterstützung der richterlichen Entscheidung unter Einhaltung der rechtlichen Rahmenbedingungen rechtmäßig. Wichtig sei, dass das System auch tatsächlich im Wesentlichen Strafmaßvorschläge generiere, die dem Richter eine praktikable Grundlage für eine vor dem Hintergrund des § 46 Abs. 1 StGB angemessene Strafe böten. Elementar sei hier auch die adäquate Ausgestaltung der Schnittstelle zum Richter sowie zum Angeklagten. Hier müssten Vorkehrungen getroffen werden, die sicherstellen, dass die Nutzung des Systems keine faktische Bindungswirkung entfalte und die in Art. 97 Abs. 1 GG garantierte richterliche Unabhängigkeit gewahrt bleibe. Gewährleistet werden müsse zudem, dass dem Angeklagten das Zustandekommen des Strafmaßes – insbesondere im Zusammenspiel zwischen Richter und algorithmenbasiertem System – nachvollziehbar sei. Die Programmentwicklung, die Einbettung in die richterliche Tätigkeit sowie der Einsatz im Strafzumessungsalltag der Gerichte sei durch eine extra einzurichtende Strafzumessungskommission zu begleiten.

Auch diese – hohen – Anforderungen an eine rein entscheidungsunterstützende KI reduzieren laut Auffassung des Verfassers die Praktikabilität des Einsatzes algorithmenbasierter Systeme in der Strafzumessung deutlich. Es bleibe daher abzuwarten, ob in den nächsten Jahren tatsächlich Strafzumessungsentscheidungen in deutschen Gerichten auf Grundlage algorithmisch generierter Strafmaßvorschläge getroffen würden. Realistischere Einsatzfelder seien daher Strafzumessungsdatenbanken sowie der Einsatz algorithmenbasierter Systeme im Strafbefehlsverfahren. Leserfreundlich werden am Ende der Dissertation die sieben zentralen Kernthesen der Arbeit zusammengefasst.

Das Fazit ist ernüchternd und eigentlich nicht neu. Dennoch bietet die Dissertation eine Fundgrube an Quellen (was nicht nur durch den ausführlichen Fußnotenapparat, sondern auch durch das beeindruckende, 51 Seiten umfassende Literaturverzeichnis belegt wird). Die präzisen und ausführlichen rechtlichen Rahmenbedingungen verdeutlichen, dass es bei aller (empirischer) Kritik an richterlichen Strafzumessungsentscheidungen keinen Königsweg durch Nutzung von KI geben kann. Unterstützung ist aber möglich und hier sollten Datenbanken ansetzen. Der Blick auf das Strafbefehlsverfahren hat zudem offengelegt, dass gerade in sehr standardisierten, einfachen Verfahren das Potential algorithmenbasierter Systeme liegen kann. Hier ist noch längst nicht alles ausgeschöpft.

## TAGUNGSBERICHT

**Erlanger Cybercrime Tag 2025 – Digitale Beweismittel in der Hauptverhandlung**

von Franka Härtlein, Dipl.-Jur. Leila Khayati  
und Ass. iur. Tabea Seum\*

*Der Tagungsbericht enthält sprachlich bereinigte und teils vom Englischen ins Deutsche übersetzte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge des Erlanger Cybercrime Tages 2025. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten. Der Erlanger Cybercrime Tag 2025 und die Erstellung dieses Tagungsberichts wurden von der Dr. Germain-Schweiger-Stiftung gefördert.*

**I. Einleitung**

Auch im Jahr 2025 öffnete der Wassersaal der Orangerie der Friedrich-Alexander-Universität wieder seine Tore für alle Cybercrime Interessierten. Am 20.3.2025 fand der 9. Erlanger Cybercrime Tag statt. Das hybride Konzept der Veranstaltung ermöglichte es auch dieses Jahr, dass sich zahlreiche Teilnehmende präsent oder auch virtuell austauschen konnten. Das Publikum war, wie auch in den vorherigen Jahren, bunt gemischt und setzte sich aus Vertretern der Wissenschaft, der Strafrechtspraxis, wie der Justiz als auch der Anwaltschaft, Fachvertreter:innen und auch Studierenden zusammen. Der angeregte Dialog in den Q&A-Sessions führte zu einem fruchtbaren Austausch aller. Professor Dr. Christoph Safferling LL.M. (LSE) und sein ICLU-Team waren hoch erfreut, dass sich mal wieder die Mühen im Vorfeld gelohnt hatten und eine erfolgreiche Tagung stattfinden konnte.

Gegenstand der diesjährigen Veranstaltung war das hochaktuelle und in der Fachliteratur wie auch in der Praxis intensiv diskutierte Thema "Digitale Beweismittel in der Hauptverhandlung". Die grenzüberschreitende Relevanz der Thematik spiegelte sich in der Beteiligung nationaler, sowie internationaler Referent:innen wider. Obwohl die Verwendung digitaler Beweismittel im Strafprozess längst keine Besonderheit mehr ist, bestehen mangels Regulierungen und Vorgaben Unsicherheiten im Umgang mit diesen. Im Rahmen der Veranstaltung wurde sich dabei unter anderem mit der Rolle des Sachverständigen befasst. Weiterhin wurde sich mit den unterschiedlichen Sprachsystemen der Rechtswissenschaft und Informatik und der damit einhergehenden Übersetzungsproblematik für Beteiligte auseinandergesetzt, Fragen und Herausfor-

derungen mit Big Data, sowie der Durchsicht und Beschlagnahme von Datenträgern diskutiert und beleuchtet. Darüber hinaus wurde ein Blick auf den internationalen Umgang mit digitalen Beweismitteln geworfen und Reformvorschläge durch die Referent:innen präsentiert.

Eröffnet wurde die Tagung mit den Begrüßungsworten des Präsidenten der FAU Erlangen-Nürnberg, Prof. Dr. Joachim Hornegger und sich einer daran anschließenden Begrüßungsrede von Professor Dr. Christoph Safferling, LL.M. (LSE), wobei die zentralen Problemstellungen und Fragen der Thematik aufgegriffen und zugleich inhaltlich in den Themenbereich eingeführt wurde. Die Referent:innen, Dr. Nicole Scheler (DFG-Graduiertenkolleg 2475 Cyberkriminalität und Forensische Informatik), Marion Liegl (FAU Erlangen-Nürnberg), Matthew Cross (IStGH Den Haag), Dr. Eren Basar (Wessing&Partner) und Gregory Kochneff (BLKA) stellten die aufgeworfenen Fragen und Probleme dann anschaulich in ihren Vorträgen dar.

**II. Die Beweiswürdigung des IT-Sachverständigen von Dr. Nicole Scheler (DFG-Graduiertenkolleg 2475 Cyberkriminalität und Forensische Informatik)**

Den Erlanger Cybercrime Tag durfte dieses Jahr Frau Dr. Nicole Scheler mit ihrem Vortrag beginnen. Die ehemalige Doktorandin und noch Assoziierte des Graduiertenkollegs Cyberkriminalität und Forensische Informatik präsentierte die Ergebnisse ihrer jahrelangen Forschung und Dissertationsschrift, die sich mit der Beweiswürdigung des IT-Sachverständigen im deutschen Strafverfahren befasste.<sup>1</sup> In ihrem anregenden Vortrag führte sie das Publikum anhand eines juristischen Falles durch die theoretischen Kernaspekte, die bei der Beweiswürdigung des IT-Sachverständigen beachtet werden müssen.

**1. Allgemeine Grundsätze zur Beweiswürdigung**

Aufgrund des stetigen technologischen Fortschritts treffen vor Gericht oft zwei Wissenschaften aufeinander: die Rechtswissenschaft und die Informatik. Wohingegen erstere klare und deutliche Antworten verlangt, arbeitet die Informatik, als Naturwissenschaft mit Wahrscheinlichkeiten und Fehlerquoten. Diese gegensätzlichen Pole und

\* Franka Härtlein ist und Leila Khayati war Studentische Hilfskraft am Lehrstuhl von Prof. Dr. Christoph Safferling, LL.M. (LSE) an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Tabea Seum ist wissenschaftliche Mitarbeiterin im DFG Graduiertenkolleg 2475 Cyberkriminalität und forensische Informatik, sowie wissenschaftliche Mitarbeiterin am Lehrstuhl von Prof. Dr. Christoph Safferling.

<sup>1</sup> vgl. Scheler, Die Tätigkeit der IT-Sachverständigen im deutschen Strafverfahren.

verschiedenen Sprachsysteme in Einklang zu bringen, ist Aufgabe des IT-Sachverständigen.

#### *a) Die freie, richterliche Beweiswürdigung, § 261 StPO*

Die freie richterliche Beweiswürdigung gem. § 261 StPO bedeutet, dass das Gericht aufgrund eigener, persönlicher und freier Überzeugung aus dem Inbegriff der Verhandlung, unabhängig von Beweisregeln formaler Art, eine Entscheidung trifft. Im Rahmen der Beweiswürdigung wird die Bedeutung des Beweises, seine mögliche Verwertung für den Tatvorwurf und die darauf aufbauende tatrichterliche Überzeugung eingeschätzt. Diese richterliche Überzeugung ist eine persönliche, subjektive Gewissheit von der objektiven Wahrheit, sodass es zur Erlangung dieser Wahrheit an einem sehr hohen Maß an Wahrscheinlichkeit bedarf, sowie der inneren Gewissheit der Richterin von der Wahrheit des Geschehens. Untermuert und begründet wird diese subjektive Ansicht durch Wissen und Argumente, die sich kommunikativ vermitteln lassen. Das Resultat der Wahrheitsfindung im Strafprozess sollte ein festgestellter Sachverhalt sein, der mit objektiv hoher Wahrscheinlichkeit mit der Wirklichkeit übereinstimmt. Begünstigt wird dies durch eine hohe Qualität der Tatsachenbasis. Eine solch hohe Qualität ergibt sich durch eine Nähe der Tatsachen zum subsumtionsfähigen Sachverhalt (Haupttatsache oder Indizien) und einer zuverlässigen Aussagekraft, mithin eines hohen Beweiswerts.

#### *b) Abgrenzung eigene Wahrnehmung der Richter:innen und Notwendigkeit der Bestellung eines Sachverständigen*

Ein eigenständiges Tätigwerden des Gerichts ist regelmäßig geboten, wenn es über ausreichend eigene Sachkunde verfügt. Dann können die Richter:innen selbstständig z.B. eine Inaugenscheinnahme oder eine Bewertung der Tatsachen, wie beim einfachen Lesen oder Nachzählen, vornehmen.

Nr. 69 RiStBV bestimmt, dass Sachverständige nur dann hinzugezogen werden sollen, wenn es für die Sachverhaltsaufklärung unentbehrlich ist. Dies lässt die Schlussfolgerung zu, dass es auf die Person der Richterin und des individuellen Kenntnis- und Wissensstands ankommen kann. Soweit eine Richterin mehr als nur Allgemeinwissen in der Forensik hat, kann sie die entsprechende Entscheidung in diesem Gebiet eigenständig treffen, wobei dann eine explizite Darlegung und Begründung im Urteil gefordert ist. Eine solche individuelle Sachkunde kann zum Beispiel durch repetitives Aufkommen der gleichen Problematiken und Lösungen in Fällen erworben werden, durch jahrelange Erfahrung auf diesem Gebiet oder Weiterbildungen.

Hingegen ist es nicht erlaubt, dass Richter:innen gezielt Wissen im Freibeweisverfahren erwerben und somit den Sachverständigen umgehen. Die Rechtsprechung hat da-

hingehend Fallgruppen fachfremder Gebiete herausgearbeitet, bei welchen sich Richter:innen die Beantwortung der Fragen nicht selbst zutrauen dürfen, wie im Bereich der Medizin oder Psychiatrie. Demgegenüber gibt es auch Standardfälle, bei welchen die richterliche Sachkunde als ausreichend erachtet wird – Stichwort: antizipierte Sachverständigengutachten. Beispielhaft kann hier die Funktionsfähigkeit und Messgenauigkeit von standardisierten Messverfahren bei Geschwindigkeitsmessungen im Bußgeldverfahren genannt werden.

#### *2. Status Quo der forensischen Informatik*

Aufgrund der Schnellebigkeit und stetigen Fortentwicklung kann der jetzige Stand der Forschung über die Methodik und Erfahrungssätze der forensischen Informatik nicht als gesichertes Erfahrungswissen definiert werden<sup>2</sup>. Bezeichnungen wie "zertifizierte und standardisiert anerkannte Software" sind demnach kritisch zu beäugen. Vielmehr sollten zur besseren Nachvollziehbarkeit und Verlässlichkeit bei Beweisfragen, umfangreiche Prüf- und Darstellungsanforderungen bezüglich der Methodik, Erfahrungssätze und der zugrundeliegenden Prämisse, herangezogen werden.

Diese Forderung lässt sich auch aus der Wissenschaft, dem Gesetz (vgl. § 110 StPO), und der aktuellen Rechtsprechung herauslesen, die eine durchschnittliche Sachkunde zur Auswertung von IT-Asservaten nicht als ausreichend erachten. Eine zentrale Ursache dafür ist die meistens bestehende Notwendigkeit einer Interpretation der gespeicherten Daten. Daneben überfordern die schieren Datenmengen Laien. Weiterhin weisen digitale Daten Besonderheiten in ihren Charakteristika auf: Sie sind flüchtig und leicht veränderbar. Um diesen Umständen gerecht zu werden, ist konsequenterweise der IT-Sachverständigenbeweis bei Fragestellungen zur forensischen Informatik das bestmögliche und sachnächste Beweismittel für digitale Spuren. Die Referentin zeigt auf, dass sich eine Pflicht zur Bestellung auch aus §§ 244 II, 261 StPO ableiten lässt.

#### *3. Herausforderungen mit dem IT-Sachverständigen*

Bei der Bestellung eines IT-Sachverständigen ergeben sich typischerweise die folgenden Schwierigkeiten: die Auswahl geeigneter Expert:innen, die verständliche Formulierung konkreter Beweisfragen für beide Seiten, die Schaffung einer gemeinsamen Kommunikationsbasis und ein einheitliches Spurenverständnis (Übersetzungsproblematik). Diese Herausforderungen erwachsen unter anderem daraus, dass mehrere Disziplinen die Wurzeln der digitalen Forensik bilden: die Informatik, die Physik und die mathematische Theorie. Bei der Auswahl können sich Schwierigkeiten ergeben, weil sich IT-Sachverständige dadurch auszeichnen, dass sie eine spezifische technologische Sachkunde auf einem konkreten Gebiet der forensischen Informatik vorweisen müssen, um die jeweiligen

<sup>2</sup> Nach Ansicht der Referentin bildet u.a. die Datenträgerforensik hiervon eine Ausnahme.

Beweisfragen beantworten zu können. Zum Beispiel könnte das eine besondere Expertise auf dem Gebiet der Datenträger sein.

#### 4. Beantwortung der Beweisfragen

Die Beantwortung der Beweisfragen erfolgt objektiv seitens des Sachverständigen. Daneben lassen sich seine Antworten in verschiedene Kategorien einordnen.

##### a) Grenzen der Objektivität

Bei der Beantwortung der Beweisfrage darf sich der IT-Sachverständige nur im Rahmen seines Auftrages bewegen. Die Pflicht zur Objektivität gem. § 79 Abs. 2 StPO ist dem Wesen des Sachverständigenbeweises immanent. Er arbeitet unabhängig und weisungsfrei von den anderen Verfahrensbeteiligten. Ermittelt er über diese Grenzen der Beweisfrage hinaus, so kann unter Umständen der Vorwurf der Befangenheit im Raum stehen.

##### b) Aussagekategorien der Antworten

Die Beantwortung der Beweisfragen kann man in drei Aussagekategorien unterteilen: Erfahrungssätze, Schlussfolgerungen mithilfe der Sachkunde und Befundtatsachen.

##### aa) Erfahrungssätze

Die 1. Kategorie umfasst die Mitteilung von Erfahrungssätzen aufgrund besonderer Sachkunde. Dabei handelt es sich um abstrakte Mitteilungen, die noch keinen Bezug zum Sachverhalt aufweisen, wie bspw. Erklärungen von Fachausdrücken oder die Übermittlung von Forschungsergebnissen.

##### bb) Schlussfolgerungen mithilfe der Sachkunde

In die 2. Kategorie werden Schlussfolgerungen eingeordnet, die aus feststehenden konkreten Tatsachen des Sachverhalts mithilfe der Sachkunde gezogen werden können. Dabei handelt es sich also um eine Art Sachverhaltsbewertung und um die häufigste und wichtigste Kategorie. Darunter zählen zum Beispiel die Mitteilungen, ob eine Bild- oder Textdatei manipuliert wurde.

##### cc) Befundtatsachen

Die 3. Kategorie zur Beantwortung von Beweisfragen ist umstritten und schwierig zu bewerten. Darunter fallen Befundtatsachen, die vom IT-Sachverständigen festgestellt werden, wenn dafür besondere Sachkunde erforderlich ist. In dieser Beweiskategorie hilft der Sachverständige bei der Generierung des Beweisstoffes, zum Beispiel durch das Auffinden von unüblichem Datenmaterial in nicht unerheblicher Menge auf einem Datenträger. Dabei ist höchst strittig, wann besondere Sachkunde bei der Sicherung und Auswertung der Datenträger erforderlich ist und wann es sich lediglich um ein illegales Outsourcing von Ermittlungstätigkeiten handelt. Weitere Probleme dieser Kategorie ergeben sich dadurch, dass die Wahrnehmungen des Forensikers in dieser Kategorie einen gewissen Grad an Schlussfolgerungen enthalten und dadurch eine strikte Grenzziehung zur 2. Kategorie schwierig ist. Dar-

über hinaus ist auch die Abgrenzung zwischen Sachverständigen und sachverständigen Zeugen nicht trivial.

##### dd) Anregungen der Referentin

Nach der Erläuterung dieser drei Kategorien, regt die Referentin an, eine weitere Kategorie zu etablieren. Unter diese vierte Kategorie soll die Vornahme bloßer Verrichtungen zur Tätigkeit des Sachverständigen, z.B. die Sicherung und Entschlüsselung von Datenmaterial, fallen.

#### 5. Würdigung der Zuverlässigkeit der Ergebnisse

Im weiteren Verlauf ihres Vortrages präsentiert *Frau Dr. Scheler* ein eigens entwickeltes Prüfungsschema, welches das Spannungsfeld zwischen freier Beweiswürdigung gem. § 261 StPO und den Grundsatz der Nachvollziehbarkeit und Transparenz bei der Beweiswürdigung in Einklang bringt. Im ersten Schritt wird die Beweisfrage analysiert und in einem zweiten Schritt die Antworten des Sachverständigen bewertet. Diese Bewertung der Sachverständigen-Ergebnisse setzt sich aus einer Nachvollziehbarkeitsprüfung und einer Transparenzkontrolle, sowie der Kategorisierung der angewandten Methoden nach deterministisch, statistisch und selbstlernend zusammen.

##### a) Kategorisierung der Methoden

Eine Datenverarbeitung, die auf deterministischen Methoden beruht, generiert nur solche Informationen aus den Daten, die in diesen Datensätzen unzweifelhaft vorhanden sind. Dabei handelt es sich um Programme, die digitale Daten in eine menschenlesbare Form übersetzen, wie die Anzeige von Bildern.

Statistische Methoden hingegen sind komplexer und errechnen Informationen aus Datensätzen. Diese Informationen lassen sich nicht ohne weiteres aus diesen Daten entnehmen und sind nur mit einem gewissen Grad an Wahrscheinlichkeit zutreffend. Die Richtigkeitswahrscheinlichkeit der Ergebnisse hängt dann von der zugrundeliegenden Heuristik und Annahme ab. Unter solche Methoden fallen u.a. Ähnlichkeitsanalysen beim Data Mining.

Noch komplexer sind dann selbstlernende Methoden. Diese Methoden entwickeln Annahmen und Heuristiken aufgrund der ihnen zugrundeliegenden Trainingsdaten. Häufiger Kritikpunkt dieser Methoden ist der Mangel an Nachvollziehbarkeit, aufgrund der selbstentwickelten Heuristiken und Annahmen.

Um die Methoden in eine Richtigkeits- und Zuverlässigkeitsskala einordnen zu können, muss man sich mit der genauen Arbeitsweise des Sachverständigen auseinandersetzen. Nur durch diesen nächsten Schritt können die weiteren Prüfungs- und Darstellungsanforderungen im Urteil ermittelt werden.

Neben der Würdigung und Bewertung der angewendeten Methoden, sollte auch die Person des Sachverständigen beurteilt werden, um einen möglichen Bias ausschließen zu können. Ein solcher ist anzunehmen, wenn der Sach-

verständige in seiner Interpretation und Analyse naheliegende Alternativhypothesen außer Acht lässt.

#### *b) Einordnung der Methoden und Erfahrungssätze in eine Zuverlässigkeitsskala*

Durch die Entwicklung einer Zuverlässigkeitsskala könnte man eine potenzielle Bindungswirkung an die Ergebnisse ableiten. Die Referentin definiert hierfür vier Abstufungen: (1) gesicherte, wissenschaftliche Erkenntnisse, (2) wissenschaftliche Erkenntnisse mit Richtigkeitswahrscheinlichkeit, (3) einfache Erfahrungssätze und (4) ungeeignete Methoden.

(1) Gesicherte, wissenschaftliche Erkenntnisse liegen immer dann vor, wenn die Erkenntnisse nach dem aktuellen Stand der Wissenschaft unangefochten sind. Es handelt sich dabei um Erkenntnisse, die auf deterministischen Methoden beruhen.

Der zweiten Stufe werden (2) wissenschaftliche Erkenntnisse mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit zugeordnet. Diese basieren in der Regel auf statistischen Methoden und es liegt keine Bindung der Ergebnisse für das Gericht vor. Dieses muss jedoch die gewonnenen Erkenntnisse einbeziehen und zusätzlich die Richtigkeit der Aussage im jeweiligen Einzelfall anhand weiterer Indizien bestätigen und widerlegen.

Ergebnissen, die sich aufgrund (3) einfacher Erfahrungssätze ergeben, kann nur eine Indizwirkung zugesprochen werden.

Schließlich und zuletzt existieren (4) Methoden, die zu völlig ungeeigneten Ergebnissen führen. Zwar gilt im Grundsatz die freie Beweiswürdigung, jedoch regelt § 244 Abs. 3 S. 3 Nr. 4 StPO eine Ausnahme davon. Demnach sind Beweismittel wertlos, wenn feststeht, dass jede Möglichkeit ausgeschlossen ist, dass das Beweismittel Sachdienliches ergeben kann. Beispielsweise wären Blackbox-Tools unter diese vierte Stufe zu subsumieren, denn diese sind nicht nachvollziehbar und intransparent.

#### *6. Endgültige Einordnung und Endergebnis*

Die meisten Methoden der forensischen Informatik sind nicht standardisiert und Erfahrungssätze nicht wissenschaftlich gesichert. Dementsprechend muss das Gericht bei der Würdigung solcher Beweise umfangreichen Prüfungs- und Darstellungsanforderungen gerecht werden und Erfahrungssätze, Methodiken und zugrundeliegende Prämissen zum Tatsachenstoff machen, was wiederum Auswirkungen auf das Recht auf Akteneinsicht gem. § 147 StPO, das Recht auf ein faires Verfahren, das Fragerecht der Beteiligten und das prozessuale Gleichgewicht hat. Zudem ermöglicht dies den Weg zu den Rechtsmittelverfahren und dadurch auch die mögliche Entwicklung von antizipierten Sachverständigenutachten, die

dann letztlich eine Beweiswürdigung abkürzen und vereinfachen.

Grundsätzlich ist und soll der Sachverständige weisungsfrei arbeiten. Eine Prämisse könnte dahingehend formuliert werden, dass die zuverlässigste Methode angewendet werden muss.

Als abschließendes Resümee hält *Frau Dr. Scheler* fest, dass die Hürden, die sie im Rahmen ihres Vortrags aufgezeigt hat, sehr gut mit unserer Strafprozessordnung lösbar sind.

#### *7. Q&A-Session*

Abschließend bot der erste Vortrag Raum für Fragen der Teilnehmenden, die zu einer zusätzlichen Vertiefung des Themas beitrugen. Und so wurde darüber diskutiert, wo konkret die Grenze von Allgemeinwissen und Fachwissen gezogen werden kann. Als Faustformel lässt sich festhalten, soweit Richter:innen das Wissen gut und nachvollziehbar eigenständig erklären können, bewegen sie sich im Rahmen des Allgemeinwissens. Ist diesen eine eigenständige Erklärung nicht möglich, spricht dies für eine begrenzte Sachkunde, sodass die Einschaltung von Expert:innen erforderlich wäre. Weiterhin wurde die Frage nach der Abgrenzung zwischen Sachverständigen und sachverständigen Zeugen vertieft. Als erstes sollte auf den Zweck der Befragung abgestellt werden. Lässt sich daraus keine Abgrenzung ziehen, stellt man auf das Vorliegen eines Auftrags ab. Im Austausch über die Entwicklung möglicher Tools und Fragen der Beweiswürdigung zeigte sich, dass der Einfluss der KI-Verordnung und etwaige Zertifizierungen, sowie deren Bewertung einen Diskussionspunkt darstellen kann.

### **III. Herausforderungen bei der Präsentation von digitalen Beweismitteln, Marion Liegl (Friedrich-Alexander-Universität Erlangen-Nürnberg)**

Als nächstes bot die IT-Forensikerin *Marion Liegl* einen humorvollen und aufschlussreichen Einblick in ihre praktischen Erfahrungen als freiberufliche IT-Sachverständige für Strafverfolgungsbehörden. Ihren Vortrag strukturierte sie anhand von drei Fällen aus Ihrer Praxiserfahrung, die die Herausforderungen bei der Präsentation digitaler Beweismittel im gerichtlichen Alltag anschaulich untermalen. Dabei befasste sich jeder Fall mit einem eigenen großen Problempunkt: (1) Auswertung und gerichtsverwertbare Aufbereitung von Big Data, (2) Die Bedeutung des Sachverständigen des IT-Sachverständigen und der Mangel an Zertifizierungsregelungen, (3) Der Umgang mit Eingriffen in den höchstpersönlichen Lebensbereich bei der Präsentation digitaler Beweismittel. Die Referentin hat neben einem Master für Digitale Forensik und elfjähriger Berufserfahrung auch Rechtswissenschaft im Nebenfach studiert, sodass sie besonders geeignet ist, die Probleme mit einer interdisziplinären Perspektive zu beleuchten.

### 1. Auswertung von Big Data

In der Präsentation des ersten Falles befasste sich die Referentin mit den Problemen, die Big Data aufwerfen. Masendaten die ausgewertet, extrahiert und analysiert werden müssen, obwohl die geeigneten Ressourcen bei den Strafverfolgungsbehörden derzeit noch fehlen.

#### a) Massendaten

Die erste Herausforderung verdeutlichte *Frau Liegl* im Kontext der Auswertung eines Mobiltelefons, die es der Staatsanwaltschaft ermöglichen sollte, eine relevante Verbindung zwischen Täter und Opfer zu ermitteln. Hierbei bestand die Aufgabe der Sachverständigen zunächst darin, Daten zu extrahieren, zu filtern, nach vorgegebenen Suchmerkmalen entsprechend zu durchsuchen und Fragen der Ermittler zu beantworten. Die Herausforderung im konkreten Fall: Als relevant stellte sich ein über mehrere Monate andauernder und im Schnitt 250 Nachrichten pro Tag umfassender Chatverlauf heraus. So war zwar schnell klar, dass sich Täter und Opfer kannten, jedoch galt es in einem nächsten Schritt, die Frage zu klären, in welchem konkreten Verhältnis die beiden zueinanderstanden. Dabei lässt sich von einer großen Masse an Daten nicht per se ein enges Verhältnis ableiten. Vielmehr muss der Inhalt der Chatnachrichten analysiert werden.

#### b) Grenzen analoger Präsentation digitaler Beweismittel

Diesen langen Chatverlauf galt es für die Beweiswürdigung „gerichtsverwertbar“ zu präsentieren. Dabei entsprach es nach den Erfahrungen der Referentin gerichtlicher Praxis, die extrahierten Daten in analoger Form, das heißt ausgedruckt, bereitzustellen. Dass diese Vorgehensweise angesichts des erheblichen Datenumfanges an ihre Grenzen stößt, führte *Frau Liegl* den Zuhörern anhand einer Berechnung plastisch vor Augen. Rechnet man mit 250 Chatnachrichten pro Tag in einem relevanten Zeitraum von ca. neun Monaten, so kommt man ungefähr auf 67.000 Nachrichten. Möchte man diese gerichtsverwertbar, d.h. auch in lesbarer Schriftgröße auf Papier drucken, ergibt das ca. 1.688 Seiten. Für die Präsentation des Chatverlaufs ergab sich somit eine erforderliche Menge von 4,2 Kilogramm Papier, soweit man doppelseitig drucken würde. Demgegenüber ist die Stelle im eigentlichen Gutachten des Sachverständigen kurz. Man findet lediglich Sätze wie "Das Telefon wurde ausgewertet und es wurde ein mutmaßlich fallrelevanter WhatsApp-Chat gefunden. Siehe Anlagen."

#### c) Grenzen des Aufgabenbereichs eines IT-Sachverständigen

Die daraufhin erfolgte Anfrage der Ermittler, ob eine Kürzung der Daten möglich sei, bildete einen Anknüpfungspunkt der nächsten Schwierigkeit und einer aktuell viel diskutierten Problematik. Es stellt sich die Frage, wo die Arbeit des Sachverständigen aufhört, und die originären Aufgaben der Strafverfolgungsbehörden anfangen. Das

Herausfiltern des für die Beweiswürdigung relevanten Inhalts aus der Masse an Daten stellt dabei eine diffizile Aufgabe dar.

*„Kann und darf der Sachverständige, der IT-Sachverständige entscheiden, was relevant ist und was nicht?“*

Die Antwort auf die aufgeworfene Frage der Referentin brachte zugleich ihr Unwohlsein bezüglich der Aufgabe zum Ausdruck und machte deutlich, dass die Grenzen der Aufgabenbereiche nicht verschwimmen sollten.

*„Ich kann mir nicht anmaßen, als IT-Sachverständige dem Gericht hier in irgendeiner Form was vorwegzunehmen.“*

Denn das Gericht muss neben der Feststellung der Tatumstände in der Lage sein, alle relevanten be- und entlastenden Begleitumstände zu würdigen. Das können neben offensichtlichen Tatsachen auch solche sein, die mittelbar Relevanz haben. Dabei stellt die Einordnung als relevante Tatsache bereits eine rechtliche Bewertung dar und entzieht sich daher einer vorbereitenden Selektion durch den IT-Sachverständigen. Diesem obliegt es, die digitalen Inhalte zugänglich zu machen, ohne den Beweiswert zu verändern. Das Sachverständigengutachten umfasst die Bestätigung der Auswertung, die Beschreibung der technischen Vorgehensweise und Bedingungen, sowie den Hinweis bezüglich des Funds eines mutmaßlich fallrelevanten Chats.

#### d) Die notwendige Fortentwicklung des Strafverfahrens

Im Ergebnis lag die pragmatische Lösung in der Aushändigung eines USB-Sticks mit den Chatinhalten, dessen Verteilung durch das Gericht angeordnet wurde. Der mobile Datenträger ermöglichte einen vollständigen und praktikablen Zugang zu den Daten. Der USB-Stick wurde an das Gericht, die Verteidigung und Staatsanwaltschaft verteilt, damit diese die Chatinhalte im Selbstleseverfahren betrachten konnten. Letztlich spiegeln sich hier weitere Herausforderungen, die mit Massendaten hervorgehen und mit denen derzeit an Gerichten gekämpft wird, wider. Daten sollen gestrafft und übersichtlich, trotzdem vollumfänglich, und gerichtsverwertbar als Beweismittel in der Hauptverhandlung präsentiert werden. Die Referentin zeigt anhand Ihres Falles, dass die Lösung des Konflikts mit Mitteln der Strafprozessordnung und einer Offenheit gegenüber bis dato auch unkonventionelle Methoden gelöst werden kann.

### 2. Anforderungen an den IT-Sachverständigen

In ihrem zweiten Beispielfall befasste sich *Frau Liegl* mit der erforderlichen Expertise des Sachverständigen und dessen Bedeutung für das Strafverfahren. Dabei spricht auch sie die Notwendigkeit einer Qualitätssicherung der Arbeit der IT-Forensiker durch Regulierungen und Standards an.

### *a) Bedeutung und Aussagekraft von digitalen Beweismitteln*

In diesem Fall waren die einzigen Beweismittel die Hauptbelastungszeugin, die auch gleichzeitig das Opfer war und die Referentin in ihrer Rolle als Sachverständige zur Interpretation eines digitalen Beweismittels. Die Verteidigungsstrategie des Angeklagten zielte darauf ab, die Glaubwürdigkeit der Beweismittel in Frage zu stellen. Er versuchte dies insbesondere dadurch zu erreichen, dass er sowohl der Belastungszeugin als auch der Referentin die Intention zuschreiben wollte, dass ihm beide die Tat fälschlicherweise anlasten wollten. Dem Angeklagten gelang es zumindest kurzzeitig, Zweifel bei den Beteiligten hervorzurufen, als er in der Hauptverhandlung Dateninkonsistenzen in den Zeitstempeln des digitalen Beweismittels nachweisen konnte. Diese waren zuvor nicht aufgefallen, da auch dieses Beweismittel aus Massen von Daten und Datensätzen bestand und im Rahmen der Hauptverhandlung mehrbändig ausgedruckt wurde.

### *b) Spontaner Einsatz der Expertise von Sachverständigen*

An dieser Stelle kam es daher für die Sachverständige darauf an, die Unstimmigkeiten aus dem Stehgreif technisch richtig und nachvollziehbar einordnen zu können. Aufgrund der Flüchtigkeit von Daten können Inkonsistenzen schnell gewollt, aber auch ungewollt entstehen. Die Aussagekraft des digitalen Beweismittels spielte eine tragende Rolle, da dieses die Aussagen der Hauptbelastungszeugin bestätigen oder dementieren sollte. *Frau Liegl* bestätigte, dass die Daten tatsächlich Inkonsistenzen aufwiesen. Anhand anderer digitaler Spuren ließ sich jedoch technisch sauber eingeordnet und plausibel erklären, dass es sich dabei nicht um eine gewollte Manipulation der Daten handelte.

Gerade die spontane Interpretation von digitalen Daten und Spuren erfordert umfänglichen technischen Sachverstand, den *Frau Liegl* im konkreten Fall einbringen und dadurch den vollen Beweiswert zur Geltung bringen konnte. Die Herausforderung besteht darin, dass ohne Kenntnis der relevanten Begleitumstände des Verfahrens und insbesondere auch vor dem Hintergrund des jeweiligen Datenmaterials, eine Vorbereitung auf die jeweilige Beweismittelpräsentation vor Gericht schwer möglich ist.

### *c) Regelungslücke trotz großer Bedeutung*

Der Expertise von Sachverständigen kommt im Strafverfahren eine hohe Bedeutung zu.

*„Wenn ich was gesagt habe, das hat man nicht hinterfragt. Das wurde einfach hingenommen“*

– so beschreibt die Rednerin ihre tragende Rolle und kritisiert vor diesem Hintergrund die derzeit nicht bestehenden Anforderungen an die Qualifikation der IT-Sachverständigen. Zwar soll § 73 Abs. 2 StPO bestimmen, dass

öffentlich bestellte und vereidigte Sachverständige bevorzugt ausgewählt werden sollen, jedoch ist dies in der Praxis nicht immer gegeben. Eine bestimmte Ausbildung ist für IT-Sachverständige nicht notwendigerweise vorgesehen. Zwar stehen den IT-Sachverständigen zertifizierte Tools zur Verfügung, allerdings geht die Arbeit über die bloße Tool-Anwendung hinaus. Es kommt auf das Verständnis und Hinterfragen der Tools und den daraus resultierenden Ergebnissen an, um sich über die Anwenderbene hinausheben zu können. *„Dafür ist eine gute Ausbildung erforderlich“*, die nach eigener akademischer Erfahrung der Rednerin auch von der Zusammenarbeit mit Juristen und interdisziplinärer Arbeit sowie Sichtweise profitiert.

Die aktuellen Umstände bezeichnet sie als Regelungslücke, die es gerade zur Gewährleistung eines fairen Verfahrens und der Wahrung der Menschenrechte, insbesondere auch im Interesse des Angeklagten, dringend zu hinterfragen gelte.

### *3. Eingriffe in den höchstpersönlichen Lebensbereich durch die Präsentation (digitaler) Beweismittel*

Im letzten Fall, der von der Referentin vorgetragen wurde, wurde sich mit der möglichen Verletzung höherrangiger Rechtsgüter auseinandergesetzt.

#### *a) Schutz des Persönlichkeitsrechts in Großverfahren*

Hierbei schildert die Referentin eine Situation, durch welche der höchstpersönliche Lebensbereich einiger Beteiligten des Strafprozesses durch die Präsentation (digitaler) Beweismittel berührt wurde. Konkret ging es um die Einführung von Videomaterial in einer Gerichtsverhandlung, welches aufgrund des hohen Interesses der Öffentlichkeit, einer großen Masse an Menschen zugänglich gemacht wurde. Das Abspielen der Videobeweismittel diente dem Zweck, den Angeklagten hierdurch zu identifizieren. Im Hintergrund dieses Videomaterials waren aber auch unbeteiligte Personen in den Aufnahmen zu sehen. Es wurden Szenen aufgezeichnet, die teilweise den Kernbereich privater Lebensführung berührten. Diese sowieso schon heikle Situation wurde durch das erhöhte Öffentlichkeitsinteresse verschärft. Denn das Gerichtsverfahren fand nicht in einem üblichen Gerichtssaal statt, sondern wurde in einen größeren Raum verlagert, um den Andrang der Öffentlichkeit, Presse, aber auch vermehrten Nebenanklagenden, Strafverteidigern usw. gerecht zu werden. Dies führte auch dazu, dass das Videomaterial, um es für alle Beteiligten sichtbar zu machen, auf einer großen Leinwand abgespielt wurde.

#### *b) Beweispräsentation vs. Persönlichkeitsrechte*

Dies rief nicht nur bei der Referentin ein besonderes Unwohlsein und Unverständnis hervor. Der unangemessene Umgang dieser sensiblen Inhalte wurde auch von einem Beteiligten gerügt und der weiteren Beweisaufnahme wi-

dersprochen, sodass die Inaugenscheinnahme mittels eines kleineren Monitors fortgeführt wurde. Die Rednerin weist an dieser Stelle auf ein Spannungsfeld zwischen vollumfänglicher Beweispräsentation und dem Schutz der Persönlichkeitsrechte hin, welches durch digitale Beweismittel, insbesondere bildliche Aufnahmen, intensiviert wird. *Frau Liegl* fordert einen sensibleren Umgang und hofft, dass dieser Fall auch die Interessierten im Publikum, ob vor Ort oder vor den Monitoren, zum Nachdenken anregt.

#### 4. Q&A-Session

In der abrundenden Q&A-Session wurde die Frage nach der Verwendung von KI für die Kürzung von Daten aufgeworfen. Doch auch der Einsatz von KI knüpft an die Problematik der Möglichkeit einer vorweggenommenen Selektion des für die Beweiserhebung Relevanten an. Zudem spielen datenschutzrechtliche Fragen eine Rolle. Daraufhin folgte eine spannende Frage zur Vorgehensweise bei der Auswertung und Sicherung des Mobiltelefonasservats. Ob ein komplettes Image des Handys vorgenommen wird, ist abhängig vom konkreten Fall und Ermittlungsauftrag. Je enger die Ermittlungsfrage gestellt wird, desto selektiver kann gesichert und ausgewertet werden.

### IV. Using digital evidence to prove international crimes: a view from international courts (englischer Vortrag ins Deutsche übersetzt) von Matthew Cross (Internationaler Strafgerichtshof in Den Haag)

Nach der Mittagspause durften die Teilnehmenden und alle Interessierten über den Tellerrand blicken und *Matthew Cross*, Appeals Counsel der Anklagebehörde am *Internationalen Strafgerichtshof*, auf der Bühne begrüßen. In seinem Vortrag gewährte er dem Publikum einen Einblick in den Umgang mit digitalen Beweismitteln vor den internationalen Strafgerichtshöfen und die damit verbundenen Herausforderungen. Der Vergleich zu nationalen Problemen und Hindernissen, sowie die Erfahrungen auf internationaler Ebene stellen einen lehrreichen Austausch und eine Inspiration dar.

#### 1. Wesentliche Merkmale internationaler Strafgerichte

Zum Einstieg erläutert der Referent die Grundzüge der internationalen Strafgerichtsbarkeit. Auf transnationaler Ebene existiert keine einheitliche Institution. Vielmehr setzt sich die internationale Strafgerichtsbarkeit aus einer Reihe von verschiedenen Gerichten und ad-hoc Tribunalen zusammen, welche jeweils ihren eigenen Verfahrens- und Beweisregeln unterliegen. Dabei nimmt der *Internationale Strafgerichtshof* in Den Haag (*IStGH*) eine zentrale Rolle ein, da er ein permanenter Spruchkörper ist. Es liegt jedoch keine Bindung der verschiedenen Gerichte und Spruchkörper untereinander vor. Diese sind unabhängig voneinander.

##### a) Zuständigkeiten

Internationale Strafgerichtshöfe sind auf die Ahndung schwerster internationaler Verbrechen ausgerichtet. Dazu

gehören Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen und das Verbrechen der Aggression sowie weitere Handlungen, die die Rechtspflege beeinträchtigen können. Unter dem letzten Punkt versteht man Straftaten wie Zeugenbeeinflussung oder Vergeltungsmaßnahmen gegen Mitarbeiter des Gerichts.

##### b) Besonderheiten der Verfahren

Aufgrund der starken Begrenzung der Zuständigkeiten und limitierten Ressourcen der Ermittlungsbehörden wird nur eine geringe Zahl von Fällen verfolgt und zur Anklage gebracht. Hinzu kommt, dass es sich um besonders komplexe und umfangreiche Sachverhalte handelt, was dazu führt, dass sich die Verfahren über Jahre hinziehen und hunderte Zeugen und zahlreiche Anklagepunkte umfassen. Zudem sind die Ermittlungen mit erheblichen praktischen Schwierigkeiten verbunden. So beginnen die Verfahren meist mehrere Jahre nach den strafrechtlichen Ereignissen.

##### c) Mangelnder Zugang zum Tatort

Eine bedeutende Schwierigkeit, die auch die hohe Relevanz der digitalen Beweismittel in diesen Strafverfahren beeinflusst, ist, dass den Ermittlern oft der Zugang zum Tatort oder der Zugang zum entsprechenden Staat verwehrt wird. Die Ermittler können sich kein Bild vor Ort von der Situation machen. Auch die Akquirierung von Zeugen und persönliche Gespräche werden dadurch erschwert. Aufgrund der zeitlichen Dauer, bis die Ermittlungen beginnen, sind Zeugen aufgrund des Alters, Krankheiten, oder Todesfällen meist schwer oder gar nicht mehr erreichbar.

Der Referent weist darauf hin, dass die geschilderten Herausforderungen internationale Gerichte dazu veranlassen, innovative und kreative Ansätze zur Untersuchung von Verbrechen zu entwickeln. Dadurch gewinnen digitale Ermittlungsmaßnahmen und die Nutzung bereits verfügbarer digitaler Daten neben den traditionellen Beweismitteln zunehmend an Bedeutung.

#### 2. Allgemeine Beweisregeln

Die Beweisregeln vor internationalen Strafgerichtshöfen orientieren sich in ihren Grundzügen an Prinzipien, die aus dem nationalen Recht bekannt sind. Diese Grundgedanken entwickeln die internationalen Gerichte dann fort und verknüpfen diese mit sog. „hybriden“ Ansätzen. Eine derartige Kombination spiegelt zum einen die bewährte Praxis der internationalen Gemeinschaft wider, während zum anderen der Umstand berücksichtigt wird, dass internationale Strafverfahren besondere Herausforderungen mit sich bringen.

Wie auch vor den nationalen Gerichten müssen Beweismittel vor dem *IStGH* relevant, beweiskräftig und nicht unangemessen vorurteilsbehaftet sein. Im Unterschied zu traditionellen *common-law*-Verfahren verschiebt sich die Praxis vor dem *IStGH* jedoch zunehmend dahin, Fragen

der Beweisulässigkeit erst am Ende des Prozesses zu klären. Dies erlaubt es den Richtern, den Beweiswert im Kontext des gesamten Beweismaterials zu bestimmen. Vor allem mit Blick auf die Praxis stellt dies eine verfahrensökonomische Entwicklung dar, weil dadurch der Umgang mit umfangreichen Beweismitteln erleichtert wird.

Zuletzt hebt der Referent hervor, dass vor dem *IStGH* grundsätzlich alle Beweisarten zugelassen sind und kein Verbot der Aussagen von Hörensagen besteht. Trotz der Vielfalt an Möglichkeiten sind Zeugenaussagen auch weiterhin das bevorzugte Beweismittel. Im Zuge des Fortschritts muss sich jedoch mit der Frage auseinandergesetzt werden, ob die zwingende Erforderlichkeit von Zeugenaussagen besteht und falls dies bejaht wird, in welchem Umfang sie heranzuziehen sind. Es ist zu hinterfragen, ob Zeugenaussagen der alleinige "Goldstandard" sind, oder auch andere Beweismittel einen Sachverhalt belastbar und substantiiert darstellen können.

### 3. Steigende Relevanz digitaler Beweismittel

Der Begriff der digitalen Beweise umfasst ein breites Spektrum an elektronischen Daten. Diese reichen von audiovisuellen Materialien in Form von Videos, Fotos und Tonaufnahmen über Satelliten- und Luftbilder bis hin zu Kommunikations- und Gerätedaten aus Mobiltelefonen oder Computern.

#### a) Chancen und Vorteile digitaler Beweismittel

Zur Veranschaulichung geht *Cross* beispielhaft auf zwei Verfahren ein, bei welchen vor allem Social Media Beiträge eine bedeutende Rolle spielten.

Der erste Fall ist das MH17 Verfahren aus den Niederlanden.<sup>3</sup> Durch die Beweiserhebung öffentlich verfügbarer Fotos und Social-Media-Beiträge gelang es den Ermittlern anhand einer Zusammenstellung des Beweismaterials eine Zeitachse der Geschehensabläufe zu rekonstruieren, um so die Nachverfolgung der Ereignisse zu ermöglichen. Im Fall des Haftbefehls gegen *Al-Werfalli*<sup>4</sup> stützten sich die Ermittlungen maßgeblich auf Fotos und Videos, die angeblich vom Verdächtigen selbst oder in seinem Auftrag erstellt und auf verschiedenen Social-Media-Plattformen geteilt wurden. Durch diese digitalen Beweismittel war der Fall relativ eindeutig und dadurch gut nachvollziehbar. Als diskutabel erwies sich insbesondere, ob eine Anklage im Wesentlichen auf öffentlich zugänglichen digitalen Daten aus Sozialen Netzwerken beruhen kann. Da der Beschuldigte mittlerweile verstorben ist, wird offenbleiben, ob diese Beweisergebnisse ausreichend waren, um das Strafverfahren weiterzuführen.

#### b) Risiken und Nachteile von digitalen Beweismitteln

Gleichzeitig weist der Referent auf die neuen Herausforderungen hin, die sich aus der zunehmenden Nutzung digitaler Beweismittel ergeben. Insbesondere sinkt mit der Entwicklung Künstlicher Intelligenz das Vertrauen in die Authentizität und Manipulationssicherheit solcher Beweismittel. Es liegt ein fortwährendes „Katz-und-Maus-Spiel“ zwischen Fälschungstechniken durch Kriminelle und den Methoden der Echtheitsprüfung durch die Gerichte vor. Hier kommen dann IT-Sachverständige ins Spiel, die die Ermittlungen und Beweisanalyse unterstützen.

### 4. Anwendung digitaler Beweismittel

In der Theorie, so *Cross*, bieten internationale Gerichte grundsätzlich geeignete Rahmenbedingungen, um den Umgang mit digitalen Beweismitteln zu erproben. Sie sind mit professionellen Richtern besetzt, verfügen über stabile Ressourcen und bearbeiten fast ausschließlich komplizierte sowie langwierige Verfahren.

#### a) Digitale Beweismittel: Eine Beweisform im Frühstadium?

Bislang gab es jedoch noch kein Verfahren vor dem *IStGH*, welches digitale Beweismittel hauptsächlich problematisierte. Dies ist vor allem der Tatsache geschuldet, dass viele der aktuellen Verfahren Ereignisse vor 2014 betreffen. Sie stammen also aus einer Zeit, in der die Digitalisierung noch nicht den Umfang erreicht hatte, den wir heute beobachten können.

Daneben führen Digitale Beweismittel nicht immer, wie oft angenommen, zu simpleren, effizienteren oder schnelleren Verfahren. Zur Veranschaulichung verweist der Referent auf das *Ayyash*-Verfahren<sup>5</sup> vor dem Special Tribunal for Lebanon. Dieses Verfahren stützte sich zwar hauptsächlich auf Mobilfunkdaten, dennoch wies das Urteil am Ende 2.227 Seiten, fast 300 Zeugen, zahlreiche Experten und mehrere tausend Beweisstücke auf. Dieses Beispiel verdeutlicht auch, dass der Umgang mit neuen Beweismitteln naturgemäß besonders aufwendig ist. Mit zunehmender Erfahrung dürfte sich jedoch eine effizientere und routiniertere Anwendung durch die Gerichte entwickeln.

#### b) Guidelines und Dokumente, insbesondere die Leiden Guidelines

Angesichts einer bislang fehlenden umfangreichen internationalen Rechtsprechung verweist der Referent zur Orientierung bei der Verwendung digitaler Beweise vor Ge-

<sup>3</sup> vgl. Tagesschau, Prozess um MH17-Abschuss, 17.11.2022, <https://bit.ly/4tclnzw>.

<sup>4</sup> The Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, ICC-01/11-01/17.

<sup>5</sup> The Prosecutor v. Salim Jamil Ayyash, Hassan Habib Merhi, Hussein Hassan Oneissi, Assad Hassan Sabra, STL-11-01/T/TC.

richt auf zwei Projekte hin, die von internationalen Expert:innen entwickelt wurden. Dabei handelt es sich zum einen um das *Berkeley Protocol on Digital Open Source Investigations*<sup>6</sup>, welches sich mit Ermittlungstechniken befasst und sich dabei insbesondere auf die Möglichkeit von OSINT-Beweisen konzentriert. Daneben können die *Leiden Guidelines*<sup>7</sup> als Ergänzung dieses Dokuments angesehen werden. Letzteres beschäftigt sich im Gegensatz zum *Berkeley Protokoll* weniger mit den Ermittlungen, sondern setzt seinen Fokus auf den bislang bestehenden Umgang, um daraus Erkenntnisse abzuleiten.

Nach *Cross* lassen sich aus den *Leiden Guidelines* diese sechs Kernprinzipien entnehmen:

*aa) Einreichung des gesamten Beweismittels*

Beweismittel sollen möglichst in ihrer Gesamtheit und nicht nur teil- oder auszugsweise verwendet werden. Nur so kann sichergestellt werden, dass der Kontext des Beweises richtig verstanden wird. Will man beispielsweise einen Videoclip in seiner Gesamtheit verstehen, sollte man sich auch den Ausschnitt davor und danach anschauen. Bei besonders umfangreichen digitalen Beweisen, beispielsweise bei einem WhatsApp-Chat mit mehreren tausenden Einträgen, kann dies auch eine Herausforderung darstellen.

*bb) Einwilligung*

Will das Gericht Bildmaterial, auf welchem eine Person zu erkennen ist, verwenden, so ist, sofern möglich, die Einwilligung der abgebildeten Person einzuholen. Damit soll garantiert werden, dass sich keiner als Subjekt eines internationalen Verfahrens wiederfindet, ohne davon in Kenntnis gesetzt worden zu sein. Dies gilt insbesondere dann, wenn es sich um sensibles Bildmaterial, wie die Darstellungen von geschlechtsspezifischer Gewalt, handelt. Damit sind weitere Schwierigkeiten verknüpft. Der Vorteil öffentlich zugänglicher Daten und Informationen für Ermittler ist, dass diese schnell und einfach auffindbar sind. Diese unkomplizierte Beweiserhebung geht verloren, wenn man in einem zweiten Schritt die Identitäten von Personen feststellen muss. Zum anderen möchte man sensibles Bildmaterial nur einem kleinen Kreis zugänglich machen. Bei der Identifizierung von Personen stehen Ermittler jedoch vor dem Dilemma, dass Material unter Umständen auch Dritten zugänglich gemacht und vorgelegt werden muss.

*cc) Authentifizierung*

Im Rahmen der Authentifizierung digitaler Beweismittel wird betont, dass es sich dabei um ein immer relevanteres und zunehmend komplexes Themengebiet handelt. Einzelne digitale Beweismittel können als sich „selbstauthentifizierende Beweismittel“ bewertet werden, sofern keine augenscheinlichen Bedenken hinsichtlich einer Manipulation (z.B. in Form von Deepfakes) bestehen. Sie bestätigen ihre Authentizität selbst, so beispielsweise Bilddateien, die alle zugehörigen Metadaten enthalten und mit Zeitstempeln versehen sind. Um die Echtheit eines Be-

weismittels zu bestimmen, wird es immer öfter erforderlich, zusätzliches Beweismaterial heranzuziehen, wie den Sachverständigenbeweises. Daneben können auch Zeugen, die in dem Beweismaterial zu sehen sind, im Rahmen ihrer Aussage die Echtheit des Beweismittels bestätigen.

*dd) Kontext der Beweiserhebung*

Der Kontext und die Umstände der Beweiserhebung spielen eine wichtige Rolle, auch im Rahmen der Überprüfung der Authentizität. Dies gilt insbesondere bei Abhörmaßnahmen oder in Situationen, in denen das Gericht Bedenken hinsichtlich der Rechtmäßigkeit der Erhebungsmaßnahme oder der Originalität des Beweismaterials haben könnte. Dann muss, wie im *Ayyash*-Fall, nachvollziehbar dargelegt werden wie das Beweismaterial erhoben wurde. Hierzu können sowohl Sachverständige als auch Zeugen angehört werden.

*ee) Interpretation und Expertise*

Soweit dem Referenten bekannt ist, existiert zur Frage, wann Richter selbst genügend Sachverstand besitzen, um digitale Beweise zu interpretieren, keine internationale Rechtsprechung. Nichtsdestotrotz ist diese Fragestellung indirekt in Verfahren aufgetaucht. Meist in Fällen, wo das Alter von Kindern untersucht werden musste bzw. festgestellt werden musste, ob diese jünger als 15 Jahre sind. Daran knüpft auch die nächste und letzte Kernaussage der *Leiden Guidelines* an.

*ff) Schlussfolgerungen*

Es ist grundsätzlich für Richter:innen möglich, aus digitalen Beweismitteln Schlussfolgerungen zu ziehen, jedoch nur insofern das Material eine „eindeutige Feststellung“ erlaubt. Diese Formulierung ist unbestimmt und schwammig, wobei die Anforderungen für eine entsprechende Feststellung besonders hoch sind, so dass diese in der Praxis zusätzlich mit weiteren Beweisen und Indizien untermauert werden sollten.

## 5. Fazit

Insgesamt zeigt sich, dass der Einsatz digitaler Beweismittel im internationalen Strafrecht weiterhin mit zahlreichen offenen Fragen verbunden ist, da sich bislang in keinem Fall vor dem *IStGH* zentral mit der Problematik auseinandergesetzt werden musste. Dabei stellt *Cross* die Vermutung auf, dass nationale Gerichte voraussichtlich früher Antworten auf diese offenen Fragen herausarbeiten werden, an denen sich internationale Gerichte später orientieren könnten.

Zum Abschluss arbeitete der Referent zwei wichtige Problematiken heraus, die neben digitalen Beweismitteln die (internationalen) Strafverfahren verändern werden: Zum einen der Einsatz digitaler Ermittlungsmethoden in Kombination mit Dritten, die dem *IStGH* bei der Beweiserhebung helfen. Zum anderen muss sich neben der Digitalisierung von Ermittlungsmethoden auch mit digitalen Straftaten befasst werden.

<sup>6</sup> Berkeley Protocol on Digital Open Source Investigations, <https://bit.ly/4t5r2H8>.

<sup>7</sup> Leiden Guidelines on the Use of Digitally Derived Evidence <https://bit.ly/3PP15gF>.

## 6. Q&A

In der sich anschließenden Q&A-Session konnten einige offene Fragen und Probleme vertieft diskutiert werden. Dabei interessierte sich das Publikum für datenschutzrechtliche Aspekte und das Herausfiltern relevanter Informationen für den Ermittlungsfall im Falle von Big Data. Der Referent erörtert an dieser Stelle, dass digitale Ermittlungen aufgrund der geforderten Objektivität häufig breit angelegt sind und daher umfangreiche digitale Informationen gesammelt werden müssen, so auch in den sozialen Medien. Auch die Anklagebehörde des *IStGH* sammelt belastende, aber auch entlastende Beweise und Indizien. Zugleich wird hervorgehoben, dass die beim *IStGH* gespeicherten (persönlichen) Daten angemessen aufbewahrt werden. Die Institution unterliegt zwar nicht Europäischen Vorgaben und Vorschriften, wie der DSVGO, entwickelt jedoch eigene, ähnliche Richtlinien.

## V. Verteidigung gegen und mit digitalen Beweismitteln von RA Dr. Eren Basar (Wessing & Partner)

Von einem wiederkehrenden Gast und regelmäßigen Teilnehmer, *Dr. Eren Basar*, wurde der vierte und vorletzte Vortrag präsentiert. Der Anwalt gab Einblicke in die praktischen Fragen und Probleme eines Strafverteidigers, wobei aufgrund seiner Spezialisierung insoweit auch immer die Bezüge zum Wirtschaftsstraf- und Unternehmensrecht zu erkennen waren.

### 1. Status Quo

Der Referent weist darauf hin, dass die Beweisführung von digitalen Spuren äußerst problematisch ist.

#### a) Allgemeines

Im Grunde dreht sich die heutige Diskussion um die Frage, ob das strenge Beweisrecht, welches im Kern seit dem 19. Jahrhundert unverändert besteht, tatsächlich für das 21. Jahrhundert geeignet ist. Die Erhebung digitaler Daten als Beweismittel und die Digitalisierung spielen dabei eine alltägliche Rolle in den Strafverfahren, wie die Analyse von Smartphones, wodurch Ermittler Zugang zu nahezu tagebuchähnlichen Informationen erlangen können. Neben diesen Beweisdaten können auch Metadaten und Zeitstempel wichtige digitale Spurenelemente sein. Über diese lassen sich beispielsweise der Versendungszeitpunkt oder der Ersteller einer E-Mail ermitteln. Besonders praxisrelevant ist § 23 Geschäftsgeheimnisgesetz.

#### b) Dritte als Datenquellen

Neben dem Beschuldigten und Strafverfolgungsorgan können mittlerweile auch Dienstleister als Dritte eine wichtige Rolle in einem Strafverfahren spielen. Diese sind eine weitere Quelle für Daten. Anfragen bei Telekommunikationsanbietern können jedoch problematisch sein. Im

Standardfall wollen Ermittler sog. Bestandsdaten ermitteln, um die Person hinter einem Accountnamen zu identifizieren. Problematisch sind dann sog. Reverse-Ermittlungen im Sinne einer nachträglichen Reverse-Local-History. Dabei handelt es sich um Anfragen bei Providern zur Übertragung von Verkehrsdaten aus einer bestimmten Zelle, um die Identität der Anwesenden in dieser Zelle zu erschließen.

#### c) Durchsicht und Beschlagnahme von Daten

§ 94 StPO lässt umfassende Ermittlungen im Rahmen der Sicherstellung und Durchsuchung zu. Der Gesetzeswortlaut spricht von "Gegenständen", wobei die Rechtsprechung den Inhalt des Begriffes konturiert. Die Ermittlungsmaßnahmen werden durch § 110 StPO erweitert. Nach der Rechtsprechung des *BVerfG* ist die Durchsicht nämlich ein eigenständiger Teil der Durchsuchungsmaßnahme.

### 2. Herausforderungen und Probleme

#### a) Sicherung und Beschlagnahme

Ein gängiges Problem der Sicherung und Beschlagnahme der Datensätze ist die ordnungsgemäße Trennung nach beweisrelevant und irrelevant. Das *BVerfG* gab bereits im Jahre 2005 eine Richtung vor und appellierte, dass der Zugriff auf verfahrensirrelevante Daten aufs Vertretbare zu reduzieren ist. Offen bleibt jedoch, wie die konkrete Umsetzung dieser Vorgaben bei der vollständigen Beschlagnahme eines E-Mail-Accounts zu erfolgen hat.

#### b) Spannungsfeld des prozessualen Gleichgewichts

Ein weiteres Problem ist der Wettlauf der technischen Möglichkeiten. Die Richtung des Verfahrens kann davon abhängig sein, welche Verfahrensbeteiligten die Daten schneller auswerten können. *Dr. Basar* weist darauf hin, dass Regelungen diesen Konflikt lösen könnten. Weiterhin könnte dadurch auch sichergestellt werden, dass die Datenqualität im Ermittlungsverfahren bereits der Wahrheit so nahe wie möglich kommt.

#### c) Aktuelle Rechtsprechung - Zwangsentsperrung des Smartphones durch Fingerabdruck

Letzes Jahr hat das *OLG Bremen*<sup>8</sup> eine Entscheidung gefällt, die eine wichtige strafprozessuale Frage diskutiert. Denn bei einer Durchsuchung eines Unternehmens ist der Umgang mit den persönlichen Smartphones der Betroffenen rechtlich umstritten. Kern des Streits ist eine Diskussion um den Grundsatz der Selbstbelastungsfreiheit des Beschuldigten. Anknüpfungspunkt ist, ob die Polizei, um das Smartphone zu entsperren, im Rahmen des § 81b StPO die Fingerabdrücke des Beschuldigten zwangsweise abnehmen darf. Und neben der Frage, ob der nemo-tenetur-Grundsatz betroffen ist, eröffnet sich noch

<sup>8</sup> Mittlerweile wurde diese Entscheidung vom *BGH* bestätigt, vgl. *BGH*, NStZ 2025, 560 ff.

ein weiteres rechtlich-dogmatisches Problemfeld, denn auch der Zweck der Vorschrift ist umstritten. Dahingehend wird debattiert, ob die Maßnahme nur einen "Zugang" zum Smartphone und dem Datensatz ermöglicht oder, ob sie eher als Vorfeldmaßnahme von § 94 und 110 StPO einzuordnen ist. Diese Auseinandersetzung ist streng von der einfachen Eingabe des Passworts zu unterscheiden, denn hierbei handelt es sich um die biometrische Erfassung von Fingern und Gesicht.

#### *d) Grenzüberschreitende Ermittlungen bei Datensätzen*

Neben dem Smartphone ist auch die Cloud eine wachsende Datenquelle für Ermittler und ein viel diskutiertes Thema. Problematisch ist vor allem die territoriale Zuordnung der gespeicherten Datensätze. Vor einigen Jahren galt die Auffassung, dass Durchsuchungen nach § 110 StPO oder Zugriffe an den deutschen Grenzen enden. Nach aktueller Rechtsprechung ist eine staatliche Eingrenzung richtigerweise nicht möglich, da die Daten durch die Cloud potenziell überall liegen können. Demnach ist es ungewiss, ob Daten in Deutschland oder in einem anderen Hoheitsgebiet liegen. Konsequenterweise ist die Durchsicht in der Cloud zulässig, auch wenn die Daten in einem anderen Staat als Deutschland liegen. Dies wird durch die e-Evidence Verordnung verschärft. Durch die Regelung ist es möglich, dass Ermittler europaweit auf Daten zugreifen können. Das hat Auswirkungen auf die Verteidigung, da der Rechtsschutz im Bereich dieser Internationalisierung noch ausgebaut werden muss. Dies hat wiederum zur Folge, dass vermehrt Datenlieferungsvereinbarungen getroffen werden. Die Möglichkeit einer solchen Ermittlungsmaßnahme wird normativ über §§ 94, 95 StPO begründet.

### *3. Geschäftsgeheimnisgesetz*

Besonders praxisrelevant ist das bereits angesprochene Geschäftsgeheimnisgesetz. Typischerweise drehen sich die Fälle um Kündigungen eines Arbeitsverhältnisses. Betroffene möchten bestimmte Daten(sätze) aus ihrer Arbeitszeit mitnehmen, wie selbst erstellte Präsentationen usw. Aufgrund von § 23 GeschGehG ist dies nicht ohne weiteres möglich. Voraussetzung der Norm ist ein materielles Geschäftsgeheimnis, also ein wichtiges Betriebsgeheimnis, welches zugleich von angemessenen Geheimhaltungsmaßnahmen geschützt wird. Diese Voraussetzung ist äußerst umstritten und die Ausgestaltung dieser Maßnahmen ist unklar. Unter anderem kann dies von der Unternehmensgröße abhängig sein.

#### *4. Anforderungen an eine angemessene Verteidigung*

##### *a) Herausforderungen und Probleme*

Der Referent fordert, dass auch für die Verteidigung in einem Strafverfahren die Möglichkeit bestehen sollte, sich alle Daten und Datenspuren anzuschauen. Um dies umfassend zu ermöglichen, braucht es einen Zugriff auf die Rohdatensätze. Dies gilt umso mehr, da die Polizei die Datensätze zur Durchsicht oder Analyse an Spezialisten, auch an externe Forensiker, delegiert. Es ist jedoch äußerst

diskutabel, ob ein Forensiker den entsprechenden juristischen und ermittlungstaktischen Blick hat, um alle wichtigen Indizien zu erkennen und zu erheben. *Dr. Basar* sieht hier die Gefahr, dass entlastende Beweise und Indizien übersehen werden. Jedoch vermutet der Referent die zukünftige Lösung darin, dass solche Dokumentanalysen von Künstlicher Intelligenz übernommen werden.

##### *b) Lösungen und Reformvorschläge*

Wie auch in vorherigen Vorträgen angesprochen, ergeben sich zwischen der freien richterlichen Beweiswürdigung gem. § 261 StPO und digitalen Spuren Spannungen. Um diesen Konflikt aufzulösen, bietet der Referent Lösungsvorschläge an, wie die Verankerung von best-practice Lösungen in der RiStBV oder die Heranziehung des Leitfadens des BSI zur IT-Forensik zusammen mit englischsprachiger Literatur. Aus diesen Quellen lassen sich einige Eckpunkte für mögliche rechtliche Regulierungen ableiten und herauslesen.

Vor allem bei der Beschlagnahme einer Festplatte sieht der Referent Reformierungs- und Regulierungsbedarf. Gegenwärtig wird diese bei der Beschlagnahme erst bezeichnet, dann übergeben und danach werden Ausdrucke und auswertungsentsprechende Vermerke hergestellt, teilweise auch kurze Übersichten. Das empfindet *Dr. Basar* als ungenügend und fordert den Zugriff auf die Rohdaten auch für Verteidiger, sodass diese die Daten eigenständig analysieren können. Für die notwendigen Ressourcen ist jeder Strafverteidiger selbst zuständig.

Die Integrität kann dann durch die Dokumentation von Gewinnungs- und Verarbeitungsprozessen, die Reproduzierbarkeit und Methodenverlässlichkeit gewahrt werden. Eine erfreuliche Entwicklung zeigt sich in der tendenziell vermehrten Besprechung und Erörterung der Beweiswürdigung und Authentizität von der Rechtsprechung in ihren Urteilen.

Abschließend möchte *Dr. Basar* folgende Reformanregungen mit auf den Weg geben: Der Schutzbereich der Beschuldigten muss gestärkt werden und die Beschlagnahme und Durchsuchung sollten nicht in jedem Verfahren zugelassen werden, v.a. wenn es um Smartphones oder tagebuchähnliche Einträge geht. Zudem sollten Basiskenntnisse der IT-Forensik auch für Juristen gefordert werden, unter anderem im Wirtschaftsstrafrecht.

#### *5. Q&A Session*

Im Rahmen der Q&A Session erörtert der Referent ausführlich Datenlieferungsvereinbarungen und die damit einhergehenden Berührungspunkte mit der Datenschutz-Grundverordnung. §§ 45, 48 DSGVO sind diesbezüglich die maßgeblichen Vorschriften. Der Beschuldigte hat keine Mitwirkungspflicht bei Strafverfahren, auch nicht bei Wirtschaftsstrafverfahren und muss der Staatsanwaltschaft nicht entgegenkommen. Der Abschluss einer Datenlieferungsvereinbarung kann aber für beide Seiten eine Win-Win-Situation darstellen. Weiterhin betont der Referent die Bedeutung der Rolle des Sachverständigen und

die Schwierigkeit, ein einmal im Raum stehendes Gutachten anzugreifen, selbst wenn dieses den strafprozessualen Ansprüchen nicht genügt und Mängel aufweist.

## VI. IT-Forensik aus Sicht der Polizei, Gregory Kochneff (Bayerisches Landeskriminalamt)

Zum Abschluss der Tagung berichtete *Gregory Kochneff*, Sachverständiger für Mobilfunkforensik beim Landeskriminalamt, über IT-Forensik aus Sicht der Polizei. Neben einem praktischen Einblick in die Mobilfunkforensik als solche und deren Herausforderungen, gewährte er den Zuschauern einen Einblick in die Welt der Ergebnisdaten, also die Probleme und Hindernisse bei der Aufbereitung der Daten für den Auftraggeber und das Leistungsspektrum eines Mobilfunkforensikers. Einige amüsante Filmausschnitte und die Bezugnahme auf praktische Beispiele trugen zu einer informativen und anschaulichen Darstellung des Themengebiets und der Unterhaltung der Zuschauer bei. Frau Liegl bestätigend erläuterte er, dass der Begriff des Sachverständigen weder geschützt ist noch zwangsläufig eine Ausbildung voraussetzt, um vor Gericht als Expert:in stehen zu dürfen.

### 1. Mobilfunkforensik

Der Referent begann damit, den Bereich der Mobilfunkforensik näher zu erläutern. In der Regel beschäftigt sich ein solcher Forensiker *post mortem* mit den Gegenständen, sprich: er analysiert in der Regel nicht an Live-Systemen.

#### a) Allgemeines

Die Arbeit des Sachverständigen beginnt durch Zusage eines Mobiltelefons inklusive des Untersuchungsauftrags durch den Ermittler, das Gerät auszulesen. In der Regel wird der Auftrag nicht weiter konkretisiert, sodass eine Vollsicherung des Gerätes und keine selektive Sicherung vorzunehmen ist. Überwiegend stammen die Daten aus dem Gerätespeicher, vereinzelt wird eine Sicherung des Speichers von Cloud-Anbietern und Telekommunikationsanbietern erforderlich. Während die Daten solcher Provider im Grunde bereits aufbereitet sind, was sich beispielsweise anhand der Abfrage einer SIM-Karte zeigt, wobei man Informationen zum Anschlussinhaber, PIN-Nummer, Rufnummer usw. erlangen kann, werden die Daten direkt aus dem Speicher des Mobilfunkgeräts vom Forensiker entsprechend selbst aufbereitet.

#### b) Tools

Die Auswertung der Daten erfolgt sodann manuell oder automatisiert durch kommerzielle, zugekaufte Tools. In manchen Fällen wird auf selbstentwickelte Tools zurückgegriffen. In bestimmten Fällen werden sog. Teststellungen durchgeführt, um das technische Verhalten des Geräts nachzustellen und Abläufe und Hypothesen diesbezüglich zu verifizieren. Auch hier liegen Grenzen in der technischen Weiterentwicklung der Mobilfunkgeräte, da man

ein altes Handy mit altem Betriebssystem nicht bzw. schwer nachahmen kann.

#### c) Weitere Speicherquellen

Ferner können die Daten auch direkt aus dem physischen Speicherort extrahiert werden. In Smartphones und Tablets sind unter anderem Speicherbausteine, wie etwa UFS-Chips, microSD-Karten, SIM-Karten und eMMC-Chips, eingebaut bzw. eingelegt. An dieser Stelle sind handwerkliche und elektrotechnische Fertigkeiten gefragt.

### 2. Ergebnisdaten

Neben der Aufbereitung der Daten ist auch die Bereitstellung für den Auftraggeber ein wichtiger Aufgabenbereich eines Mobilfunkforensikers.

#### a) Extrahieren der Daten

Ergebnisdaten werden in der Mobilfunkforensik selbst aus den Geräten extrahiert. Dabei erklärt *Herr Kochneff*, dass manchmal Chips ausgelötet oder Speicherkarten aus den Geräten montiert werden, wobei darauf zu achten ist, diese forensisch in möglichst unveränderter Form zu sichern. Zum Teil bedarf es auch invasiverer Maßnahmen, die ein Öffnen und Zerstören der Geräte bedingen. Hierfür muss eine Zerstörungsgenehmigung der Staatsanwaltschaft eingeholt werden, da das Gerät dadurch irreversibel beschädigt wird bzw. werden kann.

#### b) Aufbereitung der Daten

Für die Recherche der Ermittler werden interaktive Berichtsdateien, wie z.B. der Cellebrite Reader, benutzt. Diese Programme ermöglichen es den Forensikern, Daten aus dem Labor in einer Weise bereitzustellen, die eine ermittlungsfreundliche Datenanalyse ermöglicht. Zudem wird eine automatische Interpretation der Daten durch sog. Enrichments unterstützt, die eine Kategorisierung und Vorabfilterung der Daten gewährleisten. Nach Auffassung des Referenten zeichnet sich ein Trend bezüglich des Einsatzes von Enrichments und KI-gestützten Zusammenfassungen ab. Der Vorteil dieser Funktionen liegt darin, dass sie die Bewältigung großer Datenmassen erleichtern. Gleichzeitig haben diese Funktionen hohe Hardware-Anforderungen, sodass man für eine optimierte Auswertung leistungsstarke Computer braucht. Die Bewältigung der Big Data für Justiz und Ermittler wird darauf hinauslaufen, Technik durch Technik zu regulieren.

#### c) Bereitstellung

Die Bereitstellung der Ergebnisdaten erfolgt über CD, Festplatten, und/oder Netzwerk. Letztere können den Ermittlungsprozess beschleunigen, indem sie die Möglichkeit eines schnelleren Zugriffs auf die Daten ermöglichen; teilweise noch während der Gutachtenerstellung. Ein Faktor, der die Effizienz bei dieser Vorgehensweise limitiert,

besteht aber im Erfordernis einer funktionierenden Netzwerk-Anbindung und einer bayernweiten Zugriffsverbindung einzelner Behörden. Derzeit stehen die schleppende Digitalisierung und Kostenpunkte einer effizienten Nutzung entgegen.

### 3. Leistungsspektrum

Herr Kochneff präsentiert seine abwechslungsreichen Aufgabenbereiche, die von der technischen Analyse und Handwerkszeug, über die Gutachtenerstellung und auch in der Weiterbildung von Kolleg:innen und Praktikant:innen bestehen.

#### a) Vorfeldaufgaben

Das Leistungsspektrum beginnt bereits mit der einfachen Identifikation von Geräten und dem Modell. Ferner werden Zugriffsmöglichkeiten auf relevante Gerätedaten durch Exploits, von den kommerziellen Tools ausgenutzt. Der Rahmen des Möglichen variiert diesbezüglich aber vor dem Hintergrund der vielen Betriebssystem-Updates, neuen Geräte- und Chip-Generationen. Daneben wird der Referent auch tätig, um Geräte wieder Instand zu setzen, um so die Sicherung dieser zu gewährleisten – etwa für den Fall mutmaßlicher Schädigung der Geräte durch Beschuldigte. Je nach Fall und Umständen kann es dann zur bereits erwähnten Auslösung von Chips kommen.<sup>9</sup> Grundsätzliche nachfolgende Aufgaben bestehen in der technischen Untersuchung, Verfügbarkeit zur Beantwortung von Fragen und Gutachtenerstellung. In Großverfahren können die Ergebnisdaten in speziellen Recherche-tools gemeinsam, asservatenübergreifend, analysiert werden.

#### b) Herausforderungen - technischer Fortschritt

Der technische Fortschritt bietet zum einen neue Möglichkeiten, zum anderen führt dies im Rahmen der Mobilfunkforensik dazu, dass Forensiker ständig neu interpretieren oder einordnen müssen. Die Schwierigkeit besteht demnach vor allem darin, mit der hohen Datenmenge, Asservatenaufkommen, Applikationsvielfalt und Massen an Apps, Betriebssysteme und Sicherheitspatches<sup>10</sup> umzugehen, diese neu zu interpretieren, einzuordnen bzw. zu berücksichtigen. Das kann in der Implementation von neuen Funktionen der Messenger, wie einem Gelesen-Button bestehen, der dann neu interpretiert werden muss. Der Referent veranschaulichte diese Dimensionen, indem er den Blick auf die Identifizierung und Umgang mit kleinsten Details warf, da diese wichtige Kontextinformationen hergeben können. Beispielsweise kann es bei einer Textnachricht, die eine Drohung enthält, einen Unterschied machen, ob dahinter ein schwarzes oder ein rotes Herz gesetzt wird. In diesem Zusammenhang berichtete er von einem offiziellen Standard für die richtige Benennung der Emojis. Eine weitere spannende Neuerung von Smartphones ist die Diebstahlerkennung auf den Geräten, deren genaue Funktion und Möglichkeiten es noch genauer zu erforschen gilt.

#### c) Präsentation vor Gericht

Gewonnene Erkenntnisse müssen vor Gericht präsentiert werden.

##### aa) wiederkehrende Aufgaben

Den Vortrag von Frau Liegl bestätigend, berichtet der Referent, dass eine spezifische Vorbereitung kaum möglich und teilweise eine „Live-Interpretation“ der Daten vorzunehmen ist. Vor diesem Hintergrund können konkrete Fragestellungen der Ermittler die Arbeit vereinfachen. Trotzdem kann es zu Folgefragen kommen, je nachdem wie vertieft auch das Grund IT-Verständnis der Beteiligten ist, und im Zweifel muss ein Folgegutachten erstellt werden.

Neben der Vorstellung des Gutachtens vor Gericht, bereiten (Mobilfunk)forensiker in Großverfahren auch die Daten auf, damit man über ein Tool Zugriff auf alle dazugehörigen Asservate - PCs, Handys usw. - hat und in diesen recherchieren kann.

Dasselbe gilt für eine zuverlässige IT im Gerichtssaal – etwa im Sinne von funktionierenden Anschlüssen –, die eine anschauliche Visualisierung der digitalen Beweismittel fördert. Eine reibungslose Beweismittelpräsentation gewinnt vor allem dann an Relevanz, wenn den digitalen Beweismitteln im konkreten Verfahren eine tragende Rolle zukommt.

##### bb) Beispielfälle

Wie wichtig die digitalen Spuren sein können, die wir auf unseren Mobiltelefonen hinterlassen, unterstreicht der Referent in zwei Fällen aus seiner Praxis. Im ersten Fall verhalfen Standortdaten auf den Smartphones der Angeklagten dazu, eine Verwechslung auszuräumen. Dadurch konnte dann der Unschuldsbeweis geführt werden, der die Angeklagten vor einer mehrjährigen Haftstrafe gerettet hatte. In einem anderen Verfahren konnte mittels Datenextraktion aus einem zerstörten Mobiltelefon der relevante Geschehensablauf anhand einer Temperaturkurve rekonstruiert werden. Dabei wurde das Mobiltelefon des Opfers Monate später völlig zerstört im Wasser gefunden. Die Aufgabe des Forensikers bestand nun darin, die Platine aus dem kaputten Mobilgerät heraus zu montieren und zu reinigen. So konnte diese dann in ein baugleiches Gerät implementiert und auf die Funktionen zugegriffen werden. Die daraus gewonnenen Daten konnten den relevanten Moment in der Tatnacht sehr genau wiedergeben.

#### 4. Die Übersetzungsproblematik

Zudem betont der Referent, dass das Schaffen von Verständnis eine wichtige Rolle spielt. Solches kann etwa durch Übersetzung der IT-Sachverhalte in Laiensprache und Bildung von verständlichen Analogien erreicht werden.

<sup>9</sup> Vor allem ältere TSOP-Chips (*thin small-outline package*) lassen sich in Fest-Einbau-Navigationsgeräten oder Skimmern finden.

<sup>10</sup> „Sicherheitspatches“ sind kleine Updates für das Betriebssystem, die eine Sicherheitslücke in einem Smartphone-Betriebssystem schließen.

### *a) Anforderungen an den Sachverständigen*

Dabei kommt es auch auf die korrekte Ausdrucksweise im technischen Sinne an, ohne das Gericht mit zu vernachlässigendem Hintergrundwissen zu überfrachten und rechtliche Wertungen oder Mutmaßungen in die verbale Präsentation einfließen zu lassen. Während des Auftritts vor Gericht gilt es, sich nicht aus der Ruhe bringen zu lassen. Fragen, die spontan nicht beantwortet werden können, sollten im Zweifel zunächst unbeantwortet bleiben und auf ein Nachreichen verwiesen werden. Manchmal kann es sich auch anbieten, eine kurze Pause einzufordern. Aufgrund der extremen Fluktuation der Mobilfunkforensik, bietet sich zur Bewältigung dieser ein stetiger Austausch der Mobilfunkforensiker untereinander an.

### *b) Analogie zum Verständnis der Datensicherung eines gesperrten Mobiltelefons*

Gegenseitiges Verständnis und Kommunikation sind wichtig. Dadurch können die Strafverfolger besser nachvollziehen, wieso unter anderem die Sicherung eines entsperrten Handys lange dauern kann. Der Referent zieht dabei einen Vergleich mit einem Banküberfall, wobei ein Tunnel von einem Gebäude zum nächsten gegraben werden muss. Der Tunnel stellt dabei die Sicherheitslücken dar, die inoffizielle Kanäle zur Nutzung sind. Der Tunnel ist instabil und kann jederzeit beim Einleiten von Daten einstürzen. Kommt man nun am "Datentresor" an, kann man nicht einfach alles markieren und kopieren. Auch hier bedarf es Fingerspitzengefühl. Ist der Tresor offen, kann nur Barren für Barren transportiert werden. Auch die Sicherung der riesigen Datenmengen, die sich auf einem solchen Gerät befinden, dauert.

### *5. Q&A Session*

In Rahmen der letzten Fragerunde wurde zunächst die Funktionsweise der Enrichments genauer geklärt. Es handelt sich dabei um eine Offline-Software, die sich aktuell auf eine Analyse von Bilder- und Videodateien beschränkt und auf Deep-Learning beruht. Eine hundertprozentige Verlässlichkeit der Interpretation durch Enrichments kann aufgrund der schieren Menge an Daten und Updates nicht garantiert werden. Dennoch sei gerade eine Offline-Software geeignetes Mittel zur ersten Interpretation von Rohdaten. Zuletzt wurde über die Relevanz von Standortdaten diskutiert, welche nach Ansicht des Referenten insbesondere auch als entlastendes Beweismittel von Bedeutung sein können und damit das Einschalten der Standortverfolgung nicht nur Nachteile mit sich bringt. Insofern rät der Referent zu einer selektiven Auswahl, wann wie wo es sinnvoll ist, dass persönliche Daten abgegriffen werden und wann unter Umständen auch nicht.

### **VII. Schlussworte**

*Prof. Dr. Christoph Safferling*, LL.M. (LSE) und sein ICLU-Team danken allen Teilnehmenden für die rege Beteiligung und die lebhafteste, interdisziplinäre Diskussion. Zugleich freuen sie sich auf die Fortsetzung der Veranstaltungsreihe auch im Jahr 2026, dann zum Thema „*Legal Tech im Strafprozess - Chancen, Risiken, Perspektiven*“. Angesichts des zehnjährigen Bestehens des Erlanger Cybercrime Tages in diesem Jahr, erhält die Veranstaltung einen besonderen Charakter.