4. Jahrgang | 5. Ausgabe | ISSN 2509-6826 5 | 2019

KriPoZ

Kriminalpolitische Zeitschrift

KONTAKT
schriftleitung@kripoz.de

ALLGEMEINE BEITRÄGE | 265 – 306

BUCHBESPRECHUNGEN | 307 – 311

TAGUNGSBERICHTE | 312 – 322

ALLGEMEINE BEITRÄGE

Smart Sentencing

Ein neuer Ansatz für Transparenz richterlicher Strafzumessungsentscheidungen

von Prof. Dr. Dr. Frauke Rostalski
und Malte Völkening[*]

Abstract
Vergleichende Untersuchungen zur Strafzumessungspraxis in Deutschland ergeben regelmäßig das Bild starker Variationen in der Strafhöhe, die sich nicht ausschließlich durch normativ relevante Unterschiede der betroffenen Fälle erklären lassen. Wird die Strafzumessung in der Gesellschaft und durch den Verurteilten als willkürlich empfunden, so schwindet die Akzeptanzerwartung der Entscheidungen. Abstrakte Strafzumessungsrichtlinien nach U.S.-amerikanischem Vorbild versprechen Abhilfe, sind aber nicht hinreichend auf die Umstände des Einzelfalls konkretisierbar. Vorzugswürdig erscheint, das als angemessen empfundene Strafmaß durch einen kritischen und detailgenauen Vergleich mit ähnlichen Entscheidungen zu ermitteln. Dazu ist aber eine umfassende und transparente Datengrundlage erforderlich. Eine solche kann mittels Legal Tech automatisiert anhand der Zumessungserwägungen in den Begründungen aller einschlägigen Urteile erstellt werden.

Comparative studies regularly reveal strong variance in the level of penalties imposed by German judges that is not fully explicable by actual differences between the cases in question. If verdicts are seen as arbitrary by the society or the defendants, their prospect of acceptance decreases. Sentencing guidelines, as used in the U.S., appear to remedy these deficits but they lack individualization. Therefore, a critical and detailed comparison with similar cases and decisions seems more promising. This approach requires an extensive and transparent empirical basis which can be provided by analyzing the reasons given by other courts, a process that can be automated using Legal Tech.

I. Einleitung

„Der Richter pflegt […] bei der Strafzumessung bewußt oder unbewußt nicht vom gesetzlichen Strafrahmen, sondern von einem gewissen typischen Testfall auszugehen, für den er eine bestimmte Strafe für angemessen hielt. Und an diesem Fall und an dieser Strafe mißt er dann die kommenden Fälle und paßt die Strafe für sie jener Strafe an, die als Fixpunkt seiner gesamten Strafzumessung erscheint. Sie ist sein geheimes Metermaß.“[1] Diese Worte von *Eduard Dreher* haben heute nicht viel von ihrer Gültigkeit verloren.[2] Über die Legitimität eines solchen Verfahrens ist damit freilich noch nichts gesagt.[3] Hier stellt sich einerseits die Frage, ob die Gerichte durch das Anlegen eigener Wertmaßstäbe in unzulässiger Weise von den gesetzlichen Vorgaben abweichen und sich so an die Stelle des Gesetzgebers setzen.[4] Andererseits hat schon *Dreher* erkannt, dass das „geheime Metermaß“ der Richter ein lokal beschränktes ist, dass sich also unterschiedliche regionale Tendenzen in den Strafzumessungsentscheidungen herausbilden.[5] Dieses Problem wird spätestens seit dem 72. Deutschen Juristentag 2018 wieder intensiv diskutiert.[6] Dabei sind die Lösungsstrategien seit Jahren im Wesentlichen unverändert geblieben. Insbesondere der Ruf nach „Sentencing Guidelines“ entsprechend U.S.-amerikanischem Vorbild wird vielerorts erhoben.[7] Bislang bei weitem nicht ausgeschöpft erscheint den Autoren dieses Beitrags dabei das Potenzial von Legal Tech für die Vereinheitlichung der richterlichen Strafzumessungsentscheidungen.

II. Strafungerechtigkeit als Gefahr für die gesellschaftliche Anerkennung von Strafurteilen

Die Strafzumessungsentscheidungen in Deutschland unterscheiden sich mitunter erheblich. Angesichts der stets einzubeziehenden Besonderheiten des Einzelfalls verwundert das im Grunde wenig. Als problematisch erweisen sich Strafzumessungsunterschiede allerdings dann, wenn sie auf keinem normativ relevanten Umstand beruhen. Dies ist u.a. dann der Fall, wenn sich die Abweichungen im Wesentlichen durch die individuelle Person des entscheidenden Richters oder aber den Ort erklären, an

* *Prof. Dr. Dr. Frauke Rostalski* ist Inhaberin des Lehrstuhls für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung an der Universität zu Köln. *Malte Völkening* ist Wissenschaftlicher Mitarbeiter an diesem Lehrstuhl.

1 *Dreher,* MDR 1961, 343 (344).
2 Siehe unten unter II.
3 Dazu unten unter IV.
4 So der Vorwurf bei *Dreher,* MDR 1961, 343 (344).
5 *Dreher,* MDR 1961, 343 (344).
6 Siehe instruktiv *Kaspar*, Sentencing Guidelines versus freies tatrichterliches Ermessen – Brauchen wir ein neues Strafzumessungsrecht?, 2018.
7 *Hoven,* KriPoZ 2018, 276 (289 f.); *Weigend,* in: FS Rechtswissenschaftliche Fakultät Köln, 1988, S. 579 (601).

dem die Entscheidung getroffen wurde.[8] Weder die Rechtsanwenderpersönlichkeit noch der Entscheidungsort dürfen für die Strafzumessung relevant sein. Vielmehr gebietet es der Grundsatz der rechtlichen Gleichbehandlung sachlich gleich gelagerter Fälle, diese für die Strafhöhenbemessung sachfremden Kriterien außer Acht zu lassen.[9]

Dennoch spielen gerade diese Faktoren den Angaben der Verfasser unterschiedlicher Studien zufolge im Bereich der deutschen Strafzumessung nach wie vor eine alles andere als untergeordnete Rolle.[10] So besteht bisweilen eine erhebliche Diskrepanz der Strafzumessung zwischen verschiedenen Regionen und Gerichtsbezirken.[11] Unterschiede zeigen sich vor allem entlang der Nord-Süd-Achse.[12] Innerhalb der einzelnen Gerichtsbezirke erfolgt die Strafzumessung dagegen vergleichsweise homogen.[13] Mit dem Befund des regionalen Abweichens von Strafzumessungsentscheidungen gehen Schwierigkeiten einher, die in letzter Konsequenz die rechtsstaatlich relevante Akzeptanz von Strafurteilen gefährden. Die Bestrafung dient der (Wieder-)Herstellung des Rechtsfriedens. Durch die Straftat stellt der Täter das Recht infrage. Im Wege des Schuldspruch und ggf. der zusätzlichen Verhängung eines Strafübels reagiert die rechtlich verfasste Gesellschaft hierauf und teilt dem Einzelnen auf diese Weise mit, dass das Recht trotz seiner Tat weiterhin uneingeschränkte allgemeine Gültigkeit hat.[14] Dabei orientieren sich Schuldspruch und Strafübel ausschließlich an dem individuellen, hinreichend gewichtigen Verhaltensnormverstoß des Täters (ggf. nebst Fehlverhaltensfolgen).[15] In diesem Sinne hat die Bestrafung *tatproportional* zu erfolgen:[16] Ihr Gegenstand ist die unberechtigte Freiheitsanmaßung des Täters in Gestalt seiner Straftat, die durch Strafe ausgeglichen wird. Vor diesem Hintergrund lässt sich weder eine zu niedrige noch eine zu hohe Strafe rechtfertigen. Insbesondere dürfen Faktoren, die keinen rechtlich relevanten Bezug zu der Straftat aufweisen, bei der Strafzumessung nicht berücksichtigt werden.[17] In der Folge spielen das (willkürliche) Belieben der individuellen Richterpersönlichkeit ebenso wie der Entscheidungsort für die Strafzumessung grundsätzlich keine Rolle. Beide treffen für sich genommen keine Aussage über das Gewicht des konkreten Verhaltensnormverstoßes (ggf. nebst Fehlverhaltensfolgen). Sofern diese Faktoren gleichwohl einen (ggf. erheblichen) Einfluss auf die konkrete Strafzumessungsentscheidung haben, beeinträchtigt dies die Akzeptanz des Urteils sowohl durch den Verurteilten selbst als auch durch Dritte. Die Einbeziehung sachfremder Erwägungen erweist sich als willkürlich und bedroht daher das Rechtssicherheitsgefühl. Die (Wieder-)Herstellung des Rechtsfriedens durch Schuldspruch und Strafe kann allein gelingen, wenn der jeweilige Rechtsfolgenausspruch als angemessene Reaktion auf die Tat wahrgenommen wird. Ist dies nicht der Fall, droht er, einen gänzlich gegenteiligen Effekt hervorzurufen: Eine als willkürlich empfundene Entscheidung lässt das Vertrauen in das Funktionieren der staatlichen Ordnung schwinden. Vor allem, wenn dies eine so eingriffsintensive Maßnahme wie staatliche Strafe betrifft, birgt dies eine besondere Gefahr für den gesellschaftlichen Zusammenhalt.[18]

III. Fehlen konkreter gesetzlicher Vorgaben für die Strafzumessung im Einzelfall und Vorschlag der Einführung von Strafzumessungsrichtlinien

Wer nach Gründen für diesen Missstand im Bereich der deutschen Strafzumessungspraxis sucht, mag geneigt sein, auf die Weite der Strafrahmen der Delikte im Besonderen Teil des StGB oder aber auf die Regelung des § 46 Abs. 1 S. 1 StGB zu verweisen. Weder das eine noch das andere enthält konkrete Angaben für die angemessene Strafhöhe spezifischer Einzelfälle.[19] Trotz mitunter berechtigter Kritik, sowohl an den Deliktsstrafrahmen[20] als auch der strafzumessungsrechtlichen Kernvorschrift[21],

8 Gemeint sind hierbei freilich sachlich vergleichbare Fälle. Beispielsweise die besondere Brutalität der Tat spielt eine Rolle für deren Bewertung. Sollte diese besonders häufig in einer bestimmten Region Deutschlands auftreten, stellt dies selbstverständlich einen normativ unproblematischen Grund für die häufig strengere Bestrafung dar. Siehe *Meier*, Strafrechtliche Sanktionen, 4. Aufl. (2015), S. 255 sowie *Albrecht,* ZStW 102 (1990), 596 (598 f.) dazu, dass sich ein nicht unerheblicher Teil regionaler Unterschiede auf solche normativ relevanten Faktoren zurückführen lässt.

9 Vgl. zum Verstoß gegen Art. 3 Abs. 1 GG durch regional abweichende Praxen *Albrecht*, Strafzumessung bei schwerer Kriminalität, 1994, S. 21 ff.; *Kaspar,* Sentencing Guidelines (Fn. 6), C 86 ff. *Streng*, Strafrechtliche Sanktionen, 3. Aufl. (2012), Rn. 504 sieht einen Verstoß „zumindest gegen die *Idee* des verfassungsrechtlichen Gleichbehandlungsgebots“ (Herv. im Original).

10 Siehe nur die Nachweise bei *Kaspar,* Sentencing Guidelines (Fn. 6), C 18 ff.

11 *Meier,* Sanktionen (Fn. 8), S. 257 m.w.N. Skeptisch für die von ihm untersuchten schweren Delikte aber *Albrecht,* ZStW 102 (1990), 596 (614).

12 Allerdings mit Ausnahme Baden-Württembergs, vgl. *Grundies,* in: Hermann/Pöge, Kriminalsoziologie, 2018, S. 295 (302 f.).

13 Für die Trunkenheit im Verkehr *Schöch*, Strafzumessungspraxis und Verkehrsdelinquenz, 1973, S. 125 ff. Auch *Grundies,* in: Hermann/Pöge, S. 295 (303) sieht einen Zusammenhang zwischen Strafhöhenvarianz und OLG-Bezirkszugehörigkeit, den er mit der „hierarchische[n] Struktur der Justiz“ und der „Revisionspraxis“ erklärt. Angesichts der nur begrenzten Zuständigkeit der Oberlandesgerichte als Revisionsgerichte (§ 121 Abs. 1 Nr. 1 GVG) ist dies aber nur für Entscheidungen in Fällen leichter und mittlerer Kriminalität plausibel (vgl. § 24 Abs. 1 S. 1 Nr. 2 GVG).

14 *Rostalski*, Der Tatbegriff im Strafrecht, 2019, S. 25 f.

15 *Rostalski,* Tatbegriff (Fn. 14), S. 27, 133 f.,139; *Freund,* GA 1999, 509 (526 f.).

16 Siehe zum Konzept statt aller *Hörnle,* Tatproportionale Strafzumessung, 1999.

17 Siehe allerdings bereits *Timm*, Gesinnung und Straftat, 2012, S. 256 ff. dazu, dass die Vorschrift des § 46 StGB auch gegenwärtig Strafzumessungsfaktoren auflistet, die sich normativ nicht rechtfertigen lassen.

18 Vgl. zur hohen Sensibilität des Gleichheitsempfindens bei Strafzumessungsentscheidungen *Streng,* Sanktionen (Fn. 9), Rn. 505 m.w.N.

19 *Freund,* GA 1999, 509 (524), der im Hinblick auf die Strafrahmen auf die (wenigen) Ausnahmen einer absoluten Strafdrohung und der Anordnung einer Mindeststrafe für bestimmte Fälle verweist.

20 *Kinzig,* in: Schönke/Schröder, 30. Aufl. (2019), § 46 Rn. 72 plädiert für eine „deutlichere Konturierung der Strafrahmen“, *Streng,* in: Kindhäuser/Neumann/Paeffgen, 5. Aufl. (2017), § 46 Rn. 200 für eine Absenkung der Strafrahmenobergrenzen, wobei letzterer zugibt, dass hiervon nur eine geringfügige Verbesserung zu erwarten ist.

21 Kritisch zum unklaren Verhältnis der in § 46 Abs. 2 StGB genannten Kriterien etwa *Kaspar,* Sentencing Guidelines (Fn. 6), C 12, 66 ff; *Kudlich/Koch,* NJW 2018, 2762 (2763).

ginge allerdings die Forderung deutlich zu weit, diese hätten konkrete Lösungen für den jeweiligen Fall zu liefern, über den der Strafrichter entscheiden muss. So ist es gerade als ein Vorzug des deutschen Systems zu bewerten, dass weite Strafrahmen ein breites Reaktionsinstrumentarium an die Hand geben.[22] Ebenso verhält es sich im Hinblick auf die Vorschrift des § 46 Abs. 1 S. 1 StGB, soweit diese die Strafzumessung an der „Schuld" des Täters orientiert wissen will. Die Norm lässt sich ohne Weiteres so verstehen, dass durch die Bestrafung ein Ausgleich für die begangene Straftat in Gestalt des individuellen, hinreichend gewichtigen Verhaltensnormverstoßes (ggf. nebst Fehlverhaltensfolgen) geschaffen werden soll. Sie entspricht damit in dieser Hinsicht unmittelbar den bereits dargelegten straftheoretischen Vorgaben.

Und dennoch richten nicht wenige ihre Verbesserungsvorschläge zur Beseitigung der unliebsamen gegenwärtigen Strafzumessungspraxis auf das Gesetz bzw. zumindest dessen Konkretisierung. So erleben wir derzeit in der strafrechtswissenschaftlichen Debatte eine (neuerliche) Konjunktur der Forderung nach einer mehr oder minder stark ausgeprägten Orientierung am Vorbild der U.S.-amerikanischen Strafzumessungsrichtlinien („Sentencing Guidelines").[23] Diese sehen eine gegenüber der Vorschrift des § 46 StGB erhöhte Ausdifferenzierung relevanter Strafzumessungsfaktoren in Tabellenform vor, die der Richter bei der Begründung seiner Strafzumessungsentscheidung heranziehen kann. In den USA werden Strafzumessungsrichtlinien von einer unabhängigen Expertenkommission erarbeitet und regelmäßig angepasst. Sie enthalten detaillierte Vorgaben, anhand deren sich aus dem Strafrahmen eines Delikts unter Berücksichtigung strafschärfender und strafmildernder Umstände ein vergleichsweise präzises Strafmaß ergibt.[24] Der Fokus liegt dabei auf den Tatumständen und der Vorstrafenbelastung des Täters.[25] Während die Befolgung der Richtlinien anfangs zwingend war, sind sie seit einem Urteil des Supreme Court aus dem Jahr 2005 nur noch unverbindliche Anhaltspunkte, mit denen sich die Richter allerdings im Urteil auseinandersetzen müssen.[26] In Deutschland wird vor diesem Hintergrund seitens der Befürworter der Einführung von „Sentencing Guidelines" u.a. darüber diskutiert, inwieweit eine Orientierung des Richters an den Strafzumessungsrichtlinien verbindlich sein soll, ob bzw. mit welchem zusätzlichen Dokumentationsaufwand Abweichungen zulässig sein sollen und welche Vor- oder Nachteile mit einem Punktesystem einhergingen. Einig ist man sich zumindest im Hinblick auf die Vorzüge eines solchen Systems gegenüber der gegenwärtigen Strafzumessungspraxis: Mehr Transparenz soll die Gleichheit von Strafmaßentscheidungen befördern, was zuletzt der Strafgerechtigkeit diene.[27]

Der Idee einer Einführung von Strafzumessungsrichtlinien werden seit Langem bedeutsame Einwände entgegengehalten. So erscheint bereits fraglich, ob der große Aufwand der Erstellung solcher Richtlinien noch in einem angemessenen Verhältnis zu ihrem Nutzen steht.[28] Als problematisch erweist sich zumindest das schematische Vorgehen, das entsprechende Richtlinien dem Rechtsanwender im Rahmen der Strafzumessungsentscheidung auferlegen. Will er sich hieran *nicht* halten, bedarf es jedenfalls im U.S.-amerikanischen Modell einer besonderen Begründung, was eine neuerliche Hürde darstellen kann in der Würdigung des Einzelfalls (sofern der Richter die erhöhte Mühe scheut).[29] Strafzumessungsrichtlinien, die einem solchen schematischen Denken verhaftet sind, machen die Regel – die Besonderheit des Einzelfalls – zum Ausnahmefall. Hiermit geht die Gefahr einher, dass die individuelle Gerechtigkeit auf der Strecke bleibt.[30] Hinzu kommt, dass sich die abstrakte Umwandlung von Zumessungserwägungen in eine bestimmte Strafe besonders für solche Merkmale eignet, die häufig vorkommen und quantifizierbar sind (etwa die Schadenshöhe beim Diebstahl oder die BAK bei der Trunkenheit im Verkehr). Ein System abstrakter Richtlinien läuft daher Gefahr, sich auf derartige Merkmale zu konzentrieren und weniger gut schematisierbare Kriterien zu vernachlässigen, wenngleich diese im Einzelfall eine wesentlich höhere Bedeutung haben können.[31]

IV. Vergleichende Strafzumessung als Schlüssel zu mehr Strafgerechtigkeit

Wer so auf das Problem bestehender Missstände im Bereich der deutschen Strafzumessungspraxis blickt, kann den Eindruck gewinnen, die Wahl zwischen zwei Übeln treffen zu müssen: Dem Festhalten am bisherigen, die Praxis offenbar unzureichend anleitenden Modell auf der einen, der Einführung von irgendwie gearteten Strafzumessungsrichtlinien auf der anderen Seite. Indessen zeichnet die bislang dargelegte Kritik lediglich ein verkürztes Bild vom Spielraum desjenigen, der sich auf die Suche nach mehr Strafzumessungsgerechtigkeit begibt. So liegt der Schlüssel zur Lösung des Problems in einem Ausschöpfen der durch das Gesetz bereits in seiner gegenwärtigen Fassung eingeräumten Möglichkeiten. Diese können unter Umständen selbst durch geeignete Strafzumessungsrichtlinien konkretisiert werden, soweit diese keinen sachlich unangemessenen Schematismus in den Vorgang der Strafzumessung hineintragen – was nicht zwingend ist.[32]

---

22 Siehe dazu bereits *Freund,* GA 1999, 509 (515), der darauf verweist, dass ein vom gegenwärtigen System der Strafrahmen abweichendes „einseitiges Rechtssicherheitsdenken" die Einzelfallgerechtigkeit in unerträglicher Weise vernachlässigen würde.

23 Siehe zu früheren Vorschlägen beispielsweise *Weigend,* in: FS Rechtswissenschaftliche Fakultät Köln, 1988, S. 579 (591 ff.) und *Reichert*, Intersubjektivität durch Strafzumessungsrichtlinien, 1999, S. 273 ff. sowie aus der jüngeren Zeit *Hoven,* KriPoZ 2018, 276 (289 f.); affirmativ auch *Wohlers/Went,* in: Hirsch/Neumann/Seelmann, Strafe – Warum?, 2011, S. 173 (202 f.).

24 Ausführlich dazu *Reichert,* Strafzumessungsrichtlinien (Fn. 23), S. 204 ff.

25 *Reichert,* Strafzumessungsrichtlinien (Fn. 23), S. 205.

26 United States v. Booker, 125 S. Ct. 738 (2005). Siehe dazu sowie zur Kritik an dieser Entscheidung *Meyer,* ZStW 118 (2006), 512 (534 ff.).

27 Vgl. stellvertretend *Hoven,* KriPoZ 2018, 276 (289 f.).

28 *Kaspar,* Sentencing Guidelines (Fn. 6), C 84; *Kudlich/Koch,* NJW 2018, 2762 (2765).

29 Zur Hürde, die selbst eine bloße Orientierungshilfe für eine Abweichung darstellt, auch *Kudlich/Koch,* NJW 2018, 2762 (2765 Fn. 25).

30 *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 199.

31 Vgl. *Kudlich/Koch,* NJW 2018, 2762 (2764 f.).

32 Vgl. *Hoven,* KriPoZ 2018, 276 (290).

In erster Linie muss aber die bei der Strafhöhenbemessung unbedingt anzuwendende *Technik des Vergleichs mit anderen Fällen* der zu beurteilenden Straftatbegehung verbessert werden. Gerechte Strafzumessung kann allein unter der Voraussetzung gelingen, dass der Einzelfall in ein Verhältnis zu früheren Entscheidungen vergleichbarer Fälle gebracht wird, die sich mit den rechtlich anerkennenswerten gesellschaftlichen Wertvorstellungen decken und daher Akzeptanz hervorrufen.[33] Wer von einem vergleichbaren Fall der Deliktsbegehung als „Fixpunkt" ausgeht, von dem aus er Abweichungen nach oben oder unten vornehmen kann, besitzt einen festen Ausgangspunkt, an dem er seine Entscheidung orientieren kann.[34] Dabei erweist es sich als praktisch sinnvoll, sich jedenfalls nicht an nur selten vorkommenden Fällen auszurichten, sondern solche zu wählen, die mit entsprechenden strafzumessungsrelevanten Eigenschaften schon oft entschieden worden sind. Nimmt der Richter in seinem konkreten Fall hiervon Abweichungen vor, muss er diese begründen und dabei an den Umständen festmachen, die die von ihm zu bewertende Tat kennzeichnen. Allein auf diese Weise kann ein angemessener Einstieg in den Vorgang der Strafzumessung sowie eine Berücksichtigung der Spezifika des Einzelfalls gelingen.[35]

Auch der Rechtsprechung lässt sich die Relevanz des Vergleichs mit früheren Entscheidungen innerhalb der Strafhöhenbemessung im Einzelfall entnehmen. Danach liegt ein Rechtsfehler vor, wenn ein Instanzengericht eine verglichen mit dem „üblichen [sic]" „außergewöhnlich hohe Strafe" verhängt, ohne dies gesondert zu rechtfertigen.[36] Eine Orientierung an Erwägungen anderer Richter soll insbesondere im Bereich der Massenkriminalität zulässig sein.[37] Gleichwohl werden gegen das Modell der komparativen Strafzumessung Einwände erhoben. Diese klingen bereits unterschwellig in der Forderung an, die Fälle müssten stets vergleichbar sein.[38] Auch betont der *BGH*, dass der Strafrichter durch den Vergleich nicht von der Pflicht befreit wird, sich eine eigene Meinung über die Schuld des Angeklagten und die angemessene Strafe zu bilden.[39] Zudem konstatiert der *BGH*, dass eine umfassende Würdigung im Sinne von § 46 Abs. 1 StGB die Berücksichtigung sämtlicher Nuancen des Einzelfalls verlangt.[40] Dies sei durch den bloßen Vergleich des eigenen Falls mit der Urteilsbegründung in einem anderen Fall aber kaum möglich. Denn einerseits gibt letztere nicht alle Strafzumessungserwägungen wieder, sondern nur solche, die schlussendlich „bestimmend" waren (§ 267 Abs. 3 S. 1 Hs. 2 StPO).[41] Andererseits ist aus der Begründung nicht ohne Weiteres ersichtlich, wie stark einzelne Kriterien ausgeprägt waren, beispielsweise wie glaubhaft und umfassend ein Geständnis des Täters tatsächlich war.[42]

Dem *BGH* ist im Grundsatz zuzustimmen. Allerdings handelt es sich bei dessen Ausführungen bei näherem Hinsehen um keine echte Kritik am Konzept der komparativen – vergleichenden – Strafzumessung. Es ist eine Selbstverständlichkeit, dass Unvergleichbares nicht verglichen werden kann – aus dem dabei allein möglichen *Ab*gleich können keine Rückschlüsse für den jeweils anderen Fall gezogen werden (außer eben demjenigen, dass eine Orientierung am Abgleichsobjekt nicht möglich ist). Der *BGH* bringt insofern treffend zum Ausdruck, worauf es bei einem sachlich angemessenen Vergleich ankommt: Die Vergleich*barkeit* der Fälle. Es ist aber mitnichten davon auszugehen, dass diese unter keinen Umständen je besteht. Sie ist vielmehr durchaus dann gegeben, wenn sich der Vergleich auf diejenigen Aspekte beschränkt, in denen die Sachverhalte wertend betrachtet übereinstimmen. Geht es beispielsweise um zwei Fälle eines einfachen Diebstahls, bei denen jeweils ein Schaden in Höhe von 50 € verursacht wurde, wohingegen der Täter in einem Fall planvoll vorging, im anderen Fall nur die bloße Gunst eines unbeobachteten Augenblicks ausnutzte, so beschränkt sich die Vergleichbarkeit auf die Schadenshöhe. Infolge der Unterschiede bei der festzustellenden kriminellen Energie kann sich das Strafmaß des zweiten nicht einfach am Strafmaß des ersten Falls orientieren. Dennoch hat letzterer eine (beschränkte) Aussagekraft: Im Vergleich mit weiteren Fällen lässt sich ihm entnehmen, welchen Einfluss eine Schadenshöhe von 50 € unter Ausblendung weiterer Erwägungen auf das Strafmaß hat.

Um allerdings auf diese Weise Strafgerechtigkeit herzustellen, kommt es auf *einen* Umstand in besonderer Weise an: Der Vergleichsfall darf kein willkürlich seitens eines einzelnen Strafrichters gewählter sein. Dies betrifft zum einen die vertikale Strafgerechtigkeit im Sinne der Gleichbeurteilung sachlich gleich gelagerter Fälle *durch diesen Richter.* Er darf daher nicht in jeder neuen Strafzumessungsentscheidung einen anderen Vergleichsfall wählen, den er zum Ausgangspunkt seiner Überlegungen nimmt.[43] Ebenso kann horizontale Strafgerechtigkeit allein unter der Voraussetzung hergestellt werden, dass eine gewisse

---

33 *Freund,* GA 1999, 509 (536).

34 Siehe schon *Freund,* GA 1999, 509 (536 m. Fn. 100) dazu, dass die beste Akzeptanzerwartung allein die in der Mitte liegende Strafe, nicht etwa eine Strafe am unteren Rand der Schuldangemessenheit (so aber *Grasnick,* JA 1990, 81 [87]) aufweist. Dabei kennzeichnet die „Mitte", dass es um die Streubreite faktisch anzutreffender Einzelfallbewertungen geht. Weil die „goldene Mitte" am ehesten dem entspricht, was auch vom Verurteilten und der Gemeinschaft als „richtig" akzeptiert wird, ist eine Orientierung an Extremen zu vermeiden.

35 So auch *Meier,* Sanktionen (Fn. 8), S. 238, 257.

36 *BGH,* StV 1986, 57 (57); ebenso *BayObLG,* JR 2002, 166 (167); vgl. *BGH,* StV 1995, 173 (173 f.) und *Meier,* Sanktionen (Fn. 8), S. 241. Ähnlich auch *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 120, 201; *Miebach/Maier,* in: MüKo, 3. Aufl. (2016), § 46 Rn. 90. Ausführlich zur Kontrolle der Üblichkeit durch den *BGH Maurer*, Komparative Strafzumessung, 2005, S. 139 ff.

37 *BGH,* NJW 1979, 1666 (1667); einschränkend *BGH,* NJW 2011, 2597 (2599).

38 *BGH,* NStZ-RR 1997, 196 (197); NJW 1979, 1666 (1667); ebenso *Meier,* Sanktionen (Fn. 8), S. 238.

39 *BGH,* NJW 2011, 2597 (2599); NStZ-RR 1997, 196 (197); Urt. v. 7.1.1992 – 5 StR 614/91; NJW 1979, 1666 (1667 f.).

40 *BGH,* NJW 1973, 1805 (1806). Gegen eine Orientierung am praktisch häufigsten Fall auch *BGH,* NJW 1976, 2355 (2355). Auch *Meier,* Sanktionen (Fn. 8), S. 241 bejaht die fortbestehende Notwendigkeit der Berücksichtigung der individuellen Umstände des jeweiligen Falls.

41 Zum Maßstab siehe *Miebach/Maier,* in: MüKo, § 46 Rn. 84, 302, 314.

42 Allgemein zum Problem sprachlicher Unschärfe für Vergleiche *Maurer,* Strafzumessung (Fn. 36), S. 181.

43 Siehe dazu, dass es sich hierbei um einen Verstoß gegen den Gleichheitssatz des Art. 3 GG handelte, *Sarstedt,* in: Verhandlungen des 41. Deutschen Juristentages, II, 1956, D 29, 32.

Übereinstimmung im Hinblick darauf besteht, was bereichsspezifisch als „Leitfall" eingestuft werden kann. Hierbei handelt es sich um besonders häufig auftretende Fälle, die in den strafzumessungsrelevanten Eigenschaften übereinstimmen. Damit sind zum Beispiel auch innerhalb der Diebstahlsfälle nach § 242 StGB bestimmte Erscheinungsformen als Untergruppen zu bilden. Nach normativer Absicherung der Differenzierung zwischen solchen „Leitfällen" kann dann mit den Untergruppen weitergearbeitet werden. Vereinfacht gesprochen, müssen sich sämtliche Strafrichter *in Deutschland* in einem ersten Schritt an einem gemeinsamen Fall eines bestimmten Deliktstyps als Einstieg für ihre Strafzumessungserwägungen orientieren. An dieser Stelle zeigen sich freilich die eigentlichen Probleme der Umsetzung einer komparativen Strafzumessung und damit der Realisierung von mehr Strafgerechtigkeit.

1. Bestimmung des strafzumessungsrechtlichen Einstiegsfalls anhand rechtlich anerkennenswerter gesellschaftlicher Wertvorstellungen

Die Gewichtung individuellen Verhaltensunrechts geht mit einer besonderen Herausforderung für den zur Rechtskonkretisierung Aufgerufenen einher. An diesem Punkt seiner rechtlichen Beurteilung des Falles kommt er nicht umhin, eine Komponente einzubeziehen, die die Bedeutung von Strafurteilen in ihrer Funktion der (Wieder-)Herstellung des Rechtsfriedens nach einer begangenen Straftat *für den davon Betroffenen sowie die rechtlich verfasste Gemeinschaft* in spezifischer Weise unterstreicht. Wieviel individuelles Unrecht *wiegt,* hängt auch von den rechtlich anerkennenswerten Bewertungsmaßstäben derjenigen Gesellschaft ab, in der es sich ereignet hat.[44] Der Strafrichter muss daher innerhalb der Strafzumessungsentscheidung den Blick auf die allgemeinen Wertvorstellungen weiten, soweit diese rechtlich akzeptabel sind. Umso besser er als Seismograph im Hinblick auf eine solche Gewichtung von Verhaltensunrecht auftritt, desto mehr gelingt durch sein Urteil die (Wieder-)Herstellung des Rechtsfriedens durch Akzeptanz seiner Entscheidung.

Dabei sei zur Klarstellung betont, dass es an dieser Stelle nicht darum gehen darf, die Bestrafung des Täters in den Zweck zu stellen, Effekte bei Dritten im Sinne der Abschreckung oder Erziehung herbeizuführen.[45] Anderenfalls verkäme der Einzelne zum bloßen Mittel zum Zweck, was nicht in Einklang steht mit seiner verfassungsrechtlich garantierten Menschenwürde. Wenn hier also die Rede davon ist, dass der Richter die Bewertung des individuellen Fehlverhaltens von den rechtlich anerkennenswerten gesellschaftlichen Wertvorstellungen abhängig machen muss, ist damit nicht gemeint, dass auf einen bestimmten Zustand innerhalb der Rechtsgemeinschaft in spezifischer Weise – entgegenwirkend – reagiert werden soll. Mit der Gewichtung des individuellen Fehlverhaltens hat es nichts zu tun, wenn sich beispielsweise ähnliche Taten in der jüngeren Vergangenheit häufen, sodass eine besonders harte Bestrafung unter Umständen den Effekt zeitigen könnte, die übrigen Gesellschaftsmitglieder daran zu erinnern, wie wichtig die Normeinhaltung (auch) in diesem Bereich ist. (Richtige) Strafzumessung darf nicht mit der Gestaltung gesellschaftlicher Verhältnisse verwechselt werden.

Was allerdings (nicht zuletzt)[46] innerhalb der Strafzumessung durchaus von Bedeutung ist, sind Veränderungen im Hinblick auf allgemeine Wertvorstellungen: ob beispielsweise der Angriff auf die Ehre einer Person durch eine bestimmte Äußerung nach wie vor ebenso schwerwiegend eingestuft wird oder nicht. Diese Einschätzungen können sich mit der Zeit verändern, worauf auch der Richter zu reagieren und seine Bewertung entsprechend anzupassen hat. Komparative Strafzumessung bedeutet vor diesem Hintergrund keine Festschreibung eines bestimmten Zustandes.[47] Die Beurteilung, dass es sich bei einer spezifischen Tatbegehungsvariante um den strafzumessungsrechtlichen Einstiegfall handelt, ist nicht in Stein gemeißelt. Sie ist ihrerseits der Anpassung an künftige Entwicklungen zugänglich, die durch allgemein geänderte, rechtlich anerkennenswerte Bewertungsmaßstäbe ausgelöst werden kann. Vor diesem Hintergrund kommt auch eine blinde Übernahme fremder Erwägungen nicht in Betracht.[48] Der Vergleich mit anderen Strafmaßen kann immer nur eine (kritische) Orientierungshilfe für die eigene Entscheidung, niemals aber deren Determinierung sein.

2. Defizite empirischer Erkenntnisse zum strafzumessungsrechtlichen Einstiegsfall

In der Theorie lässt sich daher durchaus eine Methode benennen, die eine größere Strafgerechtigkeit in die deutsche Strafzumessungspraxis hineintragen kann. Verkürzt lässt sich dies wie folgt darstellen: Der Strafrichter muss diejenigen Faktoren zunächst abstrakt benennen, die bei einer spezifischen Deliktsbegehung für das Tatgewicht eine Rolle spielen. Er hat dann zu analysieren, wie solche Fälle durch andere Gerichte bewertet werden und kann daraus ableiten, was verbreitet als angemessen empfunden wird. So kann er die Erkenntnis erlangen, welche Tatbegehungsvariante durchschnittlich als bereichsspezifisch typischer Fall der Deliktsverwirklichung eingestuft und besonders häufig in einer bestimmten Weise geahndet

44 *Freund,* GA 1999, 509 (536).

45 Zur Dysfunktionalität entsprechender Strafzwecke innerhalb eines Tatstrafrechts siehe *Rostalski,* Tatbegriff (Fn. 14), S. 36 ff., 49 ff.

46 Geänderte gesellschaftliche Wertvorstellungen können, soweit sie rechtliche Anerkennung verdienen, auch in anderen Bereichen des Strafrechts Bedeutung erlangen. Zu denken ist allein an die Ebene der Strafbegründung: Die *Strafbarkeit* des Ehebruchs (§ 172 StGB i.d.F. bis zum 1.9.1969) wird von den meisten derzeit als unangemessene Reaktion auf ein Verhalten angesehen, das zumindest moralisch von vielen nach wie vor verurteilt wird. Die Aufhebung der Strafbarkeit deckt sich mit dieser veränderten gesellschaftlichen Einschätzung.

47 Siehe zu dieser Befürchtung aber *Maurer,* Strafzumessung (Fn. 36), S. 182.

48 *Maurer,* Strafzumessung (Fn. 36), S. 182 spricht von der Notwendigkeit „revisionsfeste[r] Sanktionsalternativen". Siehe ferner die Nachweise in Fn. 39.

wird. Für die Beurteilung seines eigenen Falles kann er sich nunmehr hieran orientieren. Dabei gilt es insbesondere, die Spezifika seines Entscheidungsgegenstandes herauszuarbeiten und zu bestimmen, ob es sich dabei um Gründe handelt, die ein Abweichen nach oben oder nach unten ausgehend von dem strafzumessungsrechtlichen Einstiegsfall rechtfertigen.

In der Praxis fehlt es den Strafrichtern allerdings in großem Umfang an der Möglichkeit, sich Zugang zu entsprechenden empirischen Erkenntnissen zu verschaffen.[49] Die gängige Praxis an deutschen Gerichten, zumindest gewisse „Haustarife" festzulegen,[50] kann als Ausdruck des Fehlens empirischer Daten über den eigenen Einflussradius hinaus gewertet werden. Sie sollte insofern auch nicht vorschnell verurteilt werden. Der Sache nach handelt es sich dabei um den Versuch, jedenfalls in einer gewissen Reichweite, horizontale Strafgerechtigkeit herzustellen.[51] Dass die regionalen „Haustarife" unter Umständen nicht mit den Üblichkeiten in anderen Regionen übereinstimmen, ist vor diesem Hintergrund keine böse Absicht, sondern lediglich die Folge des Umstands, dass entsprechende Einsichten für den einzelnen Richter kaum zu erzielen sind.

Gründe dafür, weshalb es an entsprechenden Erkenntnismöglichkeiten fehlt, sind vielschichtig. In erster Linie hängt dies damit zusammen, dass eine Erfassung der Entscheidungen von Ausgangsgerichten in den gängigen juristischen Datenbanken in der Breite nicht erfolgt. Es ist daher für einen Hamburger Richter nicht ohne Weiteres durch einen Blick in juris oder beck-online möglich, zu prüfen, wie ein Münchener Gericht in einem Fall des einfachen Diebstahls einer Sache im Wert von 50 Euro entschieden hat. Wollte er sich hierüber Klarheit verschaffen, bedürfte es gesteigerter Mühen, die – die entsprechende Bereitschaft des Einzelnen unterstellt – nicht selten bereits an den föderalen Strukturen und der chronischen Überlastung deutscher Gerichte scheitern dürften.

Dabei steht eines fest: Wäre es möglich, eine große Zahl an Urteilen zu betrachten, so ließen sich regionale Unterschiede eliminieren. Aussagekräftig wird ein solcher Vergleich aber erst, wenn die jeweiligen Besonderheiten der betrachteten Fälle berücksichtigt werden.[52] So ließe sich mittels statistischer Verfahren der Einfluss der jeweils enthaltenen Strafzumessungserwägungen auf das Strafmaß isolieren.[53] Ein Vergleich ist dann auch zwischen Fällen möglich, die nicht in allen, sondern nur in manchen Details übereinstimmen. Insofern ist *Meier* zu widersprechen, der annimmt, eine größere Vergleichsmasse erfordere Abstriche bei der Vergleichbarkeit.[54] Das Gegenteil ist der Fall.[55] Die eigentliche Schwierigkeit liegt vielmehr in der Sammlung und Klassifizierung einer hinreichenden Menge an Vergleichsmaterial.[56]

V. Transparenz gegen die Willkür: Datenbanklösung

In der Gerichtspraxis finden sich (zumindest mancherorts) interne Strafmaßtabellen („Haustarife"), die für häufig vorkommende Delikte (wie Diebstahl, einfache Körperverletzung, Verkehrsdelikte) und bestimmte Konstellationen die am Gerichtsort üblichen Taxen oder konkretisierten Strafrahmen enthalten. Teilweise sind diese sogar verschriftlicht.[57] Sie spiegeln die Erwartungen der Richterkollegen an eine „richtige" Entscheidung wider und erzeugen einen gewissen sozialen Konformitätsdruck.[58] Im Ergebnis kann dies zur Vereinheitlichung der Strafzumessung in der jeweiligen Region führen.[59]

Insofern enthält die Praxis schon jetzt komparative Elemente. Diese sind jedoch regional begrenzt.[60] Eine überregionale Berücksichtigung ist nicht möglich, da die „Tarife" nicht öffentlich bekannt sind.[61] Notwendig ist nach dem Gesagten eine umfassende und transparente empirische Grundlage. Hierzu ist mehrfach vorgeschlagen worden, eine bundesweite Datenbank zur Sammlung aller Strafzumessungsentscheidungen zu errichten.[62] Darin sollen die Urteile entsprechend der enthaltenen Zumessungserwägungen klassifiziert werden, sodass anhand der Merkmale des zu entscheidenden Falls die statistische Verteilung des Strafmaßes aufgrund zahlreicher möglichst passender Vergleichsentscheidungen gefunden werden kann.[63] Hieraus soll sich nur eine Orientierungshilfe

---

49 *Grasnick,* JA 1990, 81 (85).

50 Dazu noch unten V.

51 *Grasnick,* JA 1990, 81 (81).

52 Zwar gelingt *Grundies,* in: Hermann/Pöge, S. 295 ff. die Berücksichtigung einer sehr großen Datenmenge von gut 1,5 Millionen Entscheidungen (S. 298). Die Auswertung beschränkt sich aber auf die Daten des BZR (S. 297). Ein solches Vorgehen hat aufgrund der damit einhergehenden Unmöglichkeit, die jeweiligen Einzelfallumstände hinreichend detailliert zu berücksichtigen (vgl. S. 299 f.), nicht die hier erforderliche Aussagekraft. Vgl. zur Bedeutung der Berücksichtigung normativer Unterschiede zwischen den untersuchten Fällen für die Beurteilung regionaler Strafmaßvarianz (insb. bei kleineren Vergleichsgruppen) *Albrecht,* Strafzumessung (Fn. 9), S. 348 ff.

53 Als Beispiel mag hier die Untersuchung von *Albrecht,* Strafzumessung (Fn. 9), S. 612 ff. dienen.

54 *Meier,* Sanktionen (Fn. 8), S. 238.

55 Vgl. auch *Maurer,* Strafzumessung (Fn. 36), S. 182.

56 Vgl. *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 120a; kritisch zur oft unzureichenden empirischen Vergleichsbasis auch *Verrel,* JR 2002, 168 (168). *BGH,* NJW 2011, 2597 (2599) spricht angesichts der praktischen Schwierigkeiten von einer Überforderung der Gerichte durch eine Pflicht zum Vergleich mit anderen Urteilen.

57 *Kudlich/Koch,* NJW 2018, 2762 (2763); *Meier,* Sanktionen (Fn. 8), S. 240. Ein beispielhafter Abdruck aus dem Bereich der Verkehrsdelikte findet sich bei *Schäfer/Sander/van Gemmeren*, Praxis der Strafzumessung, 6. Aufl. (2017), Rn. 1720 ff.

58 Vgl. *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 120. Diese Besonderheit interner Richtlinien übersieht *Maurer,* Strafzumessung (Fn. 36), S. 177.

59 Zur Bedeutung informeller „Tarife" für die Strafzumessungsentscheidung *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 119 m.w.N.

60 *Meier,* Sanktionen (Fn. 8), S. 240; *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 119; vgl. bereits *Dreher,* MDR 1961, 343 (344). Zu den Variationen in der Strafzumessung siehe oben unter II.

61 *Meier,* Sanktionen (Fn. 8), S. 240; kritisch dazu (bezogen auf interne Richtlinien der StA) *Kinzig,* in: Schönke/Schröder, § 46 Rn. 72.

62 Entsprechende Forderungen finden sich bei *Kaspar,* Sentencing Guidelines (Fn. 6), C 115; *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 202.

63 *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 202.

ergeben, nicht aber die Einzelfallentscheidung unter Berücksichtigung der Besonderheiten des jeweiligen Falls ersetzt werden.[64]

Das Problem besteht auch hier in der Datengrundlage. Bisher ist eine solche nicht in hinreichendem Umfang vorhanden – sieht man einmal von den oben erwähnten internen Richtlinien ab.[65] Die Erstellung wäre wiederum extrem aufwendig, da sämtliche Urteile des für maßgeblich erachteten Zeitraums erfasst und händisch entsprechend den in den Texten enthaltenen Erwägungen klassifiziert werden müssten. Dies könnte für neue Urteile zwar unmittelbar durch die entscheidenden Gerichte geschehen, würde aber auch insofern eine Mehrbelastung bei ohnehin schon angespannter Personalsituation bedeuten.

VI. Legal-Tech-basierte (automatisiert erstellte) Datenbanklösung

Die Lösung für dieses Problem besteht in der automatisierten Erstellung der Datenbank mittels Legal Tech.[66] Dazu ist eine Software nötig, die nach Eingabe der Urteile die darin enthaltenen Strafzumessungserwägungen erkennt, mit den hierauf beruhenden Strafmaßen in Verbindung bringt und die Relation aus beidem in eine Datenbank schreibt. Diese Datenbank kann dann zur Abfrage detaillierter Statistiken aufgrund der jeweiligen Zumessungskriterien genutzt werden, wobei mittels statistischer Verfahren bei hinreichend großer Datenmenge auch Zusammenhänge zwischen Zumessungserwägungen gefunden werden können, die sich nicht unmittelbar aus dem Vergleich zweier Urteile ergeben.[67]

Wesentliche technische Schwierigkeit ist dabei die Erkennung der Zumessungserwägungen durch das Programm. Denn selbst die fortschrittlichste „künstliche Intelligenz" kann (zum jetzigen Zeitpunkt) nicht wirklich *verstehen*, worum es in einem Text geht.[68] Jedoch haben sich KI-Systeme als außerordentlich nützlich gezeigt, wenn es um das Auffinden von Korrelationen und Mustern in großen Datenmengen geht.[69] Hier hilft die relativ formale und gleichförmige Struktur von Strafurteilen weiter. Zwar macht § 267 StPO keine detaillierten Vorgaben für den Aufbau eines Urteils. In der Praxis ist es aber üblich, die Zumessungserwägungen gebündelt in einem eigenen Abschnitt zu benennen und näher darzulegen. Dabei werden häufig sehr ähnliche Formulierungen verwendet, wie etwa „zu Gunsten des Angeklagten [wurde] berücksichtigt, dass", „gegen den Angeklagten spricht" usw.[70] Die Variationen in den Formulierungen lassen sich mittels Natural Language Processing (NLP) erfassen.[71] Die Unterscheidung, welche Angaben im Urteil zur Strafzumessung gehören und welche nicht, erfolgt anhand des Kontextes solcher Formulierungen.

Bedeutsam für die Entnahme der Zumessungserwägungen aus dem Text der Urteilsbegründung ist naturgemäß, dass sie dort *vollständig* aufgezählt sind. § 267 Abs. 3 S. 1 Hs. 2 StPO enthält jedoch eine Beschränkung auf die „bestimmend[en]" Erwägungen. Nicht alles, was in irgendeiner Form bei der Strafzumessung berücksichtigt worden ist, muss sich also zwingend auch im Urteil wiederfinden.[72] Beim Vergleich mehrerer Urteile ist aber ohnehin eine gewisse Pauschalisierung und Fokussierung auf wichtige Faktoren notwendig. Die Berücksichtigung von Feinheiten kann nur anhand der Umstände des konkreten Falls erfolgen. Angesichts der überragenden empirischen Bedeutung einiger weniger Faktoren[73] erscheint dies auch hinnehmbar. Schwerer wiegt eine Abkürzung der Urteilsgründe gemäß § 267 Abs. 4 StPO – hier können die Strafzumessungserwägungen ganz oder teilweise entfallen. Derartige Urteile können für eine vergleichende Strafzumessung daher nicht oder allenfalls eingeschränkt berücksichtig werden.[74]

In der Praxis hat sich gezeigt, dass die Begründungen, die im Urteilstext angegeben werden, in Wahrheit nicht unbedingt auch (den erwarteten) Einfluss auf die Strafhöhe haben. So ist ein Teil der Erwägungen offenbar gänzlich wirkungslos, manche eigentlich strafmildernde Angaben korrelieren sogar mit erhöhten Strafen.[75] Auch derartige Befunde sprechen aber nicht gegen ein vergleichendes Vorgehen, solange sie im Rahmen dieser Methode aufgedeckt werden. Hier zeigt sich erneut, wie wichtig die Einbeziehung großer Datenmengen ist. Aussagekräftig bleiben die Ergebnisse trotzdem, da die im Urteil enthaltenen Erwägungen „im Kern" tragend sind.[76]

Neben den Zumessungserwägungen und dem Strafmaß sollte die Datenbank auch die zugehörigen Urteile selbst enthalten. So können die Anwender die gefundenen Ergebnisse überprüfen und insbesondere nach Besonderheiten gegenüber dem ihnen vorliegenden Fall suchen. In

---

64 *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 202.

65 Vgl. zum parallelen Problem bei der Schaffung einer Strafzumessungskommission *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 120a.

66 „Legal Tech" ist die Kurzform für „Legal Technology", also die Unterstützung juristischer Tätigkeiten durch automatisierte Informationsverarbeitung, siehe dazu *Groh,* in: Weber, Creifelds kompakt, Rechtswörterbuch, 2019 (Stichwort „Legal Tech"); ähnlich *Wagner*, Legal Tech und Legal Robots, 2018, S. 1, dort auch zu verschiedenen Klassifikationen (S. 6 ff.).

67 Vgl. dazu bereits oben unter IV.2.

68 Vgl. zu „Information Retrieval"-Systemen *Wagner,* Legal Tech (Fn. 66), S. 24, aber auch S. 33 f. zur angeblich abweichenden Konzeption bei IBMs „Watson". Insofern ähnlich *Frese,* NJW 2015, 2090 (2091). Jedoch stellt auch Watson letztlich nur Zusammenhänge her, ohne den tatsächlichen Sinn einer Aussage zu erfassen, vgl. *High,* The Era of Cognitive Systems: An Inside Look at IBM Watson and How it Works, S. 5.

69 Siehe z.B. *Lu/Li/Chen/Kim/Serikawa,* Mobile Netw Appl 23 (2018), 368 (369); *Hopgood,* Computer 36 (2003), 24 (26).

70 Die Zitate entstammen dem Urteil des *LG Verden* vom 18.3.2010 – 1 KLs 17/09.

71 Zum Einsatz von NLP bei juristischen Texten siehe etwa *Chalkidis/Kampas,* Artificial Intelligence and Law 27 (2019), 171.

72 *Miebach/Maier,* in: MüKo, § 46 Rn. 84, 302, 314.

73 Laut *Meier,* Sanktionen (Fn. 8), S. 256 und *Kinzig,* in: Schönke/Schröder, § 46 Rn. 72 (jeweils m.w.N.) hängt die Strafhöhe statistisch insbesondere von der Tatschwere (etwa der Schadenshöhe beim Diebstahl) und den Vorstrafen des Täters ab.

74 *BGH,* NJW 2011, 2597 (2598).

75 *Albrecht,* ZStW 102 (1990), 596 (620 ff.). Angesichts der Divergenz von geschriebenen Erwägungen und tatsächlicher Strafhöhenermittlung spricht *Maurer,* Strafzumessung (Fn. 36), S. 179 von der Strafzumessungstheorie als „reine[r] Begründungswissenschaft".

76 *Albrecht,* ZStW 102 (1990), 596 (626).

Anlehnung an *Streng* folgt hieraus ein zweistufiges Vorgehen: Zunächst wird anhand besonders wichtiger und universalisierbarer Merkmale nach dem üblichen Strafmaß in insofern vergleichbaren Fällen gesucht, wobei das System im besten Fall die Möglichkeit bietet, den Einfluss der angegeben Merkmale zu isolieren. In einem zweiten Schritt erfolgt dann eine Individualisierung der Strafe anhand der beim Vergleich nicht berücksichtigten Merkmale des konkreten Falls und der Unterschiede zu den Vergleichsfällen.[77]

Hier besteht nun der Vorteil, dass die digitale Unterstützung die Auswertung größerer Datenmengen ermöglicht. Folglich ist keine zu starke Beschränkung auf wenige Vergleichsmerkmale nötig. Gleichwohl muss sich auch dieses System auf quantifizierbare Merkmale fokussieren.[78] Das können neben konkreten Zahlenwerten (etwa die Schadenshöhe beim Betrug) auch binäre Variablen wie die Existenz eines Geständnisses, einschlägiger Vorstrafen oder von Verfahrensverzögerungen sein, wobei jeweils auch feinere Abstufungen (Glaubhaftigkeit und Reue, Dauer und Ursache von Verzögerungen etc.) möglich sind. Nur schwer erfassbar werden aber auf absehbare Zeit komplexere Erwägungen etwa bezüglich einer besonderen kriminellen Energie, eines Mitwirkens des Opfers oder Ähnlichem sein. Insofern zeigt sich die besondere Bedeutung der Individualisierung der Strafe auf *Strengs* zweiter Stufe, da solche nicht quantifizierbaren Merkmale in bestimmten Situationen andere Erwägungen sogar deutlich überwiegen können. So wird auf diese Weise letztlich auch der Forderung des *BGH* Rechnung getragen, beim Vergleich mit anderen Urteilen tatsächlich sämtliche Umstände zu berücksichtigen.[79] Eine unkritische Übernahme fremder Überlegungen zu einer anderen Tat darf auch bei komparativem Vorgehen nicht erfolgen.[80]

Soll die Datenbank Urteile im Volltext enthalten, müssen diese anonymisiert werden (vgl. Art. 10 S. 1 DSGVO[81]). Damit müssen zumindest der Name und sonstige Daten jedenfalls des Angeklagten entfernt werden, aufgrund derer dieser eindeutig identifiziert werden kann. Um die Identifikation auch unter Zuhilfenahme weiterer Informationen zu vermeiden, wird es außerdem notwendig sein, Orts- und Zeitangaben sowie Informationen zu Zeugen, Mittätern etc. zu schwärzen.[82] Auch hier kann Legal Tech die Arbeit wesentlich erleichtern, denn auch Daten dieser Art können aufgrund ihres Kontextes durch KI erkannt und automatisiert aus den Urteilen entfernt werden.

Die Vorteile einer in dieser Form erstellten Datenbank für Gerichte und sonstige Rechtsanwender dürften auf der Hand liegen. Vergleiche mit anderen Urteilen sind ein ohnehin genutztes Mittel, es fehlt jedoch eine zuverlässige Datengrundlage.[83] Gleiches gilt aber auch für die Kontrolle der Strafzumessung durch die Revisionsgerichte,[84] die bei der Ermittlung des Üblichen bisher überwiegend nur auf ihr subjektives Empfinden und ihre eigenen Erfahrungen rekurrieren (können).[85] Hinzu kommt das Interesse von Staatsanwaltschaften und Strafverteidigern an Transparenz hinsichtlich der zu erwartenden Strafen.[86] Insbesondere für die Verteidigung dürfte vielfach die Prozessstrategie davon abhängen, wie sich welche Erwägungen durchschnittlich auswirken – gerade auch, wenn diese Auswirkungen regional variieren. Schließlich ist auch das wissenschaftliche Interesse an einer flächendeckenden Erhebung über die Unterschiede und Gemeinsamkeiten bei der Strafzumessung nicht zu unterschätzen.

Problematisch ist derzeit noch die Verfügbarkeit von Rohdaten. Insbesondere Algorithmen, die auf Verfahren des maschinellen Lernens basieren, benötigen einen großen Pool an Trainingsdaten. Frei verfügbare Urteile gibt es zwar in großer Zahl, jedoch stammen diese meist nur von Obergerichten und enthalten damit keine oder nicht die vollständigen Strafzumessungserwägungen. Spätestens für eine flächendeckende und repräsentative Erhebung sind ohnehin Urteile aller deutschen Gerichte notwendig, ohne dass diese in irgendeiner Form gefiltert werden dürften.

VII. Schluss

Es gibt in Deutschland erhebliche Abweichungen der Strafzumessungsentscheidungen, die sich nicht durchweg durch sachliche Unterschiede in den zugrundeliegenden Fällen rechtfertigen lassen. Vielmehr spielen sowohl die individuelle Richterpersönlichkeit als auch der Entscheidungsort eine nicht unerhebliche Rolle für das konkrete Strafmaß. Dabei gilt es als offenes Geheimnis, dass innerhalb mancher Richterkollegien interne Orientierungshilfen verwendet werden, die zu einer einheitlicheren Straf-

77 Vgl. *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 120; zustimmend *Meier,* Sanktionen (Fn. 8), S. 238 f.

78 Zu einer solchen Beschränkung i.R.e. Datenbanklösung auch *Kaspar,* Sentencing Guidelines (Fn. 6), C 115.

79 Vgl. *BGH,* NJW 2011, 2597 (2598).

80 Vgl. die Nachweise in Fn. 39.

81 Zum hieraus grundsätzlich folgenden Behördenvorbehalt für nicht anonymisierte Daten über strafrechtliche Verurteilungen siehe *Bäcker,* in: BeckOK, 28. Ed. (2019), Art. 10 DSGVO Rn. 7 m.w.N. auch zur Gegenauffassung.

82 Angesichts der hohen Individualität von Strafurteilen besteht aber u.U. weiter die Möglichkeit, die geschwärzten Urteile den Originalen zuzuordnen (unterstellt, die Originale sind verfügbar). Ob daher tatsächlich von einer Anonymisierung oder lediglich von einer Pseudonymisierung gesprochen werden kann und ob eine solche den Anforderungen der DSGVO genügt, kann hier nicht entschieden werden. Zu den hohen Anforderungen an die Anonymisierung personenbezogener Daten siehe *Karg,* in: Simitis/Hornung/Spiecker genannt Döhmann, 2019, Art. 4 Nr. 1 DSGVO Rn. 57 ff.

83 Siehe oben unter V.

84 *Streng,* in: Kindhäuser/Neumann/Paeffgen, § 46 Rn. 202; *Kaspar,* Sentencing Guidelines (Fn. 6), C 115.

85 Vgl. etwa *BGH,* StV 1995, 173 (173 f.); StV 1986, 57 (57); als Gegenbeispiel darf *BayObLG,* JR 2002, 166 (167) gelten. Zum Ganzen *Verrel,* JR 2002, 168 (168).

86 Auch *Kinzig,* in: Schönke/Schröder, § 46 Rn. 72 m.w.N. fordert die Bekanntgabe der internen Zumessungsmaßstäbe gegenüber den übrigen Verfahrensbeteiligten, bezieht sich dabei allerdings auf die StA.

zumessung führen sollen. Der Vergleich mit anderen Tatbegehungsvarianten ausgehend von einem bereichsspezifisch typischen Einstiegsfall ist als Methode zur Herstellung von Strafgerechtigkeit grundsätzlich vorzugswürdig. Er setzt aber voraus, dass es einen *gemeinsamen* Fixpunkt gibt, der sämtliche Strafzumessungsentscheidungen bestimmt – und nicht bloß diejenigen in einzelnen Regionen des Landes. Gegenwärtig lässt sich dies allerdings aufgrund der fehlenden Transparenz der regionalen „Haustarife" sowie des eingeschränkten Zugangs zu den Entscheidungen der Ausgangsinstanzen kaum umsetzen. Hier kann eine umfassende Datenbank Abhilfe schaffen. Diese händisch zu erstellen, erscheint angesichts der knappen Ressourcen der Justiz nahezu ausgeschlossen. Dank der zunehmenden Möglichkeiten der Informationstechnologie könnte dieser Schritt in Zukunft aber entfallen. Automatisierte Analysemethoden sind heute in der Lage, auch komplexe Zusammenhänge aus Texten in natürlicher Sprache zu extrahieren. Mittels auf diese Weise gewonnener Daten ließe sich die Intersubjektivität der Strafzumessungserwägungen ebenso verbessern wie ihre Transparenz. *Dreher* kann daher im Hinblick auf seine Kritik am geheimen „Metermaß" des Richters darin zugestimmt werden, dass Geheimnistuerei in diesem Bereich besonders fehl am Platze ist. Einen „Fixpunkt" muss es aber geben – und zwar einen gemeinsamen. Um diesen zu finden, bedarf es entsprechender Forschung, die nicht zuletzt der hohen Bedeutung der Strafgerechtigkeit für die Akzeptanz von Strafurteilen Rechnung trägt.[87]

[87] Siehe zu einem solchen Projekt http://legaltechcologne.de/strafzumessung-mit-legaltech-transparent-machen-smart-sentencing-database; https://www.rostalski.jura.uni-koeln.de/sites/strafrechtprof2/Dokumente/Smart_Sentencing_Pressemitteilung_des_Lgal_Tech_Lab_Cologne.pdf (zuletzt abgerufen am 3.9.2019).

Strafbarkeit und Strafverfolgung des Betreibens internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen

*von Prof. Dr. Mark A. Zöller**

Abstract
Vor dem Hintergrund spektakulärer Strafverfahren gegen die Betreiber von Foren und Handelsplattformen für illegale Waren und Dienstleistungen im Darknet ist aktuell eine intensive rechtspolitische Debatte über die Notwendigkeit entbrannt, das Anbieten bzw. Zugänglichmachen von internetbasierten Leistungen zur Begehung von Straftaten eigenständig mit Strafe zu bedrohen. Der vorliegende Beitrag stellt zunächst die besonderen Rahmenbedingungen von Ermittlungen im Darknet dar und wirft vor diesem Hintergrund einen kritischen Blick auf die aktuellen Vorschläge des Bundesrates sowie des Bundesministeriums des Innern, für Bau und Heimat zur Einführung eines neuen § 126a StGB. Er gelangt zu dem Ergebnis, dass die damit vorgelegten Regelungskonzepte mit zahlreichen Widersprüchlichkeiten behaftet sind und ihnen der Nachweis tatsächlich bestehender Strafbarkeitslücken bislang nicht überzeugend gelungen ist.

Against the background of numerous spectacular criminal proceedings against operators of forums and trading platforms for illegal goods and services on the internet a lively debate has flared up on the necessity for imposing criminal sanctions for offering or making available internet-based services for committing criminal offenses. The article at hand starts by presenting the special conditions for criminal investigations within the so-called darknet. It takes a critical look at the current legislative proposals by the German Federal Assembly and the Federal Ministry of the Interior for the introduction of a new paragraph 126a to the German Criminal Code. As a result, the regulation concepts presented so far seem to include several contradictions and their protagonists have been unable to present proof for the existence of actual loopholes in criminal liability.

I. Die aktuelle Situation

In den Medien überschlagen sich derzeit die Berichte darüber, was man im sog. Darknet alles anonym ordern kann:[1] *Waren* wie Betäubungsmittel,[2] Waffen und Munition, Hacker-Programme, gefälschte Dokumente wie Reisepässe, Personalausweise oder Führerscheine und kinderpornografisches Material, aber auch illegale *Dienstleistungen* wie die Anmeldung von Wohnsitzen, Fahrzeugen, Bankkonten, die Entwicklung und Verbreitung von Schadsoftware, die Vermietung von Bot-Netzen und sogar die Ausführung von Auftragsmorden sind für alle, die ernsthaft danach suchen, nur wenige Mausklicks entfernt. Andererseits häufen sich aber auch Berichte über entsprechende Ermittlungserfolge der Strafverfolgungsbehörden. Dazu nur drei Beispiele:[3]

Beispiel 1: Am 22. Juli 2016, erschoss beim sog. Amoklauf von München[4] der zur Tatzeit 18-jährige *David S.* im Olympia-Einkaufszentrum im Stadtteil Moosach neun Menschen und tötete sich anschließend selbst. Bei der Tatwaffe handelte es sich um eine wieder schussfähig gemachte Dekowaffe vom Typ „Glock 17“. Sie war von *David S.* unter dem Pseudonym „Maurächer“ von einem 33-jährigen Marburger Waffenhändler mit rechtsextremistischem Hintergrund und dem Pseudonym „rico“ erworben worden. Der Kontakt zwischen Käufer und Verkäufer war zuvor über das Darknet-Forum „Deutschland im Deep Web“ hergestellt worden.[5]

Beispiel 2: Am 23. und 24. April 2019, haben Kräfte des Bundeskriminalamts drei mutmaßliche Betreiber des Darknet-Marktplatzes „Wall Street Market“ vorläufig festgenommen. Hierbei handelte es sich nach Angaben der Ermittler um die „weltweit zweitgrößte Handelsplattform im Darknet“.[6] Zuletzt waren dort 63.000 Verkaufsangebote, insbesondere für Betäubungsmittel, gestohlene Daten, gefälschte Ausweise und Kreditkarten, gelistet. Die Plattform hatte etwa 5.400 Verkäufer und 1.150.000 Kundenkonten. Bezahlt wurde mit Kryptowährungen wie Bitcoin[7] oder Monero. Das Umsatzvolumen soll bei 40 Mio. Euro gelegen haben. Von den Transaktionen haben die mutmaßlichen Betreiber der Plattform

* Der Verfasser ist Inhaber des Lehrstuhls für Deutsches, Europäisches und Internationales Strafrecht und Strafprozessrecht sowie Wirtschaftsstrafrecht und Direktor des Instituts für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP) an der Universität Trier.

1 Hierzu etwa *Rath*, DRiZ 2016, 292 (293); *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 (442 f.); *Fünfsinn/Krause*, FS Eisenberg, 2019, S. 641 (643); *Greco*, ZIS 2019, 435 (437 f.).

2 Diese machen den weit überwiegenden Teil der im Darknet gehandelten Güter aus; vgl. *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 (442).

3 Zu weiteren Beispielen, insbesondere den Vorläufern „Silk Road“ und „Alpha-Bay“, s. *Tzanetakis*, APuZ 2017, 41 (43 ff.).

4 Hierzu *Hartleb*, Kriminalistik 2018, 532 ff.

5 Bei „Deutschland im Deep Web“ handelte es sich ursprünglich um ein Forum zur Diskussion und zum Meinungsaustausch. Später wurde u.a. auch eine Unterkategorie „Waffen“ hinzugefügt, die – neben der Veröffentlichung von Diskussionsbeiträgen – dazu genutzt wurde, unerlaubt mit Waffen zu handeln; vgl. *LG Karlsruhe*, StV 2019, 400 (401).

6 Vgl. dazu die Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main und des Bundeskriminalamts v. 3.5.2019, abrufbar unter: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190503_WallStreetMarket.html (zuletzt abgerufen am 10.9.2019).

7 Zum Phänomen Bitcoin *Brenneis*, APuZ 2017, 29 ff.

Provisionen zwischen 2 und 6 Prozent des Verkaufspreises erhalten.

Beispiel 3: Am 28. Juni 2019 schließlich teilte das BKA mit, man habe nach monatelangen Ermittlungen den größten Online-Drogenshop Deutschlands mit der Bezeichnung „Chemical Revolution" abgeschaltet.[8] Elf Tatverdächtige seien wegen des dringenden Tatverdachts des bandenmäßigen Handeltreibens mit Betäubungsmitteln in nicht geringer Menge festgenommen worden. Als Hauptverdächtiger gilt ein aus dem Landkreis München stammender, 26 Jahre alter Mann, der diese Plattform im September 2017 aufgebaut und anschließend mit weiteren Tatverdächtigen gemeinsam betrieben haben soll. Auf der Internetseite des Onlineshops waren Betäubungsmittel und vor allem *synthetische Drogen* wie Ecstasy und Amphetamin zum Verkauf und weltweiten Versand angeboten worden. Auch hier haben die Käufer mit der Kryptowährung Bitcoin bezahlt.

II. Strafrechtliche Ermittlungen im Darknet

Allen drei Beispielen ist gemeinsam, dass es um das Betreiben internetbasierter Plattformen für illegale Waren im sog. Darknet ging. Schon der Begriff dieses Phänomens ist häufig mit Fehlvorstellungen behaftet, die für eine Betrachtung aus juristischer Sicht naturgemäß nicht förderlich sind. Die Bezeichnung als „Darknet", d.h. als „dunkles Netz" suggeriert einen Zusammenhang mit negativen bzw. illegalen Geschehnissen, die besser im Verborgenen bleiben.[9]

1. Das Phänomen „Darknet"

Für viele ist das Darknet daher ein Synonym für die Unterwelt des Internet mit all seinen Schattenseiten.[10] Bei nüchterner Betrachtung stellt es sich zunächst einmal nur als digitaler Raum dar, der mit technologischen Instrumenten abgeschirmt ist und seinen Nutzern ein hohes Maß an Anonymität gewährleistet.[11] Die meisten Dinge, die Menschen jeden Tag im Netz erledigen – Kommunizieren, Musik und Videos abrufen, Einkaufen, Restaurants suchen oder Tickets buchen – finden aber üblicherweise nur im *sichtbaren Teil des Internets* statt, der häufig auch als „Visible Web", „Surface Web" oder „Clearnet" bezeichnet wird. Mit Standardbrowsern wie Firefox, Safari oder Google Chrome erreichen wir nur *frei zugängliche* Webseiten. Auch Suchmaschinen wie Google präsentieren uns in Wirklichkeit gar nicht *alle* vorhandenen Daten zu unserer jeweiligen Suchanfrage, sondern indizieren nicht einmal das Visible Web vollständig. Das Internet gleicht insoweit einem Ozean.[12] In diesem Ozean an Informationen liegen die frei zugänglichen Webseiten unmittelbar an der Wasseroberfläche. Unterhalb dieser sichtbaren Oberfläche folgt sodann das sog. „Deep Web", also der Bereich, der durch Passwörter und Codes geschützt ist. Hierzu zählen z.B. Datenbanken und Archive. Erst auf dem Grund des Ozeans liegt schließlich das Darknet.[13]

Als „Darknet" wird jener Teil des Internets bezeichnet, der durch sog. Peer-to-Peer-Verbindungen (P2P) zwischen Nutzern geschaffen wird und nur unter Zuhilfenahme spezieller Software zugänglich ist.[14] Benötigt werden eine Verschlüsselungsplattform und die genaue Zieladresse der gewünschten Internetseite. Hierfür ist in der Praxis häufig eine vorherige Einladung durch einen bereits als vertrauenswürdig eingestuften Nutzer und eine Bestätigung durch einen Administrator erforderlich. Allerdings existieren auch im frei zugänglichen Teil des Internets Listen mit direkten Links im TOR-Netzwerk.[15] Zudem hält auch das Darknet Suchmaschinen wie Grams, Torch oder Ahmia bereit, die aber im Hinblick auf Schnelligkeit und Nutzerfreundlichkeit nicht mit den aus dem Visible Web bekannten Produkten wie Google vergleichbar sind. Natürlich besitzt die so erreichte Anonymität in besonderem Maße Anziehungskraft für potenzielle Straftäter. Aber weder sind das Darknet selbst noch seine Nutzung per se illegal. Beides ist zunächst nur Ausdruck des Wunsches vieler Internetnutzer, sich im digitalen Raum frei von staatlicher wie privater Kontrolle bewegen zu können. Hierauf sind etwa Dissidenten und Oppositionelle in autokratischen Staaten,[16] Whistleblower oder Journalisten zwingend angewiesen.[17] Es ist auch kein Zufall, dass speziell die Entwicklung des TOR-Browser vor allem durch das US Naval Research Laboratory maßgeblich unterstützt wurde. Schließlich besteht ein nachvollziehbares praktisches Bedürfnis nicht nur US-amerikanischer Streitkräfte und Nachrichtendienste dafür, dass ihre Soldaten und Agenten auch von fremdem Territorium aus unüberwacht mit der eigenen Nachrichtendienstzentrale in der Heimat kommunizieren können.[18] Andererseits zeigt eine im Jahr 2016 veröffentlichte Studie des International Institute for Strategic Studies, dass immerhin 57 Prozent von insgesamt 5205 untersuchten aktiven Seiten im Darknet als illegal einzustufen waren.[19] Nach Angaben des BKA weisen dort rund 50 kriminelle Foren und Plattformen einen Deutschlandbezug auf.[20]

Der größte und bekannteste Teil des Darknets ist das „TOR-Netzwerk".[21] Für den Zugang hierzu ist ein sog.

---

8 Presseeinladung der Generalstaatsanwaltschaft Frankfurt am Main und des Bundeskriminalamts vom 28.6.2019, abrufbar unter: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190628_PMChemicalRevolution.html (zuletzt abgerufen am 10.9.2019).

9 Zur Historie und Definition des Begriffs *Ihwas*, WiJ 2018, 138 (140 f.) m.w.N.

10 *Göppner*, Kriminalistik 2018, 623 (624).

11 Vgl. *Mey*, Darknet: Waffen, Drogen, Whistleblower, 2017, S. 11; *ders.*, APuZ 2017, 4; *Ihwas*, WiJ 2018, 138.

12 Instruktiv hierzu *Göppner*, Kriminalistik 2018, 623 (624).

13 Für eine Einstufung des Darknets als Teil des Deep Webs *Ihwas*, WiJ 2018, 138.

14 *Rath*, DRiZ 2016, 292; *Tzanetakis*, APuZ 2017, 41 (42); *Krause*, NJW 2018, 678; *Fiebig,* DRiZ 2019, 50.

15 *Rath*, DRiZ 2016, 292; *Ihwas*, WiJ 2018, 138 (141); *Greco*, ZIS 2019, 435 (436 f.).

16 Vgl. *Moßbrucker*, APuZ 2017, 16 ff.

17 Vgl. *Fiebig*, DRiZ 2019, 50.

18 Zur Abhängigkeit des Tor-Projekts von US-amerikanischen Regierungszuwendungen *May*, APuZ 2017, 4 (8).

19 Vgl. *Moore/Rid*, Cryptopolitik and the Darknet, 2016.

20 BT-Drs. 18/9487, S. 2; *Vogt,* Die Kriminalpolizei 2/2017, 4 (5); *Krause*, NJW 2018, 678 (679).

21 Allg. hierzu *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 f.; *May*, APuZ 2017, 4 ff.; *Göppner*, Kriminalistik 2018, 623 (624); *Ihwas*, WiJ 2018, 138 (139); *Greco*, ZIS 2019, 435 (436).

TOR-Browser erforderlich. Er steht auf zahlreichen frei zugänglichen Webseiten kostenlos zum Download bereit. Die Abkürzung „TOR" steht für „The Onion Router". Der Name erklärt sich aus der Tatsache, dass ihm ein stufenweises Verschlüsselungsschema zugrunde liegt, das an die Form einer Zwiebel mit ihren Schalen erinnert. Der TOR-Browser kaschiert die IP-Adresse des Ausgangsrechners, indem eine lange Reihe an Verbindungen zu verborgenen Servern ermöglicht wird. Diese Server werden als „Knoten" bezeichnet. Da jeder Knoten das gesendete Datenpaket erneut verschlüsselt, ist es bereits nach dem Passieren von drei Knotenpunkten technisch unmöglich, die Ursprungsadresse nachzuvollziehen. Erst am Ausgangsknoten erfolgt dann eine Entschlüsselung des Datenpaketes, so dass der *Empfänger* dieses ohne Probleme verarbeiten kann.

2. Besonderheiten für strafprozessuale Ermittlungen

Diese technischen Besonderheiten des Darknets haben natürlich auch praktische Folgen für die Ermittlungsarbeit der Strafverfolgungsbehörden.

a) Wirkungslosigkeit technikgestützter Überwachungsmaßnahmen

Wichtig ist zunächst die Erkenntnis, dass die ganz überwiegende Zahl der technikgestützten Zwangsmaßnahmen nach der Strafprozessordnung angesichts der Nutzung von Anonymisierungs- und Verschlüsselungssoftware im Darknet von vornherein aussichtslos ist.[22] Dies gilt insbesondere für „klassische" Telekommunikationsüberwachungsmaßnahmen (§ 100a Abs. 1 S. 1 StPO), Auskünfte über Verkehrs- und Bestandsdaten (§§ 100g, 100j StPO) oder die Beschlagnahme von Servern (§§ 94 ff. StPO). Wenn man nicht weiß, wo sich etwas befindet oder stattfindet, kann man es weder überwachen noch beschlagnahmen. Auch sofern individuelle Benutzerkennungen von Tatverdächtigen bei Darknet-Handelsplattformen oder -Foren öffentlich einsehbar sind, kommen Abfragen von Bestands- oder Nutzungsdaten nach den §§ 14 und 15 des Telemediengesetzes (TMG) bei den entsprechenden Plattformbetreibern *allenfalls hypothetisch* in Betracht. Zum einen sind die unter „Nicknames" operierenden Betreiber solche virtuellen Marktplätze nicht bekannt und infolge der von ihnen verwendeten Verschlüsselungstechnik auch nicht ermittelbar. Zum anderen verweigern diese infolge ihres illegalen Geschäftsmodells regelmäßig ohnehin jede Kooperation mit den Strafverfolgungsbehörden.[23]

Hinzu kommt, dass Kriminelle stets nach digitalen Kommunikationswegen *außerhalb* des Radars von Polizei und Staatsanwaltschaft suchen. So haben etwa die Ermittlungen im Zusammenhang mit dem Amoklauf von München ergeben, dass sich der Täter vor seiner Bluttat mit Gleichgesinnten über die Text- und Videochatfunktion der Spieleplattform „Steam" ausgetauscht hat, auf der jeden Tag allein Hunderttausende den Ego-Shooter „Counterstrike" spielen.[24]

b) Verdeckte Ermittler

Bei Ermittlungen im Darknet erlebt deshalb der Einsatz von Verdeckten Ermittlern eine Renaissance.[25] Bei solchen *Verdeckten Ermittlern* handelt es sich nach der Legaldefinition des § 110a Abs. 2 S. 1 StPO um Polizeibeamte, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität, einer sog. Legende, ermitteln. Durch das Kriterium der *Dauerhaftigkeit* unterscheiden sie sich von den *nicht öffentlich ermittelnden Polizeibeamten* (den sog. noePs),[26] durch ihre Beamtenstellung von sonstigen privaten Vertrauenspersonen (V-Leuten) aus dem Milieu. Zwar treten auch Angehörige der beiden letztgenannten Personengruppen in der digitalen Welt im Einzelfall als Käufer oder Verkäufer von Betäubungsmitteln oder Waffen auf. Meist wird es aber darum gehen, sich unter einer Legende *längerfristig* eine digitale Identität aufzubauen, um in der kriminellen Szene Vertrauen zu gewinnen und Zugang zu illegalen Handelsplattformen zu erhalten. In letzter Zeit gehen die Strafverfolgungsbehörden daher verstärkt dazu über, sich *bereits existierender* Accounts oder digitaler Identitäten zu bedienen, die über eine hohe Reputation in der Szene verfügen.[27] Das hat auch den Vorteil, dass von diesen regelmäßig keine sog. „Keuschheitsproben",[28] also die Begehung von Straftaten als Zugangsvoraussetzung wie das Posten von kinderpornografischem Bildmaterial oder die Mitwirkung an BtM-Geschäften, verlangt werden, was Polizeibeamten naturgemäß untersagt ist und diese dann im Weigerungsfall rasch enttarnt. Insofern versucht man, Beschuldigte *bereits laufender* Strafverfahren durch mehr oder minder geschickten Hinweis auf eine mögliche Strafmilderung nach der Kronzeugenregelung des § 46b StGB dazu zu bewegen, Profile und Passwörter sowie Adressen im Darknet preiszugeben. Diese werden dann von den Strafverfolgern übernommen und zur Erkenntnisgewinnung genutzt. Völlig unproblematisch ist das nicht. Schließlich ist nach § 136a Abs. 1 S. 3 StPO das Versprechen eines gesetzlich nicht vorgesehenen Vorteils verboten. Die Polizeibeamten dürfen den Inhabern der Profile daher keine konkreten Versprechungen zum Strafmaß machen, da die diesbezügliche Entscheidung den Strafrichtern vorbehalten ist.

---

22 *Krause*, NJW 2018, 678 (679); vgl. auch *Safferling*, DRiZ 2018, 206; allg. zur Problematik des „Going Dark" *Schulze*, APuZ 2017, 23 ff.

23 *Krause*, NJW 2018, 678 (679).

24 *Hartleb*, Kriminalistik 2018, 532 (534).

25 Vgl. *Göppner*, Kriminalistik 2018, 623 (625) sowie *Fiebig*, DRiZ 2019, 50 (51) mit Zitat von *May*: „Meist ist der Einsatz von verdeckten Ermittlern die einzige Chance, um Straftaten im Darknet zu ermitteln"; ebenso *Ihwas*, WiJ 2018, 138 (142): „Personale Ermittlungsmethoden versprechen im anonymen Darknet generell den größten Ermittlungserfolg".

26 Hierzu *Ihwas*, WiJ 2018, 138 (143 f.).

27 *Rath*, DRiZ 2016, 292 (293); *Ihwas*, WiJ 2018, 138 (146); *Krause*, NJW 2018, 678 (680).

28 Dazu *Safferling*, DRiZ 2018, 206 f.

c) Schnittstellen zwischen virtueller und realer Welt

Von besonderem ermittlungstaktischem Nutzen sind darüber hinaus die Schnittstellen, an denen virtuelle und reale Welt ineinander übergehen. Bei einer Handelsplattform im virtuellen Raum müssen die dort durch Kryptowährung bezahlten Waren logischerweise irgendwann an den Erwerber verschickt werden. Dazu müssen die Händler den geschützten Raum des Darknets verlassen und ihre Päckchen ganz analog auf den Versandweg zum Kunden bringen. Insofern ist es in der Szene ein offenes Geheimnis, dass hierfür häufig unter falschen Personalien angemeldete oder gehackte Packstationen des Dienstleisters DHL genutzt werden.[29] Bei entsprechender Verdachtslage, dass eine bestimmte Packstation zum Versand oder Erhalt illegaler Waren genutzt wird, kann sich dann deren Observation durch Polizeibeamte vor Ort und/oder der Einsatz von Videoüberwachungstechnik anbieten.[30] Zudem lassen sich an der Ware möglicherweise Fingerabdrücke oder DNA-Spuren finden, die jedenfalls dann Ermittlungsansätze liefern, wenn die Spurenleger bereits in den einschlägigen Datenbanksystemen wie dem beim BKA geführten Automatisierten Fingerabdruck-Identifizierungs-System (AFIS) oder der dortigen DNA-Analyse-Datei geführt werden.[31]

d) Spurensuche im Visible Web

Häufig kann auch die Spurensuche im Visible oder Clear Web wichtige Ermittlungsansätze in Bezug auf Personen liefern, die für ihre kriminellen Aktivitäten den Schutz des Darknets suchen. Erfahrungsgemäß werden zumindest von unvorsichtigen Händlern und Nutzern von Handelsplattformen im Darknet deren Pseudonyme, Profilbilder, Produktbeschreibungen oder Mail-Adressen auch im *ungeschützten* Bereich des Internets verwendet.[32] Insofern setzen auch die Strafverfolgungsbehörden mittlerweile auf die Suche in öffentlich zugänglichen Quellen mit Hilfe von sog. Open-Source-Intelligence.[33] Zu den mit Hilfe solcher, ursprünglich aus dem Bereich der Nachrichtendienste stammenden Tools durchkämmten Quellen zählen etwa soziale Medien oder Internetangebote von Tageszeitungen, Fernseh- und Radiosendern.

e) Internationale Zusammenarbeit

Schließlich müssen sich bei internetbasierten Handelsplattformen weder die Betreiber als Personen mit ihren Laptops, PCs oder Smartphones noch die von ihnen zum Betrieb genutzten Server zwingend im Inland befinden. Ohne intensive Kooperation mit ihren Kolleginnen und Kollegen im Ausland sowie bei inter- und supranationalen Einrichtungen, sind daher rein nationale Ermittlungsverfahren deutscher Strafverfolgungsbehörden häufig zum Scheitern verdammt. Bei inter- und transnational operierenden Händlern können insbesondere sog. Gemeinsame Ermittlungsgruppen (Joint Investigation Teams) entscheidende Vorteile bieten (vgl. § 93 IRG). Das zeigt auch der Fall „Wall Street Market“, bei dem der Beschlagnahme der Plattform und ihrer kriminellen Inhalte eine intensive Kooperation der Generalstaatsanwaltschaft Frankfurt am Main und des BKA mit US-amerikanischen und niederländischen Ermittlern, aber auch mit Europol und Interpol vorausging.

III. Die (vermeintliche) gesetzgeberische Lösung: ein neuer § 126a StGB

Erstaunlicherweise soll die Lösung für zukünftige Erfolge bei der Bekämpfung von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen aber vorrangig im materiellen Strafrecht zu suchen sein. Im aktuellen rechtspolitischen Diskurs wird derzeit lebhaft über die Einführung eines neuen § 126a StGB diskutiert, der das Anbieten bzw. Zugänglichmachen von internetbasierten Leistungen zur Begehung von Straftaten eigenständig mit Strafe bedrohen soll.[34]

1. Bisheriger Gesetzgebungsverlauf

Der bisherige Gesetzgebungsverlauf für diese als „Darknet-Paragrafen“ betitelte Vorschrift ist allerdings kurios. Am 18. Januar 2019 hatte Nordrhein-Westfalen einen entsprechenden Gesetzesantrag in den Bundesrat eingebracht,[35] dem anschließend auch die Bundesländer Hessen und Bayern beigetreten sind. Am 15. März 2019 hat der Bundesrat mehrheitlich dafür gestimmt, den Gesetzentwurf in einer geänderten Fassung beim Deutschen Bundestag einzubringen. Dies ist am 17. April 2019 durch den „Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen“ geschehen.[36] Darin wird u.a. die Einfügung eines neuen § 126a StGB mit folgendem Wortlaut vorgeschlagen:

§ 126a StGB-E [Anbieten von Leistungen zur Ermöglichung von Straftaten]

(1) Wer eine internetbasierte Leistung anbietet, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen

---

29 *Rath*, DRiZ 2016, 292 (293); *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 (443); *Ihwas*, WiJ 2018, 138 (147); *Krause*, NJW 2018, 678 (680).

30 Vgl. *Göppner*, Kriminalistik 2018, 623 (625) mit Hinweis auf den Fall „Shiny Flakes“. Hier hatte der mutmaßliche Täter aus seinem Leipziger Jugendzimmer heraus über die Internetseite „Shiny Flakes“ sowohl im Clear Web als auch im Darknet von Dezember 2013 bis Februar 2015 in mehreren tausend Fällen Bestellungen über insgesamt rund 600 Kilogramm an illegalen Drogen verschickt. Die Ermittler waren ihm letztlich durch von ihm falsch frankierte Postsendungen auf die Schliche gekommen, die nicht an die falschen Absenderadressen zurückgeschickt werden konnten und dann von der Deutschen Post der Polizei übergeben wurden.

31 Vgl. *Rath*, DRiZ 2016, 292 (293).

32 Vgl. *Hostettler*, APuZ 2017, 10 (14 f.).

33 *Göppner*, Kriminalistik 2018, 623 (625 f.).

34 Erste Stellungnahmen hierzu bieten etwa *Oehmichen/Weißenberger*, KriPoZ 2019, 174 ff.; *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1; *Greier/Hartmann*, jurisPR-StrafR 13/2019 Anm. 1; *Greco*, ZIS 2019, 435 ff.

35 BR-Drs. 33/19.

36 BT-Drs. 19/9508.

Taten im Sinne von Satz 2 zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Rechtswidrige Taten im Sinne des Satzes 1 sind

1. § 95 Absatz 1 des Gesetzes über den Verkehr mit Arzneimitteln,

2. §§ 29 Absatz 1 Nummer 1, 29a, 30, 30a des Betäubungsmittelgesetzes,

3. § 19 Absatz 1 des Grundstoffüberwachungsgesetzes,

4. § 52 Absatz 1 Nummer 1 und Absatz 3 Nummer 1 des Waffengesetzes,

5. § 40 Absatz 1 und 2 des Sprengstoffgesetzes,

6. §§ 19 Absatz 1, 20 Absatz 1, 20a Absatz 1, 22a Absatz 1 Nummer 1, 2 und 4 des Gesetzes über die Kontrolle von Kriegswaffen sowie

7. §§ 146, 147, 149, 152a, 152b, 184b Absatz 1, 202a, 202b, 202c, 263a, 275, 276, 303a und 303b des Strafgesetzbuches.

(2) Die Strafe darf nicht schwerer sein, als die für die Tat im Sinne von Absatz 1 Satz 2 angedrohte Strafe.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig begeht.

Allerdings handelt es sich hierbei nicht um den einzigen Entwurfstext, der derzeit im politischen Raum kursiert. In den Beschlussempfehlungen der zuständigen Bundesratsausschüsse fand sich auch eine auf Betreiben Bayerns deutlich verschärfte Fassung. Diese bayerische Vorschlagsfassung fand jedoch im Plenum des Bundesrates keine Mehrheit. Die bayerische Staatsregierung hatte das aber wohl schon vorhergesehen und entsprechend vorgesorgt. Schließlich existiert in Berlin mit dem Bundesministerium des Innern, für Bau und Heimat ein einflussreiches und vor allem CSU-geführtes Ministerium mit thematischem Bezug zum Sicherheitsrecht. Dort wurde mit Datum vom 27. März 2019 ein zwischenzeitlich von Netzpolitik.org geleakter Referentenentwurf für ein „IT-Sicherheitsgesetz 2.0“ vorgelegt, der sich derzeit noch in der Ressortabstimmung befindet. Art. 4 dieses Referentenentwurfs sieht ebenfalls die Einfügung eines neuen § 126a StGB vor. Dieser besteht – ein Schelm, wer Böses dabei denkt – exakt aus derjenigen Formulierung, mit der sich Bayern im Bundesrat nicht hatte durchsetzen können. Sie lautet wie folgt:

§ 126a StGB-E [Zugänglichmachen von Leistungen zur Begehung von Straftaten]

(1) Wer Dritten eine internetbasierte Leistung zugänglich macht, deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

(2) Die Strafe darf nicht schwerer sein, als die für die Tat im Sinne von Absatz 1 angedrohte Strafe.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten im Sinne dieser Vorschrift verbunden hat, begeht.

(4) Absatz 1 gilt nicht für Handlungen

1. wenn die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt, oder

2. die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen.

2. Gemeinsamkeiten und Unterschiede der Entwürfe

Beiden Entwürfen ist neben § 126a StGB als Regelungsstandort gemeinsam, dass sie sich inhaltlich auf internetbasierte Leistungen beziehen. Mit dem Begriff der „Leistung“ sollen denkbar weit alle Angebote bezeichnet werden, die sich an einen oder mehrere Nutzer richten, ohne auf Dauer und wiederholte Nutzung abzuzielen.[37] Das Adjektiv „internetbasiert“ soll technikbezogen auszulegen sein und alle Dienste erfassen, die auf der Netzwerkschicht des OSI (Open Systems Interconnection)-Referenzmodells über das Internetprotokoll (IP) vermittelt werden.[38] Erfasst werden damit nicht nur Dienste, die über das World Wide Web oder per E-Mail erbracht werden, sondern z.B. auch Voice-over-IP Dienste wie Skype, Facetime oder Whatsapp. Allerdings muss der Zweck oder die Tätigkeit der internetbasierten Leistung darauf ausgerichtet sein, die Begehung rechtswidriger Taten zu ermöglichen oder zu fördern. Zudem enthalten beide Entwürfe in Absatz 1 eine formelle Subsidiaritätsklausel. Danach kommt eine Strafbarkeit nach § 126a StGB nur in Betracht, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Nach dem jeweiligen Absatz 2 darf die Strafe nach § 126a StGB im Übrigen nicht schwerer sein, als die für die ermöglichte oder geförderte (Haupt-)Tat.

Vergleicht man beide Textfassungen, so fallen aber auch *gravierende Unterschiede* ins Auge. Während der Bundesratsentwurf als Tathandlung das „Anbieten“ internetbasierter Leistungen kriminalisieren will, knüpft der Referentenentwurf an den Begriff des „Zugänglichmachens“ an. Nur der Bundesratsentwurf formuliert auch tatsächlich einen „Darknet-Paragrafen“.[39] Demgegenüber verzichtet der Referentenentwurf gerade auf die Einschränkung, wonach der Zugang und die Erreichbarkeit der internetbasierten Leistung „durch besondere technische Vorkehrun-

[37] BT-Drs. 19/9508, S. 13.
[38] RefE, S. 80.
[39] Vgl. *Oehmichen/Weißenberger* KriPoZ 2019, 174 (176).

gen beschränkt" sein muss. Zusätzlich zum Bundesratsentwurf erfasst die Formulierung des Referentenentwurfs über das Fördern und Ermöglichen hinaus auch internetbasierte Leistungen, die darauf ausgerichtet sind, die Begehung von rechtswidrigen Taten zu „erleichtern". Während der Bundesratsentwurf an einen vergleichsweise überschaubaren Katalog typischer Darknet-Straftaten anknüpft, verzichtet der Referentenentwurf auf jede Einschränkung und lässt die Ausrichtung auf die Ermöglichung, Förderung oder Erleichterung *jeder denkbaren rechtswidrigen Tat* i.S. von § 11 Abs. 1 Nr. 5 StGB genügen. Auf diese Weise will das Bundesinnenministerium u.a. auch Plattformen erfassen, die auf die Begehung von Äußerungsdelikten oder die Vermittlung von Auftragsmördern gerichtet sind.[40] Im Vergleich zum Bundesratsentwurf, der im Grundtatbestand als Sanktion Freiheitsstrafe bis zu drei Jahren oder Geldstrafe vorsieht, soll nach dem Referentenentwurf die Strafobergrenze zudem erst bei fünf Jahren Freiheitsstrafe gezogen werden. Während in § 126a Abs. 3 des Bundesratsentwurfs nur die *gewerbsmäßige Tatbegehung* zu einer Qualifikation mit einem Strafrahmen von sechs Monaten bis 10 Jahren Freiheitsstrafe führt, soll dies nach der Formulierung des Referentenentwurfs zusätzlich auch bei der *bandenmäßigen Begehung* der Fall sein. Andererseits sieht lediglich der Referentenentwurf in Absatz 4 für die dort genannten Fälle einen Tatbestandsausschluss vor. Umgekehrt findet sich nur im Bundesratsentwurf eine Ergänzung des Katalogs von § 5 StGB um eine neue Nr. 10b, wonach deutsches Strafrecht unabhängig vom Recht des Tatorts auch auf solche Fallkonstellationen Anwendung finden soll, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung von rechtswidrigen Taten im Inland bezieht.[41]

3. Bewertung

a) Regelungszweck

Eine erste (verfassungsrechtliche) Bewertung fällt angesichts der divergierenden Regelungskonzepte nicht leicht. Klar ist: Die einschlägigen Handelsplattformen bieten einen niedrigschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die *herkömmliche Beschaffungswege* für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten.[42] Mit ihrer Hilfe werden somit neue Kundenkreise erschlossen, die bislang keinen Zugang zu solchen Waren und Dienstleistungen hatten. Allerdings ist schon das hierfür bemühte Rechtsgut der „öffentlichen Sicherheit und der staatlichen Ordnung"[43] denkbar weit und damit unbestimmt. Wie etwa die parallele Diskussion zur Bestimmung des Schutzgutes der §§ 129 ff. StGB zeigt, verbergen sich hinter solchen wenig aussagekräftigen Kollektivrechtsgütern in Wirklichkeit immer die im Besonderen Teil des StGB und den strafrechtlichen Nebengesetzen geschützten Individualrechtsgüter wie z.B. Leben, körperliche Unversehrtheit, Vermögen, Eigentum oder Freiheit.[44] Um den durch das Betreiben illegaler Handelsplattformen hierfür folgenden Gefahren entgegenzuwirken, erscheint es durchaus als legitimes Mittel, das öffentliche Feilbieten von Gegenständen und Dienstleistungen zur Vorbereitung von Straftaten im Internet durch eine eigenständige Strafdrohung zu unterbinden.[45] Von diesem Zweck entfernt man sich allerdings erheblich, wenn man – wie im Referentenentwurf – nicht nur auf den Darknet-Bezug, sondern auch auf einen internetbezogenen Straftatenkatalog verzichtet. Als Begründung hierfür wird angeführt, man wolle nicht die Dreistigkeit des unverdeckt Handelnden belohnen.[46] Allerdings würden damit auch Fahrlässigkeitsdelikte erfasst, zu denen weder Anstiftung noch Beihilfe möglich ist.[47] Zudem fiele auch derjenige in den Anwendungsbereich von § 126a StGB, der im Internet lediglich Angebote zur Verwirklichung von *Bagatellstraftaten*, z.B. Mustertexte für Beleidigungsdelikte oder Phishing-Mails, unterbreitet.

b) Bestimmtheit

Beide Entwurfsfassungen werfen auch unter dem Blickwinkel *ausreichender Gesetzesbestimmtheit* Fragen auf. Problematisch erscheint insoweit vor allem das Kriterium der *Zweckrichtung* der internetbasierten Leistungen zur Ermöglichung, Förderung oder Erleichterung der Begehung rechtswidriger Taten. Mithilfe dieses Merkmals sollen die *tatbestandlich erfassten* Leistungen von den *nicht strafwürdigen* Angeboten abgegrenzt werden.[48] Es zieht also die Grenze zwischen Strafbarkeit und Straflosigkeit. Die Begründung beider Entwürfe gesteht aber offen zu, dass die Prüfung der Ausrichtung einer Online-Plattform stets anhand des konkreten Einzelfalls zu erfolgen habe und allgemein verbindlichen Kriterien nicht zugänglich sei. Als mögliche Indizien werden das tatsächliche Angebot der Plattform, der dortige Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen oder etwa auch Vorgaben in Allgemeinen Geschäftsbedingungen genannt.[49] Nicht immer werden die Plattformbetreiber aber so strafverfolgungsfreundlich sein und ihrem Forum einen so eindeutigen Namen geben wie z.B. die Betreiber der zwischenzeitlich abgeschalteten Seite „crimenetwork", bei der der Name zugleich Programm war. Zudem können und werden AGBs von Handelsplattformen im Darknet häufig nur auf dem (virtuellen) Papier bestehen.[50] Infolgedessen wird die Gesetzeskonkretisierung weitgehend dem Anwender überlassen.[51]

c) Verhältnismäßigkeit

Auch ein neuer § 126a StGB muss schließlich den Anforderungen des *Verhältnismäßigkeitsgrundsatzes* genügen.

---

40 RefE, S. 81.
41 BT-Drs. 19/9508, S. 12.
42 BT-Drs. 19/9508, S. 10; RefE, S. 78.
43 Vgl. RefE, S. 78.
44 Näher hierzu nur *Zöller*, Terrorismusstrafrecht – Ein Handbuch, 2009, S. 513 ff. m.w.N.
45 Vgl. BT-Drs. 19/9508, S. 2.
46 RefE, S. 79.
47 *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).
48 Vgl. BT-Drs. 19/9508, S. 13.
49 BT-Drs. 19/9508, S. 13; RefE, S. 80 f.
50 Krit. auch *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).
51 *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 III. 2.

Insofern stellt sich bereits die Frage nach der *Erforderlichkeit*. Beide Entwürfe verweisen hierzu letztlich nur auf angebliche *Nachweisprobleme* im Rahmen einschlägiger Strafverfahren, ohne tatsächlich bestehende Strafbarkeitslücken aufzudecken.[52] Die Voraussetzungen einer *Beihilfe* (§ 27 StGB) zu den über die Plattform begangenen Straftaten seien oft nicht nachweisbar, da die Haupttaten bilateral zwischen den Beteiligten über verschlüsselte Kommunikationskanäle und vollautomatisierte Verkaufssysteme abgewickelt würden.[53] Zudem hätten die Plattformbetreiber häufig keine Kenntnisse von den Details der über ihren Dienst abgewickelten Geschäfte. Eine Zurechnung von Einzeltaten unter dem Gesichtspunkt einer *bandenmäßigen Tatbegehung* sei häufig nicht möglich, da die Führungsebene solcher Foren und Marktplätze häufig nur aus ein oder zwei Personen bestehe.[54] Und schließlich würden auch *Organisationsdelikte* wie § 129 StGB nicht weiterhelfen, da diese auf moderne, internetbasierte Beteiligungsstrukturen nicht übertragbar seien und sich die für den Tatbestand erforderliche Festigkeit der Struktur nicht nachweisen lasse.[55]

Diese Argumentation vermag im Ergebnis nicht zu überzeugen. Die These vom Bestehen nicht hinnehmbarer Strafbarkeitslücken wird schon durch die Realität der bislang geführten Strafverfahren weitgehend entkräftet, in denen man den Betreibern einschlägiger Plattformen gerade erfolgreich auch den Vorwurf der Beihilfe zu dort verwirklichten Haupttaten gemacht hat.[56] Zwar handelt es sich beim Erstellen, der Inbetriebnahme sowie der Aufrechterhaltung einer Diskussionsplattform im Darknet für sich genommen noch nicht um eine strafbare Beihilfehandlung i.S. des § 27 StGB.[57] Speziell für den subjektiven Tatbestand des Gehilfen sind die Bestimmtheitsanforderungen aber stark gelockert. Sein Vorsatz muss sich auf die Ausführung einer zwar nicht in allen Einzelheiten, wohl aber in ihren wesentlichen Merkmalen oder Grundzügen, insbesondere in ihrer Unrechts- und Angriffsrichtung konkretisierten Tat beziehen.[58] Für die Beihilfe genügt es mithin, dass der Gehilfe die Haupttat nur in ihren wesentlichen Merkmalen kennt. Das aber liegt auf der Hand, wenn er nach dem Vorbild *legaler* Verkaufsplattformen wie Amazon oder Ebay auch in seinem Darknet-Forum kundenfreundlich separate Kategorien für das Angebot evident illegaler Waren und Dienstleistungen erstellt.[59] Rein äußerlich unterscheiden sich die meisten Plattformen häufig kaum von den bekannten legalen Verkaufsplattformen im Visible Net. Auch illegale Waren und Dienstleistungen im Darknet sind regelmäßig nach Rubriken geordnet, ermöglichen es, Werbung zu schalten, bieten Treuhandmodelle[60] für die Abwicklung der Verkäufe und sogar Bewertungssysteme für Käufer und Verkäufer.[61] Vor allem aber leuchtet nicht ein, warum in einem neuen § 126a StGB eine zur Täterschaft hochgestufte Beihilfehandlung leichter nachweisbar sein soll, als etwa die klassische Beihilfe zu einem Waffen- oder Betäubungsmitteldelikt.[62] Hinzu kommt, dass sich das Betreiben von illegalen Handelsplattformen für Drogen häufig sogar schon als täterschaftliche Begehungsweise der nach dem BtMG einschlägigen Straftatbestände darstellt. So stellt etwa § 29 Abs. 1 S. 1 Nr. 8 BtMG die Werbung für Betäubungsmittel entgegen § 14 Abs. 5 BtMG unter Strafe. Unter einer solchen Werbung ist der an Dritte gerichtete Hinweis auf die Bereitschaft des Werbenden zu verstehen, Betäubungsmittel zu liefern.[63] Sofern es im Zusammenhang mit der Gestaltung der Handelsplattform an einem Hinweis auf eigene Liefermöglichkeiten fehlt, kommt eine täterschaftliche Begehung von § 29 Abs. 1 S. 1 Nr. 10 BtMG in Betracht, der es unter Strafe stellt, einem anderen eine Gelegenheit zum unbefugten Erwerb oder zur unbefugten Abgabe von Betäubungsmitteln zu verschaffen oder zu gewähren, eine solche Gelegenheit öffentlich oder eigennützig mitzuteilen oder einen anderen zum unbefugten Verbrauch von Betäubungsmitteln zu verleiten. Zudem kann sogar ein Handeltreiben nach § 29 Abs. 1 S. 1 Nr. 1 BtMG in Betracht kommen, sofern der Plattformbetreiber Provisionen oder Kommissionen für die mit seiner Hilfe getätigten Geschäfte erhält.[64] Und was eine Strafbarkeit wegen einer Beteiligung an einer kriminellen Vereinigung nach § 129 StGB anbelangt, so sei nur darauf hingewiesen, dass der Vereinigungsbegriff durch das 54. Gesetz zur Änderung des Strafgesetzbuchs vom 17. Juli 2017[65] in Umsetzung europäischer Vorgaben erweitert worden ist. Damit wurden zugleich die Anforderungen an den Nachweis des *organisatorischen Elements* einer Vereinigung erheblich herabgesetzt.[66] Die angeblichen Nachweisschwierigkeiten in den beiden Entwurfsbegründungen sind daher durch nichts näher belegt.

Der *Nutzen* einer solchen Strafnorm könnte daher – wie so häufig – auf einer *ganz anderen Ebene* gewollt sein. Mit

---

52 Vgl. *Oehmichen/Weißenberger* KriPoZ 2019, 174 (177); für das Bestehen von Strafbarkeitslücken demgegenüber *Fünfsinn/Krause*, FS Eisenberg, 2019, S. 641 (645 ff.).

53 BT-Drs. 19/9508, S. 9 f.; RefE, S. 77.

54 BT-Drs. 19/9508, S. 10; RefE, S. 77.

55 Vgl. BT-Drs. 19/9508, S. 10; RefE, S. 78.

56 S. nur *LG Karlsruhe*, StV 2019, 400 (401), das den Betreiber des Forums „Deutschland im Deep Web" im Zusammenhang mit dem sog. „Amoklauf von München" wegen Beihilfe zum vorsätzlichen unerlaubten Handeltreiben mit Waffen und Munition in Tateinheit mit fahrlässiger Tötung in 9 Fällen in Tateinheit mit fahrlässiger Körperverletzung in 5 Fällen und des unerlaubten Erwerbs der Waffe und Munition nach §§ 2 Abs. 2, 21 Abs. 1 S. 1, 52 Abs. 1 Nr. 2 lit. c WaffG, Anlage 2 Abschnitt 2 Unterabschnitt 1 S. 1 zum WaffG, §§ 222, 229, 230, 52 StGB verurteilt hat. Ausführlich zur Begründung der Beihilfestrafbarkeit *Greco*, ZIS 2019, 435 (441 ff.); zur – regelmäßig fehlenden – Haftungsbeschränkung nach den §§ 7 ff. TMG *Fünfsinn/Krause*, FS Eisenberg, 2019, S. 641 (645) sowie *Greco*, ZIS 2019, 435 (447 f.).

57 *LG Karlsruhe*, StV 2019, 400 f.

58 *BGH*, NStZ 2011, 399 (400); *LG Karlsruhe*, StV 2019, 400 (402); *Rengier*, AT, 11. Aufl. (2019), § 45 Rn. 115.

59 So auch *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 IV.

60 Hierzu *Tzanetakis*, APuZ 2017, 41 (45 f.).

61 *Rath*, DRiZ 2016, 292 (293); *Fiebig*, DRiZ 2019, 50.

62 Zweifelnd auch *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).

63 *Patzak*, in: Körner/Patzak/Volkmer, Betäubungsmittelgesetz, 9. Aufl. (2019), § 29 Teil 18 Rn. 7.

64 *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 IV.; vgl. auch *Greco*, ZIS 2019, 435 ff., der zudem auf die Möglichkeit einer Geldwäschestrafbarkeit nach § 261 StGB verweist.

65 BGBl. I S. 2440.

66 Näher hierzu *Zöller*, KriPoZ 2017, 26 ff.

der eigenständigen Kriminalisierung des bloßen Anbietens oder Zugänglichmachens von internetbasierten Leistungen wird die Strafbarkeit auf einen Zeitpunkt vorverlagert, in dem lediglich die Infrastruktur für *andere*, noch in der Zukunft liegende *Straftaten* geschaffen wird. Der geplante § 126a StGB ist nach der bisherigen Konzeption ein *abstraktes Gefährdungsdelikt* und ein typischer *Vorfeldtatbestand*. Nach beiden Entwurfsfassungen soll jedenfalls die Qualifikation nach Absatz 3 Anlasstat für Telekommunikationsüberwachungsmaßnahmen nach § 100a StPO werden. Der Referentenentwurf will die Qualifikation des § 126a Abs. 3 StGB-E sogar in den Straftatenkatalog der Online-Durchsuchung nach § 100b StPO und der Vorratsdatenspeicherung nach § 100g StPO aufnehmen. Man will also deshalb auf dem Gebiet des *materiellen Strafrechts* in das zeitliche Vorfeld von Internetkriminalität eindringen, um *Strafverfolgungsmaßnahmen* früher beginnen lassen zu können. Diese Idee dürfte sich in der Praxis als zirkelschlüssig erweisen. Schließlich wurde bereits eingangs darauf hingewiesen, dass jedenfalls klassische Telekommunikationsüberwachungsmaßnahmen im anonymen Darknet meist nicht weiterführen. Letztlich vermögen auch inkonsistente Regelungen zum *Tatbestandsauschluss* wie § 126a Abs. 4 Nr. 1 des Referentenentwurfs das Gesamtgefüge nicht entscheidend *zugunsten* einer Einstufung als *angemessene Vorschrift* zu beeinflussen. Wenn bei einer internetbasierten Leistung die Ausrichtung auf die Begehung von Straftaten nur von *untergeordneter Bedeutung* ist, wird es regelmäßig auch *nicht Zweck* dieser Leistung sein, die Begehung von Straftaten zu ermöglichen, zu fördern oder zu erleichtern.[67]

IV. Fazit

Nach alledem zeigt sich, dass die bislang auf dem Tisch liegenden Konzepte zur Kriminalisierung der Betreiber von internetbasierten Plattformen für illegale Waren und Dienstleistungen zwar ein wichtiges gesellschaftliches und rechtspolitisches Anliegen verfolgen. Der materiell-strafrechtliche Ansatz in Gestalt der Einführung eines neuen § 126a StGB ist aber weder das Licht am Ende des Darknets noch der Weisheit letzter Schluss. Er ist mit einer Reihe von Unsicherheiten und Widersprüchlichkeiten behaftet und vermag es nicht, das Bestehen von echten Strafbarkeitslücken überzeugend darzulegen. Vielleicht sollte der Blick des Gesetzgebers stattdessen in das *Strafprozessrecht* gehen. Ein erster Schritt könnten *neue strafprozessuale Befugnisse*, etwa spezialgesetzliche Vorschriften für Ermittlungen im Internet jenseits der allgemeinen Vorschriften über den Einsatz Verdeckter Ermittler nach §§ 110a ff. StPO oder zum Zugriff auf bereits bestehende Benutzerkonten und Zugangsdaten sein, die aber ihrerseits den Rahmen des Verfassungsmäßigen zu wahren haben.[68] Zumindest im Bereich des materiellen Strafrechts besteht aktuell kein dringender gesetzgeberischer Handlungsbedarf.[69]

---

[67] Treffend bemerkt von *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).

[68] Diese Voraussetzungen erfüllt der ebenfalls im Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat v. 23.3.2019 enthaltene Vorschlag eines neuen § 163g StPO-E zum staatlichen Zugriff auf Benutzerkonten erkennbar nicht; vgl. dazu *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (180 f.).

[69] Zweifel an der Erforderlichkeit eines neuen § 126a StGB äußern auch *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 IV sowie *Greco*, ZIS 2019, 435 (448).

Zur Diskussion über eine Erweiterung der Strafbarkeit von Cybergrooming

*von Prof. Dr. Axel Dessecker**

Abstract
Der Beitrag beschäftigt sich kritisch mit zwei Gesetzentwürfen, die die Strafbarkeit von Cybergrooming (§ 176 Abs. 4 Nr. 3 StGB) im vorbereitenden Stadium eines sexuellen Missbrauchs von Kindern erweitern wollen.

This article critically reviews two bills aiming at expanding the criminal offence of online sexual grooming in Germany.

I. Problemaufriss

Dass Kinder besonders vor Straftaten geschützt werden müssen, ist wohl unbestritten. Nach der Kinderrechtskonvention der Vereinten Nationen treffen die Vertragsstaaten

> *„alle geeigneten Gesetzgebungs-, Verwaltungs-, Sozial- und Bildungsmaßnahmen, um das Kind vor jeder Form körperlicher oder geistiger Gewaltanwendung, Schadenszufügung oder Misshandlung, vor Verwahrlosung oder Vernachlässigung, vor schlechter Behandlung oder Ausbeutung einschließlich des sexuellen Missbrauchs zu schützen" (Art. 19 Abs. 1 des Übereinkommens über die Rechte des Kindes).*

Das Sexualstrafrecht enthält traditionell ausgefeilte Bestimmungen über die Strafbarkeit des sexuellen Missbrauchs von Kindern. Die heutige Fassung des § 176 StGB beruht im Wesentlichen auf dem 4. Strafrechtsreformgesetz von 1973, wurde allerdings immer wieder reformiert.[1] Die Strafbarkeit des Cybergrooming (§ 176 Abs. 4 Nr. 3 StGB) besteht seit dem Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung aus dem Jahr 2003.[2] Mit dem 49. Strafrechtsänderungsgesetz wurde 2015 im Zuge der Umsetzung europäischer Vorgaben zum Sexualstrafrecht klargestellt, dass auch jede Einwirkung „mittels Informations- oder Kommunikationstechnologie" erfasst wird, was zuvor davon abhängig gewesen war, dass die Art der Einwirkung dem Schriftenbegriff des § 11 Abs. 3 StGB entsprach.[3]

Strafbar ist nach geltendem Recht das vollendete Einwirken auf ein Kind mit dem Ziel, das Kind zu sexuellen Handlungen im Kontakt mit einer anderen Person zu bewegen oder das Kind zum Objekt einer kinderpornographischen Schrift zu machen. Auf die tatsächliche Ausführung sexueller Handlungen oder die Herstellung von Kinderpornographie kommt es nicht an. Vom angestrebten Schutz der ungestörten sexuellen Entwicklung von Kindern aus betrachtet, handelt es sich um eine Strafvorschrift im Vorbereitungsstadium.[4]

Es liegt im Wesen eines rechtsstaatlichen Strafrechts, dass manche Verhaltensweisen, die eine Mehrheit der Bevölkerung vermutlich als unmoralisch oder verwerflich ansehen würde, rechtlich erlaubt sind. Dazu gehören nach einer allgemeinen Regel des Strafrechts auch versuchte Vorbereitungshandlungen, im vorliegenden Fall also solche Kommunikationsversuche seitens Erwachsener, die in sexueller Absicht erfolgen, aber erfolglos bleiben (§ 23 Abs. 1 StGB). Manche solcher Kommunikationsversuche werden von vornherein ins Leere gehen, so dass es nicht einmal zu einer Einwirkung auf ein Kind kommt. Denkbar sind verschiedene Gründe für ein solches Scheitern deliktischer Absichten in einem frühen Stadium. Die Person, die als Kommunikationspartnerin und potentielles Opfer auftritt, kann ebenfalls erwachsen sein, ohne dies zu erkennen zu geben, etwa deswegen, weil sie Polizeibeamtin[5] oder die Mutter eines Kindes ist, an das frühere Textmitteilungen gerichtet waren.[6] Die Person kann eine Jugendliche sein, die das 14. Lebensjahr bereits vollendet hat. Oder der potentielle Täter kommuniziert nicht mit einer anderen Person, sondern mit einem Computerprogramm.

Kinder gelten im Strafrecht wie im Rechtssystem insgesamt als besonders schutzbedürftig. Besonders sexueller Missbrauch von Kindern beschreibt einen Sachverhalt, der in den letzten Jahrzehnten erfolgreich als soziales Problem etabliert und über das etwa in der Presse besonders häufig berichtet wurde.[7] Das Strafrecht ist ein nahe liegendes, weil durch Gesetzesänderungen beeinflussbares Feld politischer Aktivitäten. Aus dieser Sicht überrascht es nicht, dass Sexualdelikte zum Nachteil von Kindern immer wieder Gegenstand von Gesetzentwürfen werden.

Was Verhaltensweisen des Cybergrooming betrifft, liegen zwei Gesetzentwürfe vor. Die Bundesregierung hat beim

---

* Der Verfasser ist Stellv. Direktor der Kriminologischen Zentralstelle (KrimZ) und apl. Professor an der Universität Göttingen. Wesentliche Teile des Beitrags gehen auf eine gemeinsam mit *Martin Rettenberger* verfasste Stellungnahme zum ursprünglichen Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz zurück.

1 *Bezjak*, Grundlagen und Probleme des Straftatbestandes des sexuellen Missbrauchs von Kindern gemäß § 176 StGB, 2015, S. 79 ff.

2 *Eisele*, in: FS Heinz, 2012, S. 697.

3 *Eisele*, in: FS Heinz, 2012, S. 697 (702 ff.). Wie *Fischer*, StGB, 66. Aufl. (2019), § 176 Rn. 8, bemerkt, ist die Beschreibung des Tatmittels sprachlich misslungen.

4 *Laubenthal*, Handbuch Sexualstraftaten, 2012, Rn. 477.

5 *Momsen/Bruckmann*, KriPoZ 2019, 20 (21).

6 *OLG Hamm*, Beschl. v. 14.1.2016 – III-4 RVs 144/15.

7 *Schetsche*, Die Karriere sozialer Probleme, 1996, S. 33 ff.; *Görgen/Fangerau*, in: Fangerau u.a. (Hrsg.), Präventive Strategien zur Verhinderung sexuellen Missbrauchs in pädagogischen Einrichtungen, 2017, S. 16 (27 f.).

Bundesrat einen Gesetzentwurf eingebracht, mit dem im Wesentlichen eine Strafbarkeit des Versuchs für Fälle des Cybergrooming gegenüber objektiv untauglichen betroffenen Personen oder Tatobjekten eingeführt werden soll, die durch den Straftatbestand des § 176 Abs. 4 Nr. 3 StGB nicht erfasst werden. Außerdem sieht der Entwurf eine Erweiterung der Anwendbarkeit des Straftatbestands der sexuellen Belästigung (§ 184i StGB) vor.[8]

Bisher weniger beachtet wurde ein Gesetzesantrag des Landes Hessen, der eine Versuchsstrafbarkeit für die Straftatbestände des § 176 Abs. 4 Nr. 3 und 4 StGB fordert und weiter darauf abzielt, angebliche Strafbarkeitslücken bei der Entziehung Minderjähriger (§ 235 Abs. 1 StGB) zu korrigieren.[9]

Der vorliegende Beitrag konzentriert sich auf die beiden Entwürfen gemeinsame Frage der Erweiterung einer Strafbarkeit des Cybergrooming, mit der die weiteren Regelungsvorschläge nicht unmittelbar verbunden sind. Obwohl die Entwürfe nach ihren Begründungen in erster Linie auf die Pönalisierung objektiv untauglicher Handlungen zielen, die nach geltendem Recht nicht einmal als Versuch strafbar sind, gehen sie unterschiedliche Wege. Der Gesetzentwurf der Bundesregierung schlägt vor, den Versuch des Cybergrooming gegenüber objektiv untauglichen betroffenen Personen oder Tatobjekten mittels einer Neufassung des § 176 Abs. 6 StGB unter Strafe zu stellen. Der Gesetzesantrag des Landes Hessen wurde in den Ausschussberatungen des Bundesrats verändert. Nunmehr wird vorgeschlagen, bereits den objektiven Tatbestand der § 176 Abs. 4 Nr. 3 und 4 StGB zu erweitern und Kindern solche Personen gleichzustellen, die lediglich der Täter für ein Kind hält.[10]

II. Zum Vorschlag einer Neufassung des § 176 Abs. 6 StGB

Mit der durch den Gesetzentwurf der Bundesregierung vorgeschlagenen Neufassung des § 176 Abs. 6 StGB sollen zukünftig – über die bisher strafbaren Verhaltensweisen der Beeinflussung eines Kindes unter Heranziehung bestimmter Tatmittel mit dem Ziel eines sexuellen Missbrauchs hinaus – auch Fälle strafrechtlich erfasst werden, in denen der Täter mit Missbrauchsabsicht irrig davon ausgeht, auf ein Kind einzuwirken, während er tatsächlich mit einem Jugendlichen, einem Erwachsenen oder keinem Menschen, sondern einer computergeschaffenen Phantomfigur kommuniziert. Insoweit handelt es sich um eine Kriminalisierung bisher strafloser Verhaltensweisen, die sich nur begründen lässt, wenn diese Handlungen strafbedürftig und strafwürdig sind.

1. Strafbedürftigkeit

Aus der Sicht des Grundsatzes der Verhältnismäßigkeit lässt sich Strafbedürftigkeit als Erforderlichkeit einer Erweiterung des Strafrechts fassen.[11] Dafür sollten mindestens Erkenntnisse vorliegen, dass die Verhaltensweisen, die strafrechtlich erfasst werden sollen, tatsächlich vorkommen und weniger einschneidende Maßnahmen nicht ausreichen, ihnen wirksam zu begegnen.

Was das Auftreten und die Häufigkeit des Phänomens „Cybergrooming" betrifft, liegen einige empirische Erkenntnisse vor. Die Polizeiliche Kriminalstatistik erfasst das Einwirken auf Kinder gemäß § 176 Abs. 4 Nr. 3 und 4 StGB seit 2004 mit dem gemeinsamen Straftatenschlüssel 131400, allerdings sind die Zahlen der Tatverdächtigen wegen einer Umstellung der Erfassungsmethode erst im Zeitraum seit 2009 miteinander vergleichbar. Seither ist die Zahl der erfassten Verdachtsfälle von über 900 im Jahr 2009 auf mehr als 2.400 im Jahr 2018 gestiegen. Die durchweg etwas niedrigeren Zahlen der Tatverdächtigen sind im gleichen Zeitraum von über 600 auf mehr als 1.600 angestiegen.[12] Nun liegt es nahe, dass als Belästigung erfahrene Kontaktversuche, die keine weiteren Folgen haben, eher selten bei einer Polizeibehörde angezeigt werden. Schon aus diesem Grund ist mit einer hohen Dunkelziffer zu rechnen.

Befragungen potentiell betroffener Kinder und Jugendlicher müssen andererseits die Schwierigkeit überwinden, potentiell strafbares Verhalten alltagssprachlich und dennoch präzise zu bezeichnen. In einem Fragebogen von *Bergmann* und *Baier*[13] wurden Cybergrooming-Aktivitäten mit zehn Aussagen erfasst, mit denen versucht wurde, der Bandbreite möglicher Erscheinungsformen gerecht zu werden. Am häufigsten bejahten die Befragten die Aussage: „Jemand hat dich nach deinem Aussehen oder deinem Körperbau gefragt" (26 %), am seltensten die Aussage: „Jemand hat versucht, dich zu erpressen, weil du ihm Bilder geschickt oder sehr Persönliches von dir mitgeteilt hast" (2,4 %). Die insgesamt breiter angelegte Befragung wurde in den Schulen einer Großstadt in Nordrhein-Westfalen durchgeführt und bezog sich auf Erlebnisse innerhalb der letzten zwölf Monate. Zudem sollten die Fragen nur von Befragten beantwortet werden, die angaben, sich innerhalb des letzten Jahres mit anderen im Internet unterhalten zu haben. Diese Eingangsfrage wurde von über 90 % bejaht.[14]

Die befragten Schülerinnen und Schüler der neunten Jahrgangsstufe waren durchschnittlich 14,9 Jahre alt, zum größeren Teil also keine Kinder im Sinn des Strafrechts. Schon damit wird deutlich, dass Befragungen zur Mediennutzung, Delinquenz und Viktimisierung junger Menschen wenig geeignet sind, quantitative Schätzungen zur

---

8 Gesetzentwurf der Bundesregierung: Entwurf eines ... Gesetzes zur Änderung des Strafgesetzbuches – Versuchsstrafbarkeit des Cybergroomings (BR-Drs. 365/19 vom 9.8.2019).

9 Gesetzesantrag des Landes Hessen: Entwurf eines Gesetzes zur Verbesserung des strafrechtlichen Schutzes von Kindern (BR-Drs. 518/18 vom 16.10.2018).

10 Empfehlungen der Ausschüsse zu Punkt 44 der 973. Sitzung des Bundesrates am 14.12.2018 (BR-Drs. 518/1/18 vom 12.12.2018).

11 *Stächelin*, Strafgesetzgebung im Verfassungsstaat, 1998, S. 65.

12 Polizeiliche Kriminalstatistik: Grundtabelle ohne Tatortverteilung ab 1987, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2018/Zeitreihen/Faelle/ZR-F-01-T01-Faelle_excel.xlsx?__blob=publicationFile&v=3 (zuletzt abgerufen am 3.9.2019).

13 *Bergmann/Baier*, Rechtspsychologie 2 (2016), 172.

14 A.a.O.

Größe des Dunkelfelds für bestimmte Straftatbestände anzustellen. Fragt man noch allgemeiner nach beliebigen Formen digitaler Kommunikation mit „fremden Menschen" über persönliche Inhalte und verzichtet man auf einen klar definierten Referenzzeitraum, erweitert sich der Anteil der Betroffenen auf 41 % der Befragten.[15] Die Einbeziehung jeder Art digitaler Kommunikation ohne Rücksicht darauf, ob ein sexueller Bezug erkennbar wurde, entspricht durchaus dem Anliegen des Gesetzgebers, mit § 176 Abs. 4 Nr. 3 StGB den „Tricks" und „Verführungskünsten" Erwachsener zu begegnen.[16] Allerdings lässt sich nicht jede digitale Unterhaltung als tatbestandsmäßige „Einwirkung" qualifizieren.[17]

Ohnehin wurde in der Befragung von *Bergmann/Baier*[18] nicht danach unterschieden, ob die befragten Jugendlichen davon ausgingen, es mit Gleichaltrigen oder mit Erwachsenen zu tun zu haben. Berücksichtigt man diesen für den Begriff „Cybergrooming" zentralen Umstand des Altersunterschieds, kommt man zu niedrigeren Prävalenzraten. Das zeigt eine international vergleichende aktuelle Untersuchung in Deutschland, den Niederlanden, Thailand und den USA, die etwas strengere Einschlusskriterien – Kontakt mit einer älteren Person, die Interesse an sexuellen Themen zeigt, mindestens zwei bis drei Mal im Monat – definierte. Danach waren innerhalb der letzten zwölf Monate 7 % der Befragten betroffen.[19]

Danach ist festzuhalten, dass Phänomene des Cybergrooming als auf Machtmissbrauch gegenüber und Ausbeutung von Kindern gerichtete digitale Kommunikation einen nicht zu vernachlässigenden Anteil der Kontakte von Kindern und Jugendlichen betreffen. Sie sind eine Begleiterscheinung digitaler Kommunikationsformen, die im Alltag fast aller jungen Menschen eine wichtige Rolle spielen. Trotzdem kann man davon ausgehen, dass es sich um relativ seltene Ereignisse handelt. Die meisten Online-Kontakte von Kindern werden ihre eigene Altersgruppe betreffen, nicht sexueller Art sein und ihren Eltern nicht unbekannt bleiben.[20]

Die grundsätzlich begründbare Strafwürdigkeit des Cybergrooming an sich besagt jedoch noch nichts darüber, wie bloße Versuche und insbesondere untaugliche Versuche einzuordnen wären. Es ist nachvollziehbar, dass solche strafrechtlichen Randprobleme nicht im Zentrum empirischer Forschung stehen. Auffällig erscheint das Fehlen selbst einzelner Beispiele von Strafverfahren, in denen offensichtlich strafwürdiges Cybergrooming mangels Vollendung der Tat nicht zu einer Verurteilung führte. Die Begründung zu dem Gesetzentwurf der Bundesregierung verweist lediglich in allgemeiner Form auf Erkenntnisse der Praxis.[21] Gerichtsentscheidungen, die diese Sichtweise stützen, sind bisher nicht bekannt geworden. Im Gegenteil hat die Rechtsprechung in ähnlichen Fällen bereits einen vollendeten sexuellen Missbrauch von Kindern angenommen, weil teilweise mit einem Kind kommuniziert wurde.[22]

2. Strafwürdigkeit

In der deutschen Strafrechtswissenschaft besteht wohl Einigkeit darüber, dass das Kriterium der Strafwürdigkeit unabdingbare Voraussetzung für die Kriminalisierung eines Verhaltens durch die Gesetzgebung ist.[23] Das *BVerfG* stellt in seiner Rechtsprechung darauf ab, ob ein Verhalten „in besonderer Weise sozialschädlich und für das geordnete Zusammenleben der Menschen unerträglich, seine Verhinderung daher besonders dringlich" ist.[24]

Bereits die Begründung des Entwurfs der Bundesregierung weist darauf hin, dass der Gesetzgeber in Anbetracht der weiten Vorverlagerung der Tatbestandsverwirklichung bisher bewusst davon abgesehen hat, den Versuch des Cybergrooming unter Strafe zu stellen,[25] obwohl Chatrooms und ähnliche digitale Foren der kriminalpolizeilichen Praxis bereits seit Jahrzehnten als Mittel zur Planung und Verabredung von gegen Kinder gerichteten Sexualstraftaten bekannt sind.[26]

Die Diskussion über eine Strafbarkeit des versuchten Cybergrooming wird bereits seit Jahren geführt. Sie soll in diesem Beitrag nicht in voller Breite rekapituliert werden, weil die Argumente weitgehend ausgetauscht sind. Die Begründung des Gesetzentwurfs der Bundesregierung verweist darauf, es ergebe keinen wesentlichen Unterschied für die Beurteilung des Täterverhaltens, wenn der Täter nur annehme, mit einem Kind zu kommunizieren; schon dadurch werde er „bestärkt", bei passender Gelegenheit gegenüber einem Kind sexuell übergriffig zu werden.[27] Dagegen wird beispielsweise vorgebracht, dass die Einführung der Versuchsstrafbarkeit eine noch weitere Vorverlagerung der Strafbarkeitsschwelle bedeute, die in der Praxis weitgehend unwirksam bleibe.[28]

Grundsätzlicher fällt auf, dass diese kriminalpolitische Diskussion stark von Annahmen über potentielle Täter und deren Motivationen geprägt ist, die nicht überprüft werden. In den Begründungen der aktuellen wie auch früherer Gesetzentwürfe werden die Täter solcher Delikte meist als „pädophil"[29] oder „pädosexuell"[30] bezeichnet. Sexualwissenschaftliche Untersuchungen lassen jedoch

---

15 *Bergmann/Baier*, Rechtspsychologie 2 (2016), 172 (182).
16 Gesetzentwurf der Fraktionen SPD und Bündnis 90/Die Grünen: Entwurf eines Gesetzes zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften (BT-Drs. 15/350 vom 28.1.2003), S. 17 f.
17 *Eisele*, in Schönke/Schröder, StGB, 30. Aufl. (2019), § 176 Rn. 14d.
18 *Bergmann/Baier*, Rechtspsychologie 2 (2016), 172.
19 *Wachs u. a.*, Cyberpsychology, Behavior, and Social Networking 21 (2018), 91.
20 *Genner u. a.*, MIKE: Medien, Interaktion, Kinder, Eltern, 2017; *Schrock/Boyd*, in: Wright/Webb (eds.), Computer-mediated communication in personal relationships, 2011, S. 368.
21 BR-Drs. 365/19, S. 3.
22 *OLG Hamm*, Beschl. v. 14.1.2016 – III-4 RVs 144/15.
23 Zusammenfassend *Deckert*, ZIS 2013, 266.
24 BVerfGE 96, 10 (25) im Anschluss an BVerfGE 88, 203 (258); 90, 145 (172); 92, 277 (326).
25 BR-Drs. 365/19, S. 3.
26 BT-Drs. 15/350, S. 18 unter Bezugnahme auf *Soiné*, Kriminalistik 2002, 18 (226).
27 BR-Drs. 365/19, S. 3.
28 *Bezjak* und *Eisele*, in Bundesministerium der Justiz und für Verbraucherschutz, Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 115.
29 BT-Drs. 15/350, S. 17; BR-Drs. 518/18, S. 5.
30 BR-Drs. 365/19, S. 7; BR-Drs. 518/18, S. 3 und 6.

erkennen, dass diese Konzepte je nach Definition auf eine kleine Minderheit oder die Mehrheit einer Untersuchungsgruppe wegen sexuellen Missbrauchs von Kindern mit Körperkontakt verurteilter Straftäter zutreffen, aber keineswegs auf alle dieser Personen.[31] Da es bei Cybergrooming um verbale Aussagen oder solche in Textform gegenüber Unbekannten geht, ist zudem offen, was davon bei ungestörtem Ablauf in eine tatsächliche Missbrauchshandlung umgesetzt würde. Die meisten erwachsenen Täter werden in ihrer näheren sozialen Umgebung andere Möglichkeiten haben, Kontakte zu Kindern herzustellen.

Der bisherige Verzicht auf eine Strafbarkeit des Versuchs, insbesondere gegenüber objektiv untauglichen betroffenen Personen oder Tatobjekten, wird auch mit dem Argument kritisiert, dass untaugliche Versuche grundsätzlich strafbar seien.[32] Diese Weichenstellung kann die Prüfung, weshalb der Versuch gerade bei Cybergrooming im Vorfeld einer sexuellen Handlung unter Strafe gestellt werden soll, aber nicht ersetzen. Wie die Vorschrift des § 23 Abs. 1 StGB zum Ausdruck bringt, hängt die Strafbarkeit des Versuchs bei Vergehenstatbeständen von einer ausdrücklichen Entscheidung des Gesetzgebers ab. Der Gesetzgeber hat die Strafbarkeit des Versuchs bisher aber in keinem Fall auf Fallgruppen des untauglichen Versuchs beschränkt und zugleich taugliche Versuche, die der Vollendung eines Tatbestands viel näher kommen, von der Strafbarkeit ausgenommen.

Seit 2015 wurden Fragen einer angemessenen strafrechtlichen Regelung des Cybergrooming in der vom Bundesministerium der Justiz und für Verbraucherschutz eingesetzten Reformkommission zur Überarbeitung des Sexualstrafrechts aufgrund dreier Impulsreferate ausführlich diskutiert.[33] Für die Einführung einer Versuchsstrafbarkeit hat dabei nur eines der zwölf Kommissionsmitglieder votiert.[34] Aufgrund der Beratungen dieser Kommission wurde ein konkreter Reformvorschlag für das gesamte Sexualstrafrecht vorgelegt, der Cybergrooming mit anderen Vorbereitungshandlungen zum sexuellen Missbrauch von Kindern in einem eigenen Straftatbestand zusammenfasst.[35]

Insgesamt kann der Vorschlag einer isolierten Neufassung des § 176 Abs. 6 StGB, wie er in dem Gesetzentwurf der Bundesregierung vorgebracht wird, aus diesen Gründen wenig überzeugen.

III. Zum Vorschlag einer Erweiterung der § 176 Abs. 4 Nr. 3 und 4 StGB

Der Entwurf der Hessischen Landesregierung hat ursprünglich vorgesehen, in § 176 Abs. 6 StGB die Bezugnahme auf Abs. 4 Nr. 3 und 4 zu streichen und damit sowohl den Versuch des Cybergrooming wie auch den des Zugänglichmachens pornographischer Darstellungen gegenüber einem Kind ausnahmslos unter Strafe zu stellen. Obwohl damit von vornherein zwei Tatbestände des sexuellen Missbrauchs von Kindern betroffen sind, ähnelt die Begründung stark derjenigen, welche die Bundesregierung allein für Fälle des Cybergrooming vorbringt: auch die digitale Kommunikation mit einem Gegenüber, das nur der Täter für ein Kind hält, könne einen pädosexuellen Täter darin bestärken, tatsächliche sexuelle Handlungen gegenüber Kindern vorzunehmen. Zudem wird auf „unabweisbare Bedürfnisse der Strafverfolgungspraxis" verwiesen.[36]

Der in den Ausschussberatungen des Bundesrats federführende Rechtsausschuss hat vorgeschlagen, in § 176 Abs. 4 Nr. 3 und 4 jeweils nach dem Wort „Kind" die Wörter „oder eine Person, die er für ein Kind hält" einzufügen. Der Vorschlag ist insofern mehrdeutig, als das Wort „Kind" in diesen Strafvorschriften insgesamt dreimal genannt wird. Jedenfalls läuft die Empfehlung darauf hinaus, bereits den objektiven Tatbestand der § 176 Abs. 4 Nr. 3 und 4 StGB so zu erweitern, dass Kinder solchen Personen gleichstellt werden, die lediglich der Täter für ein Kind hält.[37] Dagegen soll es offenbar nicht ausreichen, auf ein digitales Gegenüber einzuwirken, das in Wahrheit kein anderer Mensch ist. Eine Begründung hat der Rechtsausschuss des Bundesrats indes nicht geliefert.

Immerhin wird damit ein Vorschlag aufgegriffen, dem in der Reformkommission des BMJV – begrenzt auf Taten nach § 176 Abs. 4 Nr. 3 StGB – die Mehrheit der Mitglieder zugestimmt hat, während man für § 176 Abs. 4 Nr. 4 StGB einstimmig keinen gesetzgeberischen Handlungsbedarf erkannt hat.[38] Der Gesetzentwurf der Bundesregierung erwägt eine Erweiterung des objektiven Tatbestands von § 176 Abs. 4 Nr. 3 StGB zwar als Alternative zu einer Einführung der Versuchsstrafbarkeit, verwirft diesen Ansatz jedoch ausdrücklich. Genannt werden zwei Argumente. Zum einen würde eine solche Gesetzesänderung „eine in tatsächlicher Hinsicht lediglich versuchte Tathandlung rechtlich als vollendeten sexuellen Missbrauch ausgestalten". Zum anderen wäre diese Tatbezeichnung auch im Schuldspruch und in der Eintragung im Bundeszentralregister zum Ausdruck zu bringen.[39]

Die objektive Gleichstellung von Kindern mit Personen, die lediglich für Kinder gehalten werden können, stößt auf weitere Bedenken. Es ist darauf hinzuweisen, dass sich diese Vorschläge von dem Ausgangspunkt einer Effektivierung des Cybergrooming-Tatbestands entfernen. Bereits die geltende Fassung des § 176 Abs. 4 Nr. 3 StGB

---

31 *Eher/Rettenberger/Turner*, Acta Psychiatrica Scandinavica 139 (2019), S. 572 (576).
32 *Drohsel*, ZRP 2018, 213 (215).
33 Bundesministerium der Justiz und für Verbraucherschutz, Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 114 ff.
34 Bundesministerium der Justiz und für Verbraucherschutz, Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 131.
35 *Bezjak*, ZStW 130 (2018), 303 (320 f., 332 f.).
36 BR-Drs. 518/18, S. 6.
37 BR-Drs. 518/1/18.
38 Bundesministerium der Justiz und für Verbraucherschutz, Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 131 und 154.
39 BR-Drs. 365/19, S. 3.

bezieht sich nicht allein auf Einflussversuche mittels digitaler Kommunikationsmittel, sondern auch auf die persönliche Übergabe von schriftlichen Mitteilungen, etwa solchen auf einem beschriebenen Zettel.[40] Bei § 176 Abs. 4 Nr. 4 StGB geht es um beliebige Formen der Verbreitung pornografischer Inhalte. Werden Personen, die lediglich für Kinder gehalten werden können, bei diesen Strafvorschriften ebenso geschützt wie Kinder, stellt sich die Frage, weshalb dies nicht für alle Formen sexuellen Missbrauchs ohne Körperkontakt nach § 176 Abs. 4 StGB gelten sollte.

Wer sich im Sexualstrafrecht dafür einsetzt, Delikte gegenüber Personen, die wegen ihres Lebensalters als besonders schutzbedürftig gelten, in gleicher Weise unter Strafe zu stellen wie Delikte gegenüber Personen, die eine Schutzaltersgrenze bereits überschritten haben, läuft Gefahr, nicht nur die Systematik des Schutzes bestimmter Gruppen von Betroffenen zu unterlaufen, sondern den Schutz von Kindern insgesamt in Frage zu stellen. Es wäre irreführend, würde ein Gericht einen Angeklagten des sexuellen Missbrauchs von Kindern schuldig sprechen, der in Wahrheit lediglich mit einer älteren Person über Sexualität gesprochen oder in anderer Weise kommuniziert hat. Schon zum geltenden Recht weist die Rechtsprechung für die Fassung der Urteilsformel (§ 260 Abs. 4 StPO) darauf hin, dass ein Straftatbestand konkret und verständlich zu bezeichnen ist.[41]

IV. Zusammenfassung

Es hat sich gezeigt, dass sich eine vollständige Kriminalisierung aller denkbaren Verhaltensweisen des Cybergrooming in das Sexualstrafrecht nicht widerspruchsfrei einfügen lässt. Das gilt schon für den vorliegenden Gesetzentwurf der Bundesregierung. Anders als er es in seinem Titel zum Ausdruck bringt, bezieht sich die vorgeschlagene Einführung einer partiellen Strafbarkeit des Versuchs nach ihrem Wortlaut keineswegs allein auf Fälle des Cybergrooming, sondern auf alle Fallgruppen des § 176 Abs. 4 Nr. 3 StGB, also alle Kontaktaufnahmen mit Kindern zur Vorbereitung eines sexuellen Missbrauchs, die unter Einsatz bestimmter Tatmittel erfolgen. Noch weniger durchdacht erscheint der Gesetzesantrag der Hessischen Landesregierung in der Fassung, die der Rechtsausschuss des Bundesrates empfiehlt.

Beide Entwürfe beschränken sich auf punktuelle und voraussichtlich für die Strafrechtspraxis kaum relevante Korrekturen einzelner Formulierungen des Sexualstrafrechts, deren Auswahl sich schwer nachvollziehen lässt. Die in den Entwürfen aufgegriffenen Inkonsistenzen sind ersichtlich nicht die einzigen Fragen, die das geltende Recht in strafrechtlich und kriminalpolitisch wenig überzeugender Weise regelt. Es erscheint vorzugswürdig, eine breiter angelegte Reform des Sexualstrafrechts in Angriff zu nehmen, die das BMJV durch eine Reformkommission bereits gründlich vorbereitet hat.

[40] BGHR StGB § 176 Abs. 4 Nr. 3 Einwirken 1 (Gründe).

[41] *BGH*, Beschl. v. 16.12.2015 – 2 StR 191/15.

Hate Speech - zur Relevanz und den Folgen eines Massenphänomens

*von Staatsanwalt Christoph Apostel**

Abstract
Im Zusammenhang mit der Kommunikation im Internet und speziell in den sozialen Medien wird ein Anstieg von Hate Speech wahrgenommen und diskutiert. Aktualität erhielt das Phänomen durch den Fall Walter Lübcke, nach dessen Tod es zu zahlreichen Äußerungen im Netz, insbesondere durch Personen aus dem rechtsextremen Spektrum, gekommen ist, die unter das Deliktsphänomen Hate Speech subsumiert werden können. Der vorgenannte Fall und die aktuelle Debatte bieten Anlass für diesen Beitrag, Hate Speech nicht nur als für die Ermittlungsbehörden relevantes Thema, sondern aus kriminologischer Sicht und als gesamtgesellschaftliches Problem zu behandeln.

In connection with communication on the Internet and especially in social media, an increase in hate speech is perceived and discussed. The phenomenon was brought up-to-date by the case of Walter Lübcke, after whose death there were numerous statements on the Internet, in particular by persons from the right-wing extremist spectrum, who can be subsumed under the crime phenomenon Hate Speech. The aforementioned case and the current debate provide the occasion for this article not only to treat Hate Speech as a topic relevant to the investigating authorities, but also from a criminological point of view and as a societal problem.

I. Einleitung

Der mutmaßliche Mord an dem Kasseler Regierungspräsidenten *Walter Lübcke*[1] und die Reaktionen hierauf aus dem rechtsextremen Bereich haben die Debatte um Hasskriminalität im Netz angeheizt. Wie ist mit Hass und Hetze im Internet, Anfeindungen, Bedrohungen, Beleidigungen usw. umzugehen? Welchen Einfluss haben (möglicherweise) strafbare Postings auf die Gesellschaft? Welche Rolle spielt die Meinungsfreiheit? *Hate Speech* steht nicht erst seit dem vorgenannten Fall auf der Agenda der Politik. So ist zum 1. Oktober 2017 das Netzwerkdurchsetzungsgesetz (kurz NetzDG) in Kraft getreten, welches zur Eindämmung von Hass und Hetze im Internet beitragen soll. Der Fall *Walter Lübcke* offenbart jedoch, welches Ausmaß insbesondere rechter Hass im Internet annehmen kann.[2] Der vorliegende Beitrag setzt hier an, gibt zunächst einen Überblick über das Phänomen *Hate Speech*, auch im historischen Kontext, und setzt sodann seinen Schwerpunkt auf die (Rechts-) Lage und die Bewältigungsstrategien in Deutschland. Dabei kann und soll nicht auf die vielfältigen rechtlichen Einzelprobleme eingegangen werden. Thematisiert werden soll *Hate Speech* vielmehr als gesamtgesellschaftliches Problem mit seinen Folgen für Staat und Gesellschaft.

II. Definition

Eine einheitliche Definition des Begriffs *Hate Speech* existiert nicht. So kann maßgeblich auf die Intention des Sprechers abgestellt werden und *Hate Speech* als „[…] der sprachliche Ausdruck von Hass gegen Personen oder Gruppen […], insbesondere durch die Verwendung von Ausdrücken, die der Herabsetzung und Verunglimpfung von Bevölkerungsgruppen dienen“, verstanden werden.[3] Eine ausführlichere Definition hat das Ministerkomitee des Europarates in einer Empfehlung aus dem Jahr 1997 zugrunde gelegt. Danach wird *Hate Speech* definiert als

„[…] jegliche Ausdrucksformen, welche Rassenhass, Fremdenfeindlichkeit, Antisemitismus oder andere Formen von Hass, die auf Intoleranz gründen, propagieren, dazu anstiften, sie fördern oder rechtfertigen, einschließlich der Intoleranz, die sich in Form eines aggressiven Nationalismus und Ethnozentrismus, einer Diskriminierung und Feindseligkeit gegenüber Minderheiten, Einwanderern und der Einwanderung entstammenden Personen ausdrückt.“[4]

---

* Der *Verfasser* ist als Staatsanwalt in Köln in der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) tätig. Dort wurde 2017 gemeinsam mit der Polizei, der Landesanstalt für Medien NRW und verschiedenen Medienunternehmen das Projekt „Verfolgen statt nur Löschen“ initiiert, um gemeinsam gegen Hasskriminalität im Netz vorzugehen, vgl. hierzu: https://www.justiz.nrw.de/JM/schwerpunkte/zac/index.php (zuletzt abgerufen am 29.7.2019).

1 Einen guten Überblick über den Fall und den gegenwärtigen Sachstand des Ermittlungsverfahrens – soweit bekannt – bietet: „Was im Fall Lübcke bislang bekannt ist“, tagesschau.de v. 2.7.2019, online abrufbar unter: https://www.tagesschau.de/inland/luebcke-131.html (zuletzt abgerufen am 29.7.2019).

2 Das LKA Hessen geht davon aus, Tausende Strafverfahren im Zusammenhang mit dem Fall *Walter Lübcke* führen zu müssen, u.a. wegen Beleidigung, Bedrohung, Volksverhetzung und wegen öffentlicher Aufforderung zu Straftaten. Hierfür sei der Aufbau einer eigenen Arbeitsgruppe erforderlich, vgl. „LKA erwartet Tausende Verfahren wegen Hasskommentaren im Fall Lübcke“, Zeit Online v. 4.7.2019, online abrufbar unter: https://www.zeit.de/politik/2019-07/hassrede-tausende-strafverfahren-mordfall-walter-luebcke (zuletzt abgerufen am 29.7.2019).

3 *Meibauer*, in: Hassrede/Hate Speech - Interdisziplinäre Beiträge zu einer aktuellen Diskussion, 2013, S. 1.

4 *Empfehlung Nr. R (97) 20, 30.10.1997*, online abrufbar unter: http://www.egmr.org/minkom/ch/rec1997-20.pdf (zuletzt abgerufen am 29.7.2019).

„Im Kern handelt es sich bei *Hate Speech* um eine Form der kommunikativen Herstellung menschlicher Minderwertigkeit“.[5] Bei dem Versuch einer Definition wird zudem die Frage diskutiert, ob es maßgeblich auf die Betroffenenperspektive ankommen und *Hate Speech* damit unabhängig von der Intention des Sprechers vorliegen kann. „Der Vorteil einer solchen Definition, die auf die Intention des Sprechers abstellt und nicht etwa auf das Empfinden diskriminierter Dritter, besteht darin, „versehentliche“ Hassrede begrifflich auszuschließen“, was jedoch mit dem Nachteil verbunden ist, „[…] niemals sicher *wissen* zu können, wann eine Äußerung „Hassrede“ darstellt (d. h. als solche gemeint ist), da man hierzu strenggenommen die Intentionen und Gefühle des jeweiligen Sprechers kennen müsste“.[6]

III. Historischer Kontext und begriffliche Abgrenzung

Der Begriff *Hate Speech* findet seinen Ursprung in den USA der frühen 1920er Jahre, seitdem dort politische und juristische Debatten über die Einschränkung offensiver rassistischer und religiöser Sprache geführt wurden.[7] Die Diskussion um „Hassrede“ entstand zu dieser Zeit dadurch, dass auf der einen Seite Opfer rassistischer, religiöser und ethnischer Vorurteile und Diskriminierung gemeinsame Anstrengungen zur Selbstverteidigung unternahmen und sich andererseits die American Civil Liberties Union (ACLU) 1920 zur Verteidigung der Meinungsfreiheit gründete.[8] Während die meisten Länder den Ausdruck offensiver rassistischer, religiöser oder ethnischer Propaganda verbieten, hat sich das amerikanische Recht und die amerikanische Politik in eine andere Richtung entwickelt.[9] Grund hierfür ist die im ersten Zusatzartikel der Verfassung der USA besonders geschützte Redefreiheit, die selbst offensiv rassistische und verunglimpfende Äußerungen erlaubt, was in vielen Entscheidungen der obersten Gerichtshöfe der USA bestätigt worden ist.[10] „Darüber hinaus ist man sich in den USA dem nützlichen Effekt von aggressiver Rede bewusst, wie er zum Beispiel in der Bürgerrechtsbewegung zur Anwendung kam“.[11] In Deutschland hingegen ist die Würde des Menschen allen anderen Verfassungswerten vorangestellt. Die Bundesrepublik Deutschland mit seinem Grundgesetz von 1949 ist als Gegenentwurf zum nationalsozialistischen Regime entstanden und erlaubt die Einschränkung der Meinungsfreiheit etwa bei propagandistischer Gutheißung der nationalsozialistischen Gewalt- und Willkürherrschaft.[12] Die Erfahrung mit dem Nationalsozialismus „[…] führte in Deutschland zum Status der wehrhaften Demokratie, welcher beinhaltet, dass antidemokratische Kräfte, die gegen ihren Bestand wirken, nicht von ihr geschützt werden“.[13]

Begrifflich abzugrenzen ist *Hate Speech* von dem weitergehenden Begriff *Hate Crime* („Hassverbrechen“), auch *Bias Crime* („Vorurteilsgeleitete Straftat“)[14] genannt. Unter dem ebenfalls aus den USA stammenden Begriff *Hate Crime*[15] werden Straftaten verstanden, die sich „[…] gegen eine Person aufgrund ihrer politischen Einstellung, Nationalität, Volkszugehörigkeit, Rasse, Hautfarbe, Religion, Weltanschauung, Herkunft, sexuellen Orientierung, Behinderung, ihres äußeren Erscheinungsbilds oder ihres gesellschaftlichen Status“ richten.[16] Hierunter fallen insbesondere Gewaltverbrechen und Vandalismus, also Delikte, die sich gegen die körperliche Unversehrtheit oder das Eigentum anderer Personen richten.[17] Liegt ein „Hassverbrechen“ vor, so wird nach US-amerikanischem Strafrecht und anders als in Deutschland grundsätzlich eine höhere Strafe verhängt.[18] Während „Hassrede“ als Ausdruck der Meinungsfreiheit stärker geschützt wird als in Deutschland, erhalten „Hassverbrechen“ in den USA damit eine eigenständige strafrechtliche Relevanz.

IV. Zur Rechtslage in Deutschland

1. *Strafrecht*

Ein gesetzliches Verbot der „Hassrede“ als solche besteht nicht. Sie kann sich jedoch mittelbar im Rahmen verschiedener Straftatbestände auswirken. Hierunter fallen Äußerungsdelikte wie Beleidigung (§ 185 StGB), üble Nachrede (§ 186 StGB), Verleumdung (§ 187 StGB), Bedrohung (§ 241 StGB), Nötigung (§ 240 StGB) und Volksverhetzung (§ 130 StGB). Bei dem Straftatbestand der Volksverhetzung besteht die Besonderheit, dass dort „Hass“ als eigenes Tatbestandsmerkmal relevant wird. Nach § 130 StGB macht sich u.a. strafbar, wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören, gegen eine nationale, rassische, religiöse oder durch ihre ethnische Herkunft bestimmte Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zugehörigkeit zu einer vorbezeichneten Gruppe oder zu einem Teil der Bevölkerung zum Hass aufstachelt. „Hass“ wird in diesem Zusammenhang seitens der höchstrichterlichen Rechtsprechung definiert als „[…] eine gesteigerte, über die bloße Ablehnung oder Verachtung hinausgehende feindselige Haltung gegen die betreffenden

---

5 *Sponholz*, Hate Speech in den Massenmedien – Theoretische Grundlagen und empirische Umsetzung, 2018, S. 48.
6 *Marker*, in: Hassrede/Hate Speech – Interdisziplinäre Beiträge zu einer aktuellen Diskussion, 2013, S. 60.
7 Vgl. *Walker*, Hate Speech: The History of an American Controversy, 1994, S. 9.
8 A.a.O.
9 A.a.O.
10 A.a.O.; vgl. auch *Guiora/Park*, Philosophia 2017, 957 (960 ff.); *Butler*, Haß spricht. Zur Politik des Performativen, 2013, S. 85 ff.
11 *Haupt*, sozial.geschichte.extra 2006, S. 6 f.
12 Vgl. BVerfGE 124, 300.
13 *Haupt* (Fn. 11), S. 6.
14 Vgl. *Kugelmann*, Möglichkeiten effektiver Strafverfolgung bei Hasskriminalität – Rechtsgutachten, 2015, S. 8; vgl. auch „ Criminal offence + Bias Motivation = Hate Crime“, online abrufbar unter: http://hatecrime.osce.org/what-hate-crime (zuletzt abgerufen am 29.7.2019).
15 Vgl. *Pinar*, Rechtsextremismus und Hate-Crime-Gesetze, 2015, o.S., online abrufbar unter: https://www.bpb.de/politik/extremismus/rechtsextremismus/206018/rechtsextremismus-und-hate-crime-gesetze (zuletzt abgerufen am 29.7.2019).
16 BT-Drs. 16/13035; vgl. auch *Kugelmann* (Fn. 14), S. 7 m.w.N.
17 Vgl. OSCE, Prosecuting Hate Crimes – A practical guide, 2014, S. 21 f.
18 Eine Übersicht über die einschlägigen US-amerikanischen Hate-Crime-Gesetze findet sich hier: „Hate Crime Laws“, online abrufbar unter: https://www.justice.gov/crt/hate-crime-laws (zuletzt abgerufen am 29.7.2019).

Bevölkerungsteile […]".[19] „Hass" kann sich zudem auf der Rechtsfolgenebene bei der Strafzumessung auswirken. So bestimmt § 46 Abs. 2 S. 1 und 2 StGB, dass bei der Abwägung der für und gegen den Täter sprechenden Umstände besonders auch „rassistische, fremdenfeindliche oder sonstige menschenverachtende" Beweggründe in Betracht kommen. Diese wurden mit „Gesetz zur Umsetzung von Empfehlungen des NSU-Untersuchungsausschusses des Deutschen Bundestages" vom 12.06.2015, in Kraft getreten am 1.8.2015, in die Norm eingefügt.[20]

Bei der Strafverfolgung von *Hate Speech* ergeben sich zudem zahlreiche Sonderprobleme. So etwa bei der strafrechtlichen Zurechnung von Volksverhetzungen unter Einsatz von „Social Bots", bei denen es sich um „[…] teilautonome Computerprogramme zur Infiltrierung sozialer Netzwerke, die auch volksverhetzende Inhalte verbreiten können", handelt.[21] Für die Strafbarkeit des Verwenders kann festgestellt werden: „Je stärker der Einfluss des Verwenders i.R.d. Kalibrierung auf die Inhalte der Generierung oder des Repostings durch den Social Bot ist, desto leichter lässt sich die Strafbarkeit des Verwenders herleiten".[22] Fraglich ist auch die Anwendbarkeit des deutschen Strafrechts gegenüber ausländischen Anbietern sozialer Netzwerke. So wird u.a. die Auffassung vertreten, das deutsche Strafrecht finde „[…] auf die verantwortlichen Personen des ausländischen Anbieters eines sozialen Netzwerks als potenzielle Gehilfen grundsätzlich Anwendung gem. §§ 3, 9 StGB, wenn ein Nutzer des sozialen Netzwerks als Täter strafbare Hassbotschaften vom Inland aus verbreitet".[23] Hier ist kein Ort, um näher auf die Vielzahl der rechtlichen Einzelprobleme im Zusammenhang mit *Hate Speech* einzugehen. Es sollte verdeutlicht werden, dass es mit der schlichten Anwendung oben genannter klassischer Straftatbestände als Reaktion auf Hassäußerungen nicht sein Bewenden hat, sondern das Phänomen *Hate Speech* weitere komplexe Rechtsfragen aufwirft, die in der Zukunft sicherlich zunehmen werden und die es zu untersuchen gilt.

2. *Das Netzwerkdurchsetzungsgesetz (NetzDG)*

Das am 1.10.2017 in Kraft getretene Netzwerkdurchsetzungsgesetz (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken) soll sich gegen Hass und Hetze sowie gezielte Falschmeldungen (Fake News) im Internet richten. Es verpflichtet seit dem 1.1.2018 die Betreiber sozialer Netzwerke wie Facebook, Twitter und YouTube, „offensichtlich rechtswidrige Inhalte" innerhalb von 24 Stunden nach Eingang einer Beschwerde zu löschen oder zu sperren (§ 3 Abs. 2 Nr. 2 NetzDG). Für nicht offensichtlich rechtswidrige Inhalte besteht eine Maximalfrist von sieben Tagen (§ 3 Abs. 2 Nr. 3 NetzDG). Anlass für das Gesetz war die laut Bundesministerium der Justiz und für Verbraucherschutz zunehmende Verbreitung von Hasskriminalität und anderen strafbaren Inhalten in sozialen Netzwerken sowie eine Untersuchung, die zu dem Ergebnis gekommen sei, dass strafbare Inhalte bei Facebook nur in 39 Prozent und bei Twitter nur in 1 Prozent der Fälle aufgrund einer Selbstverpflichtung gelöscht worden seien.[24] Bei wiederholten Verstößen gegen das Gesetz droht den Betreibern ein Bußgeld von bis zu 50 Millionen Euro (§ 4 Abs. 2 S. 1 und 2 i.V.m. § 30 Abs. 2 S. 3 OWiG). Kritiker des Gesetzes wie die Organisation Reporter ohne Grenzen[25] oder Human Rights Watch[26] sehen hierin die Gefahr, dass die Betreiber sozialer Netzwerke aus Furcht vor hohen Bußgeldern zu früh und zu viel löschen (sog. Overblocking).[27] Zudem sehen sie die in Art. 5 Abs. 1 des GG geschützte Presse- und Meinungsfreiheit dadurch gefährdet, dass Privatunternehmen in kurz bemessenen Fristen darüber entscheiden sollen, ob Äußerungen und Posts strafbare Inhalte darstellen oder noch von der Meinungsfreiheit gedeckt sind, was in einem demokratischen Rechtsstaat grundsätzlich den Gerichten vorbehalten ist.

Ein prominenter Anwendungsfall ereignete sich bereits kurz nach Inkrafttreten des Netzwerkdurchsetzungsgesetzes. So nahm die AfD-Politikerin *Beatrix von Storch* einen Tweet der Polizei am Silvesterabend 2017/18 in arabischer Sprache zum Anlass, in einem eigenen Tweet von „muslimischen, gruppenvergewaltigenden Männerhorden" zu sprechen. Twitter sperrte daraufhin vorübergehend ihren Account. Nachdem das Satire-Magazin „Titanic" die Äußerungen der Politikerin parodiert hatte, indem es vermeintlich in ihrem Namen einen vergleichbaren Post twitterte, sperrte Twitter kurz darauf auch den Account des Satire-Magazins.[28] Gegner des Gesetzes sehen sich in ihrer Kritik bestätigt und nehmen diesen Fall als Beispiel dafür, dass Privatunternehmen nicht in der Lage sind, in angemessener Weise zwischen strafbaren und noch von der Meinungsfreiheit gedeckten satirischen Inhalten zu unterscheiden.

Allerdings lässt sich auch die Kritik am NetzDG kritisch hinterfragen. So stellt sich im Hinblick auf den Vorwurf des Overblockings die Frage, „[…] wieso Unternehmen, die Umsätze in zweistelliger Milliardenhöhe erwirtschaften, sich durch Bußgelder zu vorauseilendem Gehorsam treiben lassen, die erst nach mehrfachen und eindeutigen Verstößen erhoben werden können und nur im äußersten Extremfall 50 Mill. Euro betragen".[29] Außerdem dürften

---

19 *BGH*, NJW 1994, 1421 (1422).

20 Vgl. BGBl. I 2015, S. 925; vgl. auch *Heintschel-Heinegg*, in: BeckOK-StGB, 42. Aufl. (2019), § 46 Rn. 32; *Miebach/Meier*, in: MüKo-StGB, 3. Aufl. (2016), § 46 Rn. 187.

21 *Volkmann*, MMR 2018, 58.

22 A.a.O., S. 63.

23 *Handel*, MMR 2017, 227 (231).

24 Vgl. BT-Drs. 18/12356 v. 16.5.2017, S. 1f. Der Gesetzentwurf ist online abrufbar unter: http://dipbt.bundestag.de/dip21/btd/18/123/1812356.pdf (zuletzt abgerufen am 29.7.2019).

25 Vgl. „NetzDG führt offenbar zu Overblocking", reporter-ohne-grenzen.de v. 27.7.2018, online abrufbar unter: https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/netzdg-fuehrt-offenbar-zu-overblocking/ (zuletzt abgerufen am 29.7.2019).

26 Vgl. „Germany: Flawed Social Media Law", hrw.org v. 14.2.2018, online abrufbar unter: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law (zuletzt abgerufen am 29.7.2019).

27 Vgl. auch *Bautze*, Kritische Justiz 2019, 203 (209).

28 Vgl. *Lobo*, „Die stumpfe Pracht des NetzDG", Spiegel Online v. 3.1.2018, online abrufbar unter: https://www.spiegel.de/netzwelt/web/netzdg-berechtigtes-getoese-um-ein-daemliches-gesetz-a-1185973.html (zuletzt abgerufen am 29.7.2019).

29 *Bautze* (Fn. 27), S. 209.

Unternehmen aus der Kommunikationsbranche wie Facebook, Twitter, Youtube und Co., „[…] bei denen der Erfolg des Geschäftsmodells darauf basiert, dass sie Kommunikationsinhalte möglichst ungeschminkt transportieren“ ein geringes Interesse daran haben, vorschnell und im Übermaß Inhalte ihrer Nutzer zu löschen.[30] So zeigen erste Erfahrungen, dass eine große Zensur bislang jedenfalls ausgeblieben zu sein scheint.[31] Im Übrigen ist es bis dato lediglich in einem Fall wegen unzureichender Umsetzung der Vorgaben des NetzDG zur Verhängung eines Bußgeldes in Höhe von (nur) 2 Millionen Euro gegen ein Unternehmen (Facebook) gekommen, dessen zugrundeliegender Bescheid noch nicht rechtskräftig ist.[32]

V. Kriminologische Relevanz

1. *Hate Speech im Wandel sozialer Kommunikation*

Ein Begriff, der in der Diskussion um *Hate Speech* immer wieder Verwendung findet, ist der der „Political Correctness“, welcher „[…] als eine nicht-juristische Norm des richtigen politischen und sprachlichen Verhaltens aufgefasst werden“ kann.[33] *Hate Speech*, die dagegen verstößt, stellt somit (norm-) abweichendes Verhalten dar. Personen und Gruppen, die speziell dem rechten und islamkritischen Spektrum zugeordnet werden, verwenden den Begriff der „politischen Korrektheit“ hingegen, um auf die ihrer Auffassung nach zunehmende Einschränkung der Meinungsfreiheit hinzuweisen.[34] Insbesondere im Internet, in dessen sozialen Netzwerken und Onlineforen vorgenannte Gruppen aktiv sind, wird ein Anstieg von Ausdrucksformen, die die Voraussetzungen von „Hassrede“ erfüllen, wahrgenommen.[35] Fraglich ist jedoch, ob hiermit tatsächlich ein Zuwachs an Hass, Aggressionen und Vorurteilen verbunden ist oder entsprechende Motive und Einstellungen durch die Möglichkeiten des Internets lediglich sichtbarer werden. So kann ein Anstieg von Hassäußerungen im Internet damit erklärt werden, dass Nutzer dort relativ frei von Sanktionsdrohungen agieren können.[36] „Insgesamt zeigt sich beim Emotionsausdruck im Netz eine Tendenz zur Dramatisierung bzw. Theatralik“.[37] Dies spricht dafür, dass Hassäußerungen im Internet nicht zwingend Ausdruck tatsächlicher Hassgefühle sein müssen.

Ob Hasspostings im Internet tatsächlich Folge einer zunehmenden Verrohung der Gesellschaft sind, wie oft behauptet, oder das Internet und speziell soziale Netzwerke lediglich ein Medium bieten, um Hassgefühle leichter und schneller zum Ausdruck zu bringen und einer breiten Öffentlichkeit mitzuteilen, dürfte letztlich schwer festzustellen sein. Auch wenn die individuellen Motive schwer zu erfassen sind, lassen sich die konkreten Auswirkungen von *Hate Speech* hingegen feststellen und benennen, wie nachfolgend dargestellt.

2. *Hassäußerungen als Nährboden für Gewalt?*

In der gesellschaftlichen und politischen Debatte um „Hassrede“ wird ein Zusammenhang zwischen herabsetzenden, insbesondere rassistischen Äußerungen und Gewalttaten gesehen. So weist die vom Bundesministerium für Familie, Senioren, Frauen und Jugend geförderte Amadeu Antonio Stiftung darauf hin, Sprache bereite das Handeln vor und die Ermunterung zu Hass ebne den Weg zu Gewalt und Vernichtung.[38] Geschichtswissenschaftlich wird die These aufgestellt, dass „Hassrede“ gegen Juden eine Voraussetzung zu ihrer Vernichtung gewesen sei und diese erst eingeleitet habe.[39] Die Landesanstalt für Medien NRW äußert sich in einem Appell von November 2015 u.a. wie folgt: „Hasserfüllte Kampagnen im Netz sind Katalysator realer Gewalt. Gerade die aktuellen politischen Debatten und Geschehnisse rund um die Flüchtlingssituation zeigen, dass „Hate Speech“ und reale Gewalt oft nah beieinander liegen."[40]

Die University of Warwick (Vereinigtes Königreich) konnte in einer Studie zudem eine Verbindung von Hasskommentaren auf der Facebook-Seite der Partei Alternative für Deutschland (AfD) und Übergriffen auf Flüchtlinge in Deutschland feststellen.[41] Danach fanden Übergriffe auf Flüchtlinge gehäuft in den Wochen statt, in denen vermehrt Hasskommentare über Flüchtlinge auf der Facebook-Seite der AfD gepostet wurden.[42] Die Autoren kommen zu dem Ergebnis, dass soziale Medien nicht nur einen fruchtbaren Boden für die Verbreitung hasserfüllter

---

30 A.a.O., S. 210.

31 Vgl. *Berger*, „Netzwerkdurchsetzungsgesetz: Die große Zensur durchs NetzDG blieb bislang aus“, heise online v. 31.1.2019, online abrufbar unter: https://www.heise.de/newsticker/meldung/NetzDG-Berichte-Die-grosse-Zensur-blieb-bislang-aus-4295222.html (zuletzt abgerufen am 29.7.2019).

32 Vgl. *Schmidt*, „Millionen Bußgeld gegen Facebook“, tagesschau.de v. 2.7.2019, online abrufbar unter: https://www.tagesschau.de/inland/facebook-bussgeld-103.html (zuletzt abgerufen am 29.7.2019).

33 *Meibauer* (Fn. 3), S. 10.

34 Vgl. *Schütte*, in: Hassrede/Hate Speech – Interdisziplinäre Beiträge zu einer aktuellen Diskussion, 2013, S. 122 f.

35 Vgl. *Ergebnisbericht der forsa-Befragung zur Wahrnehmung von Hasskommentaren im Internet*, Landesanstalt für Medien NRW, 2018, S. 1, online abrufbar unter: https://www.medienanstalt-nrw.de/fileadmin/user_upload/lfm-nrw/Foerderung/Forschung/Dateien_Forschung/forsaHate_Speech_2018_Ergebnisbericht_LFM_NRW.PDF (zuletzt abgerufen am 29.7.2019).

36 A.a.O., S. 134; vgl. auch *Kaspar*, in: Online Hate Speech. Perspektiven auf eine neue Form des Hasses, 2017, S. 68.

37 *Döring*, Sozialpsychologie des Internet. Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen, 2003, S. 259.

38 Vgl. *„Geh sterben!“ - Umgang mit Hate Speech und Kommentaren im Internet,* S. 7, online abrufbar unter: http://www.amadeu-antonio-stiftung.de/w/files/pdfs/hatespeech.pdf (zuletzt abgerufen am 29.7.2019).

39 *Friesel*, in: Hassrede/Hate Speech – Interdisziplinäre Beiträge zu einer aktuellen Diskussion, 2013, S. 17 ff.

40 „Für Meinungsfreiheit – gegen Hetze im Internet“. Appell der Landesanstalt für Medien Nordrhein-Westfalen (LfM) gegen Diskriminierung und Hetze im Internet v. 20.11.2015; Der Appell ist online abrufbar unter: https://www.medienanstalt-nrw.de/fileadmin/user_upload/lfm-nrw/Aktuelle_Meldungen/Appell_DE.pdf (zuletzt abgerufen am 29.7.2019).

41 Vgl. *Müller/Schwarz*, Fanning the Flames of Hate: Social Media and Hate Crime, 2018; Das paper ist online abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082972 (zuletzt abgerufen am 29.7.2019). In diesem Zusammenhang von Interesse ist auch die Untersuchung von *Hestermann/Hoven*, KriPoZ 2019, 127 ff. zur Pressearbeit der AfD bzgl. der Kriminalitätsentwicklung in Deutschland. Die Autoren kommen zu dem Ergebnis, dass in den Pressemitteilungen der AfD unter Verwendung populistischer Rhetorik fast ausschließlich Kriminalität von Zuwanderern thematisiert und diesen zugeschrieben wird (S. 137 ff.).

42 A.a.O., S. 20 ff.

Ideen darstellen, sondern auch zu realen Gewalthandlungen anstacheln können.[43]

3. *Klima der Angst als Ziel und Folge von Hate Speech*

Selbst wenn Hassäußerungen und Bedrohungen im Netz in den meisten Fällen nicht zu realer Gewalt führen oder hiermit in Zusammenhang gebracht werden können, haben sie dennoch spürbare Auswirkungen auf die jeweiligen Adressaten. So ist es in einigen Fällen dazu gekommen, dass Kommunalpolitiker, die sich zuvor für Flüchtlinge eingesetzt hatten, aufgrund von Morddrohungen oder anderen Anfeindungen aus dem rechtsextremen Spektrum Polizeischutz erhielten oder aus Sorge um ihre Familie von ihrem Amt zurücktraten.[44] In einer Umfrage, an der 217 Abgeordnete des Bundestages sowie der Landesparlamente teilnahmen, gaben 97,5 Prozent der Befragten an, persönliche Anfeindungen im Netz erlebt zu haben.[45] Zudem gab fast ein Drittel der Befragten an, schon einmal darüber nachgedacht zu haben, sich aus den sozialen Netzwerken zurückzuziehen.[46] In einer forsa-Umfrage im Auftrag der Landesanstalt für Medien NRW im Zeitraum Januar bis Juni 2018 gaben 78 Prozent der Befragten an, schon einmal Hassrede bzw. Hasskommentare im Internet gesehen zu haben.[47] In einer weiteren Studie zur Diskussionsbeteiligung im Internet gaben 32 Prozent befragt nach den Gründen für die Nichtteilnahme an öffentlichen Diskussionen im Internet an, aus Angst vor beleidigenden Kommentaren nichts online zu stellen.[48] 27 Prozent gaben an, ihre Meinung im Internet aus Angst, bloßgestellt zu werden, nicht zu veröffentlichen.[49]

Vorgenannte Erkenntnisse belegen die Gefahr von *Hate Speech* für eine offene und pluralistische Gesellschaft. Denn wenn Menschen aus Furcht vor beleidigenden oder bedrohenden Äußerungen sich aus den sozialen Medien zurückziehen oder dies in Erwägung ziehen, bedeutet dies eine Einschränkung des politischen Diskurses zu Gunsten einer hetzenden Minderheit, der es nicht um Inhalte, sondern um persönliche Diffamierungen geht und für die die Achtung der Menschenwürde keinen sonderlich hohen Stellenwert hat. Zu Recht wird daher ein konsequentes Vorgehen gehen *Hate Speech* gefordert.[50] Hierunter fällt auch die strafrechtliche Verfolgung von Hassäußerungen, die einen wesentlichen Beitrag zur Aufrechterhaltung der Meinungsfreiheit leisten kann. Zwar erscheint es auf den ersten Blick paradox, Meinungsfreiheit durch die strafrechtliche Verfolgung und Sanktionierung und einer damit einhergehenden Einschränkung von Meinungen – denn auch rassistische und volksverhetzende Äußerungen stellen Meinungen dar, sofern sie durch das Element der Stellungnahme, des Dafürhaltens und der Beurteilung geprägt sind[51], nur eben solche, die in keiner Weise zu rechtfertigen, absolut nicht nachvollziehbar und in höchstem Maße verwerflich sind – zu schützen. Doch genau dies scheint erforderlich, um einen offenen Meinungsaustausch, auch in den sozialen Netzwerken, zu gewährleisten. Denn die Gefahr besteht – wie oben genannte Studien zeigen –, dass jemand, der fürchten muss, mit Beleidigungen, Bedrohungen und sonstigen Anfeindungen überzogen zu werden, nicht in gleicher Weise seine (ehrliche und uneingeschränkte) Meinung äußern wird, wie er es ohne diese begründete Furcht täte. Insoweit stellt *Hate Speech* eine reale Bedrohung für die Meinungsfreiheit dar, da sie Menschen von der Teilnahme am öffentlichen Diskurs abhält. Sich klar und bestimmt gegen *Hate Speech* zu positionieren und diese zu bekämpfen, ob mit den Mitteln des Strafrechts oder der Stimme der demokratischen Mehrheit, sollte daher aktuell wie auch zukünftig Aufgabe von Staat und Gesellschaft sein.

VI. Schlussbemerkung

Hate Speech wird nicht erst seit dem Fall Walter Lübcke von der Politik und der Gesellschaft als Problem wahrgenommen. Durch das 2017 in Kraft getretene Netzwerkdurchsetzungsgesetz etwa hat der Gesetzgeber sich dafür entschieden, die hinter sozialen Netzwerken stehenden Unternehmen stärker in die Verantwortung zu nehmen. Da der öffentliche Meinungsaustausch vermehrt im Internet stattfindet mit der Möglichkeit, von der ganzen Welt

43 A.a.O., S. 33.

44 Vgl. *Salzen*, „Bürgermeister werden massiv bedroht", Der Tagesspiegel v. 20.6.2019, https://www.tagesspiegel.de/politik/nach-dem-mord-an-luebcke-buergermeister-werden-massiv-bedroht/24477538.html (zuletzt abgerufen am 29.7.2019); vgl. auch *Meisner*, „Nazi-Hetze zwingt Oberbürgermeister zum Rücktritt", Der Tagesspiegel v. 8.3.2015, online abrufbar unter: https://www.tagesspiegel.de/politik/streit-um-fluechtlinge-in-sachsen-anhalt-nazi-hetze-zwingt-ortsbuergermeister-zum-ruecktritt/11473736.html (zuletzt abgerufen am 29.7.2019).

45 Vgl. Zwischen Bürgernähe und Netzhetze – Nutzung von und Einstellungen zu den sozialen Netzwerken in der Politik, 2019, S. 6; Die Studie ist online abrufbar unter: https://www.studien-metz-kommunikation.de/zwischen-buergernaehe-und-netzhetze-1 (zuletzt abgerufen am 29.7.2019).

46 A.a.O., S. 7. In einem Beitrag zu den Erfahrungen von sechs Abgeordneten des hessischen Landtags zu Hass im Netz geben diese übereinstimmend an, schon mehrfach in sozialen Medien angefeindet und beleidigt worden zu sein, wobei für sie ein Rückzug aus den sozialen Medien jedoch nicht in Betracht komme. „Den Hetzern das Feld zu überlassen, wäre ja quasi eine Kapitulation", so die Antwort von T*obias Eckert* von der SPD, vgl. *Luft/Kimpel*, „So erleben sechs Landtagsabgeordnete Hass im Netz", hessenschau.de v. 2.04.2019, online abrufbar unter: https://www.hessenschau.de/politik/so-erleben-sechs-landtagsabgeordnete-hass-im-netz,politiker-und-hass-auf-social-media-100.html (zuletzt abgerufen am 29.07.2019).

47 Vgl. Fn. 35.

48 Vgl. Hate Speech und Diskussionsbeteiligung im Internet – Zentrale Untersuchungsergebnisse der Hate Speech-Sonderstudie, Landesanstalt für Medien NRW, 2019, S. 10; Der Ergebnisbericht ist online abrufbar unter: https://www.medienanstalt-nrw.de/service/veranstaltungen-und-preise/safer-internet-day-2019/neue-forsa-daten-zum-thema-hass-im-netz.html (zuletzt abgerufen am 29.7.2019).

49 A.a.O.

50 So fordern u.a. die Vereinten Nationen (UN) in einer Initiative, stärker gegen hasserfüllte Äußerungen im Internet vorzugehen mit dem Hinweis darauf, in der Vergangenheit sei Hassrede die Vorstufe von grausamen Verbrechen gewesen, vgl. „Vereinte Nationen wollen gegen Hassrede vorgehen", Zeit Online v. 19.6.2019, online abrufbar unter: https://www.zeit.de/gesellschaft/2019-06/un-hassrede-hatespeech-antonio-guterres (zuletzt abgerufen am 29.7.2019).

51 Vgl. *BVerfG*, NJW 1983, 1415

aus auf gesellschaftliche Ereignisse, persönliche Statements oder sonstige Inhalte unmittelbar und anonym zu reagieren, stellen Hassäußerungen – welche natürlich auch im analogen Bereich vorkommen – nicht nur ein Randproblem dar. Sie stellen vielmehr eine Gefahr für einen ungezwungenen, offenen Meinungsaustausch und damit für die Meinungsfreiheit als solche dar, wenn sich Menschen aus Furcht vor Beleidigungen, Bedrohungen und sonstigen Anfeindungen aus dem öffentlichen Diskurs zurückziehen. *Hate Speech* ist daher entschieden und konsequent entgegenzutreten, notfalls mit den Mitteln des Strafrechts. Denn ansonsten droht die Gefahr, dass das Internet als öffentliches Forum einer lauten und hetzenden Minderheit überlassen wird.

Die Sicherstellung und Auswertung des Smartphones – Kriminalpolitischer Anpassungsbedarf?

von Polizeirat Stephan Ludewig[*]

Abstract
Zu Beginn der 1980er Jahre war es erstmals möglich ein Mobiltelefon auf dem freien Markt zu erwerben.[1] Durch technische Innovationen entwickelte sich das Mobiltelefon im Verlauf der folgenden Jahrzehnte zu dem zentralen Kommunikations- und Computergerät im Leben moderner Menschen und stellt für viele Nutzer heute den wichtigste Datenspeicher dar.[2] Im Rahmen ihrer Sicherstellung und Auswertung steht die Digitale Forensik vor einigen rechtlichen und technischen Herausforderungen. Der Beitrag beschäftigt sich mit einem möglichen rechtlichen Anpassungsbedarf der Ermächtigungsgrundlagen zur Erlangung elektronischer Beweismittel.

At the beginning of the 1980s it was possible for the first time to purchase a mobile phone on the open market. Through technical innovations, the mobile phone developed over the following decades into the central communication and computer device in the lives of modern people and today represents the most important data storage device for many users. Digital forensics faces a number of legal and technical challenges as part of its seizures and evaluation. The article deals with a possible legal need to adapt the bases of authorization for obtaining electronic evidence.

I. Einleitung

Nach einer Studie des Branchenverbandes *Bitkom* besaßen im Jahr 2018 acht von zehn Deutschen ein Smartphone, was einer Gesamtzahl von ca. 57 Millionen Nutzern entspricht.[3] Auf ihm lassen sich E-Mails, Adressen, Telefonnummern speichern und es enthält darüber hinaus den Terminkalender, sämtliche, zum Teil sehr intime, Kommunikationsdaten und Bilder sowie ggf. eine Historie besuchter Orte. Schon durch die Verknüpfung von wenigen dieser Informationen lässt sich ein detailliertes Nutzungs- und ggf. Persönlichkeitsprofil seines Besitzers erstellen.[4] Dies konnte jüngst im Mordprozess an der Freiburger Studentin *Maria L.*[5] beobachtet werden. Im Ermittlungsverfahren wurde das Smartphone des Angeklagten Hussein K., ein iPhone 6S, von den Ermittlern zunächst mit Hilfe eines externen Dienstleisters entsperrt und die Daten anschließend aus dem Gerät extrahiert. Insbesondere in den tiefen Dateistrukturen des Gerätes konnten umfassende Daten, wie der Gerätestandort zu bestimmten Zeitpunkten, die Standorte registrierter WLAN sowie die Daten aus einer sog. Fitness App, extrahiert werden. Aus dem Datenbestand ergab sich eine Indizienkette, die es ermöglichte, dass Tatgeschehen umfassend zu rekonstruieren.[6]

Elektronische Beweismittel erlangen nicht zuletzt Aufgrund der ubiquitären Verfügbarkeit[7] von Datenverarbeitungssystemen (DV-Systemen) für Strafverfolgungsbehörden immer größere Bedeutung. Gleichzeitig stellt dieser Bedeutungszuwachs die Strafverfolgungsbehörden und die Strafgerichte vor neue Herausforderungen und wirft sowohl mit Blick auf rechtliche Vorgaben als auch in technischer Hinsicht eine Vielzahl von Fragen auf.[8] Insbesondere im Bereich der Digitalen Forensik ist aufgrund des schnellen Fortschritts im Bereich der IT, z. T. fraglich auf welcher gesetzlichen Grundlage die Gewinnung dieser Beweismittel erfolgen kann, ob die gültigen gesetzlichen Bestimmungen auch den Bereich der Digitalen Forensik abdecken oder ob sich ggf. Anpassungsbedarf ergibt.[9] Die aktuellen Diskussionen bzgl. der Sicherstellung und Auswertung von Smartphones reichen dabei von der Auffassung, Mobiltelefone auch zum Beweis einer vergleichsweise niedrigschwelligen Verkehrsordnungswidrigkeit auslesen zu dürfen[10] bis hin zur Verortung derartiger Maßnahmen in der Nähe der „Online Durchsuchung“ und dem sich daraus ergebenden Anpassungsbedarf bestehender Vorschriften.[11]

---

* Der *Verfasser* ist derzeit in der Polizeidirektion Thüringen eingesetzt.

1 Das erste Mobiltelefon konnte im Jahr 1983 für den Preis von 3.995 USD auf dem freien Markt erworben werden wobei der Funktionsumfang des Gerätes nur in der Möglichkeit bestand Ortsunabhängige Gespräche zu führen. Vgl. https://praxistipps.chip.de/seit-wann-gibt-es-handys-entwicklung-im-zeitverlauf_101085 (zuletzt abgerufen am 26.7.2019).

2 Vgl. *Lane/Miluzzo/Lu/Peebles/Choudhury/Campbell,* in: IEEE Commun. Mag. 2010, 140.

3 Vgl. *Bitkom,* Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Smartphone-Markt-waechst-um-3-Prozent-auf-34-Milliarden-Euro (zuletzt abgerufen am 29.7.2019).

4 Vgl. *Spehr,* Jeder Schritt zählt , abrufbar unter: https://www.faz.net/aktuell/technik-motor/digital/datenschutz-und-privatsphaere-jeder-schritt-zaehlt-14494871.html?printPagedArticle=true#pageIndex_0 (zuletzt abgerufen am 29.7.2019).

5 *LG Freiburg*, Urt. v. 22.3.2018 – 6 KLs 101 Js 37818/16 – Ak 4/17 jug.

6 Vgl. *Buchheim,* Mordfall Maria L., abrufbar unter: http://www.badische-zeitung.de/freiburg/cybercrime-firma-hackte-fuer-die-polizei-hussein-k-s-handy--147897230.html (zuletzt abgerufen am 29.7.2019).

7 Vgl. BVerfGE 120, 274 (305).

8 Vgl. *Warken,* NZWiSt 2017, 289.

9 Vgl. *Czerner,* in: Labudde/Spranger, Forensik in der digitalen Welt, S. 265.

10 *Ternig/Lellmann,* NZV 2016, 454.

11 *Momsen,* DRiZ, 2018, 140; *Peters,* NZWiSt 2017, 465; *Wenzel,* NZWiSt 2016, 85.

II. Funktionsumfang moderner Smartphones

Smartphones sind technische Einheiten, die über Netzwerke mit anderen Einheiten verbunden sind und untereinander über einen stetigen Datenaustausch kommunizieren. Dabei werden permanent Daten erzeugt, gespeichert oder gesendet, was zu einer nie dagewesenen Masse an Daten führt, welche in der Gesamtschau noch nie so aussagekräftig waren.[12] Trotz einer Vielzahl weiterer Funktionen sind Smartphones in erster Linie Telekommunikationsgeräte. Mit ihnen lassen sich mobile Telefonate führen oder Kurzmitteilungen versenden. Die Daten hierzu werden, je nach Nutzerverhalten und Gerätekonfiguration, kurzfristig oder dauerhaft im Smartphone gespeichert.[13] Obwohl nicht speziell dafür entwickelt, können Smartphones als anspruchsvolle Sensoren fungieren. Eingebaute Kameras dienen als Video- und Bildsensoren. Das Mikrofon dient, wenn nicht für Telefonate verwendet, als akustischer Sensor. Die integrierten GPS-Empfänger erzeugen metergenaue Standortinformationen. Andere Sensoren wie Gyroskope, Beschleunigungs- und Näherungssensoren können gemeinsam verwendet werden, um Kontextinformationen zu ermitteln[14]. Externe Sensoren können über Bluetooth oder drahtgebundene Verbindungen, einfach mit dem Telefon verbunden werden.[15] Die Vielzahl der Sensoren ermöglicht u. a. die Verfolgung von Echtzeitaktivitäten oder die Überwachung von Vitalfunktionen.[16]

Die hohe Verfügbarkeit von Smartphones und die Möglichkeit der Vernetzung mit Alltagsgeräten macht das Smartphone auch zur Steuerungszentrale für Wearables. Vier von zehn Befragten gaben im Rahmen einer *Bitkom*-Studie an, ihr Smartphone schon einmal mit einem Wearable, wie einer Smartwatch oder einem Fitnessarmband, vernetzt zu haben.[17] Die dort erlangten Daten werden an das gekoppelte Smartphones gesendet, zum Teil gespeichert oder an Dienstanbieter übertragen.[18]

Die fortschreitende Verbesserung der Smartphones führte zu immer größeren Kapazitäten der verbauten bzw. erweiterbaren Datenspeichern. Die Speichergrößen aktuell angebotener Mobiltelefone reichen dabei von 8 bis 512 GB, wobei der ganz überwiegende Teil der Geräte Speichergrößen jenseits von 64 GB aufweist.[19] Smartphones kommen damit als mobile Datenträger ebenso in Betracht wie Laptops oder sonstige Speichermedien.[20] Die Geräte nutzen sog. Flash-Speicher, welche ggü. optischen oder magnetischen Datenträgern eine Besonderheit aufweisen. Eine Löschung der Daten findet bei diesen Speichern erst nach dem Überschreiben mit neuen Informationen statt, was eine Rekonstruktion gelöschter Daten oft möglich macht.[21] Mit der SIM-Karte[22] befindet sich ein weiterer relevanter Datenspeicher in Mobiltelefonen. Trotz bedeutend kleinerer Speicherkapazität, im Vergleich zum Gerätespeicher, werden auch heute noch Kontakt- und Anruflisten sowie Kurzmitteilungen auf SIM-Karten gespeichert.[23]

Während des laufenden Betriebes verarbeitet und speichert ein Smartphone ständig Nutzerdaten. Dies geschieht durch das Betriebssystem selbst oder durch Programme von Drittanbietern, sog. „Apps".[24] Das Betriebssystem Android bspw. ermittelt selbst dann fortwährend den Standort eines Smartphones, wenn der Nutzer annimmt, diese Funktion deaktiviert zu haben. Hierzu werden neben GPS-Daten auch WLAN und Bluetooth Informationen verwendet.[25]

Eine App kann alle Daten innerhalb des laufenden Programms verarbeiten und speichern. Hierzu zählen z. B. Starten und Beenden der App, Nutzungsdaten, Inhaltsdaten von Messangerdiensten wie WhatsApp oder mit Email-Clients empfangene Emails. Teilweise werden diese Daten zur Protokollierung über das Internet versendet.[26] Auch bei der Nutzung von Cloud-Diensten wie Dropbox, iCloud oder OneDrive werden, z. T. vom Nutzer unbemerkt und ungewollt, Daten auf anderen Geräten gespeichert bzw. mit anderen Nutzern geteilt.[27]

III. Bedeutung für das Ermittlungsverfahren

Für die Strafverfolgungsbehörden erlangen digitale Beweismittel und die Auswertung digitaler Kommunikationsinhalte immer größere Bedeutung.[28] Neben auswertbaren Computersystemen, hat sich das Smartphone zu einem wesentlichen Element der strafprozessualen Ermittlungen

---

12 Vgl. *Blechschmidt,* MMR 2018, 361.

13 Vgl. *Singelnstein,* NStZ 2012, 593 (598); *Rogge,* Der Kriminalist 2015, 29.

14 So z. B. ob und wann ein Benutzer zu Fuß, auf dem Fahrrad oder in einem Kfz unterwegs ist.

15 Vgl. *Christin/Reinhardt/Kanhere/Hollick,* The Journal of Systems and Software, 2011, 1928.

16 Vgl. *Lane/Miluzzo/Lu/Peebles/Choudhury/Campbell,* in: IEEE Commun. Mag. 2010, 140.

17 Vgl. *Bitkom,* Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro (Fn. 3).

18 Vgl. *Federrath,* in: Heinrich-Böll-Stiftung Sachsen/Lichdi, Digitale Schwellen, 2015, S. 57.

19 Vgl. aktuelle Chip Bestenliste unter https://www.chip.de/bestenlisten/Bestenliste-Handys--index/detail/id/900/#wrapper-ext (zuletzt abgerufen am 29.7.2019).

20 Unter Speichermedien sind hier externe Festplatten, USB-Sticks, CDS, DVDS und SD-Karten zu verstehen. Vgl. *Warken,* NZWiSt 2017, 289 (294).

21 In Einzelfällen ist es jedoch möglich auch diese Daten, durch aufwändige Verfahren, zu rekonstruieren. Vgl. *Rogge,* Der Kriminalist 2015, 29 (31 f.).

22 SIM steht für *Subscriber Identification Module.* Die Karte ist in europäischen Mobilfunknetzen erforderlich, um ein Mobiltelefon innerhalb des Netzes nutzen zu können. Vgl. https://wirtschaftslexikon.gabler.de/definition/sim-karte-52650/version-275768 (zuletzt abgerufen am 29.7.2019).

23 Vgl. *Rogge,* Der Kriminalist 2015, 29 (31 f.).

24 Der Begriff App ist eine Kurzform des englischen Begriffs *Application* was übersetzt Anwendung bedeutet und individuell installierbare Programme auf Smartphones bezeichnet. Vgl. *Federrath,* in: Heinrich-Böll-Stiftung Sachsen/Lichdi, Digitale Schwellen, S. 57.

25 Vgl. *Spehr,* Jeder Schritt zählt (Fn. 4).

26 Vgl. *Federrath,* in: Heinrich-Böll-Stiftung Sachsen/Lichdi, Digitale Schwellen, S. 58 f.

27 Vgl. a. a. O., S. 57.

28 Vgl. *Blechschmidt,* MMR 2018, 361 (363). Vgl. auch *Rogge,* Der Kriminalist 2015, 29.

entwickelt.[29] Daten wie E-Mails, Chatverläufe, Fotos oder Dokumente, aber auch der Verlauf besuchter Internetseiten geben in vielen Fällen Aufschluss über Tat und Täter. Daneben ermöglicht das Smartphone häufig den ungehinderten Zugriff auf die extern in einer Cloud gespeicherten Daten des Nutzers.[30] Das Smartphone wird als Tatmittel zum Aufzeichnen und Verbreiten von Videos oder Bildern mit strafrechtlich relevantem Inhalt genutzt.[31] Die gespeicherten (App-)Daten geben Ermittlungsbehörden Einblicke in Schlafphasen, Bewegungsaktivitäten oder den Standort des Gerätes. Es existiert kaum ein vergleichbares Objekt, dessen Auswertung in solchem Umfang Informationen über den Nutzer des Smartphones, sowie zu sozialen Kontakten, seinem Verhalten und möglicherweise auch Gedanken ermöglicht.[32] Draus kann, je nach Umfang und Inhalt der gewonnen Daten, ein sehr intensiver Eingriff in die Grundrechte des Betroffenen resultieren.[33]

IV. Grundrechtseingriff

Bei einem staatlichen Zugriff auf die Daten eines Smartphones können, aufgrund der Verschiedenartigkeit dieser Daten, unterschiedliche Grundrechte betroffen sein. Hierzu gehören das, insbesondere bei elektronischen Beweismitteln zum Tragen kommende, Recht auf Informationelle Selbstbestimmung (RiS) gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, sowie das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.[34] Bei gegenständlicher Beschlagnahme eines Smartphones sowie bei einem Zugriff auf Daten, die bei einem IT-Dienstleister gespeichert sind, kommt weiterhin das Grundrecht auf Eigentum gem. Art. 14 GG in Betracht.[35] Sofern auf Kommunikationsdaten zugegriffen wird, sind ebenso die Grundrechte des jeweiligen Kommunikationspartners betroffen.[36] Die allgemeinen Verfahrensgrundrechte und -prinzipien, wie die Unschuldsvermutung, das Recht auf ein faires Verfahren und der Verhältnismäßigkeitsgrundsatz gelten selbstverständlich auch für die Erlangung und Verwertung elektronischer Beweismittel aus einem Smartphone.[37]

1. Das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG

Schon 1983 erkannten die Richter des *BVerfG* im sog. Volkszählungsurteil, dass es bei bestehenden und vor allem zukünftigen Bedingungen der automatischen elektronischen Datenverarbeitung (DV), in besonderem Maße des Schutzes personenbezogener Daten bedarf. Moderne DV-Systeme können Angaben über persönliche oder sachliche Verhältnisse einer Person praktisch unbegrenzt speichern und damit jederzeit verfügbar machen. Auswertung, Abgleich und Vernetzung dieser Daten kann zu einem vollständigen Persönlichkeitsprofil, mithin zu einem „gläsernen Menschen“ führen.[38] Diese Gefahr besteht insbesondere beim Zugriff auf Kommunikationsinhalte wie sie in Smartphones gespeichert sein können.[39] Die Richter begegneten dieser Gefahr mit der Anerkennung des RiS, dessen Schutzbereich durch die Befugnis des Einzelnen gekennzeichnet ist, grds. selbst über die Offenbarung persönlicher Lebenssachverhalte zu entscheiden.[40] Das RiS schützt damit den Einzelnen gegen informationsbezogene Maßnahmen, die für ihn weder überschaubar noch beherrschbar sind, was insbesondere dann der Fall ist, wenn Datenbestände für eine Vielzahl von Zwecken genutzt oder miteinander verknüpft werden können.[41] Eingriffe in das RiS werden damit rechtfertigungsbedürftig, wobei sich diese Rechtfertigung nur aus einem formellen Gesetz ergeben kann.[42] Als Auffangtatbestand umfasst das RiS alle Eingriffe, die auf Datenerhebung gerichtet sind, sofern diese nicht dem Schutzbereich speziellerer Grundrechte, wie z. B dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG unterfallen.[43] In Abgrenzung zum ebenfalls dem allgemeinen Persönlichkeitsrecht zuzuordnenden Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[44], umfasst der Schutzbereich des RiS jedoch nur offene und punktuelle Eingriffe im Rahmen der Datenerhebung.[45]

Das *BVerfG* präzisierte die Schranke des Art. 2 Abs. 1 GG im Hinblick auf die Grundsätze der Bestimmtheit und der Normenklarheit. Gesetzliche Regelungen, die einen Eingriff in das RiS legitimieren, müssen Anlass, Zweck und Grenzen eines Eingriffs bereichsspezifisch, präzise und normenklar festlegen. Der Betroffene muss die Rechtslage jederzeit erkennen und sich auf mögliche belastende Maßnahmen einstellen können. Die Verwendung unbestimmter Rechtsbegriffe darf nicht zu Ungewissheiten führen, welche die Vorhersehbarkeit und Justitiabilität des staatlichen Handelns gefährdet.[46] Weiterhin besteht das Gebot für die Legislative, die Eigenschaften moderner DV-Systeme und die sich daraus ergebenden Nutzungsmöglichkeiten zu beobachten, um gegebenenfalls eine Anpassung der rechtlichen Rahmenbedingungen zu initiieren.[47]

---

29 Vgl. Wenzel, NZWiSt 2016, 85 (88); So wurden im Rahmen eines Prozesses wegen des Verdachts der Unterstützung einer Terroristischen Vereinigung 9.000 Bilder auf einem einzigen Smartphone des Verdächtigen gesichert von denen eine Vielzahl Bezüge zum Islamischen Staat aufwies. Vgl. *BGH*, Beschl. v. 17.8.2017 – AK 34/17 = StraFo 2017, 470.

30 Vgl. *Momsen,* DRiZ 2018, 140.

31 Vgl. *Rogge,* Der Kriminalist 2015, 29.

32 Vgl. *Momsen,* DRiZ 2018, 140 (143).

33 Vgl. *Singelnstein,* NStZ 2012, 593 (598).

34 Vgl. *Warken,* NZWiSt 2017, 289 (292); *Singelnstein,* NStZ 2012, 593 (602).

35 Vgl. *Warken,* NZWiSt 2017, 289(293), die darauf verweist, dass in diesen Fällen auch das Eigentumsrecht des IT-Dienstleisters betroffen ist.

36 Vgl. ebd.

37 Vgl. *Warken,* NZWiSt 2017, 289(291).

38 Vgl. BVerfGE 65, 1 (42 f.).

39 Vgl. BVerfGE 124, 43 (63).; *Peters,* NZWiSt 2017, 465 (466).

40 Vgl. BVerfGE 65, 1; *Franzius,* ZJS 2015, 260; *Warken,* NZWiSt 2017, 289(292).

41 Vgl. BVerfGE 118, 168 (187).

42 Vgl. BVerfGE 65, 1; *Münch/Kunig*, GG, 6. Aufl. (2012), Art. 2 Rn. 38, 41.

43 Vgl. BVerfGE 115, 166 (187 ff.); *Singelnstein,* NStZ 2012, 593 (594); *Warken,* NZWiSt 2017, 289 (292).

44 Zur Entstehung dieses Grundrechts durch die Rechtsprechung des *BVerfG* vgl. BVerfGE 120, 274 (308 ff.).

45 Vgl. *Franzius,* ZJS 2015, 260 (262); *Singelnstein,* NStZ 2012, 593 (602).

46 Vgl. BVerfGE 120, 274 (316).

47 Vgl. BVerfGE 113, 29 (58).

2. Das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG

Das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG ist im Zusammenhang mit der Sicherung und Auswertung elektronischer Beweismittel ebenfalls von Bedeutung.[48] Es soll die Vertraulichkeit der individuellen Kommunikation zwischen Menschen schützen. Von Relevanz ist dies insbesondere, wenn räumliche Distanz die Nutzung von Telekommunikationsmedien bzw. -anbietern erforderlich macht, was die Gefahr eines Zugriffs Dritter auf die Kommunikationsdaten birgt.[49] Das Grundrecht schützt die freie Entfaltung der Persönlichkeit durch Kommunikation unter Nutzung von Telekommunikationsmitteln, unabhängig von der Art der übermittelten Inhalte und umfasst auch die Kommunikationsumstände wie z. B. Ort, Zeitpunkt, Dauer oder Beteiligte eines Kommunikationsvorgangs.[50] Bei der Nutzung eines Smartphones fällt eine Vielzahl dieser Daten an, die gespeichert und ggf. ausgewertet werden können. Das lässt Rückschlüsse auf das Kommunikations- und Bewegungsverhalten sowie ggf. auf das Vorhandensein von Beziehungen zwischen den Kommunikationsteilnehmern und deren Intensität zu.[51] Der Schutzbereich umfasst jedoch nur die laufende Kommunikation und endet sobald die Information endgültig beim jeweiligen Empfänger angekommen und der Übertragungsvorgang beendet ist.[52]

Nicht geschützt sind damit Daten, die nach Ende des Übertragungsvorgangs auf einem DV-Gerät im Herrschaftsbereich des Empfängers gespeichert werden. Diese unterfallen dem subsidiären Schutz des RiS.[53] Anruflisten, SMS, Browserverläufe, E-Mails etc., die auf dem Smartphone gespeichert sind, werden daher nicht von Art. 10 Abs. 1 GG erfasst.[54] Ausgenommen hiervon sind E-Mails, die auf zugangsgesicherten Mailservern eines Providers (zwischen)gespeichert sind und vom Empfänger noch nicht abgerufen wurden.[55]

V. Eingriffsermächtigung

Im vorgenannten Rahmen stehen den Ermittlungsbehörden auf Grundlage der Strafprozessordnung verschiedene Möglichkeiten zur Sicherung und Auswertung digitaler Spuren in Smartphones zur Verfügung. Als offene und punktuelle Maßnahme, sind hierzu insbesondere die §§ 94 ff. und § 110 StPO einschlägig.[56]

Mit Inkrafttreten der StPO im Jahr 1877 hatte sicher noch niemand auf Smartphones gespeicherte Daten im Blick, denen es am Merkmal der Körperlichkeit fehlt. Dennoch sind diese Normen, wie im Falle des § 94 StPO, seit über 100 Jahren beinahe unverändert.[57] Die Rechtsprechung des *BVerfG* hat mehrfach betont, dass Grundrechte, besonders im Hinblick auf sich ständig verändernde Möglichkeiten moderner DV-Systeme, entwicklungsoffen zu interpretieren sind.[58] Dies wirkt gleichzeitig auch auf die StPO als Eingriffsbefugnis, woraus folgt, dass auch diese Befugnisse, einer fortschrittlichen Auslegung zugänglich sind.[59] Obwohl das *BVerfG* die Sicherstellung von Emails auf Grundlage des § 94 StPO grds. für zulässig erachtet[60], eröffnet die bloße Auslegung historischer, für eine analoge Welt geschaffene Normen im modernen, digitalen Kontext, anstelle gesetzgeberischer Anpassungen jedoch Unsicherheitszonen. Dies birgt die Gefahr unterschiedlicher gerichtlicher Entscheidungen, sodass insbesondere die vom *BVerfG* geforderte Normenklarheit fehlt.

1. Sicherstellung und Beschlagnahme von Gegenständen gem. § 94 StPO

§ 94 StPO regelt die Sicherstellung von Gegenständen die als Beweismittel in Betracht kommen sowie die Beschlagnahme derselben, sofern diese nicht freiwillig herausgegeben werden.[61] Für eine Beschlagnahme ohne vorherige gerichtliche Anordnung, ist die Einholung einer richterlichen Bestätigung gem. § 98 Abs. 2 StPO obligatorisch.

Der im Wortlaut der Norm verwendeten Begriff „Gegenstände“, wird in der StPO nicht näher beschrieben. Er wird daher in der Rechtsprechung und dem Schrifttum unterschiedlich interpretiert.[62] Unstreitig ist, dass Smartphones körperliche Gegenstände sind, was sie zu tauglichen Objekten der Beschlagnahme macht.[63] Streitig ist indes, ob auch gespeicherte (Kommunikations-)Daten diesem Gegenstandsbegriff unterfallen. Während das *BVerfG* und Teile der Literatur[64] die Möglichkeit sehen auch gespeicherte Daten selbst zu beschlagnahmen, wird dies von anderen Autoren als Überdehnung der Wortlautgrenze abgelehnt.[65]

---

48 Vgl. *Warken,* NZWiSt 2017, 289 (292) unter Verweis auf *BVerfG*, Nichtannahmebeschl. v. 13.11.2010 – 2 BvR 1124/10 = WM 2011, 211.

49 Vgl. *Burghart,* in: Leibholz/Rinck, GG, 2018, Art. 10 Rn. 1.

50 Vgl. BVerfGE 67, 157 (172); 85, 386 (396); 115, 166 (183); 120, 274 (307). *Burghart,* in: Leibholz/Rinck, GG, Art. 10 Rn. 31; *Wenzel,* NZWiSt 2016, 85 (89).

51 Vgl. BVerfGE 115, 166 (183); *Burghart,* in: Leibholz/Rinck, GG, Art. 10 Rn. 31.

52 Vgl. BVerfGE 124, 43 (54); *Warken,* NZWiSt 2017, 289 (292).

53 BVerfGE 115, 166.

54 Vgl. *Wenzel,* NZWiSt 2016, 85 (89).

55 Vgl. BVerfGE 124, 43 (54 f.); *Burghart,* in: Leibholz/Rinck, GG, Art. 10, Rn. 31.

56 Vgl. *Blechschmidt,* MMR 2018, 361 (363); *Wenzel,* NZWiSt 2016, 85.

57 Vgl. *Menges,* in: LR-StPO, 27. Aufl. (2019), § 94 Entstehungsgeschichte; *Ruppert,* Jura 2018, 994.

58 Vgl. BVerfGE 106, 28 (36); 115, 166 (182); 120, 274 (307); 46, 120 (144).

59 Vgl. *Ruppert,* Jura 2018, 994.

60 Vgl. BVerfGE 124, 43 (58 f.).

61 Vgl. *Hartmann/Schmidt,* Strafprozessrecht, 5. Aufl. (2015), Rn. 416.

62 Vgl. *Bär,* Handbuch zur EDV-Beweissicherung, Bd. 13, 2007, Rn. 406.

63 Vgl. *Gercke,* in: HK-StPO, 6. Aufl. (2019), § 94 Rn. 17; *Menges,* in: LR-StPO, § 94 Rn. 11; *Bär,* Handbuch zur EDV-Beweissicherung, Rn. 405; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 418; *Blechschmidt,* MMR 2018, 361 (364).

64 Vgl. BVerfGE 113, 29 (50); *BVerfG*, Nichtannahmebeschl. v. 25.7.2007 – 2 BvR 2282/06 2007 (Rn. 12), wodurch das *BVerfG* der Forderung nach einer fortschrittlichen Normauslegung nachkommt. Vgl. weiter *Hartmann/Schmidt,* Strafprozessrecht, Rn. 418; *Park,* Durchsuchung und Beschlagnahme, 4. Aufl. (2018), Rn. 804; *Blechschmidt,* MMR 2018, 361 (364).

65 Vgl. *Gercke,* in: HK-StPO, § 94 Rn. 18; *Roxin/Schünemann,* Strafverfahrensrecht, 28. Aufl. (2014), § 34 Rn. 4; *Cornelius,* in: Münchner Anwaltshandbuch IT-Recht, 3. Aufl. (2013), Teil 10 Rn. 465; *Bär,* Handbuch zur EDV-Beweissicherung, Rn. 407.

a) Voraussetzung der Beschlagnahme

Voraussetzung für die Beschlagnahme ist die potentielle Beweisbedeutung des Smartphones bzw. der darauf gespeicherten Daten, weshalb zunächst der Anfangsverdacht einer Straftat gem. § 152 Abs. 2 StPO vorliegen muss.[66] Damit ist ein Zugriff auf den umfassenden und teilw. sensiblen Datenbestand eines Smartphones unter den „[...]denkbar geringsten Voraussetzungen möglich[...]"[67]. Weiterhin müssen die Daten auf dem Smartphone für das Straf- bzw. Ermittlungsverfahren von Bedeutung sein. D.h., sie müssen mittelbar oder unmittelbar für die Tat oder die Tatumstände einen Beweis erbringen können.[68] Bei Smartphones genügt dabei schon der potentielle Beweiswert der gespeicherten Daten, um eine Beschlagnahme begründen zu können.[69] Jüngst urteilte jedoch das *LG Kiel*, dass sich aufgrund des Umfangs der auf den Geräten gespeicherten Daten, immer die Vermutung einer potentielle Beweisbedeutung dieser Daten anstellen lasse.[70] Die Vermutung der Beweisbedeutung müsse sich daher auf bisherige Ermittlungsergebnisse stützen und bereits im Vorfeld einer möglichen Durchsuchung bestehen. Die Beschlagnahme eines aufgefundenen Smartphones, das als Beweismittel nicht im Durchsuchungsbeschluss genannt werde, sei daher unzulässig.[71]

b) Beschlagnahme von Telekommunikationsdaten

Inhalts- und Verbindungsdaten können sowohl im Speicher als auch in der SIM-Karte moderner Smartphones abgelegt sein. Diese außerhalb eines laufenden Kommunikationsvorgangs gespeicherten Daten im Herrschaftsbereich des Betroffenen, unterliegen nicht dem Schutz des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG sondern dem des RiS aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. § 94 StPO stellt damit eine zulässige Ermächtigungsgrundlage für die Beschlagnahme dieser Daten dar.[72] Für Emails, die sich zum Zeitpunkt der Auswertung des Smartphones noch auf zugangsgesicherten Servern eines Providern befinden, gilt dies im Hinblick auf den Schutzbereich nicht. Diese sind bis zu ihrer endgültigen Ankunft im Herrschaftsbereich des Kommunikationsteilnehmers durch das Telekommunikationsgeheimnis geschützt.[73] Dennoch erkennt das *BVerfG* auch in diesem Fall § 94 StPO als zulässige Ermächtigungsgrundlage an, sofern der Eingriff offen und nur punktuell erfolgt.[74]

c) Auswertung des Smartphones

Für die Auswertung der nach § 94 StPO sichergestellten Gegenstände und Daten gibt es in der StPO keine einschlägigen Regelungen, weshalb sich die Maßnahmen am Zweck des Ermittlungsverfahrens und der Sicherung der Originalität des Beweismittels auszurichten haben.[75] Datenerhebung, -speicherung und -auswertung außerhalb des eigentliches Beweiszweckes verbieten sich daher. Gleichzeitig ist dem jeweiligen Datensatz von außen jedoch nicht anzusehen ob er beweiserheblich ist oder nicht, weshalb häufig zumindest eine Sichtung der Daten erforderlich ist. Die Auswertung von Smartphones kann, je nach Anforderung, auf unterschiedliche Weise erfolgen. Die Spanne reicht dabei vom einfachen Abfotografieren des Displays über den Einsatz sog. Forensik Software bis hin zum „Chip-Off"-Verfahren, bei dem einzelne Bauteile des Smartphones entfernt und anschließend mit einer Auswertungshardware verbunden werden.[76] Unter Auswertung ist die Inaugenscheinnahme des Dateninhalts zu verstehen.[77]

Durch die genannten Maßnahmen erlaubt die Beschlagnahme und Auswertung eines Smartphones nach § 94 Abs. 2 StPO den Zugriff auf einen großen heterogenen Datenbestand und damit die umfassende Gewinnung von Erkenntnissen, bis hin zur Bildung eines vollständigen Persönlichkeitsprofils des Nutzers. Damit gehen diese Maßnahmen auf Grundlage der geringsten Verdachtsform des Anfangsverdachtes weit über das ursprüngliche, mit einer Beschlagnahme bezweckte, Maß hinaus.[78] Die gesteigerten Möglichkeiten der Ausforschung führen zu deutlich sensibleren Einblicken und damit zu bedeutend intensiveren Eingriffen in die Grundrechte der Betroffenen. Die Eingriffe stützen sich dabei auf eine Ermächtigungsgrundlage, die seit Inkrafttreten der StPO unverändert Bestand hat, was einen Anpassungsbedarf insbesondere zur Begrenzung der Eingriffsintensität offensichtlich werden lässt.

Das *BVerfG* stellt in seinem Urteil zur Onlinedurchsuchung fest, dass mit der Infiltration eines komplexen informationstechnischen Systems, die entscheidende Hürde zur Ausspähung des Systems insgesamt genommen sei.[79] Die Auswertung eines Smartphones mithilfe forensischer Analysetools ermöglicht ebenfalls die vollumfängliche Ausspähung des Systems. Auch wenn dies, im Gegensatz zur Online-Durchsuchung, offen erfolgt und keine fortlaufende Überwachung ermöglicht, besteht im Hinblick auf den möglichen Umfang der gewonnenen Daten und damit der Intensität des Grundrechtseingriffs diesbezüglich zumindest eine Nähe zwischen der Auswertung von Smartphones und der Onlinedurchsuchung.[80]

2. Durchsicht von Papieren § 110 StPO

Der mögliche Umfang des Datenbestandes sowie die unterschiedlichen Arten von Daten auf einem Smartphone, stellen die Strafverfolgungsbehörden regelmäßig vor

66 Vgl. *Hartmann/Schmidt,* Strafprozessrecht, Rn. 421.
67 *Singelnstein,* NStZ 2012, 593 (598).
68 Vgl. BVerfGE 77, 1 (53); *Menges,* in: LR-StPO, § 94 Rn. 30; *Gercke,* in: HK-StPO, § 94 Rn. 28 f.
69 Vgl. *Ruppert,* Jura 2018, 994 (995).
70 *LG Kiel,* Beschl. v. 25.4.2016 – 7 Qs 24/16, in Anlehnung an *LG Berlin*, Beschl. v. 15.1.2004 – 518 Qs 44/03.
71 Vgl. *LG Kiel*, Beschl. v. 25.4.2016 – 7 Qs 24/16 (Rn. 18, 21).
72 *BVerfG*, Nichtannahmebeschl. v. 25.7.2007 – 2 BvR 2282/06 2007.
73 Vgl. BVerfGE 124, 43 (54 f.).
74 Vgl. BVerfGE 124, 43 (58 f.); *Blechschmidt,* MMR 2018, 361, (364); *Warken,* NZWiSt 2017, 417 (418).
75 Vgl. *Blechschmidt,* MMR 2018, 361 (364); *Gercke,* in: HK-StPO, § 94, Rn. 24.
76 Vgl. *Rogge,* Der Kriminalist 2015, 29 (31).
77 Vgl. *Zerbes/El-Ghazi,* NStZ 2015, 425 (427).
78 Vgl. *Singelnstein,* NStZ 2012, 593 (602).
79 Vgl. BVerfGE 120, 274 (308).
80 Vgl. *Momsen,* DRiZ, 2018, 140 (143).

Probleme. Die schiere Menge der Daten und die Komplexität der Smartphones lässt die, für eine Beschlagnahme geforderte, potentielle Beweisbedeutung auf den ersten Blick nicht erkennen. Daher kommt eine Beschlagnahme zu diesem Zeitpunkt nicht in Betracht. Jedoch gestattet § 110 Abs. 1 StPO der Staatsanwaltschaft, sowie auf deren Anordnung ihren Ermittlungspersonen, „[d]ie Durchsicht von Papieren des von der Durchsuchung Betroffenen […]“ um zu einem späteren Zeitpunkt eine Beschlagnahmeentscheidung treffen zu können.[81] Die Durchsicht von Papieren gilt daher als Teil der Durchsuchung[82] oder wird als vorläufige Sicherstellung[83] bezeichnet. Die Anwendung der Norm in Rechtsprechung und Praxis geht in zweifacher Hinsicht über den Wortlaut des Gesetzestextes hinaus. Zum einen sind nach dem *BVerfG* auch elektronische Datenträger vom Begriff „Papiere“ umfasst.[84] Zum anderen soll sich die Befugnis zur Durchsicht von Papieren auch auf Gegenstände erstrecken, die nicht auf dem Wege einer Durchsuchung in das Gewahrsam der Strafverfolgungsbehörden gelangt sind.[85] Damit ist die Durchsicht von Smartphones als Datenträger grds. zulässig.

Auch wenn die Durchsicht nach h.M. dem Schutz der Persönlichkeitsrechte des Betroffenen einer Durchsuchung dient[86], stellt sie sich in der Realität häufig als weitreichender Eingriff in dessen Lebensbereich dar.[87] Für die Bestimmung des sachlichen Umfangs der Maßnahme steht der Staatsanwaltschaft, respektive ihren Ermittlungspersonen, ein weiter Ermessenspielraum zu.[88] Damit erfolgt häufig ein ausgedehnter Zugriff auf alle im Smartphone befindlichen Daten und darüber hinaus, durch § 110 Abs. 3 StPO legitimiert, ggf. auch auf Cloud-Datenspeicher, sofern sie vom Smartphone aus erreichbar sind. Erschwerend kommt hinzu, dass dieser Zugriff aufgrund der technischen Gegebenheiten regelmäßig in den Diensträumen der Strafverfolgungsbehörde stattfinden muss[89], ohne dass der Betroffene die Möglichkeit hat persönliche oder für das Strafverfahren irrelevante Daten zurückzuhalten.[90] Eine solche Mitnahme wird z. B. dann erforderlich sein, wenn das Smartphone eine Zugangssicherung oder eine Verschlüsselung aufweist und diese erst durch technische Mittel überwunden werden muss.[91] Die Überwindung von digitalen Zugangssicherungen ist, ähnlich dem Öffnen verschlossener Behältnisse in der analogen Welt, im Rahmen der Durchsicht eine zulässige Maßnahme.[92]

Die in § 110 Abs. 3 StPO a. F. festgeschriebene Möglichkeit des Betroffenen an der Durchsicht teilzunehmen, wurde 2004 durch das JuMoG ersatzlos gestrichen.[93] Zwar könne sich nach Ansicht des *BVerfG* ein Anwesenheitsrecht auch aus Verhältnismäßigkeitserwägungen ergeben[94], die vorinstanzlichen Entscheidungen in dieser Sache zeigen jedoch die Abhängigkeit von der Beurteilung des jeweiligen Gerichtes. Auch die Durchsicht von Papieren rückt damit in die Nähe der verdeckten Maßnahmen gem. § 100a ff. StPO. So ist die Maßnahme dem Einzelnen zwar bekannt und damit Rechtschutz in Form gerichtlicher Überprüfung möglich[95], die fehlende Begrenzung der Durchsicht in sachlichem und zeitlichem Umfang sowie das nur vage zugestandene Anwesenheitsrecht durch die Rechtsprechung zeigen jedoch, dass der Durchsicht wesentliche Elemente einer offenen Maßnahme fehlen.[96] Darüber hinaus kann sich die Durchsicht von Kommunikationsdaten gegenüber dem jeweiligen Kommunikationspartner als verdeckte Maßnahme darstellen, sofern dieser nicht von der Maßnahme unterrichtet wird. Eine entsprechende Ermächtigung auch gegenüber unvermeidbar betroffenen Dritten, bspw. analog zu § 100b Abs. 3 S. 3 StPO, besteht jedoch nicht.

Auch die Maßnahme der Durchsicht von Papieren stammt aus einer Zeit, in der sie tatsächlich auf die in der Norm genannten Papiere beschränkt war. Zum Zeitpunkt ihrer Schaffung konnte der Gesetzgeber nicht die massive Eingriffsqualität vorhersehen, die sich aus der Digitalisierung sämtlicher Lebensbereiche, z. B. durch die Nutzung von Smartphones ergibt.[97]

3. Grundsatz der Verhältnismäßigkeit

Als übergeordnete Leitregel allen staatlichen Handelns wirkt auch im strafrechtlichen Ermittlungsverfahren der mit Verfassungsrang ausgestattete Grundsatz der Verhältnismäßigkeit.[98] Dies gilt sowohl für § 110 StPO als auch für § 94 StPO, obwohl den Ermittlungsbehörden nach dem reinen Wortlaut dieser Normen kein Ermessen zusteht.[99] Bei der Beschlagnahme und Auswertung von Smartphones sowie darauf befindlicher Daten setzt der Grundsatz der Verhältnismäßigkeit dem staatlichen Handeln aufgrund der besonderen Eingriffstiefe und Grundrechtsrelevanz Grenzen.[100] Insbesondere die hohe Ein-

---

81 Vgl. *Peters,* NZWiSt 2017, 465; *Blechschmidt,* MMR 2018, 361 (363).

82 Vgl. BGHSt 44, 265 (273); *Tsambikakis,* in: LR-StPO, § 110, Rn. 28; a.A. *Peters,* NZWiSt 2017, 465 (472).

83 Vgl. *BVerfG*, Nichtannahmebeschl. v. 28.4.2003 – 2 BvR 358/03 = NJW 2003, 2669; *Peters,* NZWiSt 2017, 465 (466).

84 Vgl. BVerfGE 113, 29 (51).; BT-Drs. 16/5846, S. 63. Trotz Ausweitung der Bedeutung des Begriffs „Papiere“ durch die Rechtsprechung sah der Gesetzgeber auch bei der letzten Reform des § 110 StPO im Jahr 2004 keine Veranlassung den Wortlaut zu verändern. Vgl. BT-Drs. 15/3482.

85 Vgl. *Tsambikakis,* in: LR-StPO, § 110 Rn. 21.

86 Vgl. *Tsambikakis,* in: LR-StPO, § 110 Rn. 1; *Gercke,* in: HK-StPO, § 110 StPO Rn. 1; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 531.

87 Vgl. *Peters,* NZWiSt 2017, 465.

88 Vgl. *Tsambikakis,* in: LR-StPO, § 110 Rn. 28.

89 Vgl. *Zerbes/El-Ghazi,* NStZ 2015, 425 (426).

90 Vgl. *Peters,* NZWiSt 2017, 465 (467).

91 Vgl. *Momsen,* DRiZ 2018, 140, mit Verweis auf Nutzung einer PIN als "kleines Einmaleins des privaten Datenschutzes" und der sich schon daraus ergebenden technischen Schwierigkeiten für Strafverfolgungsorgane.

92 Vgl. *Zerbes/El-Ghazi,* NStZ 2015, 425 (427); *Meyer-Goßner/Schmitt,* StPO, 62. Aufl. (2019), § 110 Rn. 6.

93 Vgl. BGBl. I 2004, Nr. 45, S. 2201.

94 Vgl. BVerfGE 113, 29 (58).

95 Auch die Durchsicht ist als „vorläufige Sicherstellung“ gem. § 98 Abs. 2 StPO richterlich überprüfbar, vgl. *Herrmann/Soiné,* NJW 2011, 2922 (2925).

96 Vgl. *Peters,* NZWiSt 2017, 465 (469).

97 *Peters,* NZWiSt 2017, 465 (469 f.).

98 Vgl. BVerfGE 20, 162 (187); *Burghart,* in: Leibholz/Rinck, GG, Art. 20 Rn. 776; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 431.

99 Vgl. *Hartmann/Schmidt,* Strafprozessrecht, Rn. 431; *Hauschild,* in: MüKo-StPO, 2014, § 94 Rn. 10.

100 *Park,* Durchsuchung und Beschlagnahme, Rn. 828.

griffsintensität erfordert eine enge Auslegung des Verhältnismäßigkeitsgrundsatzes.[101] Danach müssen die Maßnahme und der mit ihr einhergehende Grundrechtseingriff insgesamt in einem angemessenen Verhältnis zur Schwere der Straftat und der Stärke des Tatverdachts stehen. Eine nur leichte Straftat, eine geringe Beweisbedeutung der Daten oder ein nur vager Auffindeverdacht können einer Beschlagnahme und Auswertung eines Smartphones daher entgegenstehen.[102]

Über § 46 OWiG sind die Vorschriften der StPO auch im Ordnungswidrigkeitenverfahren anwendbar. Die hohe Eingriffsintensität im Hinblick auf die Auswertung eines Smartphones in Verbindung mit dem Verhältnismäßigkeitsgrundsatz dürften einer solchen Maßnahme jedoch grundsätzlich entgegenstehen.[103]

Die Beachtung des Verhältnismäßigkeitsgrundsatzes erfordert eine Beschränkung des Zugriffs auf den Datenbestand in sachlicher wie auch in zeitlicher Hinsicht. Die Strafverfolgungsbehörden sind daher verpflichtet, eine Erhebung nicht verfahrensrelevanter Daten zu vermeiden[104] und die Auswertung des Smartphones in kürzester Zeit durchzuführen.[105] In der Praxis wird sich besonders der letztgenannte Aspekt als schwierig erweisen. Moderne Smartphones stellen schon mit einfach verfügbaren Sicherungsmethoden wie einer PIN-Sperre die Strafverfolgungsbehörden vor große technische Probleme.[106] Fraglich ist daher schon in welchem zeitlichen Rahmen Ermittler, z.B. bei der Verfolgung eines niedrigschwelligen Vergehens versuchen dürfen die Sicherung eines Smartphones zu umgehen, ohne den Grundsatz der Verhältnismäßigkeit zu missachten.

Auch wenn Maßnahmen nach §§ 94 und 110 StPO als offene Maßnahmen mit nur punktuellem Eingriff gelten, reicht ihre Eingriffsintensität aufgrund des Umfangs der erhobenen Daten an die der verdeckten Maßnahmen der §§ 100a ff. StPO heran. Während bei den letztgenannten Bestimmungen der Grundsatz der Verhältnismäßigkeit in Form der Subsidiaritätsklauseln eine einfachgesetzliche Ausformung erhält[107], fehlt eine ähnliche Ausgestaltung für Sicherstellung und Durchsicht vollends.

4. Kernbereichsschutz

Neben dem Grundsatz der Verhältnismäßigkeit stellt der Schutz des Kernbereichs privater Lebensgestaltung die zweite wesentliche Begrenzung staatlicher Eingriffe, insbesondere bei der Auswertung elektronischer Daten dar. Unter Kernbereich wird ein letzter unantastbarer Bereich menschlicher Freiheit verstanden, welcher der Einwirkung der öffentlichen Gewalt, auch in Abwägung mit dem Informationsbedürfnis der Strafverfolgungsbehörden zur Sicherung einer funktionierenden Strafrechtspflege, nicht zugänglich ist.[108] Was konkret vom absolut geschützten Kernbereich umfasst wird, ist nicht abschließend geklärt.[109] Dem Kernbereich unterfällt nach dem *BVerfG* die Möglichkeit „[...]innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen[…]“ sowie die vertrauliche Kommunikation mit anderen.[110] Anhand der dargestellten technischen Möglichkeiten von Smartphones scheint es unbestritten, dass sich auf den Geräten Daten und Informationen finden lassen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Dies schließt die Beschlagnahme und Auswertung der Geräte nicht per se aus, macht aber eine Sichtung und Bestimmung möglicher Kernbereichsinhalte erforderlich, da der jeweilige Inhalt den Daten von außen nicht anzusehen ist.[111] Hier zeigt sich das Paradoxon des Kernbereichsschutzes. Um zu bestimmen was dem Kernbereich unterfällt, ist ggf. eine, wenn auch geringfügige, Verletzung eben dieses Kernbereichs erforderlich.[112] Der Gesetzgeber begegnete diesem Umstand für die heimliche Maßnahme der Online-Durchsuchung gem. § 100b StPO auf Erhebungs- und Auswertungsebene durch die gesetzlichen Regelungen zum Kernbereichsschutz in § 100d Abs. 3 StPO. Danach ist durch technische Vorkehrungen weitestgehend sicherzustellen, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, nicht erhoben werden bzw. unverzüglich zu löschen sind, falls eine Erhebung stattfand. [113]

Obwohl ein Eingriff durch Beschlagnahme und Auswertung von Smartphones, zumindest was Umfang und Informationsgehalt sichergestellter Daten anbelangt, im Vergleich zur Onlinedurchsuchung als ähnlich gravierend bezeichnet werden kann, fehlt für Beschlagnahme und Durchsicht von Papieren eine entsprechende einfachgesetzliche Regelung.

VI. Anpassungsbedarf/ Fazit

Die hohe Komplexität von Smartphones als IT-Systeme machen einen wirksamen Selbstschutz des durchschnittlichen Nutzers im Hinblick auf die gespeicherten Daten kaum möglich.[114] Smartphones erweisen sich für die Strafverfolgungsbehörden zunehmend als sehr gute Informationsquelle, da sie bei vollständiger Auswertung des Datenträgers ein umfassendes Persönlichkeitsbild des Betroffenen ermöglichen, was mit intensiven Eingriffen in dessen Grundrechtspositionen verbunden ist.

---

101 *Momsen,* DRiZ 2018, 140 (143).
102 Vgl. BVerfGE 96, 44 (51); BVerfGE 113, 29 (57); BVerfGE 124, 43 (66); *Singelnstein,* NStZ 2012, 593 (598).
103 ^Vgl. *Menges,* in: LR-StPO, § 94 Rn. 3; *Hartmann/Schmidt,* Strafprozessrecht, Rn. 413; a.A. *Ternig/Lellmann,* NZV 2016, 454, die eine Beschlagnahme und Auswertung eines Mobiltelefons zur Verfolgung einer Owi für zulässig erachten.
104 Vgl. *Singelnstein,* NStZ 2012, 593 (598).
105 Vgl. *Wenzel,* NZWiSt 2016, 85 (93) unter Verweis auf *AG Reutlingen*, Beschl. v. 5.12.2011 – 5 Gs 363/11 (Rn. 4).
106 Vgl. *Momsen,* DRiZ 2018, 140.
107 Vgl. *Gercke,* in: HK-StPO, § 100a Rn. 21.
108 Vgl. BVerfGE 109, 279 (313 ff.); *Gercke,* in: HK-StPO, vor § 94 Rn. 18; *Czerner,* in: Labudde/Spranger, Forensik in der digitalen Welt, 2017, S. 265 (273).
109 *Hartmann/Schmidt,* Strafprozessrecht, Rn. 426; *Menges,* in: LR-StPO, § 94 Rn. 77.
110 Vgl. BVerfGE 109, 279 (313).
111 *Hartmann/Schmidt,* Strafprozessrecht, Rn. 427.
112 Vgl. BverfGE 109, 279 (383), Sondervotum der Richterinnen *Jaeger* und *Hohmann-Dennhart*.
113 Vgl. BT-Drs. 18/12785, S. 56.
114 Vgl. BVerfGE 120, 274 (306).

Das *BVerfG* stellte bereits 2005 fest, dass der Gesetzgeber den Grundrechtsschutz bei staatlichen Ermittlungshandeln, ggf. durch Anpassung bestehender oder Schaffung ergänzender Regelungen effektiv sichern müsse.[115]

Im Hinblick auf die geforderte Normenklarheit und das Bestimmtheitsgebot ist zunächst an eine generelle Veränderung des Wortlauts der Normen zu denken. Der Anwendungsbereich der Beschlagnahme von Beweismitteln und der Durchsicht von Papieren wurde durch die Rechtsprechung immer weiter, z. T. über den Wortlaut hinaus, ausgedehnt. Eine Änderung der Bezeichnung „Papiere" in „Informationsträger" in § 110 StPO oder die Erweiterung des § 94 Abs. 1 StPO auf Daten könnten zur geforderten Normenklarheit beitragen.

Die hohe Eingriffsintensität ergibt sich nicht zuletzt aus der Tatsache, dass die Auswertung des Smartphones häufig nicht im Beisein des Betroffenen stattfindet. Der Betroffene hat damit keine Möglichkeit zu überprüfen, auf welche Daten tatsächlich zugegriffen wurde und ob der Zugriff für das zugrundliegende Ermittlungsverfahren tatsächlich erforderlich war. Ein grundsätzliches Anwesenheitsrecht des Betroffenen könnte die Eingriffsintensität verringern und gleichzeitig die Effektivität der Auswertung erhöhen, da der anwesende Betroffene nicht relevante Daten benennen und so eine langwierige Auswertetätigkeit aller im Smartphone gespeicherter Daten unterbleiben könnte. Zugleich würde dadurch der zeitliche Umfang der Maßnahme reduziert und so den Verhältnismäßigkeitsanforderungen genüge getan werden.

Ein weiterer Aspekt im Rahmen von Verhältnismäßigkeitsabwägungen stellt die Beschränkung der Zulässigkeit der Beschlagnahme und Auswertung von Smartphones nur für Ermittlungen bei bestimmten Straftaten dar. Diskussionen in der Literatur, die eine Smartphoneauswertung schon bei Ordnungswidrigkeiten als zulässig erachten, bis hin zu Forderungen, diese Maßnahmen nur unter den strikten Voraussetzungen des § 100a StPO als rechtmäßig anzusehen, zeigen exemplarisch den vorhandenen Regelungsbedarf. Ob für diese Beschränkung ein strikter Katalog oder bspw. mindestens ein Verbrechenstatbestand zu fordern ist, wäre in einem Gesetzgebungsverfahren mit Blick sowohl auf die Bedeutung der betroffenen Grundrechte und der Eingriffsintensität als auch auf das Erfordernis der Funktionstüchtigkeit der Strafrechtspflege, zu erörtern.

Den §§ 94 und 110 StPO fehlt in Bezug auf erlangte Daten eine einfachgesetzliche Regelung zum Schutz des Kernbereichs (analog zu § 110 d StPO). Insbesondere die in § 100d Abs. 2 StPO festgeschriebene Pflicht zur Löschung der Daten, Verwertungsverbote sowie der in § 100d Abs. 3 StPO geforderte Einsatz technischer Mittel kommen auch für die Durchsicht und Auswertung beschlagnahmter Smartphones in Betracht und könnten dazu beitragen die Eingriffsintensität der Maßnahme zu reduzieren.

Wie sich gezeigt hat, sind die derzeitigen Eingriffsermächtigungen der StPO nur bedingt geeignet, die tiefgreifenden Grundrechtseingriffe, die sich aus der Beschlagnahme und Auswertung von Smartphones ergeben, zu rechtfertigen. Die Anpassung der Eingriffsermächtigungen an die fortschreitende Digitalisierung aller Lebensbereiche, die sich insbesondere bei Smartphones zeigt, erscheint daher kriminalpolitisch geboten.

[115] Vgl. *BVerfG,* Urt. v. 12.4.2005 – 2 BvR 581/01 (Rn. 64).

Gewalt gegen Polizistinnen und Polizisten und Präventivmaßnahmen zur Eigensicherung

Zu einem vernachlässigten Blickwinkel auf Konflikte zwischen Polizei und Bevölkerung

*von Prof. Dr. Dr. Markus Thiel**

Abstract
Gewalt gegen Polizistinnen und Polizisten ist ein Phänomen, das in jüngerer Zeit aufgrund der Anzahl der festzustellenden Übergriffe und ihrer sich wandelnden Qualität eine besondere Dringlichkeit erreicht hat und zwingend einer kurzfristig wirksamen und langfristig wirkenden „Gegenstrategie" bedarf. In der Diskussion stehen dabei u. a. strafrechtliche Erwägungen, die sich etwa mit der Ahndung von Widerstandshandlungen und Übergriffen gegen Polizeivollzugsbeamte und einer wirkungsvolleren Verfolgung derartiger Delikte beschäftigen. Der gefahrenabwehrrechtliche Blickwinkel erscheint im Kontext der Thematik demgegenüber eher vernachlässigt. Dieser Aufsatz untersucht, welchen Beitrag das präventive Polizeirecht, namentlich die Regelungen zur sog. „Eigensicherung", zur Bewältigung der Problematik leisten kann. Dazu werden die Eigensicherung in den Kontext des Gefahrenabwehrrechts eingeordnet und das bestehende Maßnahmeninstrumentarium am Beispiel des nordrhein-westfälischen Polizeigesetzes untersucht; es schließen sich Überlegungen zu einer Ausweitung des präventiven „Eigensicherungsrechts" an.

Violence against policemen and policewomen is a phenomenon that has become particularly urgent in recent times due to the number of attacks and their changing quality. It urgently requires a "counter-strategy" that is effective in the short term and in the long term. In the discussion are among other things criminal law considerations, which deal with the punishment of acts of resistance and attacks against police officers and a more effective prosecution of such offences. In the context of the topic, however, the perspective of the law on the prevention of danger seems rather neglected. This essay examines the contribution that preventive police law, in particular the regulations on so-called "self-protection", can make to coping with the problem. To this end, self-protection is placed in the context of risk prevention law, and the existing range of measures is examined using the example of the North Rhine-Westphalian Police Act; this is followed by considerations on extending the preventive "self-protection law".

I. Einleitung

Die Medien berichten zunehmend häufiger sowohl von Fällen übertriebener polizeilicher Gewalt[1] als auch von erheblichem Widerstand und Gewalttätigkeiten gegenüber Polizeibeamtinnen und Polizeibeamten.[2] Es ist deutlich eine negative Entwicklung im Hinblick auf die Eskalation von – im Zusammenhang mit unerwünschten Eingriffsmaßnahmen grundsätzlich in der Natur der Sache liegenden und von der Rechtsordnung „antizipierten" – Konflikten zwischen Sicherheitskräften und verschiedenen Bevölkerungsteilen festzustellen; der Handlungsbedarf wird dringlicher.

Dabei ist „Polizeigewalt" ein medial und gesellschaftlich besonders sensibel wahrgenommenes Phänomen, begrifflich allerdings missverständlich: Dem Staat kommt das sog. „Gewaltmonopol"[3] zu, und zur Erfüllung ihrer Aufgaben darf die Polizei bei Beachtung der gesetzlichen Vorgaben, namentlich des Verhältnismäßigkeitsgrundsatzes, in vielen Fällen in rechtmäßiger Weise „Gewalt" ausüben,[4] etwa bei der Zwangsmittelanwendung in Gestalt des unmittelbaren Zwangs, der „Einwirkung auf Personen oder Sachen durch körperliche Gewalt, ihre Hilfsmittel oder durch Waffen" (vgl. § 58 Abs. 1 PolG NRW). Nicht jede polizeiliche Gewaltanwendung ist damit unzulässig oder auch nur unerwünscht. Problematisch sind indes zum einen die rechtswidrige, also nicht gerechtfertigte polizeiliche Gewaltanwendung, zum anderen der Exzess, also in Ausmaß, Intensität und Adressat „überschießendes" Handeln bei dem Grunde nach rechtmäßiger Gewaltausübung – derartige Fehltritte sind disziplinar-, dienst- und strafrechtlich zu ahnden. Hilfreich ist es, sich zur Abgrenzung von (rechtmäßiger) „Polizeigewalt" im Rahmen der poli-

* Der Verfasser ist Leiter des Fachgebietes III.4 – Öffentliches Recht mit Schwerpunkt Polizeirecht an der Deutschen Hochschule der Polizei in Münster.

1 Z.B. aktuell den Fall eines Bundespolizisten, der in der Nähe von Prüm auf eine andere Person eintritt; s. etwa auch *Steinke*, Wie gewalttätig ist die Polizei?, SZ v. 17.12.2018; derzeit wird an der Ruhr-Universität Bochum eine umfangreiche Studie zu illegaler Polizeigewalt durchgeführt (Forschungsprojekt „Körperverletzung im Amt durch Polizeibeamte", *Singelnstein*).

2 S. etwa tz v. 20.8.2019: Brutale Gewalt gegen Polizeibeamte; Focus online v. 6.5.2019: Gewalt gegen Polizisten hält an; zur Einrichtung einer zentralen Anlaufstelle Berliner Morgenpost v. 9.7.2019; s. auch *Börner*, JZ 2018, 870 ff.

3 *Müller*, Das staatliche Gewaltmonopol – historische Entwicklung, verfassungsrechtliche Bedeutung und aktuelle Rechtsfragen, 2007; *Kley*, Staatliches Gewaltmonopol – ideengeschichtliche Herkunft und Zukunft, 2006.

4 S. instruktiv zu aktuellen Entwicklungen etwa *Behr*, APuZ Nr. 21-23/2019, 24 ff., etwa zur Gewaltvermeidung und -reduzierung in Konzepten des *smart policing*; *Keidel*, Polizei und Polizeigewalt im Notstandsfall, 1972.

zeilichen Aufgabenerfüllung und (rechtswidriger) „Polizeigewalt“ im Sinne eines Missbrauchs[5] von Zwangsbefugnissen die englischsprachigen Begriffe *force* und *violence* vor Augen zu halten. Rechtswidrige *violence* seitens der Polizei ist auch in Deutschland durchaus kein marginaler Ausnahmefall; sie bedarf der eingehenden Aufarbeitung und Ahndung, sie erfordert Ausbildungs- und Fortbildungskonzepte, Vermeidungsstrategien und strukturelle Veränderungen, ist aber nicht Thema dieses Beitrags.

In der Öffentlichkeit deutlich weniger präsent ist Gewalt, die sich gegen Polizeibeamtinnen und -beamte richtet und – sofern sie nicht ihrerseits im Einzelfall von Notwehr- oder Nothilferechten gedeckt ist – im Regelfall rechtswidrig ist.[6] Die Vorfälle häufen sich, die Angriffe werden brutaler, Polizistinnen und Polizisten werden inzwischen sogar „außer Dienst“ tätlich angegriffen.[7] Längst nicht mehr sind Kollektivbeleidigungen wie „Bullenschweine“ oder „ACAB“ das größte Problem: Beim G20-Gipfel in Hamburg 2017 wurden Polizeibeamtinnen und -beamte von Häusern herab mit Steinen beworfen,[8] im Hambacher Forst werden sie von „Aktivisten“ mit Exkrementen aus Kübeln übergossen.[9] Bundesweit wurden 2018 rund 38.000 Gewalttaten gegen Polizeivollzugsbeamte registriert.[10] Derartige Gewaltphänomene werden häufig hingenommen oder mit perfiden Bemerkungen wie „Augen auf bei der Berufswahl!“ oder „Niemand muss Polizist sein!“ kommentiert, und nicht selten wird ihnen gar als Ausdruck eines vermeintlichen zivilen Ungehorsams oder legitimen Widerstands gegen einen als Gegner wahrgenommenen Staat und seine „Handlanger“ Beifall gezollt. Diese Entwicklungen gehen mit einem stetig sinkenden Respekt auch gegenüber Rettungskräften einher – Gaffer, die sich dreist am für ehrenamtliche Einsatzkräfte bereitgestellten Buffet bedienen,[11] sind da noch zu den harmloseren Ereignissen zu zählen.[12]

In der Wissenschaft wird das Phänomen der Gewalt gegen Polizeivollzugskräfte eingehend erforscht.[13] Aus rechtswissenschaftlicher Sicht liegt dabei ein Schwerpunkt auf der strafrechtlichen Bewältigung ihrer Erscheinungsformen – beispielhaft genannt werden können die Diskussion um die Ausweitung der Strafbarkeit wegen Widerstands gegen Vollstreckungsbeamte nach § 113 StGB[14] und die Kontroversen um weitere repressive Maßnahmen zur Verbesserung ihres Schutzes.[15] Zudem wird erörtert, wie die Gewährleistung der Sicherheit der handelnden Beamtinnen und Beamten in Ermittlungsverfahren verbessert werden kann. Vergleichbare Fragen stellen sich allerdings auch im präventiven Handlungsfeld, das bei der Diskussion um Gewalt gegen Polizeivollzugskräfte eher vernachlässigt erscheint. Mit derartigen Gesichtspunkten befasst sich das Konzept der polizeilichen Eigensicherung,[16] das vor allem Gegenstand der Einsatzlehre ist, aber auch vielfältige rechtliche Bezüge aufweist. Obwohl Aspekte der Eigensicherung in – häufig ein zügiges Handeln erfordernden – Gefahrenlagen von besonderer praktischer Bedeutung sind, stehen ihre gefahrenabwehrrechtlichen Rahmenbedingungen eher im Schatten; insbesondere fehlt derzeit noch eine auf breiterer Front geführte Debatte um eine eventuelle Ausweitung präventiv-polizeilicher Eigensicherungsmaßnahmen.

Dieser Beitrag befasst sich im Überblick mit einer rechtlichen Bestandsaufnahme der Regelungen zur polizeilichen Eigensicherung am Beispiel des „Referenz-Bundeslandes“ Nordrhein-Westfalen (II.), diskutiert Entwicklungsperspektiven (III.) und schließt mit einem Fazit (IV.).

II. Rechtliche Bestandsaufnahme

Im Kontext der bisherigen wissenschaftlichen Studien wird der Begriff der „Eigensicherung“ häufig definiert als „jedes aktive Verhalten von Polizeibeamten gegen Personen zum Schutz der eigenen körperlichen Unversehrtheit im Rahmen einer konkreten polizeilichen Maßnahme“.[17] Diese Definition trifft zwar den Kern der Problematik, weil sie die in der Praxis problematischsten Fallkonstellationen erfasst, greift aber zu kurz: Eigensicherungsmaßnahmen können auch zum Schutz anderer Rechtsgüter der Polizeibeamtinnen und -beamten erforderlich werden (z.B. der persönlichen Freiheit, der Rechts der persönlichen Ehre etc.), und sie müssen sich nicht zwangsläufig gegen Personen richten – der Schusswaffengebrauch gegenüber einem gefährlichen Tier ist ebenfalls ohne weiteres als Handlung zum Zwecke der Eigensicherung zu qualifizieren. Im Regelfall geht es allerdings tatsächlich um eine Verhinderung von Körperverletzungen und Gesundheitsschädigungen bzw. Maßnahmen zur Abschwächung ihres Ausmaßes und ihrer Folgen. Vollständiger, aber zugleich abstrakter sind Definitionen, die die Eigensicherung als das „taktisch richtige Verhalten im Einsatz zur

---

5 Vgl. *Braun/Albrecht*, DÖV 2015, 937 ff.

6 Dazu etwa *Wagner-Kern*, Recht und Politik 2018, 7 ff.; im Kontext des Linksextremismus *Goertz*, Kriminalistik 2019, 149 ff.; *Thieme*, APuZ Nr. 21-23/2019, 43 ff.; s. auch *de Maizière*, DRiZ 2016, 244 ff.

7 Vgl. den jüngsten Fall eines Angriffs auf Polizisten in Zivil in Hamm; ob die Opfer als Polizeibeamte erkannt worden sind, ist allerdings nach wie vor zweifelhaft, vgl. WAZ v. 29.8.2019.

8 Eine Bilanz zieht *Heinemann*, Zwei Jahre nach den G-20-Krawallen – die große Bilanz, Hamburger Abendblatt v. 1.7.2019.

9 Vgl. *Blasius*, Mit Fäkalien beworfen: Polizisten brechen Einsatz ab, WAZ v. 21.9.2018; zur Gesamtthematik *Schink*, NuR 2019, 77 ff.

10 *Bundeskriminalamt*, Gewalt gegen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte, Bundeslagebild 2018.

11 S. *Meltz*, Gaffer laben sich an Feuerwehr-Proviant, General-Anzeiger, 28.10.2016.

12 Zu Gewalterfahrungen von Rettungskräften im Einsatz *Rau/Leuschner*, Neue Kriminalpolitik 2018, 316 ff.

13 S. schon *Lottmann*, Polizeikurier 4/2000, 4 ff.; *Jager/Klatt/Bliesener*, NRW-Studie Gewalt gegen Polizeibeamtinnen und Polizeibeamte. Die subjektive Sichtweise zur Betreuung und Fürsorge, Aus- und Fortbildung, Einsatznachbereitung, Belastung und Ausstattung, 2013.

14 Dazu *Schiemann*, NJW 2017, 1846 ff.; *Busch*, Cilip – Bürgerrechte & Polizei 2017, Blog v. 26.4.2017; *Busch/Singelnstein*, NStZ 2018, 510 ff.; *Kulhanek*, JR 2018, 551 ff.; *Magnus*, GA 2017, 530 ff.; zum strafrechtlichen Schutz von Polizeibeamtinnen und -beamten insgesamt *Puschke/Rienhoff*, JZ 2017, 924 ff.

15 *Wagner-Kern*, Recht und Politik 2018, 7 ff.

16 Vgl. *Huber/Jäger*, in: Schriftenreihe der Polizei-Führungsakademie: Die polizeiliche Eigensicherung, 3&4/2001, S. 7 ff.; *Lorei*, Akzeptanz polizeilicher Eigensicherungsmaßnahmen durch Bürger, ebd., S. 50 ff.

17 *Mentzel/Schmitt-Falckenberg/Wischnewski*, Eigensicherung und Recht, 2003, S. 3; *Birr*, Normenkonflikte bei Polizeibeamten im Rahmen der Eigensicherung, 2014, S. 10.

Verhinderung beziehungsweise Reduzierung von Gefährdung für Einsatzkräfte“ beschreiben. Für die nachfolgende rechtliche Bewertung am Beispiel Nordrhein-Westfalens soll dieses weite Begriffsverständnis zugrunde gelegt werden.

1. Eigensicherung als Element der öffentlichen Sicherheit

Der Gedanke der polizeilichen Eigensicherung ist dem Schutzgut der öffentlichen Sicherheit zuzurechnen. Zu dieser sind nach gängiger Polizeirechtsdogmatik zu rechnen: Die Unverletzlichkeit der objektiven Rechtsordnung, der subjektiven Rechte und Rechtsgüter des Einzelnen und des Bestands und der Funktionsfähigkeit des Staates und anderer Träger hoheitlicher Gewalt, ihrer Einrichtungen und Veranstaltungen.[18] Die Polizei hat nach den Polizeigesetzen der Länder die Aufgabe, Gefahren für die öffentliche Sicherheit (und für die öffentliche Ordnung) abzuwehren (vgl. etwa § 1 Abs. 1 S. 1 PolG NRW). Maßnahmen zum Schutz der im Einsatz befindlichen Polizeibeamtinnen und -beamten sind damit aus gefahrenabwehrrechtlicher Sicht nicht nur eine Realisierung straf- und zivilrechtlicher Notwehr- und Nothilferechte, wie sie sich etwa aus §§ 32, 34, 35 StGB und §§ 227, 228 BGB ergeben,[19] sondern können auf solche öffentlich-rechtliche Eingriffsermächtigungen des präventiven Polizei- und Ordnungsrechts gestützt werden, die an die Abwehr von Gefahren für die öffentliche Sicherheit bzw. Ordnung anknüpfen oder von einer Gefahrenlage unabhängig sind, aber in den Aufgabenbereich der Polizei fallen (vgl. dazu § 1 Abs. 1 PolG NRW).

Polizeibeamtinnen und -beamte im Dienst sind Grundrechtsträger, so dass ihre Rechte auf Leben, körperliche Unversehrtheit, Gesundheit, Freiheit (Art. 2 Abs. 2 GG), informationelle Selbstbestimmung, persönliche Ehre (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) usw. als Individualrechtsgüter von der öffentlichen Sicherheit geschützt werden. Die Annahme, Polizistinnen und Polizisten könnten sich im Dienst nicht auf ihre Grundrechte berufen, ist zwar gelegentlich etwa im Zusammenhang mit der kontroversen Debatte um eine gesetzliche Pflicht zur individuellen (nicht nur nachträglich individualisierbaren) Kennzeichnung von Polizeibeamtinnen und -beamten geäußert worden,[20] muss in dieser Pauschalität jedoch – gleichsam als Rückfall in die düsteren Zeiten der „besonderen Gewaltverhältnisse“[21] mit einer generellen Ausschaltung der Grundrechtsgeltung – ausdrücklich verworfen werden. Die Frage, ob sie sich im Dienst auf ein konkretes Grundrecht berufen können, kann nur für jedes Grundrecht anhand der Umstände des Einzelfalls bestimmt werden. Nicht zugänglich dürften etwa die Schutzbereiche der Meinungsäußerungsfreiheit (Art. 5 Abs. 1 GG) und der Versammlungsfreiheit (Art. 8 Abs. 1 GG) sein; von diesen auf individuelle Kommunikation und Einwirkung auf die Meinungsbildung in der Öffentlichkeit ausgerichteten Grundrechten können Polizeivollzugskräfte im Dienst keinen Gebrauch machen. Uneingeschränkt Geltung beanspruchen dagegen das Recht auf Leben, körperliche Unversehrtheit und persönliche Freiheit (Art. 2 Abs. 2 GG) – wollte man Polizeibeamtinnen und -beamte im Dienst nicht als Träger individueller Rechtsgüter, sondern allein als „verlängerte Arme“ der Staatsgewalt schützen, stünde dies aufgrund der damit verbundenen Herabwürdigung zu bloßen Objekten in unauflösbarem Widerspruch zur absolut gewährleisteten Unverletzlichkeit der Menschenwürde (Art. 1 Abs. 1 GG). Auch der persönliche Schutzbereich der verschiedenen Einzelausprägungen des allgemeinen Persönlichkeitsrechts, etwa des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), ist eröffnet. Kollisionen mit Grundrechten anderer sind dann auf Ebene der Rechtfertigung bzw. der Verhältnismäßigkeit zu berücksichtigen.

Zur öffentlichen Sicherheit gehört ferner die Unverletzlichkeit der objektiven Rechtsordnung.[22] (Drohende) Verstöße gegen den objektiven Tatbestand von Verbots- und Strafnormen, die sich zu Lasten von Polizeibeamtinnen und -beamten auswirken, stellen damit ebenfalls eine Gefahr für die öffentliche Sicherheit dar, der die eingesetzten Kräfte mit dem Instrumentarium der Polizeigesetze begegnen dürfen. Schließlich ist die Funktionsfähigkeit der Polizei auch zur Schutzkomponente des Bestands und der Funktionsfähigkeit des Staates, seiner Einrichtungen und Veranstaltungen zu rechnen. Polizeibehörden sind dabei „Einrichtungen“ des Staates.[23] Gewalthandlungen gegen einzelne Polizeibeamtinnen und -beamte dürften aber meist keine relevante Beeinträchtigung der Funktionsfähigkeit der betroffenen Polizeibehörde als solche darstellen. Bei größeren Krawallen und ähnlichen Phänomenen kann dies im Einzelfall anders zu bewerten sein.

Nach alledem umfasst die Abwehr von Gefahren für die öffentliche Sicherheit auch den Schutz der in der Öffentlichkeit tätigen Polizeibeamtinnen und -beamten vor Rechtsgut- und Rechtsnormverletzungen.

2. Spezifische Eigensicherungsmaßnahmen

Mit hinreichender Wahrscheinlichkeit drohende oder fortgesetzte Gewalt gegen Polizeibeamtinnen und -beamte ist damit als Gefahr für die öffentliche Sicherheit zu qualifizieren. Damit stehen den Einsatzkräften grundsätzlich alle Eingriffsbefugnisse des präventiven Polizeirechts zur Verfügung, die tatbestandlich an eine solche Gefahrenlage anknüpfen oder von einer solchen unabhängig sind (z.B. die Befragung, vgl. § 9 Abs. 2 PolG NRW). Die Polizei kann eine Person, die gewalttätig zu werden droht, etwa zum Unterlassen auffordern (vgl. § 8 Abs. 1 PolG NRW), mit einem Platzverweis belegen (§ 34 Abs. 1 PolG

18 *Denninger*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. (2018), D Rn. 16 ff.; *Kingreen/Poscher*, Polizei- und Ordnungsrecht mit Versammlungsrecht, 10. Aufl. (2018), § 7 Rn. 2 ff.; *Thiel*, Polizei- und Ordnungsrecht, 3. Aufl. (2016), § 8 Rn. 8 m.w.N.

19 Dazu *Birr*, Normenkonflikte bei Polizeibeamten im Rahmen der Eigensicherung, S. 10 f.

20 Bezüglich des allgemeinen Persönlichkeitsrechts *Braun*, DPolBl. 3/2017, 28 f.; dagegen *Thiel*, NWVBl. 2018, 50 (51).

21 Vgl. *Klein*, DVBl. 1987, 1102 ff.; *Sachs*, NWVBl. 2004, 209 ff.; *Sademach*, DVP 2013, 6 ff.; zur historischen Entwicklung *Wenninger*, Geschichte der Lehre vom besonderen Gewaltverhältnis, 1982.

22 *Kingreen/Poscher*, Polizei- und Ordnungsrecht mit Versammlungsrecht, § 7 Rn. 7 ff.

23 Vgl. *Kingreen/Poscher*, Polizei- und Ordnungsrecht mit Versammlungsrecht, § 7 Rn. 30.

NRW) und diesen mit einer Ingewahrsamnahme durchsetzen (§ 35 Abs. 1 Nr. 3 PolG NRW), oder die Person direkt in Unterbindungsgewahrsam nehmen (§ 35 Abs. 1 Nr. 2 PolG NRW). Zur Durchsetzung von Anordnungen, die der Eigensicherung dienen („Lassen Sie das Messer fallen!“) kommt bei Vorliegen der gesetzlichen Voraussetzungen die Anwendung unmittelbaren Zwangs in Betracht.[24] Vor diesem Hintergrund können zahlreiche polizeiliche Standardbefugnisse ohne weiteres zum Zweck der Eigensicherung eingesetzt werden.

Darüber hinaus enthalten die Polizeigesetze Ermächtigungsgrundlagen für spezifische Eigensicherungsmaßnahmen, die teilweise auch zum Schutz anderer Personen für Gefahren für Leib und Leben angewandt werden dürfen. So erlauben verschiedene Vorschriften die Anfertigung von Bild- bzw. Tonaufnahmen (ohne Speicherung) und -aufzeichnungen (mit Speicherung), die vor allem dazu dienen sollen, als „offene“ Maßnahmen das polizeiliche Gegenüber von Übergriffen abzuhalten – sei es durch eine „disziplinierende“ Wirkung des „anwesenden“ und eingeschalteten technischen Gerätes oder aufgrund der Besorgnis der Schaffung objektiver Beweismittel.[25] Gemäß § 15b PolG NRW kann die Polizei zur Abwehr einer Gefahr „zum Zwecke der Eigensicherung“ bei Personen- oder Fahrzeugkontrollen Bildaufnahmen und -aufzeichnungen durch den Einsatz optisch-technischer Mittel in Fahrzeugen der Polizei herstellen. Der Einsatz ist – falls nicht offenkundig – durch geeignete Maßnahmen erkennbar zu machen oder der betroffenen Person mitzuteilen. Die Maßnahme ermöglicht es, das Handeln der Beamtinnen und Beamten z. B. bei Verkehrskontrollen durch begleitende Aufzeichnungen zu sichern.

Kontrovers diskutiert wurden und werden die Befugnisnormen für den Einsatz der sog. „Body-Cam“.[26] Dabei handelt es sich um Aufnahmegeräte, die von den Polizeibeamtinnen und -beamten offen „körpernah“, also regelmäßig an der Uniform, getragen werden, und mit denen Bild- und Tonaufnahmen bzw. -aufzeichnungen hergestellt werden können. Die konkrete gesetzliche Ausgestaltung variiert in den Bundesländern, die die „Body-Cam“ normiert haben, im Detail – so finden sich Bestimmungen, die ein automatisches sog. „Pre-Recording“ ermöglichen. Dabei handelt es sich um eine kontinuierliche Aufzeichnung für einen bestimmten Zeitraum, die nur unter bestimmten Voraussetzungen verlängert werden darf und ansonsten „überschrieben“ wird (vgl. etwa § 21 Abs. 5 und 6 PolG BW: wenn Tatsachen die Annahme rechtfertigen, dass eine längere Speicherung zum Schutz von Polizeibeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist). In anderen Ländern – wie etwa in Nordrhein-Westfalen – ist ein solches „Pre-Recording“ nicht vorgesehen. Gemäß § 15c Abs. 1 PolG NRW kann die Polizei „bei der Durchführung von Maßnahmen zur Gefahrenabwehr und zur Verfolgung von Straftaten und Ordnungswidrigkeiten mittels körpernah getragener Aufnahmegeräte offen Bild- und Tonaufzeichnungen anfertigen, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine konkrete Gefahr für Leib oder Leben erforderlich ist“.[27] Der Einsatz der „Body-Cam“ kann und soll angesichts dieser normativen Ausgestaltung jedenfalls auch Eigensicherungszwecken dienen, weil er deeskalierende Wirkung entfalten soll – diese ist indes zweifelhaft,[28] weil die Konfrontation mit einem Aufnahmegerät das polizeiliche Gegenüber durchaus auch zu Gewalttätigkeiten provozieren kann. Der nordrhein-westfälische Gesetzgeber betrachtet die Maßnahme als auch zur Verbesserung der Eigensicherung geeignet, was ihm aufgrund der gesetzgeberischen Einschätzungsprärogative auch zuzugestehen ist; im Rahmen einer detaillierten und sicherheitsspezifischen Gesetzesfolgenabschätzung hätten aber jedenfalls Erkenntnisse aus dem Ausland und aus anderen Bundesländern eingehendere Berücksichtigung finden müssen.[29] Stattdessen hat sich der Gesetzgeber für die Normierung einer Evaluierung und eines „Ablaufdatums“ bei Nichtverlängerung entschieden (§ 15c Abs. 9 PolG NRW).

Besonderheiten gelten für den Einsatz der „Body-Cam“ in Wohnungen, also beispielsweise in Fällen der häuslichen Gewalt; § 15c Abs. 2 PolG NRW sieht vor, dass in Wohnungen die Anfertigung technischer Aufzeichnungen nur zulässig ist, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine dringende Gefahr für Leib oder Leben erforderlich ist. Diese Einbeziehung der „Dritten“ in den Schutzzweck der Vorschrift stößt mit Blick auf die grundrechtliche Gewährleistung der Unverletzlichkeit der Wohnung in Art. 13 GG auf Probleme bei der verfassungsrechtlichen Einordnung und bei der Frage, wer den Einsatz des technischen Mittels (hier also: das Einschalten der mitgeführten „Body-Cam“) anordnen darf. Art. 13 Abs. 5 GG sieht vor, dass der Einsatz technischer Mittel durch eine gesetzlich bestimmte Stelle angeordnet werden darf, wenn diese Mittel „ausschließlich zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen“ vorgesehen sind. Dies ist aber aufgrund der auch „drittschützenden“ Zielrichtung des § 15c Abs. 2 PolG NRW nicht der Fall; und auch sonst fügt sich die Vorschrift nicht recht in die Dogmatik des Art. 13 GG ein, dürfte aber in einer „Gesamtschau“ als verfassungsgemäß zu qualifizieren sein.[30]

---

[24] Vgl. *Mentzel/Schmitt-Falckenberg/Wischnewski*, Eigensicherung und Recht, 2003, S. 10 ff.

[25] Eingehend *Starnecker*, Videoüberwachung zur Risikovorsorge. Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse, 2017, S. 79 ff.; *Arnd*, Kriminalistik 2016, 104 ff.; zur Beweisverwertung s. *Jansen*, StV 2019, 578 ff.

[26] Dazu etwa *Kipker/Gärtner*, NJW 2015, 296 ff.; *Lachenmann*, NVwZ 2017, 1424 ff.; *Parma*, DÖV 2016, 809 ff.; *Ruthig*, GSZ 2018, 12 ff.; *Zander*, Kriminalistik 2017, 393 ff.; rechtsvergleichend *Weigel*, FoR 2015, 57 ff.; zu Transparenzanforderungen *Kipker*, DuD 2017, 165 ff.

[27] Kritisch etwa *Arzt/Schuster*, DVBl. 2018, 351 ff.

[28] Vgl. *Baier/Manzoni*, Kriminalistik 2018, 685 ff.; *von der Burg*, KrimJ 2018, 139 ff.

[29] Vgl. dazu *Thiel*, NWVBl. 2018, 50 (56).

[30] Vgl. *Thiel*, NWVBl. 2018, 50 (53 f.).

Ein drittes Beispiel für spezifische Eingriffsbefugnisse zur Eigensicherung ist die in einigen Polizeigesetzen ausdrücklich eingeräumte Variante der Durchsuchung einer Person zum Zwecke der Eigensicherung.[31] Gemäß § 39 Abs. 2 S. 1 PolG NRW kann eine Person, „deren Identität" nach dem PolG NRW oder anderen Rechtsvorschriften „festgestellt werden soll, nach Waffen, anderen gefährlichen Werkzeugen und Explosivmitteln" durchsucht werden, „wenn das nach den Umständen zum Schutz des Polizeivollzugsbeamten oder eines Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist". Nach Satz 2 gilt dasselbe, „wenn eine Person nach anderen Rechtsvorschriften vorgeführt oder zur Durchführung einer Maßnahme an einen anderen Ort gebracht werden soll".[32] Geschützte Dritte sind dabei namentlich solche Personen, mit denen der Adressat in Kontakt kommen kann, z. B. ein Polizeiarzt.[33]

Der knappe Überblick verdeutlicht, dass das Polizeirecht den handelnden Einsatzkräften neben den allgemeinen Ermächtigungsgrundlagen zur Gefahrenabwehr, die auch zur Eigensicherung zur Anwendung kommen können, zusätzliche spezifische Eigensicherungsmaßnahmen an die Hand gibt. Das zur Verfügung gestellte gesetzliche Handlungsinstrumentarium ist damit als differenziert und umfangreich zu bewerten.

III. Perspektiven

Angesichts der Veränderungen im Phänomenbereich „Gewalt gegen Polizeibeamtinnen und -beamte", die durch einen zahlenmäßigen Anstieg der entsprechenden Gewalttaten, aber auch durch qualitative Verschiebungen hin zu vermehrter und gravierender körperlicher Gewalt geprägt sind, stellt sich indes die Frage, ob dieser Bestand des präventiven Eigensicherungsinstrumentariums auch künftig noch ausreichend sein wird. Sollte dies nicht der Fall sein, wäre etwa eine Ausweitung der spezifischen Eigensicherungsbefugnisse denkbar. Dies könnte einerseits durch eine Schaffung neuartiger spezifischer Ermächtigungsgrundlagen, die vorrangig auf den Rechtsgüterschutz der eingesetzten Polizeivollzugskräfte abzielten, andererseits durch die Absenkung der tatbestandlichen Anforderungen (oder auch der Verfahrensvorgaben) bei den bereits normativ geregelten Maßnahmen bewerkstelligt werden.

So wäre z.B. an die Aufnahme einer Ermächtigungsgrundlage zum Einsatz von „Drohnen" (unbemannte Luftfahrtsysteme) insbesondere zur Anfertigung von Bildaufnahmen und -aufzeichnungen im Zusammenhang mit besonders gefahrenträchtigen Einsatzsituationen zu denken.[34] Für Übersichtsaufnahmen bei Versammlungen gelten dabei besondere Anforderungen (vgl. §§ 12a, 19a VersG)[35]; doch auch außerhalb des Versammlungsrechts bestehen Anwendungsbereiche,[36] in denen schon gegenwärtig Drohnen eingesetzt bzw. in Pilotprojekten erprobt werden.[37] Allerdings könnte die Nutzung von Drohnen zur Anfertigung von Bildaufnahmen bzw. -aufzeichnungen in vielen Ländern schon gegenwärtig durch die allgemeinen Ermächtigungsnormen für die Datenerhebung durch den offenen Einsatz optisch-technischer Mittel abgedeckt sein, obwohl diese Regelungen meist die stationäre „Videoüberwachung" an öffentlich zugänglichen Orten im Sinn haben. Im Übrigen wäre die Schaffung einer eigenständigen Ermächtigungsnorm zum Drohneneinsatz zum Zweck der Eigensicherung unter eng ausgestaltenden Anforderungen in besonderen Einsatzsituationen verfassungsrechtlich zulässig.

Eine Reduzierung der gesetzlichen Anforderungen der bereits bestehenden Vorschriften zu polizeilichen Eigensicherungsbefugnissen dürfte demgegenüber auf verfassungsrechtliche Hürden stoßen, zumal sie regelmäßig an die Direktiven der verfassungsgerichtlichen Judikatur und das europäische Datenschutzregime angepasst sind. So erschiene es insbesondere nicht vertretbar, grundsätzlich bei jeder polizeilichen Maßnahme durchgängig Aufzeichnungen mit einer „Body-Cam" vorzunehmen, um den Einsatz begleitend zu beobachten oder die erhobenen Daten im Nachgang auszuwerten.

Ausgehend von der Erkenntnis, dass das polizeiliche Instrumentarium an Standardmaßnahmen aufgrund der Einordnung von „Eigensicherungsfällen" als Gefahrenlagen ohnehin zur Anwendung kommt, und angesichts der dargestellten, ergänzenden spezifischen Eigensicherungsmaßnahmen erscheint es derzeit nicht als erforderlich, die Vorschriften zur präventiven Eigensicherung – über bloße Klarstellungen hinsichtlich der einsetzbaren technischen Mittel hinaus – auszuweiten. Der vorhandene „Werkzeugkasten" ermöglicht einen effektiven Selbstschutz für Polizeibeamtinnen und -beamte auch gegenüber Maßnahmenadressaten, die keinen Respekt vor den Einsatzkräften und ihren Anordnungen haben, sie als Vertreter eines verhassten Staatsapparats betrachten und vor massiven körperlichen Angriffen nicht zurückschrecken. Die Entscheidung, ob und in welchem Umfang von den eingeräumten Befugnissen indes Gebrauch gemacht wird und diese gegebenenfalls mit körperlicher Gewalt als Mittel des unmittelbaren Zwangs bis hin zum Gebrauch der Schusswaffe effektuiert werden, wird allerdings nicht allein durch rechtliche Vorgaben, insbesondere den Verhältnismäßigkeitsgrundsatz, gesteuert; sie muss sich namentlich an einsatztaktischen Erwägungen orientieren.

Verfügbar ist mithin ein reichhaltiges präventivpolizeiliches Arsenal, das derzeit keiner eigensicherungsbezogenen Ausweitung bedarf. Eine solche gäbe auch ein für die Konfliktlösung wenig zielführendes Signal einer weiteren „Aufrüstung" der Polizeivollzugskräfte über die Erweiterung der Eingriffsbefugnisse in den jüngsten Polizeirechtsnovellen hinaus. Ansatzpunkte für eine dauerhafte

---

31 *von Prondzinski*, DPolBl. 4/2013, 28 ff.; *Mentzel/Schmitt-Falckenberg/Wischnewski*, Eigensicherung und Recht, S. 13.

32 Eingehend *Bialon/Springer*, Eingriffsrecht, 4. Aufl. (2018), Rn. 600 ff.; *Nimtz/Thiel*, Eingriffsrecht Nordrhein-Westfalen, 2017, Rn. 862 ff.

33 Vgl. *Tegtmeyer/Vahle*, Polizeigesetz Nordrhein-Westfalen – PolG NRW, 12. Aufl. (2018), § 39 Rn. 12.

34 Zu rechtlichen Aspekten *Buckler*, GSZ 2019, 23 ff.

35 Dazu etwa *OVG Koblenz*, NVwZ-RR 2015, 570 ff.; *VerfGH Berlin*, NVwZ-RR 2014, 577 ff.; *Martini*, DÖV 2019, 732 ff.; *Muckel*, JA 2015, 878 ff.

36 Vgl. *Kurz*, Drohnen über dem Bodensee?, FAZ v. 4.1.2013, zu Plänen des damaligen Bundesinnenministers *Friedrich*.

37 Vgl. *Truscheit*, „Leiser als Hubschrauber", FAZ v. 20.11.2017.

und nachhaltige Verbesserung der dargestellten Gewaltproblematik dürften andernorts zu suchen sein. Das Ansehen der Polizei und der handelnden Beamtinnen und Beamten muss wieder gesteigert werden, der Respekt muss wiederhergestellt, und die Hemmschwelle für Rechtgutverletzung muss wieder angehoben werden. Zugleich ist seitens der Polizei eine sachgerechte Erfüllung der ihr zugewiesenen Aufgaben namentlich der Gefahrenabwehr und der Strafverfolgung zu leisten – ein „Kleinbeigeben" bei Widerstandshandlungen trägt den staatlichen Schutzpflichten und dem Strafverfolgungsgebot regelmäßig nicht hinreichend Rechnung und wird zudem die Bereitschaft zu weiterem Widerstand eher steigern als verringern; Kooperation, Verständigung und Konsens bedürfen einer entsprechenden Bereitschaft auf allen Seiten. Fehlt diese, muss die Polizei mit den ihr zur Verfügung stehenden Mitteln in aus rechtsstaatlicher Sicht einwandfreier Weise reagieren können. Dabei ist sie neben der Eigensicherung letztlich auch auf eine nachgelagerte „Fremdsicherung" angewiesen: Auf eine Unterstützung durch Politik, Justiz, Medien und Öffentlichkeit. Gewalt gegen Polizeibeamtinnen und -beamte darf nicht mehr als hinzunehmendes Berufsrisiko oder als „Bagatelldelikt" behandelt, als Akt zivilen Ungehorsams und legitimen Widerstands gegen unliebsame staatliche Entscheidungen bejubelt oder als sportliche Freizeitaktivität verstanden werden. Dies zu bewerkstelligen ist allerdings nicht die Aufgabe des präventiven Polizeirechts, und es kann von ihm auch nicht geleistet werden.

IV. Fazit

Gewalt gegen Polizeibeamtinnen und -beamte nimmt an Quantität und Qualität zu. Das präventive Polizeirecht sieht vielfältige Instrumente zur „Eigensicherung" vor: Da eine Gefahr für die öffentliche Sicherheit vorliegt, wenn Rechtsgüter von Polizeivollzugskräften bedroht oder verletzt werden, kann die Polizei auf das ihr zur Verfügung gestellte Instrumentarium zur Gefahrenabwehr zurückgreifen. Darüber hinaus sehen die Polizeigesetze spezifische Eigensicherungsbefugnisse vor. Insgesamt sind diese Möglichkeiten zur Eigensicherung derzeit (noch) als hinreichend anzusehen; eine Schaffung neuer Eigensicherungsbefugnisse oder eine Absenkung der Voraussetzungen der schon jetzt zugelassenen Maßnahmen erscheint nicht erforderlich. Die Bewältigung des Phänomens „Gewalt gegen Polizeivollzugskräfte" kann nicht allein durch das präventive Polizeirecht erfolgen, sondern muss durch eine breite öffentliche Diskussion und die Entwicklung tragfähiger Konzepte erreicht werden.

BUCHBESPRECHUNGEN

Barton/Eschelbach/Hettinger/Kempf/Krehl/Salditt [Hrsg.]: Festschrift für Thomas Fischer zum 65. Geburtstag

von Rechtsreferendar Martin Linke

2018, Verlag C. H. Beck, ISBN: 978-3-406-72459-6, S. 1263, Euro 179,00

I. Einleitung

Zu seinem 65. Geburtstag wurde *Thomas Fischer*, Vorsitzender Richter am *BGH* a.D. eine Festschrift gewidmet, die mit 86 Beiträgen zu insgesamt 10 Rubriken aus der Feder von 89 Autoren aufwartet. Traditionell werden die Aufsätze in verschiedene Kategorien unterteilt. Bereits der Blick in das Inhaltsverzeichnis verspricht durch ausgewiesene Experten verfasste spannende, teils grundlegende dogmatische Fragen betreffende, teils hoch aktuelle Beiträge. Die Erwartungshaltung an die Festschrift ist daher schon vor der Lektüre einzelner Abhandlungen hoch. Und sie wird nicht enttäuscht.

II. Zum Inhalt anhand ausgewählter Beiträge

1. Aus der Rubrik „Zur Person“

Den Beginn der Festschrift stellen sieben Beiträge der Rubrik „Zur Person“ dar. In einem „obiter dictum“ geht *Renate Künast* auf verschiedene Themenfelder ein, die *Thomas Fischer* insbesondere in seiner Kolumne „Fischer im Recht“ aufgegriffen hat. Hierbei scheut sie sich auch nicht davor, den Jubilar zu kritisieren, vor allem im Hinblick auf seine Positionen zum – in dieser Festschrift mehrfach vorkommenden – Sexualstrafrecht. Nichtsdestotrotz würdigt sie die Person *Fischers* u.a. mit den Worten: „Solche Kämpfer braucht das Recht und der Rechtsstaat.“

Kritik ist auch der Kernaspekt des darauffolgenden, von *Hans-Ullrich Paeffgen* verfassten, Beitrags mit dem Titel „Gottes Werk und Teufels Beitrag“. Adressat der Kritik ist hierbei nicht *Thomas Fischer*, der *Paeffgen* hinsichtlich „Duktus und Typus“ an *Martin Luther* erinnert, sondern zum einen (wieder mal) das reformierte Sexualstrafrecht und daneben – was auch nicht neu ist – der ehemalige Bundesjustizminister *Heiko Maas*, in einer Fußnote *St. Heiko* genannt (S. 68 Fn. 26). *Paeffgen* schließt sich hier zunächst der vernichtenden Kommentierung des § 184j StGB durch *Renzikowski*[1] im 3. Band des Münchener Kommentars an und bezieht ebenfalls engagiert Stellung gegen diese Norm, wobei insbesondere auf Publikationen *Hörnles* eingegangen wird. Darüber hinaus bekommt auch der dem *Maas*'schen – so wörtlich – „Gülleacker“ (S. 68 Fn. 28) entstammende § 89c StGB sein Fett weg.

2. Aus der Rubrik „Strafrecht Allgemeiner Teil“

Besonders ins Auge stechen wird dem Jubilar der Beitrag von *Thomas Hillenkamp*, der sich mit dem Anatomie-Fall *Ferdinand v. Schirachs* befasst. Es ist kein Geheimnis, dass *Thomas Fischer* auf die Werke *Schirachs* nicht besonders gut zu sprechen ist.[2] *Hillenkamp* widmet sich hier dem in der Wissenschaft umstrittenen, in der Rechtsprechung in dieser Gestalt bislang nicht beurteilten, Fall des fehlenden subjektiven Rechtsfertigungselements bei fahrlässigen Delikten. Hierbei benennt er auch die weiteren auftretenden rechtlichen Probleme des Falls, eher er, unter Darstellung des Meinungsspektrums und der Argumente für seine Position, zu Recht zu dem Ergebnis kommt, dass einzig Straffreiheit für den Angeklagten und nicht die 1,5 Jahre Freiheitsstrafe mit Bewährung richtige Folge gewesen wären.

Mit Autos und dem Tod von Menschen geht es auch im anschließenden Beitrag weiter. Gegenstand der Abhandlung ist hier der 2017 in Kraft getretene § 315d StGB. *Wolfgang Mitsch* beleuchtet die Problematik des erfolgsqualifizierten Versuchs einer Teilnahme an illegalen Kraftfahrzeugrennen. *Mitsch* stellt sich auch in diesem Beitrag[3] gegen die herrschende Meinung, der zufolge ein erfolgsqualifizierter Versuch bei solchen Delikten nicht möglich sei, deren Grundtatbestände keine Versuchsstrafbarkeit anordnen (S. 260ff.). Mit seiner Argumentation zur grundsätzlich möglichen Strafbarkeit dieser werden sich die Vertreter der herrschenden Meinung auseinanderzusetzen haben, insbesondere, da das Hauptargument – der Wortlaut des § 18 StGB – angegriffen wird. Anhand konkreter unterschiedlicher Fallgestaltungen untersucht er, ob und inwieweit ein erfolgsqualifizierter Versuch überhaupt in Betracht kommt. Hierzu wird insbesondere auf die Frage des Gefahrverwirklichungszusammenhangs eingegangen.

3. Aus der Rubrik „Strafrecht Besonderer Teil“

Die Reihe der Beiträge zum Besonderen Teil des Strafrechts eröffnet *Volker Erb* mit einem Aufsatz zu einem in vielen Strafvorschriften vorkommenden Merkmal, das wie kaum ein anderes hinsichtlich seiner korrekten Handhabung umstritten ist: Das gefährliche Werkzeug. Nachdem zur Rekapitulation des Problems zunächst dargestellt

[1] Auf seinen, in Co-Autorenschaft erschienenen, Beitrag in dieser Festschrift wird noch eingegangen.

[2] S. die Rezension *Fischers* zu „Strafe“, StV 2018, 393ff.

[3] S. hierzu kürzlich *Mitsch*, NZWiSt 2019, 121 (123ff).

wird, worin die Schwierigkeiten sachgerechter Auslegung liegen, kritisiert *Erb* Gesetzgeber und Rechtsprechung in Bezug auf deren Versäumnisse. Ersterem wird vorgeworfen, explizit hinweisende Rechtsprechung nicht zum Anlass genommen zu haben, auf die bestehenden Probleme reagiert zu haben (S. 306f.); Letzterer, dass sie trotz der Bedenken nicht von Restriktionsansätzen Gebrauch machte. Die so genannte „subjektive Lösung" sei hierbei das einzige, zur Konkretisierung geeignete Gegenmittel (S. 313).

Nachdem an vielen Stellen dieser Festschrift bereits über das Sexualstrafrecht geschimpft wurde und an späterer Stelle noch wird, widmet sich *Klaus Laubenthal* der Herausforderung eines Vorschlags zur „Systematisierung der Delikte gegen die sexuelle Selbstbestimmung". Nach einem historischen Überblick über den Inhalt dieses Abschnitts bei Inkrafttreten des RStGB beginnt *Laubenthal* seine „Neuordnung des 13. Abschnitts". Seine systematischen Überlegungen fußen auf den einzelnen, durch die Straftatbestände geschützten Rechtsgütern und werden dann, entsprechend seiner Kategorisierung, in 6 Normgruppen eingeteilt.

Unter dem Titel „Wollt ihr das totale Strafrecht?" beschäftigen sich *Alexander Aichele* und *Joachim Renzikowski* unter anderem mit der schon an anderer Stelle angesprochenen Strafrechtskatastrophe des § 184j StGB. Wer selbst einmal die „unübliche, aber unvermeidliche Vorbemerkung" *Renzikowskis* zu § 184j StGB im Münchener Kommentar[4] gelesen hat, erahnt, wohin die Reise in diesem Beitrag geht. Zu Beginn wird der Norm bereits bescheinigt, in einer „liberalen, von der Tradition subjektiver Rechte geprägten Ordnung, nichts verloren [zu] haben" (S. 491). Einer knappen Darstellung der Grundlagen der Unschuldsvermutung folgt eine kritische Analyse des § 184j StGB. *Aichele/Renzikowski* betrachten hierbei zunächst das zur Legitimation von Strafnormen herangezogene Phänomen der „Strafbarkeitslücke" und widmen sich anschließend ausführlich der Gesetzesbegründung unter Einsatz wörtlicher Ausschnitte aus den Plenarprotokollen. Es folgen lesenswerte vernichtende Ausführungen zur Auslegung der einzelnen Tatbestandsmerkmale. Abschließend wird dem Leser noch mit auf den Weg gegeben, wie er einer Strafbarkeit nach § 184j StGB entgehen kann: indem er Menschenansammlungen einfach meidet.

„Rennen und Rasen" lautet die von *Thomas Weigend* beigetragene Abhandlung, die sich thematisch mit dem ebenfalls bereits genannten § 315d StGB befasst. Der Norm wird grundsätzlich Daseinsberechtigung bescheinigt, wenn auch die Modalität des so genannten Einzelrasens in § 315d StGB nicht überzeugend sei; besser wäre eine Verortung in § 315c StGB gewesen (S. 572). Jenes „Alleinrasen" bildet neben der Erörterung der qualifizierten Fälle den Hauptkern des Beitrags. Ein Schwerpunkt wird bei der – auch im Rahmen anderer Delikte relevanten – Frage nach der Einbeziehung von Tatbeteiligten in den Schutzbereich der Norm gesetzt.

4. Aus der Rubrik „Strafverfahrensrecht"

Als der Bundesgerichtshof am 26. April 2017[5] ein Urteil zur Problematik so genannter legendierter Verkehrskontrollen fällte, rief dies in kurzer Zeit eine Vielzahl an Urteilsanmerkungen und -besprechungen hervor.[6] Auch in der hiesigen Festschrift wird diesen legendierten Kontrollen eine Abhandlung durch *Eberhard Kempf* gewidmet. Schulmäßig werden nach knapper Übersicht über die Entscheidung des 2. Strafsenats zunächst die Bedenken gegen die Lösung des *BGH* vorgetragen, ehe die einzelnen, sich in Fällen legendierter Kontrollen ergebenden Problemstellungen durchleuchtet werden (S. 678ff.). Im Ergebnis sieht *Kempf* – wie es der Titel seiner Abhandlung erahnen lässt („Zur Rechtswidrigkeit so genannter legendierter Kontrollen") – eben jene als rechtswidrig an.

III. Schlussbemerkung

Dargestellt werden konnte nur ein kleiner Ausschnitt dessen, was den Leser dieser Festschrift erwartet. Was bleibt als Fazit festzuhalten? Man kann das Werk in einem Punkt kritisieren. Nämlich dahingehend, dass irgendwann der Zeitpunkt kommt, an dem man sämtliche Beiträge gelesen hat und das Werk endet. Diese Festschrift zu lesen ist ein Hochgenuss und bereitet für einen beträchtlichen Zeitraum Lesevergnügen. Abschließend lässt sich eine Feststellung *Mitschs*, die er in Bezug auf das von ihm beleuchtete Thema im Zusammenhang mit dem 6. Strafrechtsreformgesetz trifft (S. 266)[7], auf die Festschrift insgesamt erstrecken: Für den Wissenschaftler ist sie in ihrer Gesamtheit eine Spielwiese.

---

4 *Renzikowski*, in: MüKo-StGB, 3. Aufl. (2017), § 184j Rn. 1.

5 *BGH*, Urt. v. 26.4.2017 – 2 StR 247/16 = KriPoZ 2017, 257.

6 Vgl. bspw. *Albrecht*, HRRS 2017, 446; *Börner,* StraFo 2018, 1; *Kochheim,* KriPoZ 2017, 316; *Lange-Bertalot/Aßman,* NZV 2017, 572; *Mitsch,* NJW 2017, 3124; *Schiemann*, NStZ 2017, 651 (657).

7 „Dass das neue Gesetz zugleich einem nach dem 6. Strafrechtsreformgesetz verblassten dogmatischen Problem eine neue Spielwiese eröffnet hat […]".

Thomas Giering: Die Wechselwirkung zwischen Strafe und Sicherungsverwahrung bei der Strafzumessung. Zugleich ein Versuch der Bestimmung des Verhältnisses von Strafe und Sicherungsverwahrung nach vorpositiven Begründungsansätzen und geltender Rechtslage

von Prof. Dr. Anja Schiemann

2018, Duncker & Humblot, Berlin, ISBN: 978-3-428-15181-3, S. 385, Euro 89,90.

Die Dissertation beschäftigt sich mit dem Verhältnis von Strafe und Sicherungsverwahrung gem. §§ 66, 66a StGB, wobei primär die Rechtsprechung überprüft wird, die eine Wechselwirkung zwischen Strafe und Sicherungsverwahrung im Bereich der Strafzumessung annimmt. Da die Sicherungsverwahrung neben der Strafe einen Freiheitsentzug für den Täter bedeutet, der über das Maß der verwirklichten Schuld deutlich hinausgehen kann, schränkt die Rechtsprechung diese Belastung dadurch ein, dass unter dem Gesichtspunkt der Wechselwirkung die Sicherungsverwahrung bei der Bemessung der Freiheitsstrafe berücksichtigt wird.

Um die Wechselwirkung zwischen Strafe und Sicherungsverwahrung auf ein theoretisches Fundament zu stellen, erläutert der Verfasser zunächst sehr dezidiert historische und aktuelle Ansätze der Straftheorie (S. 36 ff.), um danach die Straftheorie der Rechtsprechung vor dem Hintergrund der geltenden Gesetzeslage zu beleuchten (S. 89 ff.). *Giering* kommt zu dem Ergebnis, dass die Rechtsprechung die verschiedenen Strafzwecke miteinander kombiniert und vereint – und insofern eine Vereinigungstheorie auf der Grundlage des Schuldausgleichs vertreten wird. Der Verfasser kritisiert hier aber eine Beliebigkeit in der Argumentation in den Urteilen, da der Theorie das ordnende Prinzip fehle. Das Nebeneinander der straftheoretischen Elemente, die die Rechtsprechung je nach Fall argumentativ nutzt, lehnt *Giering* demzufolge ab (S. 98 f.).

Der Verfasser positioniert sich im folgenden schmalen Kapitel eindeutig und bringt die freiheitsgesetzliche Straftheorie zur Anwendung. Diese Theorie weise einen strikten Tat- und Täterbezug auf. Die Tatschuld begründe und begrenze die staatliche Strafe. Der Vorteil dieser Theorie gegenüber der h.M. sei die stringente Ableitung, zudem löse sich die Antinomie der Strafzwecke auf (S. 100). Weiterhin bekennt sich der Verfasser zur Willensschuld (S. 101).

Nach diesem ersten theoretischen Teil zur Strafe, werden in einem zweiten Teil die Maßregeln der Besserung und Sicherung in den Blick genommen (S. 102 ff.). Die Maßregeln des geltenden Rechts werden in erfrischender Kürze vorgestellt, um sich dann den eigenständigen Maßregeltheorien sowie den aus den Straftheorien entwickelten Maßregeltheorien zu widmen. Der Verfasser kommt hier zu dem Ergebnis, dass alle Begründungsansätze für die Maßregeln der Besserung und Sicherung Einwänden ausgesetzt sind (S. 137). Die verschiedenen Maßregeln der Besserung und Sicherung nach geltendem Recht seien daher jeweils nur für sich zu rechtfertigen, so dass auf einen einheitlichen Rechtfertigungsgrund verzichtet werden müsse (S. 138).

Daher geht *Giering* im Folgenden auf die Rechtfertigung der Sicherungsverwahrung explizit ein und sieht diese vorpositiv nach einem freiheitsgesetzlichen Ansatz als staatliche Reaktion auf habituelle Schuld – sie habe demnach Strafcharakter. Allerdings sei ihre Ausgestaltung als Strafe (noch) nicht angezeigt, was primär an den Schwierigkeiten der Feststellung des Ausmaßes habitueller Schuld im Strafverfahren liege. Bis aber nach freiheitsgesetzlichen Gesichtspunkten ein überzeugendes Konzept geliefert werden könne, müsse man im Grunde die zweispurige Ausgestaltung nach geltendem Recht dulden (S. 144). An dieser Stelle hätte es sich durchaus angeboten, ein wenig tiefer zu schürfen und zumindest grundsätzliche Ideen für ein solches „überzeugendes“ Konzept zu präsentieren.

Im nächsten Unterabschnitt führt der Verfasser eine eigene Terminologie ein. Er differenziert nach klassischer Strafe und „strafrechtsgleicher Unterbringung“ für die Sicherungsverwahrung (S. 144). Gleichwohl benutzt er im Laufe seiner Arbeit wohlüberlegt die Begriffe „Sicherungsverwahrung“ und „Sicherungsverwahrter“, sofern die geltende Rechtslage der §§ 66 ff. StGB beurteilt wird (S. 145).

Die historische Entwicklung des Rechts der Sicherungsverwahrung wird im Anschluss nur in einem knappen Überblick geschildert, um den Zugang zu den Normen herzustellen (S. 146 ff.). Details zu den einzelnen Gesetzesänderungen werden dagegen zu Recht ausgespart, da diese nicht zielführend für die Untersuchung wären. Danach werden grundsätzliche Bedenken gegen die Sicherungsverwahrung referiert (S. 150 ff.). Fokussiert wird hierbei auf die Zweifel an der Erforderlichkeit der Sicherungsverwahrung, den betroffenen Personenkreis und den Katalog der Adressaten sowie die Unsicherheiten im Umgang mit den notwendigen Prognosen.

In einem weiteren Unterabschnitt wird der Einordnung der Sicherungsverwahrung in den europa- und verfassungsrechtlichen Kontext nachgegangen (S. 158 ff.). Der Verfasser kommt zu dem Ergebnis, dass weder die EMRK

an sich, noch der EGMR die Zulässigkeit einer sichernden Maßnahme wie der Sicherungsverwahrung nach deutschem Recht in Abrede stellen. Lediglich die nachträgliche Anordnung oder Verlängerung der Sicherungsverwahrung entspräche nicht den Vorgaben der Konvention. Konventionsrechtlich sei die Unterbringung nach §§ 66, 66a StGB als „Strafe" i.S. des Art. 7 Abs. 1 EMRK einzustufen, was nach Auffassung von *Giering* seine Einordnung der Sicherungsverwahrung als strafrechtsgleiche Unterbringung unterstreiche (S. 175).

Durch die Deutung der Unterbringung gem. §§ 66, 66a StGB als Strafe ließen sich im Unterschied zur herrschenden Auffassung auch unmittelbare Einsichten in die Notwendigkeit der Anwendung von Verfassungsnormen gewinnen. So seien die Zuständigkeit des Bundesgesetzgebers und die Anwendung des Bestimmtheitsgebotes ohne weiteres begründbar. Zudem lasse sich aus dem aus der Strafgerechtigkeit ableitbaren Resozialisierungserfordernis nicht mehr an der Vereinbarkeit der Sicherungsverwahrung mit der Menschenwürdegarantie zweifeln.

Erst recht spät, nämlich ab S. 222 ff. geht *Giering* in einem dritten Teil auf die Strafzumessung ein. Dies erstaunt angesichts der Tatsache, dass der Obertitel der Dissertation als Schwerpunkt der Arbeit auf die Wechselwirkung zwischen Strafe und Sicherungsverwahrung bei der Strafzumessung verweist. Allerdings ist über die Hälfte der Ausarbeitung eher grundsätzlichen Ausführungen gewidmet. Dies rechtfertigt sich jedoch vor dem Hintergrund, dass der Verfasser einen eigenen Standpunkt jenseits der herrschenden Meinung zu legitimieren versucht.

Nach einer dezidierten Untersuchung der Rechtsprechung zur Wechselwirkung von Strafe und Sicherungsverwahrung bei der Strafzumessung, stellt *Giering* fest, dass die Rechtsprechung von einem einheitlichen Ziel geprägt sei. Pauschal werde darauf abgestellt, dass die Strafe niedriger ausfallen könne, wenn eine Unterbringung nach § 66 StGB angeordnet werde. In der Begründung divergieren die Entscheidungen allerdings. Die Unterschiede ließen sich bereits innerhalb der jeweiligen Rechtsprechung der Tat- und Revisionsgerichte ausmachen. Zudem folgten die Tatgerichte nicht stets der Rechtsprechung der Obergerichte.

Die inhaltlichen Argumente seien dabei vielschichtig und reichten von spezialpräventiven Begründungen über eine möglicherweise negativ generalpräventive Begründung auf präventiver Ebene der Spielraumtheorie bis hin zu allgemeinen Erwägungen bzgl. der belastenden Folgen kumulierender Anordnung einer freiheitsentziehenden Strafe und einer Sicherungsverwahrung (S. 253). Die revisionsrechtliche Sicht des *BGH* verkompliziere zudem die Problematik und trage zur Revisibilität der Strafzumessungsentscheidungen des Tatgerichts, sowie die beschränkte Anfechtung von Straf- und Maßregelausspruch mit ihrem eigenständigen Maßstab zur Uneinheitlichkeit der Rechtsprechung bei. Dadurch sei eine erhebliche Anwendungsunsicherheit entstanden.

Daher folgt nach dieser Bestandsaufnahme eine ausführliche kritische Auseinandersetzung mit der Rechtsprechung. Dem hehren Ziel der Rechtsprechung, die strafrechtlichen Sanktionen gegenüber dem Straftäter nicht unverhältnismäßig auszugestalten, werde nicht Genüge getan. Auf Basis der Spielraumtheorie komme eine Berücksichtigung ohnehin nur innerhalb des Schuldrahmens der zur Aburteilung stehenden Straftaten in Betracht. Als tragfähiges Argument zur Begründung der Wechselwirkung lasse sich lediglich der Aspekt der Gesamtabwägung von Rechtsfolgen herausstellen. Die Wechselwirkung sei aber auf Vorschlag des Verfassers grundsätzlich nur bei der Gesamtstrafenbildung vorzunehmen (S. 311). Letztlich kommt *Giering* aber zu dem Ergebnis, dass die strafzumessungsrechtliche Abstimmung den Zusammenhang zwischen der abzuurteilenden Tat und der habituellen Schuld des Täters nur unzureichend aufgreift und in der Folge den gesteigerten Resozialisierungsanspruch des Gewohnheitstäters nur eingeschränkt umsetzt (S. 312).

Daher spürt der Verfasser im Folgenden weiteren theoretischen Ansätzen nach (S. 312 ff.). Alternative Konzepte überzeugten im Vergleich mit der Rechtsprechung durch ihre Klarheit, da sie den Zusammenhang zwischen Strafe und Sicherungsverwahrung als Aspekt eines strikt unrechts- und schuldgebundenen Zumessungsvorgangs ausweisen würden (S. 334). Allerdings sei auch nach diesen Strafzumessungstheorien die Reichweite der Wechselwirkung beschränkt. *Giering* plädiert daher dafür, eine intensive Abstimmung von Strafe und Sicherungsverwahrung als Recht des Täters zum Nutzen der Gesellschaft unter Inanspruchnahme des vikariierenden Systems vorzunehmen (S. 335).

Daher ist der letzte Teil der Dissertation einem eigenen Ansatz gewidmet (S. 336 ff.). Strafe und Sicherungsverwahrung werden als zwei Komponenten der Strafgerechtigkeit verstanden. Der konsequente Vorwegvollzug der Sicherungsverwahrung beruhe auf dem gesteigerten Resozialisierungsinteresse und -anspruch des Straftäters sowie der gesellschaftlichen Mitverantwortung. Durch die Aufnahme in das vikariierende System des § 67 StGB erfolge eine Anrechnung des Maßregelvollzugs auf die Höhe der Freiheitsstrafe. Zudem finde eine Orientierung an der Aussetzung zur Bewährung zum Zweidrittelzeitpunkt statt. Dadurch sei eine weitergehende strafmildernde Berücksichtigung der Sicherungsverwahrung bei der Strafzumessung der unbedingten Freiheitsstrafe nicht notwendig (S. 350). Dadurch würden die Interessen aller Beteiligten optimal berücksichtigt. Denn den Gewohnheitstätern werde frühzeitig ein Hilfsangebot zur Seite gestellt und damit ihrem gesteigerten Wiedereingliederungsinteresse Rechnung getragen. Durch die frühzeitige Arbeit mit den Sicherungsverwahrten werde zudem das Sicherheitsbedürfnis der Allgemeinheit optimal umgesetzt. Ein frühzeitiges Eingehen auf die in habitueller Weise verkehrte Rechtseinsicht fördere dieses Ziel im Vergleich zu einem nachfolgenden Vollzug besser (S. 356).

Die Dissertation von *Giering* bietet zweierlei. Zum einen gelingt eine theoretische Fundierung von Strafe, Maßregel und Strafzumessung unter Einbeziehung aller wichtigen Quellen. Zum anderen werden Denkanstöße gegeben, wie die Wechselwirkung von Strafe und Sicherungsverwahrung nicht nur rechtstheoretisch, sondern auch in praktischer Hinsicht gelingen kann. Insoweit kann die Lektüre dazu anregen, den theoretischen Ansatz des Autors kritisch zu reflektieren und in weitere Reformüberlegungen einfließen zu lassen.

TAGUNGSBERICHTE

Erlanger Cybercrime Tag 2019: Cyber-Finanzkriminalität und Virtuelle Geldwäsche

von Akad. Rat a.Z. Dr. Christian Rückert
und Wiss. Mit. Marlene Wüst

Der Tagungsbericht enthält sprachlich bereinigte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten. Dementsprechend wurde auch auf Fußnoten verzichtet. Der Erlanger Cybercrime Tag 2019 wurde vom Bundesministerium des Innern, für Bau und Heimat gefördert.

Am 13. März 2019 fand die Veranstaltungsreihe „Erlanger Cybercrime Tag" (ECCT) zum dritten Mal statt. Nach den erfolgreichen Tagungen zu virtuellen Kryptowährungen sowie zur Underground Economy des Darknet in den letzten Jahren, widmete sich der ECCT dieses Jahr der Cyber-Finanzkriminalität und der Virtuellen Geldwäsche. Annähernd 100 Besucher versammelten sich im Wassersaal der Erlanger Orangerie, um die Vorträge zu hören und sich über die Tagungsthemen auszutauschen. Wie in den letzten Jahren, fand sich ein breit gefächertes Publikum bestehend aus Vertreterinnen und Vertretern der Polizei- und Finanzbehörden, der Anwaltschaft, der Informatik und der Rechtswissenschaft sowie aus Wirtschaft und Industrie, insbesondere aus dem Bankenwesen, ein. Außerdem hatten erfreulicherweise auch zahlreiche Studierende den Weg zur Tagung gefunden.

Mit den Themen „Cyber-Finanzkriminalität und Virtuelle Geldwäsche" griff der ECCT erneut brandaktuelle Problemfelder auf. Finanzielle Transaktionen werden heute fast ausschließlich online vorgenommen, Bankgeschäfte werden nahezu vollständig im virtuellen Raum des Internets abgewickelt. Die Digitalisierung des Geldkreislaufs hat eine zunehmende Verlagerung der Finanzkriminalität in den virtuellen Raum zur Folge. Parallel ist in den letzten Jahren ein Anstieg der Verwendung von modernen IT-Technologien zur Geldwäsche zu beobachten. Bereits in den Begrüßungsworten der Vizepräsidentin Education der FAU, *Professor Dr. Bärbel Kopp*, und des Sprechers des Fachbereichs Rechtswissenschaft der FAU, *Professor Dr. Jan-Reinhard Sieckmann*, sowie in der Einführungsrede des Veranstalters, *Professor Dr. Christoph Safferling, LL.M. (LSE)*, wurden die gesellschaftlichen und rechtsdogmatischen Fragestellungen aufgeworfen, die diese Entwicklung mit sich bringt: Auf welche neuen Formen der Finanzkriminalität müssen sich Strafverfolger, Unternehmer und Bürger[1] einstellen? Sind die bestehenden Strafgesetze ausreichend oder bedarf es einer Anpassung an die neuen Phänomene? Welche neuen Ermittlungsmaßnahmen und -werkzeuge müssen den Strafverfolgungsbehörden zur Verfügung gestellt werden, um eine wirksame Strafverfolgung von Finanzdelikten auch im virtuellen Raum zu ermöglichen? Und welche neuen Anforderungen ergeben sich durch die Virtualisierung der Finanzkriminalität und der Geldwäsche für die anwaltliche Beratung und die Compliance von Unternehmen?

Zur Beantwortung dieser und weiterer Fragen, hatte die International Criminal Law Research Unit (ICLU) von *Professor Dr. Christoph Safferling, LL.M. (LSE)* mit *Dr. Boris Hemkemeier* (Commerzbank AG), *Professor Dr. Philipp Maume*, *S.J.D. (La Trobe)* (TU München), *Andrea Link* (BayLKA) und *RA Dr. Alexander Cappel* (Norton Rose Fulbright) herausragende Experten aus unterschiedlichen Bereichen eingeladen.

I. Cyber-Finanzkriminalität: Online-Betrug gegen Firmenkunden (*Dr. Boris Hemkemeier,* Commerzbank AG)

Die Tagung wurde durch einen Vortrag von *Dr. Boris Hemkemeier*, Direktor für Information Security Consulting & Research bei der Commerzbank in Frankfurt, eingeläutet. *Dr. Hemkemeier* führte das interessierte Publikum in das Thema der Cyber-Finanzkriminalität aus der Sicht von Banken und Unternehmen ein.

1. Vom beleghaften Betrug zum Cybercrime

Online-Banking wurde in Deutschland erstmals in dem Jahr 1983 mit BTX durchgeführt, im Internet erst seit Mitte der 90er Jahre; die Commerzbank betreibt es seit 1996. Mit Cybercrime, womit im Folgenden Angriffe auf die Kunden und ihre Geräte gemeint sind, sieht sich die deutsche Kreditwirtschaft erst seit den Jahren 2004-2005 konfrontiert. Bis heute sind die Schadenszahlen in klassischen, „analogen" Betrugsformen wesentlich höher als im Online-Banking, obgleich die subjektive Risikowahrnehmung der Kunden eine andere ist. Als Reaktion auf den Cybercrime hat man verstärkt in die Sicherheit der Technik beim Online-Banking sowie im Freigabeverfahren in-

[1] Aus Gründen der besseren Lesbarkeit wurde an gegebenen Stellen das generische Maskulinum verwendet. Diese Formulierung umfasst gleichermaßen weibliche und männliche Personen.

vestiert. Dies hat zur Folge, dass die Täter nicht mehr primär die Technik angreifen, sondern vermehrt auch deren Nutzer. Aus diesem Grund reichen sichere Netzwerke und Apps nicht mehr aus, sondern präventive Ansätze müssen die Nutzer erreichen.

a) Die Sicherheitsstrategie im Cybercrime

Zum strategischen Plan der Cybercrime-Bekämpfung der Commerzbank gehören vier Säulen: Prävention, Detektion, Reaktion und Strafverfolgung. In einem ersten Schritt müssen präventiv ein sicheres Online-Banking sowie sichere Onboarding-Prozesse geschaffen werden. Kommt es dennoch zu Cybercrime-Vorfällen, ist eine frühzeitige Detektion dieser notwendig. Ziel ist es, einen Angriff in Echtzeit sehen und erkennen zu können. Wird ein Angriff entdeckt, muss hierauf reagiert werden. Diese Reaktion kann verschiedene Facetten haben, z.B. das Stoppen einer verdächtigen Zahlung oder die Änderung interner Prozesse. Die vierte Säule der engen Zusammenarbeit mit den Strafverfolgungsbehörden ist ausgesprochen wichtig. Wie *Darwin* sagte: „Bessere Mausefallen enden mit schlaueren Mäusen". Eine gute Prävention bewirkt zum einen eine Verdrängung der Täter zum Wettbewerber, zum anderen die Entwicklung neuer, intelligenterer Angriffe. Gegen dieses Wettrüsten ist es nachhaltig allein wirksam, die Täter aus dem Verkehr zu ziehen. Die Bedeutsamkeit der engen Zusammenarbeit von Banken und Strafverfolgungsbehörden wird durch das föderale Prinzip Deutschlands verstärkt. Hiernach werden Cybercrime-Fälle nach dem Tatortprinzip lokal ermittelt, was das Erkennen eines etwaig bestehenden Zusammenhangs zwischen einzelnen Fällen erschwert. Banken können dahingegen einfacher einen Überblick gewinnen, welche Fälle zu einer gemeinsamen Serie gehören.

b) Wandel durch Digitalisierung

Im digitalen Zahlungsverkehr hat sich die Art des Betruges im Vergleich zum analogen Zahlungsverkehr verändert. Beim SEPA-Überweisungsträger dient die Unterschrift des Kunden, die aber durchaus fälschbar ist, als Autorisierung für den Zahlungsvorgang. Die digitalen Signaturen im Electronic-Banking können dahingegen nicht mehr einfach gefälscht werden. Sie sind an den Zahlungsauftrag gebunden und können nur durch den Kunden erzeugt werden. Aus diesem Grund ist im Zuge der Digitalisierung der Kunde in den Fokus der Cyberkriminellen gerückt. Im Folgenden sollen ein paar – primär aus dem Privatkundengeschäft stammende – Beispiele für industrialisierten Cybercrime dargestellt werden.

2. Beispiele für industrialisierten Cybercrime

Schadsoftwares werden per E-Mail, z.B. durch fiktive Telekom-Rechnungen, verbreitet. Ist der PC infiziert, bleibt die Schadsoftware solange inaktiv, bis der Kunde eine Zahlung per Online-Banking, PayPal oder ähnlichem beginnt. In diesem Moment greift die Schadsoftware ein und greift Benutzernamen und das Passwort ab. Die zur Freigabe von Transaktionen noch fehlenden TANs werden von den Betrügern oftmals durch simples Nachfragen erlangt. Auch wenn nur wenige auf solch eine Anfrage reagieren, ist dies bei Millionen betroffenen Kunden eine beachtliche Anzahl. Teilweise wird die Anfrage auch unter einem Vorwand gestellt, z.B. dass die Bank ein neues Freigabeverfahren einführt und zur „Qualifizierung für das neue Verfahren" eine Entwertung aller alten TANs notwendig ist.

Eine der tückischsten Methoden ist der sog. Rücküberweisungs-Trojaner. Die Schadsoftware blendet eine Nachricht an den Nutzer ein, dass er irrtümlich einen Geldeingang erhalten habe, der ihm nicht zusteht und nun zurücküberwiesen werden müsse. Dies sei einerseits in der Filiale möglich, zusätzlich wird jedoch ein Link mit einer vorausgefüllten Überweisungsmaske eingefügt. Um den Druck zu erhöhen, erfolgt außerdem ein Hinweis, dass das Konto bis zur Rücküberweisung gesperrt werde. Bei einer Prüfung des Kontostandes durch den Nutzer erscheint tatsächlich ein höherer Saldo. Das trojanische Pferd hat in den Umsatzlisten einfach eine weitere Zeile hinzugefügt und den Saldo entsprechend manipuliert. Dem Kunden ist durchaus bewusst, dass er jetzt Geld überweist, aber der Kontext des vermeintlichen Geldeingangs ist eine Täuschung.

Die Commerzbank betreibt eigene Detektionssysteme, um diese Angriffe auf Kunden in Echtzeit zu erkennen und Zahlungen zu überprüfen. Eine Sicherheitsgarantie für Privatkunden sichert einen möglichen Schadensfall ab, wenn der Kunde eine Anzeige stellt und bei der Aufklärung unterstützt.

3. Social Engineering: Cybercrime im Firmenkundengeschäft

Das Firmenkundengeschäft unterscheidet sich vom Privatkundengeschäft dahingehend, dass Banking deutlich weniger standardisiert ist. Im Gegensatz zum Online-Banking durch Privatkunden wird hier in der Regel nicht die Online-Seite der Bank oder deren App genutzt, sondern eigene Systeme oder Clients. Die Heterogenität der verwendeten Systeme erschwert den Tätern einen Angriff und macht diesen weniger lukrativ. Aus diesem Grund versuchen die Täter ihre kriminellen Absichten über eine Manipulation des Kunden zu verwirklichen (sog. Social Engineering). Technische Angriffe bilden im Firmenkundengeschäft eine Ausnahme. Im Folgenden werden verschiedenste Szenarien des Social Engineering skizziert:

a) Ein Betrugsszenario ist das „Remote Access Tool". In diesem Fall wird ein Mitarbeiter vermeintlich von der Bank angerufen und darauf hingewiesen, dass ein Update ihres Zahlungssystems durchgeführt werden muss. Unter diesem Vorwand wird der Mitarbeiter gebeten, alle Legitimationsmedien anzuschließen, die Zugangsdaten zu offenbaren, sowie eine Fernwartungssoftware zu starten. Hierdurch erhalten die Täter freien Zugriff auf die Banking-Systeme der Firma.

b) Einen Klassiker des Social Engineering bilden gefälschte Zahlungsbestätigungen. Hier weist der vermeintliche Käufer nach Abschluss eines Geschäfts gefälschte Zahlungsbestätigungen oder Formulare nach, bis der Verkäufer die Ware versendet. Verbreitet sind in diesem Zusammenhang auch gefälschte Bankgarantien. Um die Glaubhaftigkeit zu stärken sind diese oftmals mit komplexen Texten sowie Unterschriften von Vorständen der Bank versehen. Für Rückfragen sind zum Teil E-Mail-Adressen oder Links zu einer Webseite angegeben, die jedoch zu einer gefälschten Domain führen.

c) Weit verbreitet sind ferner Rechnungen für nicht erbrachte Leistungen. Diese gehen häufig mit einer vermeintlichen E-Mail des Vorgesetzten einher, der um eine Bezahlung der Rechnung mit dem Hinweis bittet, dass eine Rückmeldung nicht notwendig sei. Auffällig ist, dass sich die Höhe der Rechnungen oftmals an Grenzwerten wie 10.000 € oder 50.000 € orientieren, deren Überschreitung eine strengere Prüfung zur Folge hat.

d) Ein weiteres sehr bekanntes Betrugsszenario ist die Schecküberzahlung. Bei diesem Szenario stellt der Kunde „versehentlich" einen zu hohen (gefälschten) Scheck aus, um dann eine Rücküberweisung des überschüssigen Geldes zu verlangen. Eine Neuheit stellt hier das Vorgehen der Betrüger dar, den Scheck nicht dem Kunden zu übergeben, sondern diesen im Namen des Kunden direkt bei der Bank einzureichen. Die Firma erreicht dann lediglich der für sie nicht zuordenbare überschüssige Betrag. Aus diesem Grund fragt die Commerzbank bei Unsicherheiten direkt beim Kunden nach, ob er den Scheck eingereicht hat.

e) Das meiste Betrugsvolumen macht der Mandatsbetrug aus. In diesem Fall teilt der Betrüger im Namen eines echten Lieferanten dem Kunden mit, dass sich seine Kontoverbindung geändert habe und das Geld zukünftig auf ein anderes Konto überwiesen werden solle. Dieser Betrug fällt leider häufig erst auf, wenn der wirkliche Lieferant nach einer Weile nach seinem Geld fragt. Deswegen wird empfohlen, Stammdatenveränderungen nur bei klarer Legitimation oder nach Rückfrage beim Lieferanten vorzunehmen.

f) Neben diesem „klassischen" Betrug innerhalb einer Kunden-Lieferanten-Beziehung ist das Betrugsszenario des „Man in the Middle" seltener und raffinierter. Hier mischen sich die Täter in das Geschäft ein indem sie Domains registrieren, die fast so aussehen wie die Domains der beteiligten Geschäftspartner. Der „Man in the Middle" macht zunächst nichts anderes, als die Dokumente jeweils an die Geschäftspartner weiterzuleiten. Die Geschäftspartner kommunizieren also über eine dritte Person miteinander, ohne dies zu merken. Sobald die Bankverbindung übermittelt wird, ändert der Täter diese.

g) Als „Königsdisziplin" wird der sog. CEO Fraud oder „Fake President" angesehen. Hier erhält ein zur Freigabe von Transaktionen befugter Mitarbeiter eine vermeintliche E-Mail von seinem Chef, durch die er mit einer streng geheimen Finanztransaktion betraut wird. Zudem meldet sich ein angeblich mit der Vorbereitung der Transaktion beauftragter Anwalt bei dem Mitarbeiter und erklärt dessen Zustimmung. Insgesamt handelt es sich um ein lukratives Geschäft für die Täter, für das sie viel Aufwand betreiben. Eine Rückfrage durch die Bank, ob es sich um einen Betrug handeln könnte, wird in diesen Fällen meist abgelehnt und auf die strenge Vertraulichkeit des Geschäfts verwiesen. Der CEO-Fraud endet auf zwei Weisen: entweder wird er entdeckt oder der Firma gehen die liquiden Mittel aus.

h) Ein weiteres Betrugsszenario ist die Ransome Ware. Dieser Trojaner wird z.B. mittels eines E-Mail-Anhangs verschickt. Wird der Anhang geöffnet, erhält die Schadsoftware Zugang auf den Rechner und verschlüsselt die Laufwerke. Nach der Verschlüsselung wird ein Lösegeld (meist in Bitcoin) gefordert. Dieses Betrugsmittel hat sich dahingehend verändert, dass nicht mehr nur Konsumenten angegriffen werden. Mittlerweile werden Firmen vorher ausspioniert und Back-Ups beseitigt, bevor diese mit einer Ransom Ware attackiert und sehr hohe Lösegelder gefordert werden.

4. Schutzmöglichkeiten und Maßnahmen im Betrugsfall

Der wichtigste Punkt beim Schutz vor Betrügereien im Firmenkundengeschäft ist die Firmenkultur. Unter den Mitarbeitern muss ein Bewusstsein für die Betrugsrisiken herrschen und Rückfragen zu Kontonummeränderungen oder ungewöhnlichen Zahlungen müssen – insbesondere, wenn es um große Geldsummen geht – erlaubt sein. Wurde man dennoch Opfer eines Betrugs ist es wichtig, sofort die Bank zu kontaktieren. Je weniger Zeit vergangen ist, desto höher sind deren Chancen, das Geld verfolgen zu können. Die Bank kann unmittelbare Überweisungsrückrufe tätigen, die weitaus erfolgreicher sind als ein alleiniger Swift Recall bei der Zielbank. Zudem verfügt die Commerzbank über ein weltweites Netzwerk mit internationalen Banken und kann je nach Modus Operandi hohe Recovery Rates erzielen. Darüber hinaus kann sie Kontakte zu Ermittlungsbehörden, die auf Cybercrime bzw. Wirtschaftskriminalität spezialisiert sind, vermitteln. Eine enge Zusammenarbeit der Banken mit den Strafverfolgungsbehörden ist – wie eingangs erörtert – der ausschlaggebende Punkt im Umgang mit Cyber-Finanzkriminalität.

5. Diskussion

In der Diskussion wurde näher auf die genauen Vorgehensweisen der Bank und der von ihr verwendeten Mechanismen bei der Detektion und Prävention von Betrugsfällen eingegangen. Insbesondere wurde thematisiert, wie detailliert das Kundenverhalten von der Bank beobachtet wird und welche Daten diese erhebt. Um die Transaktionen nachvollziehen und regulatorische Anforderungen erfüllen zu können, werden klassische Webserverlogs eingesetzt, die sowohl die IP-Adresse als auch den verwendeten Browser bzw. die verwendete App speichern. Darüber hinaus wurde die angesprochene Rückkehr zum klassischen Betrug diskutiert und festgehalten, dass sich die

moderne Cyber-Finanzkriminalität sowohl durch klassischen Betrug als auch durch ein Ausnutzen der Technik auszeichnet.

II. Cyber- Finanzermittlungen – Herausforderungen und Chancen durch moderne IT-Technologie (*Andrea Link,* BayLKA)

Nach der Betrachtung der Cyber-Finanzkriminalität aus dem Blickwinkel der Banken erfolgte ein Perspektivenwechsel. *Andrea Link*, die als Wirtschaftskriminalistin beim Bayerischen Landeskriminalamt (BayLKA) tätig ist, thematisierte in ihrem Vortrag die Besonderheiten von Finanzermittlungen.

Von einer Veröffentlichung dieses Vortrags wird aus ermittlungstaktischen Gründen abgesehen.

III. Virtuelle Kryptowährungen und Geldwäscheregulierung *(Professor Dr. Philipp Maume, S.J.D [La Trobe]*, Technische Universität München)

Im Anschluss an die Darlegung der Möglichkeiten bei Cyber-Finanzermittlungen beleuchtet der Vortrag von *Professor Maume* vor allem dogmatische Fragen der Geldwäscheregulierung im Bereich der Kryptowährungen.

1. Geldwäsche und Regulierung von Kryptowährungen

Geldwäscheregulierung ist technologieneutral, das heißt, es werden Akteure und nicht Technologien reguliert. Das hat den Vorteil, dass auch für neue Technologien bereits ein Regulierungskorsett vorhanden ist, das nur noch angepasst werden muss. Deshalb ist auch die Aussage falsch, Kryptowährungen und ICOs seien nicht reguliert. Es fehlt jedoch bislang an einer spezifischen, auf die Geldwäschegefahren der Kryptowährungen zugeschnittene, Regulierung.

2. Technischer Hintergrund von Tokensystemen

Die Blockchain ist eine „kontinuierlich erweiterbare Liste von Datensätzen, die durch kryptografische Verfahren miteinander verbunden sind und deren Speicherung dezentral auf den Rechnern der Teilnehmer erfolgt". Grundlage ist die Distributed Ledger Technology. Ledger bedeutet Speichereinheiten. Es handelt sich also um eine Datenbank. Diese Datenbank wird ständig fortgeschrieben und die Datensätze werden in sog. Blöcken gespeichert und aneinandergereiht. Daher kommt der Begriff Blockchain. Auf dieser Blockchain können Transaktionen durchgeführt werden. Die Transaktionen in der Datenbank funktionieren durch die sog. Tokenisierung. Der Begriff Token meint in diesem Zusammenhang schlicht „Werteinheit". Durch Tokenisierung schafft man eine Form von virtueller Umlauffähigkeit auf der Blockchain. Die Teilnehmer einer Blockchain verfügen über gewisse Rechte. Auf der Blockchain hat jeder User einen sog. Public-Key. Das ist eine Ziffernfolge, mit der er identifiziert werden kann. Man kann beliebig viele Public Keys generieren, d.h. ein bestimmter User kann unter verschiedenen Identitäten auf einer Blockchain gespeichert sein. Zu jedem Public Key hat der User auch einen Private Key, mit dem er Transaktionen ausführen kann und den der User geheim halten sollte. Die Schlüsselpaare werden von den Nutzern in einer sog. Wallet verwaltet.

Zur Durchführung einer Transaktion genügt das Absenden der Nachricht in das System, dass ein Token von einem Public Key auf einen anderen Public Key übertragen werden soll. Der Token ist dann dem anderen Public Key zugewiesen. In der Rechtswissenschaft wird dies bisweilen unscharf als Übertragung oder Übereignung bezeichnet. Es wird bei der Übertragung z.B. eines Bitcoins aber nichts verschickt, sondern nur eine Zuordnung geändert. Was die Blockchain-Technologie so interessant macht, ist, dass es durch die dezentrale Speicherung zwar nicht unmöglich, aber zumindest extrem schwierig ist, Transaktionen zu fälschen oder nachträglich zu verändern. Außerdem sind Transaktionen von überall auf der Welt möglich. Die Blockchain ist auch nicht an ein bestimmtes Bankensystem oder an ein Transaktionsformat gebunden, es gibt also keine Schnittstellenproblematik. Die Blockchain ist auch sehr flexibel: Je nach verwendeter Programmierung kann sie offen einsehbar sein oder eben nicht.

In der Praxis haben sich drei verschiedene Tokenarten herausgebildet. Zunächst gibt es die sog. Investment oder Security Token. Diese sind wertpapierähnlich, das bedeutet, dem Inhaber dieses Tokens stehen Rechte an einem Unternehmen zu, i.d.R. eine Beteiligung am Gewinn oder eine fixierte Rückzahlung im Sinne einer Anleihe. Daneben gibt es die sog. Currency Token, auch virtuelle Währung genannt. Currency Token zeichnen sich dadurch aus, dass sie im Regelfall keine besonderen Rechte repräsentieren. Sie basieren nur darauf, dass andere ihnen einen Wert zumessen. Drittens gibt es sog. Utility Token, welche mit einem digitalen Gutschein vergleichbar sind. Der Inhaber dieses Token hat ein Recht gegen ein Unternehmen, z.B. Zugriff auf Rechenleistung oder Speicherplatz in einer Cloud. Geldwäscherechtlich sind alle Tokenarten relevant. Sie werden alle auf die gleiche Art und Weise technisch übertragen und können alle zur Zahlung oder zum Tausch genutzt werden.

Aus Regulierungsperspektive ist interessant, dass Blockchains im Grundsatz pseudonym sind, weil die Transaktionshistorie einsehbar ist und jeder User durch mindestens einen Public-Key repräsentiert wird. Man kann eine Transaktion einem Public-Key und damit einer Person zuordnen. Das bedeutet, dass die Aktivitäten einer Person über die Blockchain verfolgbar sind, wenn man die Person identifiziert hat. Allerdings sind einige Token sogar anonym, d.h. man kann keinen Zusammenhang zwischen Public-Key und den Transaktionen herstellen. Das sind die sog. Privacy Token, z.B. Monero. Außerdem existieren Services, wie Mixer oder Tumbler, die durch eine Abfolge von Transaktion, Teilung von Token, Zirkulartransaktion usw. den Rückschluss auf den Inhaber erschweren.

Es gibt drei Möglichkeiten, Token zu erhalten:
(1) Ein Ersterwerb von Token erfolgt durch ein Initial Coin Offering, bei dem ein Emittent neue Token an Investoren oder Käufer ausgibt.

(2) Ein Zweiterwerb findet beispielsweise statt über Kryptowechselstellen, die Fiat-Geld in Token tauschen oder andersherum. Viele Geschäftsmodelle sind hier sehr intransparent. Es ist oft unklar, ob der Kunde bei solchen Wechselstellen tatsächlich selbst Token erhält (sog. On-Chain-Transaktion) oder, ob der Dienstleister die Token behält und man nur einen Herausgabeanspruch oder sogar nur einen Anspruch auf Bilanzausgleich erwirbt (sog. Off-Chain-Transaktion). Die konkrete Geschäftsart hat wegen der Erlaubnispflicht von Einlagengeschäften eine große Bedeutung im Bereich der Finanzmarktregulierung und im Insolvenzrecht.

(3) Schließlich können an sog. Kryptobörsen im Wege des Zweiterwerbs verschiedene Tokenarten gegeneinander getauscht werden, z.B. Bitcoin gegen Ethereum.

3. Token im System der Geldwäscheregulierung in Deutschland

Rechtsquelle der Geldwäscheregulierung in Deutschland ist vor allem das Gesetz über das Aufspüren von Gewinn aus schweren Straftaten oder Geldwäschegesetz (GWG). In seiner jetzigen Fassung basiert es auf der 4. Geldwäscherichtlinie und wird gerade an die 5. Geldwäscherichtlinie angepasst.

Geldwäscheprävention betrifft, anders als die Straftat der Geldwäsche, nur die sog. Verpflichteten. Verpflichtete sind Kreditinstitute, Banken, Finanzdienstleistungsinstitute, Zahlungsinstitute etc. Ferner gibt es nach § 2 GWG bestimmte Dienstleister, die ebenfalls geldwäscherelevant sind, z.B. Wirtschaftsprüfer, Rechtsanwälte, Immobilienmakler etc. Gleiches gilt für sog. Güterhändler. Der Güterhändler reicht dabei vom kleinen Onlineshop bis hin zu großen Industriekonzern.

Die Verpflichteten müssen nach dem GWG gewisse Pflichten im Rahmen der Geldwäscheprävention erfüllen, z.B. eine Identitäts- und Legitimationsprüfung ihrer Kunden durchführen (sog. KYC-System) und Geldwäscheverdachtsmeldungen abgeben. In diese Regulierung könnten Kryptowährungen über zwei Stellschrauben eingepasst werden:
(1) Erfassung der Dienstleister im Kryptowährungssektor als Verpflichtete und (2) Auslösung von Pflichten durch Kryptowährungstransaktionen.

Damit Kryptowährungstransaktionen vom GWG erfasst wären, müsste es sich um Transaktionen i.S.v. § 1 Abs. 5 GWG handeln. Hiernach ist eine Geldbewegung oder sonstige Vermögensverschiebung erforderlich. Es ist unklar, ob eine Tokentransaktion eine Vermögensverschiebung ist. Grund hierfür ist, dass die Verwaltung eines Tokens auf seinem Public Key nach bislang herrschender Meinung kein absolutes Recht, sondern nur eine faktische Zugriffsmöglichkeit darstellt. Dennoch kann die Tokentransaktion unter den Transaktionsbegriff des GWG subsumiert werden. Nach h.M. genügt für die Vermögensverschiebung der Erwerb eines Gegenstands, dem tatsächlich ein Wert beigemessen wird. Dies ist aufgrund der oben geschilderten Erwerbs- und Verkaufsmöglichkeiten für Token offensichtlich der Fall.

Was die Art der Regulierung angeht, so kann man einen Blick auf die unterschiedlich scharfe Regulierung von Bargeld und Giralgeld werfen. Bargeld ist anonym, aber seine Umlauffähigkeit ist aufgrund seiner Körperlichkeit stark eingeschränkt. Giralgeld lässt sich leicht und schnell in großen Mengen weltweit übertragen, die Transaktionen sind jedoch durch das Bankensystem überwacht. Token dagegen sind pseudonym (ggf. sogar anonym) übertragbar und weisen eine hohe Umlauffähigkeit auf. Sie besitzen daher ein noch über dem Bargeld liegendes Gefährdungspotential für die Geldwäsche. Allerdings sind Token mangels Körperlichkeit offensichtlich kein Bargeld, sodass eine direkte Anwendung der Vorschriften über Bargeld ausscheidet.

Eine weitere Möglichkeit bestünde darin Token als E-Geld zu erfassen. E-Geld ist jeder elektronisch gespeicherte monetäre Wert in Form einer Forderung an den Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge durchzuführen und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird. Wären Token E-Geld, wären die Geschäfte von Token-Emittenten erlaubnispflichtig nach dem ZAG. Die allermeisten Token sind jedoch kein E-Geld. Bei Currency Token fehlt es schon am zentralen Emittenten, die anderen Tokenarten werden nicht allgemein als Zahlungsmittel entgegengenommen.

4. Erfassung von Token durch die 5. Geldwäscherichtlinie

Abhilfe soll auf europäischer Ebene durch Ergänzung der 5. Geldwäscherichtlinie geschaffen werden. Dort wird eine virtuelle Währung definiert als „die digitale Darstellung eines Werts“, der „von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann“. Currency Token werden von dieser Definition erfasst, wohl auch die anderen Tokenarten.

Die 5. Geldwäscherichtlinie führt auch neue Arten von Geldwäschepräventionsverpflichteten ein. Allen voran sind dies die Wechselstuben, die definiert werden als Dienstleister, die virtuelle Währung in Fiatgeld oder umgekehrt, tauschen. Weiterhin gibt es sog. Walletanbieter. Hierunter sind die Anbieter elektronischer Geldbörsen zu verstehen, in denen virtuelle Währungen gespeichert oder auch übertragen werden können.

Die fehlerhafte Annahme, eine Kryptotokentransaktion entspreche einer Zahlung im Bankensystem und die hierauf beruhende Übertragung der bisherigen Geldwäschepräventionsregeln auf Tokensysteme, führt zu Inkonsistenzen. Ein Beispiel hierfür sind Güterhändler. Güterhändler haben nach § 10 Abs. 6 GWG Sorgfaltspflichten, insbesondere die Durchführung eines KYC-Checks in den Fällen des § 10 Abs. 3 S. 1 Nr. 3 (Geldwäscheverdacht) und bei Transaktion, bei welchen sie Barzahlungen über mindestens 10.000 Euro tätigen oder entgegennehmen, zu erfüllen.

Das heißt Bargeld wird schärfer reguliert, was mit Blick auf die geldwäscherechtliche Systematik auch überzeugend ist. Allerdings ist die Zahlung mit Kryptowährungen der Transaktion gleichgestellt und nicht derjenigen mit Bargeld. Das bedeutet, ein Güterhändler muss hier einen KYC-Check nur bei einem Geldwäscheverdacht vornehmen. Angesichts der guten Eignung von Kryptowährungen zur Geldwäsche ist dies ein Wertungswiderspruch. Hieran ändert sich auch nichts durch die 5. Geldwäscherichtlinie. Möglich bliebe somit nur, bei jeder Zahlung mit Kryptowährungen einen Geldwäscheverdachtsfall zu bejahen. Dies erscheint jedoch unwahrscheinlich, weil die Rechtsprechung hierfür bislang konkrete Anhaltspunkte verlangt. Das kann bei einer Kryptowährungstransaktion durchaus der Fall sein, wenn z.B. eine besonders hohe Summe transferiert wird oder eine Stückelung von Transaktionen vorgenommen wird. Weiterhin könnte man erwägen, die Regeln über Bargeld analog anzuwenden. Hiergegen spricht jedoch das Analogieverbot. Das Problem ist also bislang – auch durch die 5. Geldwäscherichtlinie – nicht gelöst.

Ein weiteres Regulierungsproblem besteht darin, dass die Geldwäscherichtlinie nur innerhalb der EU gilt. Man sollte daher erwägen, neue Wege zu gehen. Im Projekt BITCRIME wurde z.B. vorgeschlagen, die Vorteile wie Transparenz und Fälschungssicherheit für die Geldwäscheprävention fruchtbar zu machen. Durch die Verfolgbarkeit der Transaktionen können Transaktionen (und deren Nachfolger in gewissen Teilen) „geblacklisted" werden. Hierin liegt freilich ein starker Grundrechtseingriff, weil die Token hierdurch (teilweise) entwertet werden. Ferner könnte man auch mit einem Whitelisting-Verfahren arbeiten, bei dem „saubere" Transaktionen oder Adressen gelistet werden. Für beides bräuchte man ein zentrales Register, das von einer (halb-)staatlichen Stelle verwaltet wird.

5. Abschließende Thesen

Da Kryptowährungen die besonderen Risikopotentiale von Bargeld und Giralgeld vereinen, wäre eine gesonderte Regulierung geboten. Im derzeitigen GWG und auch nach der 5. Geldwäscherichtlinie wird diesen Besonderheiten nicht ausreichend Rechnung getragen. Die Reform und Erweiterungen der 5. Geldwäscherichtlinie sind sinnvoll, basieren aber auf dem Fehlschluss, das Banksystem und oder die Zahlung im Banksystem wäre mit der Zahlung in Kryptowährungen vergleichbar. Daher sollte eine spezielle Kategorie in das GWG aufgenommen werden, was auch unter Geltung der 5. Geldwäscherichtlinie möglich ist, da diese nur eine Teilharmonisierung erfordert. Vorzugswürdig, aber wohl schwer realisierbar, wäre dagegen ein komplett neuer transaktionsbezogener Ansatz.

Im Diskussionsteil wurde u.a. der regulatorische Umgang mit „anonymeren" Token wie z.B. Monero diskutiert und festgestellt, dass hier noch größere Probleme bestehen, als bei Bitcoin. Weiterhin wurden praktische Fragen zum Umgang mit einer potenziell zu erwartenden großen Menge an Verdachtsmeldungen gestellt. Es wurde empfohlen, nach „Gebräuchlichkeit" der jeweiligen Token für geldwäscherelevante Straftaten zu priorisieren. Schließlich wurde auch eine Regulierung der Kryptotokendienstleister nach KWG (und nicht „nur" nach dem GWG erwogen).

IV. Beratung, Compliance und Verteidigung in (virtuellen) Geldwäscheverfahren (*RA Dr. Alexander Cappel,* Norton Rose Fulbright)

Nachdem die dogmatischen Fragen der Geldwäscheregulierung im Bereich der Kryptowährungen im Vorfeld geklärt wurden, greift der Vortrag von *RA Dr. Alexander Cappel* (Norton Rose Fulbright) Themenkomplexe der Beratung, Compliance und Verteidigung in (virtuellen) Geldwäscheverfahren auf.

1. Beratung, Compliance und Verteidigung in (virtuellen) Geldwäscheverfahren

In der Beratung zum Thema Geldwäscheprävention besteht in der Praxis das große Problem darin, dass es oft allenfalls Anhaltspunkte, selten aber klare Beweise dafür gibt, dass in bestimmten Sachverhalten ein Fall von Geldwäsche vorliegt. Unternehmen können dann nur entweder bestimmte Geschäftsmodelle ablehnen oder diese trotz Unsicherheit durchführen. Denn ex post betrachtet ist es oftmals leicht zu sagen, das Risiko wäre im Voraus abzusehen gewesen.

Die Probleme des § 261 StGB sollen in diesem Vortrag anhand eines Praxisbeispiels aufgezeigt werden. Dieser ist ein häufiges Einfallstor in der Praxis, weil Mandanten des Öfteren der Meinung sind, das GWG beträfe nur Banken und § 261 StGB nur „den" Geldwäscher. Wie falsch eine solche These sein kann und welches Risiko mit dieser Fehleinschätzung für die Mitarbeiter der Unternehmen sowie für das Unternehmen selbst einhergeht, wird im Folgenden näher erörtert. Darauf aufbauend wird erläutert, wie man in der Praxis risikobasiert an das Thema Kryptowährungen herangeht und mit welchen Stellschrauben sich ein Unternehmen auf der Compliance-Seite gut aufstellen kann, um geldwäscherechtliche Risiken weitestgehend zu minimieren. Dabei lässt gerade die Ungenauigkeit des Gesetzgebers den Unternehmen einen großen Spielraum.

2. Der Ausgangsfall

Der Ausgangsfall des Vortrages stellt sich wie folgt dar: Ein Start-up „X", welches im Internet b2b-Software für mittelständische Unternehmen vertreibt, akzeptiert alle Arten von Zahlungsmittel, darunter auch Kryptowährungen. Das Unternehmen hat Geschäftsbeziehungen zu einer Vielzahl an im Internet agierender Unternehmen, darunter das Unternehmen „D", welches als Haupteinnahmequelle im Darknet Waffen vertreibt. D möchte Software von X kaufen und diese mit einer Kryptowährung bezahlen. X ist ein klassischer Güterhändler und hat bisher keine Compliance-Maßnahmen getroffen. Auch die Kunden des X werden nicht vorher überprüft, insbesondere wird die Herkunft der Gelder, die zur Zahlung dienen, nicht erforscht. Dem Mitarbeiter „M" des X kommt die Zahlung des D

komisch vor und er äußert seine Bedenken gegenüber seinem Chef, dem CEO „C“. Letzterer sieht keinen Handlungsbedarf und weist den M an, die Zahlung anzunehmen. Der Fall kann dahingehend variieren, dass das Geld in jedem Fall aus der inkriminierten Quelle stammt oder dass das Geld aus einer anderen Quelle kommt und man nur die entsprechenden Informationen über das Unternehmen D findet. Vorliegend wird von trennbaren Quellen ausgegangen.

Es wird deutlich, dass das weitsichtigere Compliance-Handeln auf wirtschaftliche Interessen trifft. Der unternehmerische Wille, ein Geschäft machen zu wollen, bevor der Konkurrent zuvorkommt, ist sicherlich nachvollziehbar. Dabei entstehen jedoch Risiken sowohl für X und M als auch C. Zunächst muss festgestellt werden, was Geldwäsche eigentlich ist. Dies ist jeder Vorgang, der darauf gerichtet ist, Spuren unrechtmäßiger Herkunft von Erlösen aus Straftaten zu verschleiern, um so die unerlaubt erlangten Vermögenswerte als scheinbar legales Vermögen in den regulären Wirtschaftskreislauf einzuschleusen. Als Beispiel lässt sich der illegale Waffenhändler anführen, der Ware von einem Güterhändler kauft, die er wiederrum schnell weiterveräußern kann und somit das Geld „gewaschen“ wird.

3. Der Rechtsrahmen

Fraglich ist weiterhin, ob ein Geldwäscheverdacht vorliegt. Gesetzlich ist dazu wenig geregelt, so dass Unternehmen oftmals auf Auslegungshinweise von Behörden angewiesen sind oder Literatur konsultieren müssen. Letztlich kommt es aber auf das Geschäft an. Dabei gibt es klassische sog. „Red-Flags“ im Rahmen der Geldwäsche, wie etwa brachen-untypische oder wirtschaftlich unsinnige Geschäfte. Jedoch könnte man hier aufgrund der Neuheit von Kryptowährungen allein die Zahlung mit ihnen als branchen-untypisch charakterisieren. Dies wird wohl in wenigen Jahren schon anders zu sehen sein. Dann wird dies branchen-typisch sein. Zudem könnte die mit Kryptowährungen einhergehende Anonymität bzw. Pseudonymität ein Verdachtsmoment begründen. Diese liegen jedoch in der Natur der Sache, was gegen ein solches Verdachtsmoment spricht. Aus Compliance-Gesichtspunkten heißt dies, dass man feststellen muss, ob gewisse Handlungen überhaupt etwas mit einem konkreten Geschäft zu tun haben und, ob es für sie überhaupt einen plausiblen Grund gibt.

Der Rechtsrahmen ist (neben den EU-Geldwäscherichtlinien) in § 261 StGB, im GWG, aber auch für Finanzunternehmen wie Banken im KWG geregelt. Daneben gibt es in verschiedenen Aufsichtsbehörden vielfältige Veröffentlichungen zum Thema Geldwäsche wie Rundschreiben, Anwendungs- und Auslegungshinweise der BaFin. Es gibt aber auch von verschiedenen Regierungspräsidien hilfreiche Handreichungen zum Thema Geldwäsche, die eine Auslegungshilfe darstellen.

4. Der Straftatbestand der Geldwäsche nach § 261 StGB

Der Straftatbestand der Geldwäsche ist ein klassisches Anschlussdelikt. Es ist also vorher eine Straftat begangen worden und der Geldwäscher versucht die Herkunft von inkriminierten Gegenständen zu verschleiern. Es geht nicht nur um Geld, sondern dies kann jeden Gegenstand betreffen, so dass auch Kryptowährungen darunterfallen und allgemein bewegliche und unbewegliche Sachen, die in irgendeiner Form vermögenswerten Charakter haben. Daneben bedarf es einer tauglichen Vortat, entweder eines Verbrechens oder eines Vergehens aus dem Katalog des § 261 StGB. Da dieser sehr weit ist, muss der Berater seinen Mandanten stets fragen, woher das Geld seiner Kunden stammt bzw. womit diese ihr Geld verdienen. Der § 261 StGB kennt sodann drei Handlungsvarianten: Den Verschleierungstatbestand, den Vereitelungs- und Gefährdungstatbestand und den Isolierungstatbestand. Diese sind denkbar weit formuliert.

Im Vorsatzbereich besteht für die Mandanten ein großes Risiko dahingehend, dass bereits Eventualvorsatz ausreichen kann. Aus Sicht von *Dr. Cappel* stellt die größte Gefahr in der Beratung zur Geldwäsche aber die Leichtfertigkeit dar. Diese liegt bereits dann vor, wenn – wie im vorliegenden Fall – leicht durch eine schnelle Recherche herausgefunden werden kann, dass der Kunde mit Waffen handelt.

Aus Sicht der Unternehmen ist dabei gar nicht eine einige Jahre später ergehende Entscheidung des *BGH* darüber interessant, ob tatsächlich Geldwäsche vorlag. Kritisch ist bereits die Einleitung eines Ermittlungsverfahrens und die (öffentlichkeitswirksame) Durchführung von Ermittlungsmaßnahmen wie Durchsuchungen. Gerade beim Leichtfertigkeitstatbestand fällt es leicht, einen Anfangsverdacht der Geldwäsche zu begründen.

5. Verpflichtungen für Güterhändler nach dem GWG

Neben dem StGB können den Güterhändler aber auch Pflichten nach dem GWG treffen. Das GWG richtet sich an einen Kreis bestimmter Verpflichteter, in erster Linie Banken. Ein Güterhändler ist jede Person, die gewerblich Güter veräußert, unabhängig davon, in wessen Namen und auf wessen Rechnung. Als Güterhändler ist man wie alle anderen verpflichtet, jedoch mit gewissen Erleichterungen. Die Kernpflichten des GWG sind das Risikomanagement, die Kundensorgfaltspflichten und die Pflicht zur Meldung von Verdachtsfällen. Der Güterhändler hat nur in zwei dieser drei Fälle einen „Emergency Exit“, denn in Hinblick auf die Meldung von Verdachtsfällen hat er ihn gerade nicht.

Tatsächlich gab es im Jahr 2017 jedoch nur eine verschwindend geringe Anzahl von Verdachtsmeldungen durch Güterhändler. Daraus könnte man nun schließen, dass bei Güterhändlern solche Verdachtsmomente nicht auftauchen und somit kein Meldebedarf besteht. Die Erfahrung zeigt aber vielmehr, dass Start-Ups, Hidden Champions und der klassische Mittelständler das Thema gar nicht auf dem Schirm haben und diese sich über ihr Risiko und ihre Verpflichtungen gar nicht bewusst sind. Die Frage ist nun, ab wann man ein Risikomanagement implementieren muss. Grundsätzlich sind alle nach dem GWG Verpflichteten davon betroffen. Somit muss ein System erstellt werden, das sicherstellt, dass man nicht zur

Geldwäsche missbraucht werden kann. Es muss dann eine Person benannt werden, die für die Implementierung zuständig ist. Erfahrungsgemäß lassen sich selten Personen dafür bereiterklären, diese Aufgabe zu übernehmen. Der Güterhändler muss aber nur dann über ein wirksames System zum Risikomanagement verfügen, wenn er im Rahmen einer Transaktion Barzahlungen über mindestens 10.000 € vor- oder entgegennimmt. Erfolgen die Zahlungen bei einem Güterhändler nur über Kryptowährungen, so sind diese nicht als Barzahlung anzusehen, so dass sich diese nicht unter eben Genanntes subsumieren lassen. Muss er allerdings ein Risikomanagement einrichten, muss seine Risikoanalyse auf die Kundenstruktur, das Kundenrisiko, das Produkt- oder Dienstleistungsrisiko sowie das geographische Risiko eingehen. Dabei ist fraglich, ob die Zahlung mit Kryptowährungen per se schon auffällig ist. Je nach Ergebnis der Risikoanalyse gilt es dann, die richtigen Maßnahmen zu treffen. Dabei wird häufig pauschal auf online verfügbare Policys zurückgegriffen, unabhängig davon, ob diese auf den konkreten Einzelfall passen oder nicht. Eine solche „Feigenblatt-Compliance" fällt den Behörden allerdings im Regelfall sehr schnell auf und wird nicht als ordnungsgemäße Aufsicht akzeptiert.

Im Bereich der Kundensorgfaltspflichten ist auch Sorgfalt im Hinblick auf Kryptowährungen geboten, etwa dann, wenn eine Verbindung zu Geldwäsche oder Terrorismus nicht auszuschließen ist. Es stellt sich dann die Frage, ob jeder Fall einer Zahlung mit Kryptowährungen schon die Gefahr von Geldwäsche indiziert. Zwar sind Kryptowährungen recht neu, allerdings stellen sie eine „normale" Art der Zahlung dar und sind somit nicht per se verdächtig. Eine KYC-Prüfung ist somit nicht schon aufgrund der Zahlung mit Kryptowährungen notwendig. Das entbindet allerdings nicht von der Pflicht, sich mit dem Geschäft seines Kunden auseinanderzusetzen, je nach Geschäftsgröße durch eine Google-Recherche oder eine Kundenanfrage, und ggf. ein Geschäft abzulehnen. Im Rahmen der verstärkten Sorgfaltspflichten ist insbesondere auf sog. PEPs (politisch exponierte Personen) oder besonders ungewöhnliche Transaktionen hinzuweisen. Hier ist ein besonderes Monitoring vonnöten. Das Gesetz lässt den Anwender letztlich im Unklaren, welche Maßnahmen genau getroffen werden müssen. Auch hier stellt sich die Frage, ob Zahlungen mit Kryptowährung als ungewöhnlich einzustufen sind und somit das Anwendungsfeld der verstärkten Sorgfaltspflichten eröffnet ist. Auch hier plädiert *Dr. Cappel* aber dafür, dass der neuartige Charakter der Kryptowährungen eine Zahlung mit ebendiesen nicht per se ungewöhnlich macht. Die Verpflichtung, Verdachtsfälle zu melden, besteht jedoch weiterhin und ist davon unberührt.

6. Drohende Konsequenzen bei Nichteinhaltung der notwendigen Compliance

Wann werden nun Compliance-Maßnahmen im Bereich der Geldwäsche notwendig? Zum einen also beim Vorliegen eines Verpflichtetenstatus und zum anderen im Rahmen des für den Güterhändler relevanteren Fall des § 261 Abs. 5 StGB (leichtfertige Geldwäsche). Für die Unternehmensleitung gilt § 130 OWiG, der von den Behörden im Geldwäschebereich schnell bejaht wird und Bußgelder bis zu 10 Millionen Euro nach sich ziehen kann. Der Bußgeldkatalog für etwaige Verstöße gegen das GWG ist in § 56 GWG geregelt, welcher Geldbußen bis 1 Million Euro, für Banken bis zu 5 Millionen oder 10 Prozent des Gesamtumsatzes festlegt.

Die Tatsache, dass die notwendigen Compliance-Maßnahmen nicht detailliert feststehen, ist einerseits schlecht für die Vorhersehbarkeit von Sanktionen, bietet aber anderseits den Unternehmen einen hohen Grad an Flexibilität. Hier sind individuelle Lösungen notwendig und möglich. Kleine und mittelständische Unternehmen können nicht die gleichen Pflichten haben wie große Banken. Individualisiert werden können Maßnahmen zur Transaktionsüberprüfung und Recherchen bezüglich der Geschäftspartner. Unternehmensintern können sog. Red Flags bestimmt werden, z.B. Zahlungen mit Kryptowährungen. Auch die Verwendung von speziellen präventiven Softwarelösungen ist möglich, aber eine Kostenfrage. Dabei ist auch im Blickfeld zu behalten, dass das Unternehmen die von ihm selbst gesetzten Maßstäbe effektiv einhalten können muss. Hier muss also mit Augenmaß gearbeitet werden und es darf nur in schwierigen Fällen vom Standardprogramm abgewichen wird.

7. Question & Answers-Session

In der Q&A-Session wurden das Verhältnis von Dokumentationspflichten und Datenschutz thematisiert und festgehalten, dass die KYC-Pflichten des GWG einen datenschutzrechtlichen Erlaubnistatbestand enthalten. Außerdem müssen im Rahmen der Pflichten gesammelte Informationen bei Vorhandensein entsprechender Eingriffsbefugnisse auch an die Strafverfolgungsbehörden herausgegeben werden. Nach Auffassung von *Dr. Cappel* gibt es kaum rechtssichere Möglichkeiten, verbindliche Auskünfte hinsichtlich der notwendigen Compliance-Maßnahmen von Behörden zu erlangen. Schließlich wurde darauf eingegangen, dass der Begriff des „Güterhändlers" auch solche Unternehmer erfasst, die ausschließlich im Endkundenvertrieb tätig sind. Besonders im Fokus der Behörden stehen dort Waren, die leicht zu Geld zu machen sind wie Autos, Schmuck, Gutscheine etc. Allerdings plädiert *Dr. Cappel* für eine maßvolle Anwendung der GWG-Bestimmungen, um nicht jeden Bereich des alltäglichen Lebens geldwäschetechnisch zu „überregulieren"

V. Resümee

Die sich an die Vorträge anschließenden interessierten Nachfragen sowie die rege Diskussion, die beim Stehempfang in lockerer Atmosphäre fortgesetzt wurde, verdeutlichen die aktuelle Brisanz und Relevanz des Tagungsthemas. Mit dem Erlanger Cybercrime Tag wurde eine Plattform für Expertinnen und Experten verschiedener Fachrichtungen sowie Interessierte geschaffen, auf der diese sich jährlich über aktuelle Entwicklungen im Bereich des Cybercrime austauschen können. *Professor Safferling* und sein Team der International Criminal Law Research Unit freuen sich, die interdisziplinäre Veranstaltungsreihe „Erlanger Cybercrime Tag" im nächsten Jahr fortzusetzen.

Workshop Sicherheits- und Strafrecht im Angesicht der Digitalisierung

von Ass. iur. Nicole Selzer

Amadeus Peters (HIIG), *Sebastian Golla* (Johannes Gutenberg-Universität Mainz) und *Christian Rückert* (Friedrich-Alexander Universität Erlangen-Nürnberg) luden am 27. Juni 2019 zum Workshop „Sicherheits- und Strafrecht im Angesicht der Digitalisierung" für NachwuchswissenschaftlerInnen ein, der in den Räumlichkeiten des Alexander von Humboldt Instituts für Internet und Gesellschaft (HIIG) in Berlin stattfand. Der Workshop wurde mit dem Ziel ins Leben gerufen, Fragen rund um das Thema Sicherheitsrecht im Zusammenhang mit der Digitalisierung zu identifizieren, zu untersuchen und zu diskutieren und damit jungen WissenschaftlerInnen eine Plattform für aktuelle Forschungsvorhaben und Forschungsthemen zu geben.[1]

Nach einer herzlichen Begrüßung durch die drei Veranstalter, wobei *Christian Rückert* zeitgemäß per Videochat zugeschaltet wurde, eröffnete *OStA Thomas Goger* von der Zentralstelle Cybercrime Bayern als Keynote-Speaker den Workshop. Am 1. Januar 2015 gründete er gemeinsam mit einem weiteren Kollegen die Zentralstelle Cybercrime bei der Staatsanwaltschaft in München, die mittlerweile 14 Staatsanwälte umfasse. In Gießen sei die erste Zentralstelle gründet worden, Berlin und Nordrhein-Westfalen verfügen ebenfalls über derartige Schwerpunktabteilungen. Bevor *OStA Goger* über tägliche Herausforderungen im Bereich Cybercrime berichtete, verwies er auf die Polizeiliche Kriminalstatistik (PKS), die einen Schaden für Cybercrime in Höhe von 51 Mio. EUR in 2016 (72 Mio. EUR in 2017) ausweise. Dies sei im Vergleich zu anderen Deliktsfeldern ein äußerst geringer Schaden. Die Aussagekraft der PKS sei aber vor allem im Bereich Cybercrime sehr gering. Grund hierfür sei, dass Auslandstaten nicht erfasst würden. Da es sich in diesem Phänomenbereich aber gerade um Delikte handle, die einen grenzüberschreitenden Bezug aufwiesen und Täter oftmals im Ausland ansässig seien, sei eine erhebliche Verzerrung gegeben. Eine Anpassung der Statistik sei daher dringend erforderlich. Erkenntnissen der Staatsanwaltschaft zufolge, seien IT-Kenntnisse bei den Tätern nicht erforderlich, da jegliche Dienstleistung i.S.v. „crime-as-a-service" einkaufbar sei, wodurch eine sehr viel größere Zahl potenzieller Täter bestehe, als man geheimhin für möglich halte. Fast anekdotisch fuhr *OStA Goger* fort, dass die Strafprozessordnung analog geblieben sei. Zwar sei bereits am 3. August 1984 die erste E-Mail in Deutschland versandt worden, direkt erfasst sei sie von der Strafprozessordnung aber immer noch nicht. Dafür aber das antiquierte Fax und Telegramm. Zwar könne man sich behelfen, dies sei aber auch problembehaftet.

Im Anschluss trug *Dr. Raphael Bossong* (Stiftung Wissenschaft und Politik) zur digitalen Beweissicherung vor und ging hierbei auf den US „Cloud Act" und die „E-Evidence"-Initiative der EU ein. Derzeit gelte für Strafverfolgungsbehörden in der EU ein rein freiwilliges Verfahren zur Abfrage von Bestandsdaten von US Serviceprovidern. Alternativ könne ein formelles Verfahren zur Mutual Legal Assistance (MLA) eingeleitet werden, das über das US Justizministerium laufe und im Durchschnitt zehn Monate dauere. Der Cloud Act schaffe die Verpflichtung für US Firmen Kommunikations- und Personenstammdaten zu US-Bürgern und Anwohnern zu übergeben, wenn diese durch Strafverfolgungsbehörden oder Gerichte von „complying countries" angefordert würden. Zudem erhielten „complying countries" direkten Zugang zu Daten, die privatwirtschaftlich in den USA gespeichert würden. Problematisch sei allerdings, dass keine Einzelfallprüfung wie im MLA Prozess erfolge, wodurch ein Einfallstor für Datenabfragen aus den USA durch Drittstaaten entstehen könne. Die E-Evidence-Verordnung sehe den direkten Zugriff auf elektronische Beweise (bspw. E-Mails) von Dienstleistern oder gesetzlichen Vertretern in einem anderen Mitgliedsstaat vor. Der Dienstleister bzw. gesetzliche Vertreter sei verpflichtet innerhalb von zehn Tagen oder in Notfällen innerhalb von sechs Stunden zu antworten. Kritisch sei hierbei neben anderen Punkten die Auslagerung der Entscheidung zur Datenherausgabe an privatwirtschaftliche Akteure mit kurzen Bearbeitungsfristen, die beschränkte Benachrichtigung Betroffener sowie die Aushebelung der Territorialität durch verpflichtende Schaffung eines rechtlichen Vertreters in der Union.

Dr. Oskar Josef Gstrein, M.A., LL.M (Rijksuniversiteit Groningen – Campus Fryslân) berichtete über das EU-Forschungsprojekt ‚Cutting Crime Impact' (CCI).[2] Das Projekt habe zum Ziel, die Auswirkung von Kriminalität zu verringern, indem innovative Instrumente zur Verhütung und Bekämpfung zusammen mit sechs europäischen Strafverfolgungsbehörden entwickelt werden. Ein besonderer Fokus liege darauf, die Chancen und Risiken der Digitalisierung in diesem Bereich auch aus (grund-)rechtlicher, ethischer und sozialer Perspektive interdisziplinär aufzuarbeiten. Das Projekt werde bis Oktober 2021 Maßnahmenpakete (‚toolkits') für vier Teilbereiche entwickeln: predictive policing, community policing, crime prevention through urban design and planning (CP-UDP) sowie measuring and mitigating citizens' feeling of insecurity.

Catharina Pia Conrad (Universität Bremen) sprach über die technischen (Un-)Möglichkeiten des Kernbereichsschutzes bei der strafprozessualen Online-Durchsuchung

[1] https://www.hiig.de/events/workshop-sicherheits-und-strafrecht-im-angesicht-der-digitalisierung/ (zuletzt abgerufen am 22.7.2019).

[2] https://www.cuttingcrimeimpact.eu (zuletzt abgerufen am 22.7.2019).

und stellte die These auf, das gesellschaftlich Wünschenswerte (Kernbereichsschutz) sei mit dem technisch Möglichen nicht vereinbar und neue Ansatzpunkte seien notwendig, um den Kernbereichsschutz zu gewährleisten. Problematisch sei die enorme Datenmenge und -vielfalt, die im Rahmen einer Online-Durchsuchung anfalle, wodurch die Erstellung von Persönlichkeitsprofilen möglich sei, welche mit dem Kernbereichsschutz nicht vereinbar seien. Einen neuen Ansatzpunkt sieht *Conrad* insbesondere in der Übertragung der Grundsätze des additiven Grundrechtseingriffs auf den Schutz des Kernbereichs der privaten Lebensgestaltung.

Jan Mysegades (Deutsches Forschungsinstitut für die öffentliche Verwaltung Speyer) referierte über die Rolle moderner Software als Beweismittel im Strafprozess. Nachdem er Beispiele für Algorithmen erläuterte und anschauliche Praxisbeispiele präsentierte, u.a. die Gesichtserkennungssoftware die beim G20 Gipfel in Hamburg und am Bahnhof Berlin Südkreuz verwendet wurde, verwies er auf die Gefahr falsch positiver Ergebnisse. So wurden bspw. in Amerika 28 amtierende Kongressabgeordnete von Amazon ‚Recognition' fälschlicherweise als Straftäter identifiziert. *Mysegades* zufolge sei die mangelnde Nachvollziehbarkeit derartiger Algorithmen das Problem. Die Datenübertragung und -auswertung sei von den Betroffenen nicht überprüfbar. Der Zugang der Öffentlichkeit und der Verteidigung seien erschwert. Eine positive Ausnahme bilde allerdings das Programm SKALA der Polizei und des Landeskriminalamtes Nordrhein-Westfalen. Unter prozessrechtlichen Gesichtspunkten ergebe sich die Frage, wie das Beweismittel in die Hauptverhandlung eingeführt werde – als Sachverständigengutachten, Urkunde oder Augenschein. Zudem müssen neue Methoden auch der Reproduzierbarkeit, Gleichförmigkeit und Validität unterliegen, woran mangels Nachvollziehbarkeit Zweifel bestünden. Die bisherige Rechtsprechung zu „standardisierten Verfahren" nehme faktisch eine Beweislastumkehr vor. Im Gegenzug sei es jedenfalls zwingend notwendig, verstärkte Einsichtsrechte der Verteidigung zu gewähren. *Mysegades* plädiert hinsichtlich moderner Software als Beweismittel für mehr Transparenz durch Black Box-Testing und Zertifizierung sowie für technische Garantien über Blindbeweise („zero-knowledge-proof").

Hieran schloss sich die Vorstellung des Forschungsprojektes MEDIAN durch *Dr. Jan Fährmann* (Hochschule für Wirtschaft und Recht Berlin) an. MEDIAN stehe für die mobile berührungslose Identitätsprüfung im Anwendungsfeld Migration.[3] Das Verbundprojekt laufe bis Juli 2021 und habe die Entwicklung eines mobilen Demonstrators zur polizeilichen Identitätsfeststellung zum Ziel, wobei der HWR unter Leitung von *Prof. Dr. Hartmut Aden* die Aufgabe zukomme, hohe Standards für Recht, Datenschutz und Ethik bei der mobilen Kontrolle sicherzustellen. Dabei solle neben der polizeilichen Perspektive die Sicht der Betroffenen einbezogen werden, damit die Kontrollen für beide Seiten möglichst wenig belastend werde. Auch solle geprüft werden, wie technische Anwendungen ausgestaltet werden können, damit sie rechtswidrigen Verhalten entgegenwirken oder dieses ausschließen, bspw. sog. „Racial Profiling".

Dimitris Zachos (Martin-Luther-Universität Halle-Wittenberg) erörterte den Begriff „virtuelle Handlung" aus strafrechts- bzw. handlungstheoretischer Sicht. *Zachos* stellte fest, dass in den letzten zwei Jahrzehnten immer wieder für das Strafrecht interessante Konstellationen vorgekommen seien, bspw. der virtuelle Mord („MapleStory"), der virtuelle Diebstahl („Runescape") oder die virtuelle Vergewaltigung („Lamda MOO"). In diesen Fällen habe der Begriff der „virtuellen Handlung" keiner wesentlichen Erweiterung oder Abänderung des Handlungsbegriffs auf handlungstheoretischer bzw. strafrechtsdogmatischer Ebene bedurft. Auch unter begriffsgeschichtlicher Betrachtung deute der Ausdruck „virtuell" nicht auf eine „falsche" bzw. „alternative" Realität hin. Demnach müsse auch keine kategorische Unterscheidung zwischen „Realem" und „Virtuellem" erfolgen. Der Aspekt der Virtualität erweitere und bereichere vielmehr den geistigen Horizont bzw. das Erkenntnispotenzial. Bei Handlungen, die lediglich systeminterne Konsequenzen zur Folge haben (bspw. virtueller Mord, virtuelle Vergewaltigung innerhalb eines Onlinespiels) sei das Verhalten nicht strafbar. Bei Handlungen, die dagegen auch extravirtuelle Folgen aufwiesen (bspw. virtueller Diebstahl von erworbenen Gegenständen innerhalb eines Onlinespiels), sollte das Strafrecht gleichwohl ultima ratio sein. An erster Stelle sollten *Zachos* zufolge systeminterne Sanktionen (bspw. dauerhafter Ausschluss vom Onlinespiel) stehen und ggf. zivilrechtliche Sanktionen (Schadensersatz) folgen.

Abschließend beschäftigte sich *Benedikt Kohn* (Universität Augsburg) mit Chancen und Risiken des Einsatzes Künstlicher Intelligenz im Rahmen der Strafzumessung. Hierbei wies er zunächst auf bestehende Probleme bei der Strafzumessung hin. So böten die weitgefassten Strafrahmen im Strafgesetzbuch den Richterinnen und Richtern zwar viel Spielraum für Einzelfallgerechtigkeit, führten allerdings auch zu lokalen Straftraditionen und in der Folge zu großen regionalen Unterschieden. Auch durch die Unvollkommenheit der menschlichen Natur würden Ungleichbehandlungen entstehen. Einen Ausweg könnte hier der Einsatz von Künstlicher Intelligenz bieten. In den USA seien dafür bereits *Risk Assessment Tools* im Einsatz. Diese Programme, die ursprünglich nur dafür entwickelt wurden, die Rückfallwahrscheinlichkeit von Straftätern für die Fragen der Untersuchungshaft zu bestimmen, würden zunehmend für Strafzumessungsentscheidungen eingesetzt werden. Dies würde bspw. für das Eingruppieren in die Stufen der in den USA üblichen *Sentencing Guidelines* verwendet werden. Der Einsatz der Künstlichen

[3] https://campus4u.hwr-berlin.de/qisserver/rds;jsessionid=ED197FB5BFE4731EA299E5C2B46F7979.qis2?state=verpublish&status=init&vmfile=no&publishid=1131&moduleCall=webInfo&publishConfFile=webInfoProjekt&publishSubDir=forschung (zuletzt abgerufen am 22.7.2019).

Intelligenz könne zwar dabei helfen, menschliche Voreingenommenheit auszuschließen, aber gleichwohl zu Ungleichbehandlungen führen. Problematisch sei, dass das Verfahren nicht transparent und eine Überprüfung unmöglich sei.

Zusammenfassend, *Amadeus Peters, Sebastian Golla* und *Christian Rückert* haben eine angenehme Atmosphäre für den Austausch und Diskurs geschaffen. Der Workshop beinhaltete eine Bandbreite spannender Vorträge zu zukunftsorientierten Themen. Strafprozessuale Herausforderungen der Gegenwart und Zukunft wurden ausgiebig diskutiert. Der Workshop zeigte, dass einiger Diskussions- und Handlungsbedarf besteht und der Digitalisierung in Bezug auf das Sicherheits- und Strafrecht im weiteren Sinne mehr Aufmerksamkeit geschenkt werden sollte. Zu hoffen bleibt, dass dieses gelungene Format eine Neuauflage erfährt und künftig fester Bestandteil der Tagungslandschaft in Deutschland wird.