Juristische Fakultät
Lehrstuhl für Kriminologie
MAKrim XV

Masterarbeit

Titel:

Hasskriminalität im Internet
als politisch motivierte Kriminalität

Aktuelle Herausforderungen
aus kriminologischer und kriminalistischer Perspektive

Erstgutachter:
Dr. Holger Plank

Zweitgutachter:
Kay Riedmüller

Vorgelegt von:
Philipp Heid
Matrikelnummer: 108118202570
E-Mail: philipp.heid@yahoo.de

Abgabedatum: 31.01.2021

Inhaltsverzeichnis

Tabellen- und Abbildungsverzeichnis

Abkürzungsverzeichnis

AG Kripo	Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem BKA
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BT	Besonderer Teil des Strafgesetzbuchs
BVerfG	Bundesverfassungsgericht
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
EuGH	Gerichtshof der Europäischen Union
GG	Grundgesetz
IMK	Innenministerkonferenz
LG	Landgericht
LKA	Landeskriminalamt
NetzDG	Netzwerkdurchsetzungsgesetz
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PKS	Polizeiliche Kriminalstatistik
PMK	Politisch motivierte Kriminalität
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
ZET	Zentralstelle zur Bekämpfung von Extremismus und Terrorismus bei der Generalstaatsanwalt München
ZIT	Zentralstelle zur Bekämpfung der Internetkriminalität bei der Generalstaatsanwaltschaft Frankfurt am Main

1. Einleitung

Aufgrund gesellschaftlicher Entwicklungen und infolge entsprechender Ereignisse in den vergangenen beiden Dekaden hat der polizeiliche Staatsschutz einen immensen Bedeutungszuwachs erfahren. Dieser hat den Auftrag, politisch motivierte Kriminalität zu bekämpfen, worunter zunächst die klassischen Staatsschutzdelikte[1] zu subsumieren sind, auch wenn bei der Betrachtung des Einzelfalls eine politische Motivation nicht festgestellt werden kann (vgl. Bundesministerium des Innern, für Bau und Heimat 2020: 22). Auch Straftaten der Allgemeinkriminalität aus dem Strafgesetzbuch (StGB) und den strafrechtlichen Nebengesetzen sind dazu geeignet, als politisch motivierte Kriminalität klassifiziert zu werden, wenn durch ihre Begehung beispielsweise der demokratische Willensbildungsprozess beeinflusst werden soll, sich die Taten gegen die freiheitlich demokratische Grundordnung richten oder Delikte gegen Personen begangen werden und hierbei entsprechende Zurechnungskriterien[2] erfüllt sind (vgl. ebd.: 22).

Politisch motivierte Kriminalität wird in verschiedene Phänomenbereiche unterteilt und betrachtet. Zu den bekannten Phänomenen gehören die politisch motivierte Kriminalität -rechts, -links sowie diese mit religiöser oder ausländischer Ideologie. Eine weitere Rolle spielt jedoch auch beispielhaft und in nicht abschließender Aufzählung die Szene der Reichsbürger und Selbstverwalter[3]. Politisch motivierte Straftaten mit unklaren Hintergründen werden unter der Kennung „nicht zuzuordnen“ erfasst, die einen nicht nur unerheblichen Anteil an der Gesamtmenge der registrierten Delikte hat (vgl. Bundesministerium des Innern, für Bau und Heimat 2020a: 2).

Aufgrund verschiedener herausragender Vorkommnisse in den Jahren 2019 und 2020 sind rechtsextremistische und -terroristische Bestrebungen und Straftaten in den gesellschaftlichen, medialen und politischen Fokus ge-

[1] Dies meint die §§ 80 bis 83, 84 bis 91, 94 bis 100a, 102 bis 104a, 105 bis 108e, 109 bis 109h, 129a, 129b, 130, 234a und 241a StGB.

[2] In Betracht kommen die politische Einstellung, Nationalität, Volkszugehörigkeit, Rasse, Hautfarbe, Religion, Weltanschauung, Herkunft sowie das äußere Erscheinungsbild, eine Behinderung, die sexuelle Orientierung oder der gesellschaftliche Status.

[3] Reichsbürger und Selbstverwalter gehen im Allgemeinen von einem Fortbestand des Deutschen Reiches aus, was damit begründet wird, dass die Weimarer Reichsverfassung nicht abgeschafft worden sei, weswegen die Bundesrepublik Deutschland von dieser Szene nicht anerkannt wird (vgl. Keller 2019: 757 f.).

rückt.[4] Diese Ereignisse und die daraus resultierenden Folgen stellen den polizeilichen Staatsschutz vor große und zum Teil auch neue Herausforderungen, beziehungsweise machen eine entsprechende Schwerpunktsetzung erforderlich.

Das Bundeskriminalamt (BKA) hat diesbezüglich zwei große Themen für die zukünftige Befassung benannt. Hierbei handelt es sich einerseits um die Identifizierung und die Bewertung des Gefahrenpotentials von sowie den Umgang mit solchen Personen und Netzwerken, von denen zukünftig die Gefahr einer rechtsterroristischen Straftat ausgehen könnte (vgl. Münch 2020: 4). Bei dem zweiten Aufgabengebiet handelt es sich um die Bekämpfung der Hasskriminalität im Internet (vgl. ebd.: 5). Entsprechende Inhalte sind unter Bezugnahme auf die einleitenden Ausführungen regelmäßig als politisch motivierte Kriminalität zu klassifizieren.

1.1 Themendarstellung und Gliederung der Arbeit

Die Herausforderungen, die sich im Umgang mit dem letztgenannten Phänomen und bei dessen Bekämpfung stellen, werden in der vorliegenden Arbeit mit dem Titel „Hasskriminalität im Internet als politisch motivierte Kriminalität - Aktuelle Herausforderungen aus kriminologischer und kriminalistischer Perspektive“ herausgearbeitet und in der Folge für die Untersuchung der nachfolgend beschriebenen Fragestellungen und Implikationen nutzbar gemacht.

Als Fallvignetten, auf welche im Zuge der Arbeit wiederkehrend Bezug genommen wird und aus denen entsprechende Implikationen abzuleiten sind, werden das rechtsterroristisch motivierte Tötungsdelikt zum Nachteil des Kasseler Regierungspräsidenten Dr. Walter Lübcke am 2. Juni 2019 und der antisemitisch motivierte Anschlag in Halle vom 9. Oktober 2019 herangezogen.

Während im Nachgang des Tötungsdelikts zum Nachteil des Kasseler Regierungspräsidenten eine Vielzahl von Äußerungen im Internet festgestellt wurden, die unter politisch motivierte Hasskriminalität zu subsumieren waren

[4] Hierzu gehören die rechtsterroristisch motivierten Tötungsdelikte zum Nachteil des Kasseler Regierungspräsidenten Dr. Walter Lübcke am 2. Juni 2019 und in Hanau am 19. Februar 2020 sowie der antisemitisch motivierte Anschlag in Halle vom 9. Oktober 2019.

(vgl. Apostel 2019: 287), vermittelte der Täter des Anschlags von Halle seine Einstellung und Gesinnung medial im Internet (vgl. Pfahl-Traughber 2020: 77). Die Thematik der politisch motivierten Hasskriminalität im Internet ist inzwischen zum Zentrum einer rechtspolitischen Diskussion geworden. Insgesamt kann vermutet werden, dass entsprechende Inhalte bei polarisierten Gesellschaftsteilen den Nährboden für Mobilisierungs- und Radikalisierungstendenzen bilden (vgl. Münch 2020: 5 f.). Hiernach wäre Hasskriminalität als ein gesamtgesellschaftliches Problem zu verstehen. Zur wirksamen Bekämpfung dieses Phänomens scheint eine Stärkung der rechtsstaatlichen Normenkontrolle erforderlich (vgl. Rüdiger 2019: 40), wozu insbesondere die Täter dieser Delikte mit den Mitteln des Strafprozessrechts identifiziert werden müssen. Neben der Aktualität der genannten Fallvignetten ergibt sich die herausragende Bedeutung der Thematik auch aus dem Umstand, dass Hasskriminalität im Internet mit 3,7 Prozent einen bedeutenden Anteil an der Gesamtmenge der registrierten politisch motivierten Kriminalität im Jahr 2019 hatte, wobei hiervon wiederum 73 Prozent dem Phänomenbereich - rechts zuzuordnen waren (vgl. Bundeskriminalamt 2020). Dieses Phänomen ist daher insgesamt von großer Aktualität und Relevanz. Die inhaltliche Befassung der Arbeit beschränkt sich unter Bezugnahme auf die vorstehenden Ausführungen auf die politisch motivierte Hasskriminalität im Internet, die dem Phänomenbereich - rechts zuzuordnen ist.

Bei der Hasskriminalität im Internet handelt es sich in der Regel um Äußerungsdelikte mit einem Unwerturteil über einzelne Personen oder Personengruppen (vgl. Koreng 2017: 152), welche über das Internet publiziert werden, das in diesen Fällen als Tatmittel dient. Hieraus resultieren Herausforderungen und Besonderheiten im Umgang mit und bei der Bekämpfung des Phänomens. Für eine umfassende Analyse der Thematik muss daher zunächst eine Betrachtung der kriminologischen und kriminalistischen Implikationen erfolgen, ehe die damit in Zusammenhang stehenden kriminalpolitischen Maßnahmen bewertet werden können. Diese Abfolge ermöglicht zunächst die Beschreibung der Wirksamkeit präventiver und repressiver Maßnahmen sowie die Identifikation von Problemfeldern. Hierauf aufbauend ist eine valide Argumentation zu bereits erfolgter Gesetzgebung und aktuellen Initiativen möglich.

Das sich der Einleitung (erstes Kapitel) anschließende zweite Kapitel widmet sich zunächst der Bestimmung des Gegenstandsbereichs und der Verdeutlichung von Problemstellungen im Zusammenhang mit Hasskriminalität im Internet. Da bislang keine einheitliche oder verbindliche Definition von Hasskriminalität im Internet existiert, erfolgt nach der Darlegung bestehender Definitionsmöglichkeiten eine definitorische Eingrenzung, welche Inhalte im weiteren Verlauf der Arbeit als politisch motivierte Hasskriminalität im Internet verstanden werden sollen (Kapitel 2.1). Im Anschluss erfolgt ein Überblick zu der im Grundgesetz (GG) verankerten Meinungsfreiheit sowie zu den in Frage kommenden Straftatbeständen de lege lata (Kapitel 2.2). Dieses Kapitel abschließend wird die Problematik verdeutlicht, die sich aus den computerbasierten Delikten der Hasskriminalität ergeben, welche aufgrund der bestehenden Vernetzung global begangen werden können und deren Inhalte entsprechend abrufbar sind (vgl. Busching 2015: 298 f.), während nationales Straf- und Strafprozessrecht Anwendung finden (Kapitel 2.3).

In dem sich anschließenden dritten Kapitel werden die kriminologischen Implikationen von politisch motivierter Hasskriminalität im Internet bearbeitet. Solche ergeben sich hinsichtlich der Ursachen, Erklärungsansätze und ihrer Auswirkungen. In Bezug auf die Ursachen (Kapitel 3.1) wird der Blick auf gesamtgesellschaftliche Entwicklungen gerichtet. Wesentliche zu betrachtende Begrifflichkeiten für rechtsmotivierte Delikte sind hierbei Globalisierung, soziale Desintegration, Entsolidarisierung und Migration. Als Besonderheit für die internetbasierten Delikte der Hasskriminalität, welche für die Tatbegehung konstitutiv ist, tritt in Unterscheidung zu Straftaten in der analogen Welt der Aspekt der Distanz hinzu (vgl. Meier 2015: 95 f.). Im Anschluss erfolgt eine Erörterung zur Häufigkeit und Ausprägung des Phänomens (Kapitel 3.2). Für Erklärungsansätze zur Hasskriminalität im Internet (Kapitel 3.3) werden ausgewählte Kriminalitätstheorien betrachtet, welche für diese digitalen Straftaten nutzbar gemacht werden können. Hierzu bietet Rüdiger (vgl. 2017: passim) einen vielversprechenden Ansatz, der aufbauend auf dem Broken-Windows-Ansatz und unter Bezug auf die Routine Activity Theorie von einem Broken-Web-Phänomen spricht und hieraus Ableitungen trifft. Auch der bislang weniger beachtete Ansatz der Space Transition Theory (vgl. Jaishankar 2008: passim) findet Eingang in diese Erörterungen. Hinsichtlich der Auswir-

kungen von Hasskriminalität im Internet (Kapitel 3.4) werden die inhärenten Einschüchterungseffekte und aufkommenden Zweifel an der Durchsetzungsfähigkeit rechtsstaatlicher Normen thematisiert, die sich in die analoge Welt übertragen können. Dieses Kapitel schließt mit einem Zwischenfazit (Kapitel 3.5), in welchem zunächst herausgearbeitet wird, dass aufgrund der fortschreitenden Digitalisierung und der ihr innewohnenden Komplexität und Geschwindigkeit bei der Betrachtung von politisch motivierter Hasskriminalität im Internet der soziologische Kriminalitätsbegriff zugrunde gelegt werden sollte (vgl. Brodowski und Freiling 2011: 27). Sodann werden die Ergebnisse der vorherigen Ausführungen zusammengeführt und zu einem Erklärungsansatz über die Wirkung von Hasskriminalität in der digitalen und analogen Welt verbunden. Zum Abschluss wird anhand dieser Synthese die Präventabilität des Phänomens betrachtet, wobei auf die Schlussfolgerungen verschiedener Kriminalitätstheorien zurückgegriffen wird.

Im vierten Kapitel werden die kriminalistischen Implikationen der Hasskriminalität im Internet thematisiert. Diese computerbasierten Delikte erweitern das klassische Spurenaufkommen um digitale Spuren (vgl. Kunze 2018: 163 f.). Daher werden zunächst die forensischen Aspekte bei der Sicherung und Auswertung digitaler Spuren betrachtet (Kapitel 4.1). Anschließend werden vor dem Hintergrund einer Kriminalistik, definiert als „die Wissenschaft von der Aufdeckung, Untersuchung und Verhütung von Straftaten und kriminalistisch relevanten Sachverhalten“ (Ackermann 2019: 18), die Anforderungen an die Ablauf- und Aufbauorganisation herausgearbeitet (Kapitel 4.2). Danach erfolgt eine Betrachtung der Möglichkeiten und Grenzen einer automatisierten Erkennung von entsprechenden Inhalten (Kapitel 4.3). Zum Abschluss dieses Kapitels werden die kriminalistischen Herausforderungen an die Strafverfolgungsbehörden und die daraus zu treffenden Ableitungen in einem Zwischenfazit bilanziert (Kapitel 4.4).

Aus der rechtspolitischen Diskussion zur Thematik ergeben sich wiederum kriminalpolitische Aktivitäten, welchen im fünften Kapitel nachgegangen wird. Hierbei stehen die Regelungen des am 1. Oktober 2017 in Kraft getretenen Netzwerkdurchsetzungsgesetzes[5] (Kapitel 5.1), das inzwischen beschlosse-

[5] Veröffentlicht im Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 61, ausgegeben zu Bonn am 7. September 2017, S. 3352-3355.

ne Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (vgl. BT-Drs. 19/17741 und 19/18470) (Kapitel 5.2), welches umfangreiche strafrechtliche, strafprozessrechtliche und telemedienrechtliche Änderungen beinhaltet sowie der Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes (vgl. BT-Drs. 19/18792) (Kapitel 5.3) im Zentrum der Betrachtung und Analyse.

Zum Abschluss der Arbeit werden in einem Fazit (Kapitel 6) vor dem Hintergrund der Ergebnisse der vorstehenden Kapitel Handlungsnotwendigkeiten und -möglichkeiten aufgezeigt.

1.2 Forschungsleitende Hypothesen und Fragestellungen

Die vorstehenden Ausführungen führen bezüglich der Themenstellung zur Annahme der zwei nachfolgenden forschungsleitenden Hypothesen, die anhand der skizzierten Fragestellungen untersucht werden:

Erstens verdeutlichen die kriminologischen und kriminalistischen Implikationen zur Hasskriminalität im Internet legislative und organisationale Handlungsnotwendigkeiten. Diese Hypothese soll im Rahmen der Arbeit anhand der nachfolgenden forschungsleitenden Fragestellungen analysiert werden: Ist die Hasskriminalität im Internet phänomenologisch und ätiologisch hinreichend beschrieben und sind diese Aspekte zu einem kriminologischen Erklärungsansatz verbunden? Welche kriminalistischen Anforderungen bestehen im Rahmen der Strafverfolgung an die computerbasierten Delikte der Hasskriminalität im Internet und wie kann diesen Anforderungen in der Praxis Rechnung getragen werden?

Zweitens wird davon ausgegangen, dass die bislang erfolgten sowie avisierten legislativen Maßnahmen in Zusammenhang mit der Hasskriminalität im Internet positive Veränderungen bewirken werden, welche jedoch für eine zielgerichtete und verfassungsgemäße Bekämpfung des Phänomens nicht ausreichend sind. Diese Hypothese soll im Rahmen der Arbeit durch folgende forschungsleitenden Fragestellungen analysiert werden: Welche Intentionen werden mit den kriminalpolitischen Initiativen bezüglich der Hasskriminalität im Internet verfolgt und tragen diese evidenzbasiert und zielgerichtet zur Beseitigung bestehender Defizite bei?

1.3 Methodisches Vorgehen

In Bezug auf das methodische Vorgehen handelt es sich um eine literaturtheoretische Arbeit. Aus der vergleichenden Textanalyse sollen kriminologische und kriminalistische Ableitungen zur Beantwortung der Frage getroffen werden, wie mit dem Thema der Hasskriminalität im Internet umzugehen ist, um eine zielgerichtete, evidenzbasierte und verfassungsgemäße Prävention und Bekämpfung des Phänomens zu ermöglichen.

Die thematische Befassung soll einen literaturtheoretisch-analytischen Beitrag dazu leisten, mögliche Fragmentierungen zwischen der kriminologischen und kriminalistischen Theorie, der tatsächlichen Ausprägung des Phänomens sowie seinen Bekämpfungsansätzen zu beseitigen.

2. Bestimmung des Gegenstandsbereichs und Problemstellungen

> *„Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten.“* (Artikel 5 Abs. 1 Satz 1 GG)

Die Thematik der politisch motivierten Hasskriminalität im Internet bedarf in Bezug auf verschiedene, mit ihr in Zusammenhang stehende Aspekte eingangs einiger grundlegender Überlegungen und Hinweise, um einerseits den im weiteren Verlauf der Arbeit zugrunde gelegten Rahmen klar zu bestimmen und andererseits charakteristische Problemstellungen zu verdeutlichen, die wiederholt aufzugreifen sein werden. Dieses Grundlagen schaffende Kapitel nimmt daher eine definitorische Rahmung des Gegenstandsbereichs vor, gibt einen kursorischen Überblick über die nach geltendem Recht in Frage kommenden strafrechtlichen Tatbestände und schließt mit einer Betrachtung der Implikationen, die sich aus der Anwendung von nationalem Straf- und Strafprozessrecht auf computerbasierte Delikte ergeben.

2.1 Definition politisch motivierter Hasskriminalität im Internet

Eine einheitliche oder gar verbindliche Definition für das Phänomen der Hasskriminalität im Internet existiert bislang nicht (vgl. Apostel 2019: 287; Krause 2019: 752). Deutlich wird dies nicht zuletzt durch den Umstand, dass die Begrifflichkeiten Hassrede, Hasssprache, Hasskommentare und Ha-

tespeech in den verschiedenen genutzten Beschreibungen synonym verwandt werden. Auch der Begriff des Hasspostings findet teilweise Verwendung und meint Beiträge im Internet, insbesondere in sozialen Medien und Netzwerken. Es erfolgt daher zunächst ein Überblick zu den, beziehungsweise eine Verweisung auf die bisher existierenden Definitionen, aus welchen im Anschluss durch eine Synthese eine phänomenologische Beschreibung abgeleitet wird, die in der weiteren Arbeit als Rahmung zugrunde gelegt wird.

Eine politische Thematisierung der Hasskriminalität erfolgte bereits 1997. Den Ausführungen des Europarates (1997: 2) folgend, „umfasst der Begriff ‚Hassrede' jegliche Ausdrucksformen, welche Rassenhass, Fremdenfeindlichkeit, Antisemitismus oder andere Formen von Hass, die auf Intoleranz gründen, propagieren, dazu anstiften, sie fördern oder rechtfertigen, einschliesslich [sic!] der Intoleranz, die sich in Form eines aggressiven Nationalismus und Ethnozentrismus, einer Diskriminierung und Feindseligkeit gegenüber Minderheiten, Einwanderern und der Einwanderung entstammenden Personen ausdrücken."

Weitere, seither genutzte Definitionsansätze verknüpfen das Vorliegen von Hasskriminalität eng mit den Zuordnungskriterien der politisch motivierten Kriminalität (vgl. Fn. 2).[6] Diesem Ansatz folgend, wurde für den Zuständigkeitsbereich der Polizei von der Kommission Staatsschutz[7] eine Definition vorgelegt, wonach politisch motivierten Hasspostings „solche Straftaten zugerechnet [werden], die in Würdigung der Umstände der Tat oder der Einstellung des Täters Anhaltspunkte dafür geben, dass diese wegen einer zugeschriebenen oder tatsächlichen politischen Haltung, Einstellung und/oder Engagements, Nationalität, ethnischer Zugehörigkeit, Hautfarbe, Religionszugehörigkeit, Weltanschauung, sozialen Status, physischer und/oder psy-

[6] Beispielhaft wird auf die Definitionen der Europäischen Kommission gegen Rassismus und Intoleranz (vgl. 2016: 3) und der Bundeszentrale für politische Bildung (vgl. 2017) sowie die Ausführungen der Wissenschaftlichen Dienste des Deutschen Bundestags (vgl. 2016: passim) verwiesen. Auch Anbieter sozialer Medien und Netzwerke verweisen in ihren Richtlinien und Gemeinschaftsstandards auf entsprechend zu schützende Eigenschaften (vgl. Facebook 2020; Twitter 2020; Google 2020).

[7] Innerhalb der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) ist die Kommission Staatsschutz im Arbeitskreis II - Innere Sicherheit (unter anderem Gefahrenabwehr, Bekämpfung des Terrorismus, Angelegenheiten der Polizei) der Arbeitsgemeinschaft Kripo (AG Kripo) untergeordnet (vgl. Innenministerkonferenz 2020; Münch 2020a: 580 f.).

chischer Behinderung oder Beeinträchtigung, sexuellen Orientierung und/oder sexuellen Identität oder äußeren Erscheinungsbildes kausal gegen eine oder mehrere Person(en), Gruppe(n), oder Institution(en) gerichtet sind“ (BT-Drs 19/11908, S. 5).

In Anlehnung an Geschke et al. (vgl. 2019: 15) ist ein vorurteilsgeleiteter und negativ konnotierter Sprachgebrauch zum Nachteil von spezifischen Gruppen von Menschen für Hasskriminalität konstitutiv. Hieraus ergibt sich die Unterscheidung von individuellen Formen der Abwertung. Im Ergebnis handelt es sich daher um politisch motivierte Hasskriminalität, wenn xenophobe Haltungen, beispielsweise in Bezug auf die Nationalität, die ethnische Zugehörigkeit, die Hautfarbe oder Religionszugehörigkeit, oder sonstige Motive, wie den sozialen Status, eine physische oder psychische Behinderung oder Beeinträchtigung, das Geschlecht, die sexuelle Identität oder Orientierung sowie das äußere Erscheinungsbild handlungsleitend sind und sich aufgrund ihres Wesens eine sozialschädigende Wirkung entfaltet. Von politisch motivierter Hasskriminalität im Internet ist auszugehen, wenn entsprechende Inhalte in Schrift, Bild, Ton, Video, Sprache oder durch sonstige elektronische Datenübermittlung in das Internet eingestellt, dort verbreitet oder unabhängig von einer Speicherung durch Informations- oder Kommunikationstechnik übertragen werden. Dies inkludiert sowohl Internetseiten und deren Kommentarbereiche, soziale Medien und Netzwerke, Foren, Möglichkeiten des Live-Chats sowie Online-Multiplayer-Spiele, die jedermann mit oder ohne vorherige Anmeldung zugänglich sind, als auch geschlossene Nutzergruppen, bei welchen nur ausgewählten Personen der Zugang oder die Mitgliedschaft ermöglicht wird.[8] Die Delikte können gegen Personen, Personengruppen, Institutionen oder Sachen gerichtet sein, welchen die genannten Zuordnungskriterien täterseitig zugerechnet werden oder auf welche diese evident zutreffen sowie alternativ, verbunden mit den beschriebenen Haltungen und Motiven, ad libitum auf ein anderes Ziel ausgerichtet sein. Die ein sozialethisches Unwerturteil enthaltende Meinungsäußerung oder Publikation kann darüber hinaus im Falle der Befürwortung einer rechtsautoritären Diktatur

[8] Die unterschiedliche Bedeutung und Wirkung zwischen öffentlich wahrnehmbarer Hasskriminalität in Internet und solcher in geschlossenen Gruppen werden in Kapitel 3 am Beispiel der Fallvignetten Lübcke und Halle herausgearbeitet.

sowie durch chauvinistische, ausländerfeindliche, sozialdarwinistische oder den Nationalsozialismus verharmlosende Inhalte (vgl. Stöss 2010: 59 f.) dazu geeignet oder darauf ausgerichtet sein, die demokratische und pluralistische Gesellschaftsordnung und den liberalen Rechtsstaat öffentlich in Frage zu stellen, abzulehnen oder anzugreifen.

2.2 Strafrechtlicher Überblick (lex lata)

Als Teil des Rechtsstaatsprinzips gebietet Artikel 20 Absatz 3 GG in Verbindung mit Artikel 1 Absatz 3 GG die Gesetzmäßigkeit der Verwaltung.[9] Bei jeglicher hoheitlichen Handlung besteht eine Rechtsbindung, weshalb die vollziehende Gewalt und die Rechtsprechung zur Einhaltung von Gesetz und Recht verpflichtet sind (vgl. BVerfGE 40, 237, 248 f.). Die Kundgabe von Meinungen wird daher zunächst vor dem Hintergrund ihres grundrechtlichen Schutzes beleuchtet, ehe in Frage kommende strafrechtliche Tatbestände (lex lata) betrachtet werden.

2.2.1 Meinungsäußerungen, Grundrechtsschutz und Schranken

Das Grundrecht auf Meinungsfreiheit aus Artikel 5 Absatz 1 Satz 1 Variante 1 GG gibt jedem das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten. „Meinungen sind durch die subjektive Beziehung des Einzelnen zum Inhalt seiner Aussage geprägt“ (BVerfGE 90, 241, 247). Hierunter fallen Äußerungen, wenn sie durch ein Element der Stellungnahme und des Dafürhaltens geprägt sind (vgl. BVerfGE 61, 1, 9; 90, 241, 247; 124, 300, 320) und auch Werturteile, die einen polemischen oder verletzenden Aussageinhalt haben (vgl. BVerfGE 54, 129, 138 f.; 61, 1, 7 f.; 93, 266, 289 f.; stRspr.). Im Unterschied hierzu sind Tatsachenbehauptungen, die durch Abgrenzung zwischen behaupteter Äußerung und Realität auf ihren objektiven Wahrheitsgehalt hin überprüft werden können, von der Meinungsfreiheit nur dann geschützt, wenn sie einen Beitrag zur Bildung von Meinungen leisten können (vgl. BVerfGE 90, 241, 247). Vorsätzlich oder nachweislich falsche Tatsachenbehauptungen unterfallen diesem Grundrechtsschutz nicht, da sie der verfassungsrechtlichen Voraussetzung einer zutreffenden Meinungsbildung nicht dienlich sind (vgl. BVerfGE 54, 208, 219; 61, 1, 8; 90,

[9] Zur Konkretisierung dieses Prinzips durch die Grundsätze des Vorrangs und des Vorbehalts des Gesetzes vgl. von Danwitz 2008: 11 ff.

241, 247 f.[10]; stRspr.). Grundsätzlich besteht demnach die Möglichkeit, dass Inhalte, die der politisch motivierten Hasskriminalität zuzuordnen sind, vom Grundrecht der Meinungsfreiheit geschützt sind.

Sofern Äußerungen der Meinungsfreiheit unterliegen, knüpfen strafrechtliche Ermittlungen und Verurteilungen an den Schutzbereich an und greifen mithin in dieses Grundrecht ein. Die verfassungsrechtliche Rechtfertigung ist hierzu gegeben, weil das Grundrecht auf Meinungsfreiheit gemäß Artikel 5 Absatz 2 GG seine Schranken in den Vorschriften der allgemeinen Gesetze sowie zugunsten des Jugendschutzes und der persönlichen Ehre findet.[11] An allgemeine Gesetze, zu welchen die Strafgesetze gelten, besteht dabei der Anspruch, dass sie sich nicht gegen eine Meinung und deren Äußerung richten dürfen oder diese verbieten und dass sie dem Schutz eines schlechthin zu schützenden Rechtsguts dienen, welches von der Rechtsordnung allgemein und unabhängig davon geschützt wird, ob es durch eine Meinungsäußerung oder auf andere Weise verletzt werden kann (vgl. BVerfGE 7, 198, 209 f.; 93, 266, 291; 111, 147, 155; 124, 300, 321 f.; stRspr.). Hierbei ist zu berücksichtigen, dass „die ‚allgemeinen Gesetze' zwar dem Wortlaut nach dem Grundrecht Schranken setzen, ihrerseits aber aus der Erkenntnis der wertsetzenden Bedeutung dieses Grundrechts im freiheitlichen demokratischen Staat ausgelegt und so in ihrer das Grundrecht begrenzenden Wirkung selbst wieder eingeschränkt werden müssen" (BVerfGE 7, 198, 209).

Es bedarf daher regelmäßig einer Abwägung zwischen der grundrechtlich geschützten Meinungsfreiheit und den durch Äußerungen potentiell verletzten Schutzgütern. Für den Abwägungsprozess haben sich in der Rechtsprechung in Ermangelung eines verbindlichen Abwägungsschemas verschiedene Gesichtspunkte entwickelt, aus denen Kriterien für die konkrete Abwägung hervorgehen[12]. Lediglich in den verfassungsrechtlich spezifisch defi-

[10] Mit dieser Entscheidung, die einen Bezug zu politisch motivierter Hasskriminalität im Internet haben kann, stellte das Bundesverfassungsgericht (BVerfG) heraus, dass die Leugnung des Holocaust durch das NS-Regime, die sogenannte „Auschwitzlüge", nicht von der Meinungsfreiheit gedeckt ist, da die Behauptung unter Bezugnahme auf voneinander unabhängige Nachweise unwahr ist (vgl. BVerfGE 90, 241, 249).

[11] Zur Freiheit der Meinungsäußerung und ihrer Schranken siehe auch Artikel 10 der Europäischen Menschenrechtskonvention sowie die Rechtsprechung des Europäischen Gerichts-hofs für Menschenrechte, Urteil vom 7. Februar 2012, Az. 40660/08 und 60441/08.

[12] Zu berücksichtigen sind beispielhaft die Schwere der Beeinträchtigung, wobei es grundsätzlich unerheblich ist, ob es sich um berechtigte Kritik handelt oder ob das Werturteil

nierten Fällen einer Schmähkritik[13], einer Formalbeleidigung[14] oder einer Verletzung der Menschenwürde[15] kann diese Abwägung unterbleiben, wobei das Vorliegen einer solchen Fallkonstellation einer Begründung bedarf, an welche jeweils strenge Kriterien anzulegen sind (vgl. BVerfG, Beschluss vom 19. Mai 2020, Az. 1 BvR 2397/19, Rn. 18 bis 25; Bundesverfassungsgericht 2020). Bei jeder der drei Fallgruppen tritt die Meinungsfreiheit hinter das Persönlichkeitsrecht oder andere betroffene Grundrechte zurück.

2.2.2 Tatbestandliche Übersicht

Bei politisch motivierter Hasskriminalität im Internet fungieren Computer und die damit einhergehende Vernetzung als Tatwerkzeug. Bei diesen inhaltsbezogenen Straftaten, werden „Computersysteme zwar in einer an sich rechtlich zulässigen Weise [genutzt], aber zur Verbreitung per se strafbarer Inhalte missbraucht“ (Hilgendorf und Valerius 2012: 40, Rn. 123). Vor dem Hintergrund der zugrundeliegenden phänomenologischen Beschreibung der politisch motivierten Hasskriminalität im Internet (vgl. Kapitel 2.1) wird deutlich, dass von entsprechenden Tathandlungen diverse strafrechtliche Tatbestände betroffen sein können. Diese verteilen sich auf verschiedene Abschnitte des Besonderen Teils (BT) des StGB und orientieren sich dabei materiellrechtlich schutzgutbezogen. Aufgrund der komplexen Ursachen-Wirkungs-Zusammenhänge (vgl. Kapitel 3) wird hierbei entgegen anderer, engerer definitorischer Rahmungen hinsichtlich der inkludierten Strafnormen ein weites Verständnis in Bezug auf das gegenständliche Phänomen angenommen.

„richtig“ ist (vgl. BVerfGE 93, 266, 294), „eine Vermutung für die freie Rede, wenn es um Beiträge zum geistigen Meinungskampf in einer die Öffentlichkeit wesentlich berührenden Frage geht“ (BVerfG, Beschluss vom 12. Mai 2009, Az. 1 BvR 2272/04, Rn. 29) sowie der Wahrheitsgehalt einer Aussage, wenn die Meinungsäußerung auch Tatsachenelemente enthält (vgl. BGH, Urteil vom 16. Dezember 2014, Az. VI ZR 39/14).

[13] Eine Schmähung liegt nicht schon wegen der herabsetzenden Wirkung einer Meinungsäußerung vor. Dies gilt auch für eine überzogene oder gar ausfällige Kritik. Der Charakter einer Schmähung ist erst gegeben, „wenn in [einer herabsetzenden Äußerung] nicht mehr die Auseinandersetzung in der Sache, sondern die Diffamierung der Person im Vordergrund steht. Sie muß [sic!] jenseits auch polemischer und überspitzter Kritik in der Herabsetzung der Person bestehen“ (BVerfGE 82, 272, 283 f.).

[14] Im Unterschied zur Schmähkritik, bei welcher es am Bezug zum Thema mangelt und die Diffamierung im Fokus steht, begründet sich die Unzulässigkeit der Formalbeleidigung bereits aus der Form und Art der Äußerung (vgl. BVerfG, Beschluss vom 19. Mai 2020, Az. 1 BvR 2397/19, Rn. 21).

[15] Das unantastbare Grundrecht der „Menschenwürde als Wurzel aller Grundrechte ist mit keinem Einzelgrundrecht abwägungsfähig“ (BVerfGE 93, 266, 293). Insbesondere der Straftatbestand der Volksverhetzung gemäß § 130 StGB begründet regelmäßig das Vorliegen dieser Fallkonstellation.

Strafnorm	Tatbestand
§ 86 StGB	Verbreiten von Propagandamitteln verfassungswidriger Organisationen
§ 86 a StGB	Verwenden von Kennzeichen verfassungswidriger Organisationen
§ 90 StGB	Verunglimpfung des Bundespräsidenten
§ 90a StGB	Verunglimpfung des Staates und seiner Symbole
§ 90b StGB	Verfassungsfeindliche Verunglimpfung von Verfassungsorganen
§ 90c StGB	Verunglimpfung von Symbolen der Europäischen Union
§ 91 StGB	Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat
§ 100a StGB	Landesverräterische Fälschung
§ 104 StGB	Verletzung von Flaggen und Hoheitszeichen ausländischer Staaten
§ 105 StGB	Nötigung von Verfassungsorganen
§ 106 StGB	Nötigung des Bundespräsidenten und von Mitgliedern eines Verfassungsorgans
§ 111 StGB	Öffentliche Aufforderung zu Straftaten
§ 126 StGB	Störung des öffentlichen Friedens durch Androhung von Straftaten
§ 130 StGB	Volksverhetzung
§ 130a StGB	Anleitung zu Straftaten
§ 131 StGB	Gewaltdarstellung
§ 140 StGB	Belohnung und Billigung von Straftaten
§ 164 StGB	Falsche Verdächtigung
§ 166 StGB	Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen
§ 185 StGB	Beleidigung
§ 186 StGB	Üble Nachrede
§ 187 StGB	Verleumdung
§ 188 StGB	Üble Nachrede und Verleumdung gegen Personen des politischen Lebens
§ 189 StGB	Verunglimpfung des Andenkens Verstorbener
§ 240 StGB	Nötigung
§ 241 StGB	Bedrohung

Abbildung 1: Auflistung der in Frage kommenden strafrechtlichen Tatbestände

Für einen kursorischen Überblick können zwei Kategorien gebildet werden, welche zwischen Straftaten, die eine individuelle Betroffenheit auslösen und Delikten, die gegen ein Kollektiv gerichtet sind, unterscheiden. Die relevantesten Strafnormen und Anforderungen an die Erfüllung der Tatbestände durch Hasskriminalität im Internet werden nachfolgend erörtert.

Die erste Teilmenge umfasst Straftaten gegen die persönliche Ehre und die persönliche Freiheit. Von praktischer Bedeutung erscheint hierbei insbesondere der Tatbestand der Beleidigung gemäß § 185 StGB[16], aber auch die Delikte der Nötigung gemäß § 240 StGB und der Bedrohung gemäß § 241 StGB sind in dieser Kategorie von Belang. Für die Verwirklichung einer Beleidigung ist es lediglich notwendig, dass die Äußerung von der beleidigten oder einer dritten Person wahrgenommen wird (vgl. Fischer 2020:

[16] Zur Frage, ob bei einer ehrbeeinträchtigenden Äußerung eine entsprechende Strafbarkeit im Spannungsverhältnis von Meinungsfreiheit und Persönlichkeitsrecht in Betracht kommt, hat das BVerfG im Mai 2020 verfassungsrechtliche Vorgaben gemacht, die auf den bereits erwähnten Abwägungsprozess anzuwenden sind (vgl. BVerfG, Beschlüsse vom 19. Mai 2020, Az. 1 BvR 2459/19, 1 BvR 2397/19, 1 BvR 1094/19 und 1 BvR 362/18).

§ 185 StGB, Rn. 14). Eine versuchte Nötigung liegt bereits vor, wenn mit der Anwendung des Nötigungsmittels begonnen wurde (vgl. ebd.: § 240 StGB, Rn. 56) und für die Bedrohung bedarf es entweder des In-Aussicht-Stellens oder alternativ des Vortäuschens der Verwirklichung eines Verbrechens (vgl. ebd.: § 241 StGB, Rn. 3a, 5). Die aufgeführten Tatbestände können folglich über das Internet begangen werden. In Abhängigkeit der konkreten Tatbegehung können ergänzend Delikte von strafrechtlichen Nebengesetzen verletzt werden. In Betracht kommen die Normen zum Schutz personenbezogener Daten gemäß § 42 Bundesdatenschutzgesetz und in Bezug auf die unbefugte Veröffentlichung von Bildaufnahmen nach § 33 Kunsturhebergesetz.

Zum zweiten Teilbereich gehören im weitesten Sinne Straftaten, welche sich gegen den demokratischen Rechtsstaat oder die öffentliche Ordnung richten. In der Praxis dürften das Verbreiten von Propagandamitteln verfassungswidriger Organisationen gem. § 86 StGB, das Verwenden von Kennzeichen verfassungswidriger Organisationen gemäß § 86a StGB, die öffentliche Aufforderung zu Straftaten gemäß § 111 StGB, die Störung des öffentlichen Friedens durch Androhung von Straftaten gemäß § 126 StGB, die Volksverhetzung gemäß § 130 StGB sowie die Belohnung und Billigung von Straftaten gemäß § 140 StGB hierbei die größte Relevanz aufweisen. Der nicht legal definierte Begriff der Propaganda gem. § 86 StGB enthält einen inhaltlich werbenden und auf Unterstützung gerichteten Aspekt, wobei sich das Propagandamittel gegen die freiheitliche demokratische Grundordnung oder gegen den Gedanken der Völkerverständigung richten muss (vgl. Fischer 2020: § 86 StGB, Rn. 3 f.). Kennzeichen gem. § 86a StGB umfassen verkörperte und nichtkörperliche Erkennungszeichen verbotener Vereinigungen (vgl. ebd.: § 86a StGB, Rn. 3). Eine Aufforderung zur Straftat im Sinne des § 111 StGB „ist eine bestimmte, über bloßes Befürworten hinausgehende [...] Erklärung, dass andere etwas tun [...] sollen“ (ebd.: § 111 StGB, Rn. 4). Während dies also als Anstiftung zu fassen ist, bezieht sich § 126 StGB auf eigene Taten des Täters oder solche, auf die er Einfluss nehmen kann, wobei das Vortäuschen des Bevorstehens einer entsprechenden Tat ausreichend ist (vgl. ebd.: § 126 StGB, Rn. 5). § 130 Absatz 1 Nr. 1 StGB kann durch Aufstacheln zu Hass, also „eine auf die Gefühle des Adressaten abzielende, über bloße Äußerung von Ablehnung und Verachtung hinausgehende Form

des Anreizens zu einer feindseligen Haltung“ (Fischer 2020: § 130 StGB, Rn. 8) und durch Aufforderung zu Gewalt- oder Willkürmaßnahmen begangen werden, was sich an der Tathandlung zu § 111 StGB orientiert. § 130 Absatz 1 Nr. 2 StGB umfasst den bereits skizzierten Angriff auf die Menschenwürde.[17] § 140 StGB meint in der Tathandlung des Billigen das Gutheißen einer konkreten rechtswidrigen Vortat (vgl. ebd.: § 140 StGB, Rn. 7). Mit dem Sechzigsten Gesetz zur Änderung des Strafgesetzbuches[18] wurde der Schriftenbegriff des § 11 Abs. 3 StGB zu einem Inhaltsbegriff fortentwickelt. Seit dem 1. Januar 2021 wird daher unabhängig vom Trägermedium oder einer Speicherung auf den Inhalt selbst abgestellt, da dieser „der eigentliche Grund für die Strafbarkeit darauf bezogener Handlungen ist“ (BT-Drs. 19/19859, S. 2). Die Verwirklichung der §§ 86, 86a, 111, 130 und 140 StGB ist durch das Verbreiten von Inhalten möglich, sodass Tathandlungen der Übertragung mittels Informations- oder Kommunikationstechnik erfasst sind.[19] In Bezug auf § 126 StGB ergibt sich die Eignung zur Friedensstörung auch aus Veröffentlichungen im Internet (vgl. Fischer 2020: § 126 StGB, Rn. 10).

Im Ergebnis ist einerseits festzuhalten, dass der Meinungsfreiheit in einer freiheitlichen, pluralistischen und demokratischen Gesellschaft ein hoher Stellenwert zukommt, da sie für diese konstituierend und unabdingbar ist (vgl. BVerfGE 93, 266, 292 f.). Dass dies verfassungsrechtlich eine entsprechende Würdigung erfährt, ist auch deshalb notwendig, um eine einschüchternde oder abschreckende Wirkung auf den Gebrauch des Grundrechts und somit eine schleichende Erosion der Meinungsfreiheit zu verhindern (vgl. BVerfGE 43, 130, 136; 54, 129, 136; 93, 266, 292; 114, 139, 349 f.). Hierdurch werden im Umkehrschluss nicht alle sozialschädlichen beziehungs-

[17] Für Beispiele aus der Rechtsprechung siehe Krause 2019: 753.

[18] Veröffentlicht im Bundesgesetzblatt Jahrgang 2020 Teil I Nr. 57, ausgegeben zu Bonn am 3. Dezember 2020, S. 2600-2605.

[19] In Bezug auf konkrete Tathandlungen kann die Entwicklung der Rechtsprechung mit Spannung beobachtet werden. So beantragte die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Generalstaatsanwaltschaft Frankfurt am Main inzwischen Strafbefehle wegen der Billigung von Straftaten nach § 140 StGB, nachdem ein rassistisch motiviertes Tötungsdelikt durch das sogenannte Liken eines Beitrags mit der Eignung zur öffentlichen Friedensstörung öffentlich gebilligt worden sei (vgl. Steinke 2020). Ziel der Verfolgung sei hierbei nicht eine hohe Strafe, sondern die Schaffung des Bewusstseins, dass ein Gutheißen oder Billigen von politisch motivierter Hasskriminalität im Internet diese verstärke (vgl. ebd.).

weise als problematisch empfundenen Verhaltensweisen pönalisiert. Andererseits ist zu konstatieren, dass die tradierten Tatbestände grundsätzlich dazu geeignet sind, politisch motivierte Hasskriminalität im Internet zu erfassen (vgl. Krause 2019: 754), sodass es keiner lex specialis für dieses Phänomen bedarf. Da sich die Tatbestände in ihrem Ursprung jedoch auf die analoge Lebenswelt beziehen, besteht dennoch die Gefahr, dass sie auf Delikte im virtuellen Raum phänomenspezifisch nicht immer ausreichend wirksam sind. Legislativ bleiben im Spannungsverhältnis zwischen Meinungsfreiheit und staatlichem Strafanspruch daher die Fragen der Anpassung des materiellen Rechts im Hinblick auf Schutzgüter und die Tat- oder Angriffsmittel sowie der Verschärfung von Strafandrohungen. Kriminalpolitische Maßnahmen in diesem Kontext werden im weiteren Verlauf der Arbeit thematisiert (vgl. Kapitel 5).

2.3 Anwendung nationalen Straf- und Strafprozessrechts auf Hasskriminalität im Internet

Nationale Grenzen sind für Handlungen im Internet nicht von Bedeutung, da sie aufgrund der globalen Vernetzung weltweit vorgenommen werden können. Dies betrifft legale und illegale Aktivitäten gleichermaßen. Im Gegensatz hierzu sind das Strafrecht und die Strafverfolgung eine Angelegenheit der Nationalstaaten. Das deutsche Strafrecht ist auf im Ausland begangene Delikte nur bei Bestehen eines völkerrechtlich legitimierenden Anknüpfungspunktes möglich.

Der örtliche Geltungsbereich des deutschen Strafrechts richtet sich nach § 3 ff. StGB, wobei das Territorialitätsprinzip die Grundlage bildet. Als Handlungsort einer Tat ist hierbei zunächst jeder Ort anzusehen, an dem durch den Täter eine Tätigkeit vorgenommen wird, die auf die Tatbestandsverwirklichung gerichtet ist, sodass auf die körperliche Anwesenheit des Täters abzustellen ist (vgl. Busching 2015: 296; Schiemann 2018: 152). Auch nach der Rechtsprechung des Bundesgerichtshofs (BGH) ist der Aufenthaltsort entscheidend und der „Radius der Wahrnehmbarkeit einer Handlung ist nicht Teil ihrer selbst“ (BGH, Beschluss vom 19. August 2014, Az. 3 StR 88/14, Rn. 9).

Allerdings kann in Form eines Ubiquitätsprinzips auch dem Erfolgsort einer Straftat gemäß § 9 Abs. 1 3. Alternative und 4. Alternative StGB eine tatort-

begründende Wirkung zukommen. Da es sich bei politisch motivierter Hasskriminalität im Internet um Publikations- und Äußerungsdelikte handelt, deren Inhalte unabhängig vom Handlungsort des Täters weltweit zugänglich sind und abgerufen werden können, stellt sich die Frage nach der Begründung eines tatbestandsmäßigen Erfolgsorts und damit nach einer strafanwendungsrechtlichen Einordnung (vgl. Schiemann 2018: 153).

In Bezug auf völkerrechtlich legitimierende Anknüpfungspunkte ist die Entwicklung der Rechtsprechung in den Blick zu nehmen. So urteilte der BGH im Jahr 2000, dass ein zum Tatbestand gehörender Erfolg im Inland gem. § 9 Abs. 1 3. Alternative StGB eintritt, wenn ein im Ausland handelnder ausländischer Staatsangehöriger auf einem ausländischen Server Inhalte in englischer Sprache hochlädt, die den Tatbestand der Volksverhetzung gem. § 130 Abs. 1 oder 3 StGB erfüllen (vgl. BGHSt 46, 212). Der völkerrechtlich legitimierende Anknüpfungspunkt wurde aus der Bedeutung des inländischen Rechtsguts und dem besonderen Bezug auf das Gebiet der Bundesrepublik Deutschland aufgrund der „Einzigartigkeit der unter der Herrschaft des Nationalsozialismus an den Juden begangenen Verbrechen“ (BGHSt 46, 212, 224) abgeleitet. In Abweichung hierzu entschied der BGH (vgl. Beschluss vom 19. August 2014, Az. 3 StR 88/14, Rn. 8) in 2014, dass die Erfüllung des Tatbestands des § 86a StGB durch einen im Ausland handelnden Täter in Ermangelung eines zum Tatbestand gehörenden Erfolgs einen solchen gem. § 9 Abs. 1 3. oder 4. Variante nicht begründe und im Hinblick auf völkerrechtliche Fragen die Strafbarkeit nicht ausnahmslos auf Sachverhalte mit internationalem Bezug erstreckt werden könne.[20]

Während diese Rechtsprechung für eine umfassendere Berücksichtigung des völkerrechtlichen Nichteinmischungsgebots spricht, erfolgte durch das Sechzigste Gesetz zur Änderung des Strafgesetzbuchs (vgl. Fn. 18) im Gegensatz hierzu eine Erweiterung des Strafanwendungsrechts für Auslandstaten mit besonderem Inlandsbezug gem. § 5 StGB. Diese Änderung betrifft den Geltungsbereich der für das gegenständliche Phänomen relevanten Tatbestände der §§ 86, 86a, 111 und 130 StGB in den Konstellationen, bei wel-

[20] Eine ähnliche Begründung für die Nicht-Anwendbarkeit des deutschen Strafrechts betreffend den Tatbestand des § 130 Abs. 3 StGB bei diesen Voraussetzungen findet sich im BGH Beschluss vom 3. Mai 2016, Az. 3 StR 449/15, Rn. 13.

chen der im Ausland handelnde Täter deutscher Staatsangehöriger ist oder seine Lebensgrundlage im Inland hat. Die Novellierung stellt eine direkte Reaktion auf die vorgenannte Rechtsprechung des BGH dar (vgl. BT-Drs. 19/19859, S. 22 f.). Der Anwendungsbereich des § 5 StGB ist nunmehr unabhängig vom am ausländischen Tatort geltenden Recht eröffnet, wenn neben dem personalen auch ein sachlicher Inlandsbezug besteht. Für die §§ 86, 86a und 130 StGB ist ein solcher über die im Inland wahrnehmbare Verbreitung[21] oder das Zugänglichmachen gegenüber der inländischen Öffentlichkeit[22] gegeben, im Falle des § 130 Abs. 2 Nr. 1 StGB muss zudem die Eignung zur Störung des inländischen öffentlichen Friedens bestehen (vgl. ebd.: S. 32). Der sachliche Inlandsbezug des § 111 StGB begründet sich, wenn sich die Aufforderung auf eine im Inland zu begehende Tat bezieht (vgl. Fischer 2020: § 111 StGB, Rn. 6) und diese im Inland wahrnehmbar ist.[23]

Die Geltung des deutschen Strafrechts für Auslandstaten von nicht deutschen Staatsangehörigen stützt sich auf § 7 Abs. 2 Nr. 2 StGB. Das dort normierte Prinzip der stellvertretenden Strafrechtspflege sichert die gerechte Verfolgung eines ausländischen Straftäters, wenn der eigentlich zur Verfolgung berufene Staat die Tat nicht verfolgen will oder kann, sodass diese Norm eine subsidiäre Ergänzung der Strafgewalt anderer Staaten darstellt (vgl. BGH, Beschluss vom 23. April 2019, Az. 4 StR 41/19, Rn. 9).

Vor dem Hintergrund des umfangreichen Tatbestandskatalogs (vgl. Kapitel 2.2.2) und den unterschiedlichen Tatkonstellationen ergibt sich hierbei eine Fülle rechtlicher Problemstellungen in Bezug auf das Phänomen der politisch motivierten Hasskriminalität im Internet. Über die Frage hinaus, ob der jeweils einschlägige Straftatbestand einen Erfolg voraussetzt, an dessen Ein-

[21] Dies ist nach Auffassung des Gesetzgebers der Fall, „wenn die Datei auf dem Rechner des Adressaten im Inland, sei es im flüchtigen Arbeitsspeicher oder auf einem permanenten Speichermedium, angekommen ist, wobei es unerheblich ist, ob der Adressat die Möglichkeit des Zugriffs auf die Daten genutzt oder ob der Anbieter die Daten übermittelt hat“ (BT-Drs. 19/19859, S. 44).

[22] Hierzu genügt dem Gesetzgeber „die Eröffnung eines Lesezugriffs [...] auf einen Inhalt [...], der auf einem ausländischen Server abgespeichert ist (BT-Drs. 19/19859, S. 44).

[23] Dies soll nach Auffassung des Gesetzgebers bereits gegeben sein, wenn die Inhalte „bei Einstellung in das Internet auf einen ausländischen Server abgelegt werden, aber vom Inland aus - zum Beispiel über einen Hyperlink - abgerufen werden können“ (BT-Drs. 19/19859, S. 45).

tritt im Inland angeknüpft werden kann[24], ist beispielsweise an den Einsatz von Bot-Netzen oder die Frage, wie ausländische Host-Provider zu bewerten sind, zu denken (vgl. Apostel 2019: 289).

Die territoriale Schrankenlosigkeit des Internets verursacht auch in Bezug auf die an den Territorialitätsgrundsatz gebundene Strafverfolgung, bereits beginnend bei der Datenerhebung im Ausland, Hemmnisse, da internationale Maßnahmen nur durch zeitaufwendige Rechts- und Vollstreckungshilfe durchgeführt werden können. Die bestehende Vernetzung und damit einhergehende technologische Abhängigkeit macht aufgrund der Geschwindigkeit und Schnelllebigkeit für eine zielgerichtete und erfolgreiche Bekämpfung des netzwerkspezifischen Phänomens der politisch motivierten Hasskriminalität jedoch weitergehende Kooperationen erforderlich (vgl. Haase 2017: 243). Ein universeller Konsens der internationalen Staatengemeinschaft besteht hierzu bislang nicht. Dies ist sicherlich auch darauf zurückzuführen, dass international unterschiedliche Anforderungen an die Balance zwischen Strafverfolgungsinteresse, betroffenen Individualrechten und staatlichen Souveränitätsinteressen bestehen (vgl. European Criminal Policy Initiative 2013: 412).

Zumindest für die Mitgliedsstaaten des Europarates existiert bei entsprechender Ratifizierung das Zusatzübereinkommen SEV Nr. 189 zum Übereinkommen über Computerkriminalität SEV Nr. 185, welches die internationale Zusammenarbeit bei rassistischen oder fremdenfeindlichen Delikten zum Gegenstand hat (vgl. Europarat 2003). Für die Bundesrepublik Deutschland finden die Regularien seit März 2011 Anwendung (vgl. Bundesgesetzblatt, Jahrgang 2011, Teil II, Nr. 8, ausgegeben zu Bonn am 22. März 2011).

Alle Aspekte und Problemstellungen der Anwendung von nationalem Straf- und Strafprozessrecht auf Hasskriminalität im Internet können an dieser Stelle nicht abschließend thematisiert werden. Eine Sensibilisierung für die Komplexität der Thematik ist durch die bestehenden Ausführungen jedoch gegeben. Nachfolgend werden die kriminologischen Implikationen in den Blick genommen.

[24] So bedürfen beispielsweise konkrete und abstrakte Gefährdungsdelikte einer differenzierenden Betrachtung. Vertiefend für die Bestimmung des Tatortes bei Internetdelikten vgl. Fischer 2020: § 9 StGB, Rn. 5 ff.

3. Kriminologische Implikationen

> *„Das tägliche Leben ist vielfach weder on- noch offline, sondern beides, so dass sich eine neue Art von Welt – die Onlife-Welt – zu bilden beginnt.“* (Hoffmann-Riem 2018: 22)

Bei der Kriminologie handelt es sich um die empirische und interdisziplinäre „Wissenschaft vom abweichenden Verhalten und den gesellschaftlichen Reaktionen darauf“ (Neubacher 2020: 22). Sie hat die Auffindung von Gesetzmäßigkeiten zum Ziel, welche theoretisch abgeleitet und methodisch kontrolliert werden (vgl. ebd.: 24). Losgelöst vom aktuell gültigen Strafrecht liegt ihr hierbei der soziologische Verbrechensbegriff zugrunde, welcher auf die Sozialschädlichkeit von Verhaltensweisen abstellt (vgl. Kunz und Singelnstein 2016: 11). Zu ihrem umfassenden Gegenstandsbereich gehören unter anderem die Kriminalphänomenologie, welche Kriminalität als Einzel- oder Massenphänomen, ihre Entwicklung und Erscheinung beschreibt, die Kriminalätiologie als die Lehre von den Kriminalitätsursachen und ihren kriminologischen Erklärungsansätzen sowie die Viktimologie und die Kriminalstatistik (vgl. Neubacher 2020: 25; Ackermann 2019: 46).

Von besonderer Bedeutung bei den nachfolgenden Ausführungen ist der Umstand, dass es sich bei dem zu betrachtenden Phänomen um medial vermittelte Informationen und Kommunikation handelt. Aus kriminologischer Perspektive erwachsen hieraus einige Besonderheiten, die in die Überlegungen einzubinden sind. Dies sind die weite Verbreitung des Internets sowie die nahezu jederzeit bestehende Zugangsmöglichkeit hierzu, eine subjektiv häufig empfundene, aber nur scheinbare Anonymität und der Aspekt der Distanz (vgl. Meier 2015: 95 f.). Auf die beiden letztgenannten Aspekte wird nachfolgend vertiefend eingegangen.

Für die politisch motivierte Hasskriminalität im Internet wird im hiesigen Kapitel zunächst eine phänomenologisch-ätiologische Betrachtung von Ursachen und ihrer Ausprägung sowie eine Beschreibung von Erklärungsansätzen und ihrer Auswirkungen vorgenommen, ehe die Ergebnisse dieser Analyse in einem Zwischenfazit zusammengeführt werden und hieraus die Präventabilität des Phänomens abgeleitet wird.

3.1 Ätiologie politisch motivierter Hasskriminalität im Internet

Die Ursachen politisch motivierter Hasskriminalität im Internet im Phänomenbereich rechts liegen vorrangig im makro-soziologischen Bereich begründet, womit die gesamtgesellschaftliche Situation, Struktur und Entwicklung gemeint sind. Es erfolgt daher eine Analyse derjenigen gesellschaftlichen Elemente, welche für das Phänomen von besonderer Bedeutung erscheinen. Dieser Betrachtung liegt die Annahme zugrunde, dass eine monokausale Erklärung nicht geeignet ist, sondern, dass verschiedene Faktoren ursächlich sind und dass zwischen den zu betrachtenden, zentralen Begrifflichkeiten Interdependenzen bestehen. Diese Annahme stützt sich auf den Umstand, dass dem modernden und demokratisch verfassten Staat und hierdurch seiner Gesellschaft aufgrund zentraler Phänomene, die infolge ihres prägenden und tiefenwirksamen Charakters als Megatrends bezeichnet werden können (vgl. Wendekamm und Model 2019: 261), Komplexität und Transformation immanent ist. Hierzu zählen insbesondere die Globalisierung, soziale Desintegration, Entsolidarisierung, Migration und Digitalisierung.

Bereits Ende des 20. Jahrhunderts wurde eine postmoderne Gesellschaftsstruktur beschrieben, die sich durch einen „tiefgreifenden sozialen Strukturwandel in allen gesellschaftlichen Lebensbereichen“ (Preglau 1997: 283) auszeichnet. Aus ökonomischen Umbrüchen, der wirtschaftlichen Liberalisierung mit dem einhergehenden Wandel des Arbeitsmarktes sowie soziokulturellen Veränderungen und dem damit zusammenhängenden Pluralismus der durch vielfältige Lebensentwürfe und Handlungsmuster gekennzeichneten, individuellen Lebensformen folgte insbesondere eine gestiegene soziale Mobilität, mit welcher individuelle Freiheit und persönliche Verantwortung parallel einhergehen (vgl. ebd.: 283 ff.; Welsch 2008: 5; Singelnstein und Stolle 2012: 17 ff.). Die mit dieser Sozialstruktur einhergehenden Autonomie- und Risikospielräume bestehen nicht nur fort, sondern sind nicht zuletzt infolge der fortschreitenden Globalisierung weiter gewachsen, sodass das Individuum zur Erhaltung des Status quo in seine „Wettbewerbsfähigkeit und Ressourcenausstattung“ (Rosa 2016: 179) investieren muss und somit einem „Zwang zu Selbstmanagement“ (Heinze 2019: 21) unterliegt. Die geschilderten Aspekte, welche im Rahmen einer Sinus-Studie (vgl. Sinus 2018: 17) positiv als „erweiterte Entfaltungsspielräume und Wahlmöglichkeiten“ der Multi-

optionsgesellschaft beschrieben wurden, verursachen jedoch auch eine gesellschaftliche Konfliktsituation und ein Konkurrenzverhalten hinsichtlich des sozioökonomischen Status. Normen und Werte, welche für eine gesellschaftliche Integration elementar sind, verlieren hierdurch an Bedeutung, es kommt zu einer Entsolidarisierung der gesellschaftlichen Mitte (vgl. Nachtwey 2016: 167; Sinus 2018: 20[25]) und „letztendlich zu einer Verschiebung von ‚Solidaritäts-Grenzen' [...] einer Gesellschaft, weil diese angesichts erzwungener Selbstoptimierung nicht mehr plausibel erscheinen" (Musyal 2018: 37).

Diese Entwicklung, in deren Zentrum kollektive sozioökonomische Abstiegsängste stehen, ruft ein subjektiv empfundenes Bedrohungsgefühl hervor und fördert eine gesellschaftliche Verunsicherung (vgl. Heinze 2019: 11; Musyal 2018: 36 f.; Sinus 2018: 17). Diese Verunsicherung wird durch gesellschaftlich wahrgenommene prekäre Situationen und deren Wirkungen auf und in der Gesellschaft vergrößert. Hierzu zählen in besonderem Maße transnationale Entwicklungen, wie die ab 2007 spürbar gewordene Finanz- und Wirtschaftskrise, die sich daran anschließende griechische Staatsschuldenkrise, die Klimakrise sowie die 2015 beginnende und fortdauernd thematisierte europäische Flüchtlingskrise (vgl. Musyal 2018: 34; Eckert 2020: 243 ff.). Grundsätzlich bewirkt eine Krise, dass Routinen nicht mehr funktionieren und dass der Zustand vor dem Eintritt des Ereignisses nicht mehr hergestellt werden kann, was wiederum Kontrollverluste erzeugt (vgl. Heitmeyer: 2020). Es ist daher herauszustellen, dass bereits der Denomination von Ereignissen und Zuständen als Krisen eine nicht zu unterschätzende Wirkung zukommt.

An dieser Stelle bedarf der Aspekt der Migration mit den Elementen des Flüchtlingszustroms und der Asylpolitik einer dezidierten Betrachtung. Prima facie handelt es sich hierbei um eine kulturelle Konfliktsituation, da unterschiedliche Werte und Normenverständnisse aufeinandertreffen. Berücksichtigt man jedoch, dass der Zustrom „[f]ür die Masse der bereits heute unter existenzieller Unsicherheit, einer prekären sozialen Situation und ungewissen Aussichten leidenden Bevölkerung [...] hingegen noch mehr Konkurrenz und sinkende Aussichten auf eine Verbesserung der Zustände [signalisiert]" (Bauman 2016), wird deutlich, dass es sich auch hier de facto im Kern um

[25] Die Sinus-Studie spricht an dieser Stelle gar von einer „Erosion der gesellschaftlichen Mitte" (Sinus 2018: 20).

eine auf sozioökonomischer Verunsicherung basierende gesellschaftliche Auseinandersetzung handelt, die jedoch Ressentiments zur Folge haben. Dies verdeutlicht sich am Beispiel der Fallvignette Halle. Die Bundesanwaltschaft attestiert dem Täter eine von Enttäuschungen und Scheitern geprägte Existenz und sieht es als erwiesen an, dass er sich von Migranten zurückgedrängt gefühlt habe (vgl. Jaeger 2020).

Als Ergebnis dieser multifaktoriellen Verunsicherung bleiben dichotomes Denken und eine rechtspopulistische Meinungsbildung (vgl. Musyal 2018: 35) sowie antidemokratische und antiegalitäre Positionen (vgl. Küpper 2017: 30 ff.), deren Verbalisierung bestehende Institutionen delegitimiert und eine gesellschaftliche Verrohung und Enthemmung fördert (vgl. Séville 2019: 38). Hiervon betroffen sind nicht nur ökonomisch schlechter gestellte Schichten, sondern auch „Personengruppen in ökonomisch (noch) komfortablen Positionen, die sich aber politisch ohnmächtig und kulturell entfremdet oder [...] aufgrund der allgemeinen sozial- und wirtschaftspolitischen Konkurrenzsituation bedroht fühlen“ (Miliopoulos 2018: 228). Brevi manu, die Ursachen des Phänomens sind in konkreten Faktoren der gesellschaftlichen Situation, Struktur und Entwicklung begründet, sodass sich politisch motivierte Hasskriminalität als Reaktion von Einzelnen und Gesellschaftsteilen auf die Transformationsprozesse der modernen Gesellschaft darstellt.

Als Folge der Digitalisierung sind ein veränderter Medienkonsum sowie eine Wandlung des Kommunikationsverhaltens in der Gesellschaft zu verzeichnen. Das Klima der gesellschaftlichen Verunsicherung trifft im Internet, in welchem im Unterschied zu tradierten Medien Gatekeeper[26] kaum eine Rolle spielen (vgl. Rieger et al. 2020: 354 f.), auf die medial vermittelten und somit einem breiten Publikum zugänglich gemachten Inhalte rechtspopulistischer und teilweise rechtsextremer Akteure. Dies ist insbesondere deshalb problematisch, da „Menschen mit bereits vorhandenen extremen politischen Einstellungen häufiger in homogenen Echokammern zu finden sind und [sie] sich stärker von anderen Meinungen abwenden“ (Rieger 2019). Ferner kommt es zu einer Überschätzung der Zustimmung zu diesen Einstellungen und die empfundene Richtigkeit der Ansichten steigt (vgl. ebd.). Während ei-

[26] Der Begriff meint eine Entscheidungsfunktion, in welcher darüber befunden wird, welche Information veröffentlicht wird.

ne liberale Demokratie ein differenzierendes Weltbild ermöglicht und zum Ziel hat, bewirken die genannten Umstände eine Fokussierung auf ein ethnozentrisches Weltbild (vgl. Eckert 2020: 242 f.). In der weiteren Debatte werden die ökonomischen und politischen Ursachen der dargelegten gesellschaftlichen Verunsicherung und des empfundenen Kontrollverlusts nicht mehr artikuliert und stattdessen auf kulturalistische Argumentationen umgelenkt (vgl. Musyal 2018: 38; Spoo 2017).

Neben dem reinen Konsum von Informationen erlauben das Internet und insbesondere die sozialen Medien auch die Produktion und Distribution eigener und fremder Ansichten. Über die weite Verbreitung, den nahezu jederzeit möglichen Zugang und die einfache Bedienbarkeit hinaus, ist insbesondere der Aspekt der Distanz konstitutiv für die medial vermittelte Hasskriminalität im Internet (vgl. Meier 2015: 95 f.). Diese besteht im Rahmen einer potentiellen Tathandlung zunächst zwischen dem Täter und dem Rechtsgutträger, beziehungsweise dem betroffenen Rechtsgut (vgl. Kapitel 2.2.2) und nimmt vor allem Einfluss auf die Faktoren Täter und Sozialkontrolle. Meier (vgl. 2015: 97) führt hierzu aus, dass die Distanz auf der Täterseite im Unterschied zu analogen Taten zunächst eine absinkende Hemmschwelle und damit eine gestiegene Handlungsbereitschaft bewirkt, da die Abwertung des Opfers und die Neutralisierung des Unrechts erleichtert werden. Letzteres ist unter Bezugnahme auf die Theorie der Techniken der Neutralisierung jedoch nur erforderlich, wenn die Normen und Werte, die einer Tatbegehung entgegenstehen können, überhaupt internalisiert sind und der Normbruch zur Dissonanzreduktion einer inneren Rechtfertigung bedarf (vgl. Sykes und Matza 1957: 666 f.; Lüdemann und Ohlemacher 2002: 63). Weiterhin begünstigt die Distanz auf der Täterseite die Entstehung einer Illusion der Anonymität, welche eine Handlung ohne Konsequenzen sowie frei von rechtlicher, sozialer und moralischer Verantwortlichkeit möglich erscheinen lässt (vgl. Meier 2015: 97). Dass es sich hierbei nur um eine scheinbare Anonymität handelt, zeigen beispielhaft die Exekutivmaßnahmen[27] der Ermittlungsbehörden wegen Delikten der Hasskriminalität im Internet in Zusammenhang mit der Fall-

[27] Der Begriff meint offen gegen Beschuldigte durchgeführte Ermittlungsmaßnahmen. In Betracht kommen beispielhaft die Durchführung von Durchsuchungen und Vernehmungen sowie die Sicherstellung oder Beschlagnahme von Beweismitteln.

vignette Lübcke gegen Beschuldigte mit einer Anzahl im mittleren zweistelligen Bereich im Juni 2020 (vgl. Burger und Iskandar 2020). Es handelt sich somit eher um einen Glauben an die Anonymität, der entweder darauf zurückzuführen ist, dass der Täter sich nicht darüber bewusst ist, dass er digitale Spuren, die zu seiner Identifizierung geeignet sind, im Rahmen der Tatbegehung verursacht oder sich in der irrigen Annahme begründet, dass die Tat nicht verfolgt würde. Letztlich erschwert die Distanz auch die Kontrolle der Tathandlungen, da bei Tathandlungen im Internet sowohl die regulierende, auf den Täter Einfluss nehmende Sozialkontrolle durch soziale Kontrollinstanzen[28] geschwächt ist oder ganz entfällt und auch die Beweisführung in strafrechtlichen Verfahren insbesondere auf digitale Ermittlungen gestützt werden muss (vgl. Meier 2015: 98).[29]

Während sich die Ursachen politisch motivierter Hasskriminalität durch die Analyse der dargelegten gesellschaftlichen Elemente erklären lassen, sind die fortschreitende Digitalisierung und der damit einhergehende Wandel des Medienkonsums und der Mediennutzung in qualitativer und quantitativer Hinsicht ursächlich für die Verbreitung von politisch motivierter Hasskriminalität im Internet, wobei dem Faktor der Distanz hierbei eine dissoziative sowie kriminovalente Wirkung und daher herausgehobene Bedeutung zukommt. Die unterschiedlichen Kontexte der Fallvignetten Lübcke und Halle sind diesbezüglich herauszustellen.

Dr. Walter Lübcke, der getötete Regierungspräsident von Kassel, welcher aufgrund seines Amtes unter anderem eine Zuständigkeit für Fragen in Zusammenhang mit Migration und Asylpolitik in einem eher kommunalen Bereich hatte, argumentierte im Herbst 2015 in einer gesellschaftlich polarisierenden Rede im Rahmen einer öffentlichen Veranstaltung für eine Asylbewerberunterkunft in seinem Zuständigkeitsbereich und distanzierte sich hierbei von jeglicher Fremdenfeindlichkeit (vgl. Holscher und Schneider 2019). Er wurde aus diesem Grund für die rechtsextremistische Szene zum Feind-

[28] Bezugnehmend auf die Bindungstheorie von Hirschi, ist mit sozialen Kontrollinstanzen innerhalb der „Elements of the Bond“ (Hirschi 1969: 16 ff.) das „attachment to meaningful others“ (Neubacher 2020: 103) gemeint, wozu beispielsweise Eltern, Lebenspartner und Freunde gehören.

[29] Auf die Problemstellungen bei der Anwendung nationalen Straf- und Strafprozessrechts auf Hasskriminalität im Internet mit Auslandsbezügen (Kapitel 2.3) wird an dieser Stelle nochmals hingewiesen.

bild und zum Ziel von Hasskommentaren im Internet (vgl. Pfahl-Traughber 2020: 76). Nach dem Tötungsdelikt zu seinem Nachteil am 2. Juni 2019 wurde online eine Vielzahl von Beiträgen festgestellt, die unter Hasskriminalität im Internet zu subsumieren waren (vgl. Kapitel 2.1) und denen diesbezüglich eine strafrechtliche Relevanz (vgl. Kapitel 2.2.2) zukam, wobei eine breites Portfolio an Tatbeständen von Beleidigungen und Bedrohungen über Volksverhetzungen bis hin zum öffentlichen Aufruf zu Straftaten und des Verunglimpfens des Andenkens Verstorbener gegeben war (vgl. Apostel 2019: 287; Zeit online 2019; Burger und Iskandar 2020). In der Gesamtschau handelt es sich um Delikte, die keinesfalls nur von einem rechtsextremen, sondern vor dem Hintergrund der vorausgegangenen Ausführungen vielmehr von einem einen breiten Teil der Gesellschaft abbildenden Personenkreis begangen wurden, weshalb dem gesamtgesellschaftlichen Zusammenhang „des völkischen Diskurses von ‚Großem Austausch'[30], ‚Überfremdung'[31], ‚Volkstod'[32] und ‚Soros-Verschwörung'[33], der in Zeiten des gesellschaftlichen Rechtsrucks nicht mehr nur in der klassischen Neonazi-Szene gepflegt wird, sondern [...] sich über Webforen und Imageboards längst transnational organisiert" (Voigts 2019), eine herausragende Bedeutung zukommt.

Im Unterschied hierzu übertrug der Attentäter von Halle seine Tathandlung über eine mitgeführte Kamera live ins Internet, äußerte sich währenddessen zu seiner Gesinnung sowie zu korrelierenden Verschwörungstheorien und lebte hierbei den Gewaltfetischismus aus, in welchen er in einer virtuellen Gemeinschaft im Internet versunken war (vgl. Pfahl-Traughber 2020: 77). Während persönliche, analoge Kontakte oder Beziehungen zur rechtsextre-

[30] Der Begriff, welcher für aktuelle rechtspopulistische und -extreme Argumentationen benutzt wird, postuliert die Dystopie eines Bevölkerungsaustauschs durch Migration (vgl. Camus 2016: passim), „systematisch begünstigt und herbeigeführt durch ‚volksverräterische' Eliten" (Backes 2020: 10).

[31] Eine solche Entwicklung wurde insbesondere von der Partei „Alternative für Deutschland (AfD)" in Zusammenhang mit dem im Jahr 2015 einsetzenden Zustrom von Asylsuchenden beschrieben und politisch instrumentalisiert (vgl. Frankfurter Allgemeine Zeitung 2016).

[32] Auch hierbei handelt es sich um eine Argumentation der „AfD" im Rahmen der Instrumentalisierung der Asylpolitik (vgl. Tagesspiegel 2017).

[33] Mit dieser erneut von der „AfD" verwendeten These wird die Förderung der illegalen Einwanderung durch enorme Geldmittel des philanthropischen Investors George Soros vermutet (vgl. Dachsel 2018; Schindler 2020). Die Nennung von Soros erfolgt unter anderem, um antisemitische Ressentiments im Gewand einer modernen „Elitenkritik" zu bedienen.

men Szene fehlen, scheint seine Radikalisierung im Internet in einer virtuellen Gemeinschaft erfolgt zu sein, deren gemeinsame Gesinnung von rassistischen Stereotypen getragen wurde (vgl. ebd.: 78). Dem Feindbild unterfielen hierbei Personen jüdischen Glaubens (vgl. Hartleb 2020: 316). Die Spiralwirkung einer Echokammer, in welcher sich bereits extreme Tendenzen in einem homogenen Netzwerk weiter verfestigen (vgl. Rieger 2019), scheint sich in diesem Fall extrem zugespitzt zu haben und es wird davon ausgegangen, dass getragen von diesen medial vermittelten Überlegungen und Überzeugungen die analoge Tathandlung entstanden ist (vgl. Münch 2020: 5). Als ein wesentlicher Aspekt des Gerichtsverfahrens vor dem Oberlandesgericht (OLG) Naumburg[34] wurde versucht, die digitale Radikalisierung des Täters zu rekonstruieren, welche sich unter anderem durch die Verbalisierungen im Tatvideo, in welchem die Tötungsart und die Opferauswahl als „achievement“ bezeichnet wurden (vgl. Hartleb 2020: 316) sowie auch in Ansätzen in den öffentlichkeitswirksamen Bestrebungen des Täters und seiner Betonung der großen medialen Verbreitung und Wahrnehmung seiner Tat bestätigte (vgl. Albrecht und Fielitz 2019: 183; Quack 2020).

3.2 Quantitative Beschreibung des Phänomens

Nachdem die Betrachtung der bisherigen kriminologischen Implikationen insbesondere dazu führt, politisch motivierte Hasskriminalität im Internet als qualitatives Problem zu erfassen, erfolgt nunmehr eine quantitative Beschreibung.

Naheliegend erscheinen hierzu zunächst die Darstellung einer Analyse amtlicher Kriminalstatistiken[35] und vor allem eine Auswertung der Polizeilichen Kriminalstatistik (PKS), in welcher die der Polizei durch Anzeigen oder Ermittlungen bekannt gewordenen Straftaten abgebildet werden (vgl. Neubacher 2020: 37). Hierbei ist zu berücksichtigen, dass die Daten der PKS Einschränkungen und Verzerrungen unterliegen, die bei ihrer Interpretation zu berücksichtigen sind. Zunächst handelt es sich nur um die Daten des soge-

[34] Der Täter wurde am 21. Dezember 2020 wegen zweifachen Mordes, des versuchten Mordes in mehreren Fällen sowie wegen Volksverhetzung zu einer lebenslangen Freiheitsstrafe mit anschließender Sicherungsverwahrung verurteilt (vgl. Rietzschel 2020).

[35] Für einen allgemeinen Überblick zu den Arten amtlicher Kriminalstatistiken siehe Kunz und Singelnstein 2016: 203 ff.

nannten Hellfeldes, also jene, die amtlich erfasst wurden.[36] Ferner ist zu beachten, dass sich aus der PKS nicht die registrierte Kriminalität im Sinne des raumzeitlichen Geschehens krimineller Handlungen ablesen lässt, sondern das Registrierungsverhalten der Polizeibehörden, also „die amtliche Registrierung und Rekonstruktion des angenommenen Verdachts eines solchen Geschehens“ (Kunz und Singelnstein 2016: 206).

Für politisch motivierte Hasskriminalität im Internet ist weiterhin zu berücksichtigen, dass unter dieses Phänomen diverse Straftatbestände subsumiert werden können, die sich materiell-rechtlich schutzgutbezogen auf verschiedene Abschnitte des StGB verteilen (vgl. Kapitel 2.2.2). Dies bedeutet, dass beispielsweise aus der Gesamtzahl der registrierten Delikte zum Tatbestand der Beleidigung gemäß § 185 StGB weder ersichtlich ist, ob diese politisch motiviert ist, noch, ob sie über das Internet begangen wurde.

Wie bereits im zweiten Kapitel dargelegt, handelt es sich bei politisch motivierter Hasskriminalität im digitalen Raum um Äußerungsdelikte, bei welchen das Internet als Tatmittel eingesetzt wird. Delikte mit diesem Tatmittel werden mittels Sonderkenner erfasst und in der Tabelle 05 der PKS abgebildet (vgl. Bundeskriminalamt 2019: 13 f.). Allerdings wird aus dem Kanon der klassischen Staatsschutzdelikte (vgl. Fn. 1) nur die Volksverhetzung gemäß § 130 StGB in der PKS ausgewiesen (vgl. Bundeskriminalamt 2019a: 6). Zu diesem Tatbestand wurden für das Jahr 2018 in Summe 1.895 Fälle und für das Jahr 2019 insgesamt 1.317 Delikte registriert, wobei die Aufklärungsquote mit 73,3 Prozent in 2018 und 78,1 Prozent in 2019 sehr hoch ist (vgl. Bundeskriminalamt 2020a: Zeile 270). Für die sonstigen Delikte, die dazu geeignet sind, als politisch motivierte Kriminalität klassifiziert zu werden (vgl. Kapitel 1), kann am Beispiel der im Internet begangenen Beleidigung verdeutlicht werden, dass aus der Tabelle 05 nicht ersichtlich ist, ob den dort ausgewiesen Fällen eine politische Motivation zugrunde liegt. Die Daten dieser weiteren Delikte lassen sich der Falltabelle 05 folglich nicht entnehmen.

Valide Daten zum gegenständlichen Phänomenbereich können darüber hinaus aus dem ergänzend zur PKS herausgegebenen Lagebild „Politisch motivierte Kriminalität“ (vgl. Bundesministerium des Innern, für Bau und Heimat

[36] Zum Verhältnis von Hell- und Dunkelfeld siehe Neubacher 2020: 37 ff.

2020a: 7) entnommen werden. Hiernach wird das Phänomen seit dem 01.01.2019 unter dem neu geschaffenen Tatmittel „Hassposting“ erfasst und für das Jahr 2019 wurden 1.524 Fälle registriert. Bei einem Quervergleich zwischen den Phänomenbereichen (1.108 Fälle PMK-rechts, 169 Fälle PMK-nicht zuzuordnen, 21 Fälle PMK-religiöse Ideologie, 199 Fälle PMK-links und 27 Fälle PMK-ausländische Ideologie) fällt auf, dass der weit überwiegende Anteil der Straftaten mit 72,7 Prozent dem Phänomenbereich rechts zugeordnet wurde. Bei einem Längsvergleich ist festzustellen, dass die Erfassung für die Jahre 2017 und 2018 unter dem Oberthema Hassposting erfolgte und hierbei für 2017 insgesamt 2.270 Fälle und für 2018 insgesamt 1.472 Fälle, hiervon 1.130 Fälle PMK-rechts, erfasst wurden (vgl. Bundesministerium des Innern, für Bau und Heimat 2019: 6).

Diese Daten des Hellfeldes stehen schon in einem offensichtlichen Widerspruch zu behördlichen Verlautbarungen in Zusammenhang mit der Fallvignette Lübcke, bei welcher für das Jahr 2019 mit einer Zahl von Ermittlungsverfahren im vierstelligen Bereich gerechnet wurde (vgl. Zeit online 2019) und die nur einen Anlass für die Entstehung politisch motivierte Hasskriminalität im Internet darstellte. Die Gründe für diese geringe Fallzahl des Hellfeldes liegen darin, dass entsprechende Inhalte im Internet im Regelfall weder aktiv durch die Polizei wahrgenommen werden, noch von der Bevölkerung zur Anzeige gebracht werden[37], sofern sie von Privatpersonen überhaupt als strafrechtlich relevant bewertet werden (vgl. Kunz und Singelnstein 2016: 200 ff.).

Um die quantitative Bedeutung des Phänomens besser beurteilen zu können, erscheint daher eine Betrachtung von Erkenntnissen der Dunkelfeldforschung angezeigt. Auch wenn sich hiernach kein abschließendes oder vollständiges Bild ergibt, ist dies für die Beurteilung der Kriminalitätslage von immenser Bedeutung (vgl. Neubacher 2020: 47 ff.). Aufgrund des Deliktes kommen vorrangig Erkenntnisse aus Opferbefragungen in Betracht, bei welchen eine Bevölkerungsstichprobe oder -gruppe zu potentiellen Erfahrungen mit diesem Phänomenbereich befragt werden (vgl. Prätor 2014: 45; Neubacher 2020: 49).

[37] Für die Determinanten zur Anzeigebereitschaft und zum Anzeigeverhalten siehe Neubacher 2020: 41 ff.

Den nachfolgenden Erkenntnissen ist voranzustellen, dass den jeweiligen Forschungsprojekten verschiedene Forschungsfragen und -methoden sowie unterschiedliche Definitionen von Hasskriminalität zugrunde liegen, sodass über diese Daten nur eine grobe Einhegung des quantitativen Aufkommens möglich ist. Insbesondere die Frage, ob es sich bei den von den Befragten beschriebenen Erfahrungen um politisch motivierte Hasskriminalität im Sinne der Definition handelt, kann nicht exakt differenziert werden.

Das vom Bundesministerium der Justiz und für Verbraucherschutz geförderte und derzeit an der Universität Leipzig durchgeführte Forschungsprojekt „Der strafrechtliche Umgang mit Hate Speech im Internet“ beschäftigt sich aus kriminologischer, strafrechtlicher und strafprozessualer Perspektive mit diesem Phänomen (vgl. Höft 2020: 5). Im Rahmen einer repräsentativen Bevölkerungsumfrage mit mehr als 1.000 Teilnehmenden wurde festgestellt, dass 18 Prozent aller Befragten persönlich von entsprechenden Inhalten betroffen waren und dass sich die Tendenz abzeichnet, dass jüngere Befragte häufiger betroffen sind, da bei den 16-30-Jährigen der Anteil der Betroffenen bei 32 Prozent liegt (vgl. ebd.: 6). In früheren Erhebungen, bei deren Forschungshintergrund sich zumindest in Teilen die Zurechnungskriterien für politisch motivierte Kriminalität (vgl. Fn. 2) in der Stichprobe wiederfinden (vgl. Dieckmann, Geschke und Braune 2017: 23 f.), lag der Anteil der selbst erlebten Diskriminierungen im Internet mit 12,1 Prozent zwar niedriger, jedoch wurde zur strukturellen Diskriminierung im Internet, was die Beobachtung von entsprechenden Handlungen meint, ein Wert von 40,5 Prozent erhoben (vgl. ebd.: 25, 28). In einer dritten Umfrage „gibt die überwiegende Mehrheit der Befragten (78 %) an, schon einmal Hassrede bzw. Hasskommentare im Internet gesehen zu haben“ (Landesanstalt für Medien NRW 2018: 1).

Für die Wahrnehmung entsprechender Inhalte in Zusammenhang mit einer politischen Motivation wird an dieser Stelle abschließend auf die Erkenntnisse von Reineman et al. (vgl. 2019: 88) verwiesen, wonach über ein Drittel der befragten Jugendlichen auf Videoplattformen und etwa die Hälfte der Teilnehmenden in sozialen Netzwerken auf extremistische Inhalte abseits journalistischer Berichterstattung gestoßen sind.

Auch die Gründe für entsprechende Inhalte können mit Forschungserkenntnissen belegt werden. Eine „Untersuchung fragte danach, welche inhaltlichen Themen nach Einschätzung der Befragten am häufigsten Hate Speech nach sich ziehen. [...] Mit 63 Nennungen wird das Thema ‚Migration' von Befragten am häufigsten genannt, daran schließen sich ‚AfD' (40 Nennungen) und ‚Flüchtlinge' (34 Nennungen) an. Es folgen der Überbegriff ‚Politik' (28 Nennungen) und die beiden verwandten Themen ‚Klima' und ‚Klimawandel' (jeweils 17 Nennungen). Die Top 10 werden von den Themen ‚Berichterstattung', ‚Feminismus', ‚Islam' (jeweils 15 Nennungen) sowie ‚Integration' (12 Nennungen) komplettiert." (vgl. Papendick et al. 2020: 13). Der Großteil der genannten Aspekte ist für die dargelegten sozioökonomischen Abstiegsängste mitverantwortlich (vgl. Kapitel 3.1), weshalb diese Erkenntnisse einem empirischen Beleg der theoriegestützten Ausführungen darstellen.

Bereits dieser kurze Überblick ist trotz der mit ihm einhergehenden Einschränkungen bei der Interpretation der Daten für die Annahme geeignet, dass das Dunkelfeld der politisch motivierten Hasskriminalität im Internet das Hellfeld um ein Vielfaches übersteigen dürfte und dass entscheidende Faktoren dafür sorgen, dass ein Großteil der Delikte im Dunkelfeld verbleibt und mithin einer Verschiebung in das Hellfeld entgegenstehen[38]. Es ist daher zu konstatieren, dass das Phänomen auch als quantitatives Problem betrachtet werden und ihm entgegengewirkt werden muss.

3.3 Kriminologische Erklärungsansätze

In Anknüpfung an die Ausführungen der vorstehenden Kapitel werden nachfolgend ausgewählte kriminologische Erklärungsansätze betrachtet und dahingehend analysiert, inwiefern sie für das Phänomen der politisch motivierten Hasskriminalität im Internet nutzbar gemacht werden können. Schon aufgrund der Vielzahl der existierenden Kriminalitätstheorien[39] wird deutlich, dass einzelne Theorien nicht dazu geeignet sind, einen ubiquitären Erklä-

[38] Zu diesen Faktoren zählen insbesondere die Wahrnehmung eines Sachverhaltes als potentielle Straftat, die individuelle Anzeigebereitschaft, welcher ein mitunter komplexer Abwägungsprozess zugrunde liegen kann sowie die sich anschließende behördliche Bearbeitung (vgl. Kunz und Singelnstein 2016: 207; Neubacher 2020: 41 ff.).

[39] Eine Übersicht über die Vielfalt kriminologischer Kriminalitätstheorien, deren Ansätze und Erklärungsmodelle ist unter https://soztheo.de/kriminalitaetstheorien abrufbar (zuletzt am 01.01.2021 überprüft).

rungsansatz für alle Kriminalitätsformen zu liefern. Diese sind, wie auch die Gesellschaft und das soziale Leben, aus denen Kriminalität hervorgeht, zu vielfältig und haben teilweise eine breit angelegte und sich damit negativ auf den Erkenntnisgehalt auswirkende Reichweite (vgl. Neubacher 2020: 89). Während dies auf analoge und digitale Straftaten in gleichem Maße zutrifft, ist für letztere zudem zu beachten, dass sie, obwohl es sich mittlerweile um tägliche Erscheinungen handelt, im Vergleich zu analogen Delikten vergleichsweise neu und damit jung sind, weshalb entsprechende cyberkriminologische Theorien noch am Anfang stehen (vgl. Plank 2020: 60).

Eine allgemein auf Cyberkriminalität anzuwendende Theorie ist das Broken-Web-Phänomen (vgl. Rüdiger 2017: passim), welche wiederum auf zwei herkömmliche Kriminalitätstheorien Bezug nimmt. Hierbei handelt es sich einerseits um die Broken-Windows-Theorie, welche im Kern besagt, dass öffentlich sichtbare Schäden schnellstmöglich repariert werden müssen, da die Bevölkerung hierdurch andernfalls zu weiteren Schädigungen animiert wird und die Kriminalitätsrate steigt. Mit der Begründung „vandalism can occur anywhere once communal barriers - the sense of mutual regard and the obligations of civility - are lowered by actions that seem to signal that ‚no one cares'" (Kelling und Wilson 1982), wird hierbei argumentiert, dass eine fehlende Normenkontrolle schwache oder fehlende Schutzmechanismen symbolisiert, sodass gleichgelagerte Kriminalität herausgefordert wird.[40] Andererseits wird der Routine Activity Approach herangezogen, nach welchem das örtliche und zeitliche Zusammentreffen der drei Faktoren eines motivierten Täters, eines lohnenden Ziels und der Abwesenheit geeigneter Schutzmechanismen für die Entwicklung von Kriminalitätsraten von Bedeutung ist (vgl. Cohen und Felson 1979: 604). Hiernach ist über die bloße Existenz einer Rechtsordnung ein gewisses, je nach Deliktsart variierendes Maß an Rechtsdurchsetzung erforderlich, da Normbrüche ohne erkennbare Intervention und Sanktionierung Zweifel am Rechtssystem aufkommen lassen (vgl.

[40] Die Broken-Windows-Theorie ist umstritten. Ihr wird beispielhaft entgegengehalten, dass nicht nur beobachtete Unordnung zu weiterem Vandalismus und schwereren Straftaten führen kann, sodass hierbei kein zwingender Kausalzusammenhang bestehe, sondern dass dies auch auf eine geschwächte Sozialkontrolle sowie mangelnden sozialen Zusammenhalt zurückgeführt werden kann (vgl. Sampson und Raudenbush 1999: 626). Auch die aus diesem Ansatz abgeleiteten polizeitaktischen Maßnahmen, wie beispielsweise der Zero Tolerance Ansatz, stellen einen Anlass für Kritik dar (vgl. Rüdiger 2018: 268 m. w. N.).

Rüdiger 2017: 50 f.). Die Entdeckungs- und Verfolgungswahrscheinlichkeit einer Straftat stellen dabei wesentliche Elemente der Rechtsdurchsetzung dar.

Infolge der Ansätze der Broken-Windows-Theorie und des Routine Activity Approach, verursachen sichtbar im Internet begangene Straftaten einerseits einen Anlass zur Nachahmung und damit für weitere Kriminalität und erwecken andererseits den Anschein, dass im digitalen Raum etwaige Schutzmechanismen nicht funktionieren oder nicht existent sind, sodass scheinbar keine effektive Strafverfolgungswahrscheinlichkeit gegeben ist (vgl. ebd.: 52; Rüdiger 2018: 268 ff.). Dieser Faktor wird auch anhand der hohen Aufklärungsquote deutlich (vgl. Kapitel 3.2), welche darauf schließen lässt, dass Täter nur selten oder geringe Maßnahmen ergreifen, um die Ermittlung ihrer Identität zu erschweren. Zwischen diesen Elementen bestehen Interdependenzen, sodass durch Folgedelikte ein Broken Web Circle in Gang gesetzt werden und sich „im Netz das Gefühl einer Unrechtskultur als erlebte Normalität für den digitalen Raum etablieren [kann]“ (Rüdiger 2019: 38).

Gerade die Delikte der politisch motivierten Hasskriminalität, deren Visualität regelmäßig durch Postings, Kommentare oder Tweets gegeben ist, stellen hierbei eine große Herausforderung dar (vgl. ebd.: 38). Diese Argumentationslinien sind dazu geeignet, sowohl die vermehrten Tatbegehungen durch einen breiten gesellschaftlichen Personenkreis (vgl. Kapitel 3.1), als auch die empirisch belegte, quantitativ große Rezeption politisch motivierter Hasskriminalität in der Gesellschaft (vgl. Kapitel 3.2), zu erklären.

Auch eine bislang weniger berücksichtigte Kriminalitätstheorie, die Space Transition Theory (vgl. Jaishankar 2008: passim), welche jedoch speziell für Delikte der Cyberkriminalität entwickelt wurde, kann für das gegenständliche Phänomen herangezogen werden. Die Theorie enthält sieben Aussagen zu Cyberkriminalität (vgl. Jaishankar 2007: 7), von denen die folgenden vier Thesen für die hiesige Argumentation von Bedeutung erscheinen: Erstens sollen Personen, die aufgrund ihres Status kriminelles Verhalten in der analogen Welt unterdrücken, dazu neigen, kriminelle Handlungen im Cyberspace zu begehen. Dies könnte auf die von einem breiten gesellschaftlichen Personenkreis begangene politisch motivierte Hasskriminalität zutreffen, de-

ren Motivation in den dargelegten Ursachen zu finden ist. Zweitens sollen sich flexible digitale Identitäten sowie eine dissoziative Anonymität und das Fehlen von Abschreckungsfaktoren kriminovalent auswirken. Hierbei ist darauf hinzuweisen, dass es sich nur um eine Illusion der Anonymität handelt (vgl. Kapitel 3.1), jedoch sind der Aspekt einer subjektiv empfundenen Anonymität und unter Bezugnahme auf die Broken Web Theorie das Element fehlender Abschreckungsfaktoren anschlussfähig. Drittens wird ein Import von digitaler Kriminalität in die analoge Welt sowie vice versa für wahrscheinlich gehalten. Diesbezüglich wird sowohl auf die von einem breiten gesellschaftlichen Personenkreis begangenen Delikte politisch motivierter Hasskriminalität im Internet, deren Ursachen in der analogen Welt begründet sind, als auch auf das Radikalisierungspotential in homogenen Echokammern und damit verbunden, anhand der Fallvignette Halle, auf die Gefahr analoger Handlungen (vgl. Kapitel 3.1), verwiesen. Viertens soll der Widerspruch von Normen und Werten der analogen Welt mit denen der digitalen Welt zu Cyberkriminalität führen. Hierzu wird auf die Möglichkeit einer erlebbaren Normalität von politisch motivierter Hasskriminalität im Internet sowie die Herausforderung von gleichgelagerter Kriminalität verwiesen.

Als Ergebnis der Ausführungen zu kriminologischen Kriminalitätstheorien wird festgehalten, dass unterschiedliche Aspekte der verschiedenen Ansätze durchaus für die Erklärung des Phänomens herangezogen werden können, obwohl die Theorien den Anspruch haben, Cyberkriminalität per se zu erklären und dadurch allgemeingültige Erklärungsansätze versuchen abzubilden. Daher ist über die Notwendigkeit einer Ausdifferenzierung hinaus festzuhalten, dass die Validität verschiedener Elemente einer empirischen Überprüfung bedarf.

3.4 Auswirkungen politisch motivierter Hasskriminalität im Internet

An die Vorüberlegungen anknüpfend wird nachfolgend den Auswirkungen des Phänomens nachgegangen, wobei zwischen der individuellen Wirkung auf Personen und der auf die Gesellschaft differenziert wird.

In Bezug auf die Opfer dieser Delikte erfolgt eine Beschränkung auf die primäre Viktimisierung, also die unmittelbaren Konsequenzen dieser Delikte, zu welchen auch immaterielle Folgen, wie seelische Schädigungen, gezählt

werden (vgl. Neubacher 2020: 134 ff.). Diesbezüglich kann auf eine Viktimisierungsstudie Bezug genommen werden, welche die Auswirkungen von antisemitischem und homophobem hate speech untersuchte und zu dem Ergebnis kam, dass eine entsprechende Viktimisierung psychische Auswirkungen haben kann und „the overall short- and long-term effects suggest that the consequences of hate speech might be similar in form (but sometimes not in intensity) to the effects experienced by recipients of other kinds of traumatic experiences“ (Leets 2002: 354).

Neben diesen mitunter schwerwiegenden psychischen Auswirkungen verursacht das Phänomen bei der zukünftigen Mediennutzung Einschränkungen in Bezug auf die persönliche Entfaltung. Unter nochmaliger Bezugnahme auf das Forschungsprojekt „Der strafrechtliche Umgang mit Hate Speech im Internet“ der Universität Leipzig kann festgehalten werden, dass 42 Prozent der dort Befragten angaben, dass sie aufgrund erlebter Hasskriminalität im Internet eigene Beiträge vorsichtiger formulieren, um das Risiko eines Angriffs auf sich selbst zu minimieren oder ganz auf eigene Beiträge verzichten (vgl. Höft 2020: 7). Während dies auf 68 Prozent der bereits in der Vergangenheit von Hasskriminalität persönlich betroffenen Personen zutrifft, gilt dies auch für 37 Prozent der bislang nicht persönlich Betroffenen (vgl. ebd.: 21). Dies bedeutet, dass bereits der bloßen Wahrnehmung entsprechender Inhalte enorme Einschüchterungseffekte inhärent sind, was zu einer Abnahme der Meinungsvielfalt im digitalen Raum und damit des Pluralismus führt. Dies stellt einen fundamentalen Einschnitt in die zivilisatorische Errungenschaft der grundrechtlich garantierten Meinungsfreiheit und dadurch eine in einem liberalen Rechtsstaat nicht hinnehmbare Entwicklung dar.

Politisch motivierte Hasskriminalität entfaltet jedoch auch eine gesamtgesellschaftliche Wirkung, indem sie zur Polarisierung von Personen und Gesellschaftsteilen führt. Die mit den rechtspopulistischen oder -extremistischen Inhalten einhergehenden „Ideologien tendieren dazu, Konfliktlinien zu verallgemeinern und zu verstetigen. Die Erwartungen oder Befürchtungen von Gegnerinnen und Gegnern orientieren sich an zunehmend allgemeineren Kategorien, denen dann immer mehr Menschen als ‚Freund oder Feind’ zugerechnet werden, bis diese Unterscheidung selbst zum Inbegriff von Politik überhaupt wird“ (Eckert 2020: 241). Der Polarisierungseffekt wird im Internet

verstärkt, da insbesondere bei sozialen Netzwerken und Videoplattformen Empfehlungsalgorithmen[41] dafür sorgen, dass vermehrt gleiche oder ähnliche Inhalte vorgeschlagen oder angezeigt werden (vgl. Rieger et al. 2020: 357 f.). Neben weiteren Problemstellungen entsteht hierbei durch Selektion insbesondere das Risiko der Wirklichkeitsverzerrung durch Filterblasen und Echokammern (vgl. Saurwein, Just und Latzer 2017: 4). Dies bedeutet, dass auf diesen Algorithmen basierende Empfehlungen oder auch die Zahl, der auf solche Inhalte erfolgte Reaktionen, nicht unmittelbar als Abbildung realer Meinungen verstanden werden dürfen, da beispielsweise eine Analyse belegt, dass „fünf Prozent aller Accounts, die bei Facebook mit hasserfüllten Inhalten interagieren, für die Hälfte aller Likes verantwortlich sind“ (Rieger et al. 2020: 358).

Die angezeigte Freund-Feind-Dichotomie wirkt sich negativ auf die Ambiguitätstoleranz in der Gesellschaft aus, indem sie die Intoleranz gegenüber einer pluralistischen Gesellschaftsstruktur, der Meinungsvielfalt und dem Recht auf Meinungsäußerung fördert. Da der liberale Rechtsstaat wiederum zum Schutz dieser demokratischen Normen und Werte verpflichtet ist, erleidet dieser selbst einen Reputationsverlust.[42] Die damit einhergehenden grundlegenden Irritationen in das bestehende System und seine Institutionen (vgl. Heinze 2019: 23) führt zu einer höheren Zustimmung zu autoritären Regierungsformen (Musyal 2018: 39) und kann eine politische Radikalisierung zur Folge haben (vgl. Eckert 2020: 215). Hierbei steht als herausragender Einzelfall die Fallvignette Halle in Form einer konkreten Handlung eines laut Plädoyer der Bundesanwaltschaft aus juristischer Sicht fanatisch, ideologisch-motivierten Einzeltäters (vgl. Jaeger 2020) pars pro toto für die Gefahren, die sich aus zunächst populistischen, dann polarisierenden und später radikalisierten Diskursen ergeben können.

Indem sie auf elementare Prinzipien negative Effekte hat, stellt politisch motivierte Hasskriminalität im Internet bei der Kumulation der individuellen und

[41] Der Prozess der algorithmischen Selektion weist Elementen auf Basis externer Informationen durch eine automatisierte statistische Bewertung eine Relevanz zu. Die Selektion ist hierbei eine Priorisierung von Elementen aus der gesamten Datenmenge, welche nach der Priorisierung die Strukturierung, Ordnung und Sortierung zur Folge hat (vgl. Saurwein, Just und Latzer 2017: 1).

[42] Ein solcher wird durch die Dokumentation „Erosion des Vertrauens“ des Instituts für Demoskopie Allensbach (vgl. 2019: passim) empirisch belegt.

der gesamtgesellschaftlichen Auswirkungen eine Ursache für die Gefährdung der Demokratie dar.

3.5 Zwischenfazit

Bevor der Präventabilität des Phänomens und einer Antwort auf die forschungsleitenden Fragen zu den kriminologischen Implikationen nachgegangen wird, werden zwei Kernelemente der bisherigen Ausführungen bilanziert.

Bei dem ersten Aspekt handelt es sich um den der politisch motivierten Hasskriminalität im Internet zugrunde zu legenden Kriminalitätsbegriff. Schon die Mehrzahl der existierenden Definitionen, als auch die für diese Arbeit gewählte phänomenologische Beschreibung stellen auf die Sozialschädlichkeit entsprechender Äußerungen ab (vgl. Kapitel 2.1). Es ist zudem deutlich geworden, dass die Digitalisierung vor allem durch die Begriffe Komplexität und Geschwindigkeit gekennzeichnet ist, sodass vor dem Hintergrund zukünftiger technischer Entwicklungen und damit verbundener neuer Handlungsmöglichkeiten sowie nicht zuletzt auch aufgrund einer sich weiterentwickelnden Rechtsprechung und gesetzlichen Aktivitäten de lege ferenda, die sich negativ auf das gesellschaftliche Zusammenleben auswirkende Verhaltensweisen am geeignetsten erscheinen, um das vielschichtige Phänomen zu erfassen. Dies trifft im besonderen Maße zudem auf den Umstand der territorialen Schrankenlosigkeit des Internets und damit auf die Frage der Anwendbarkeit nationalen Strafrechts im digitalen Raum zu (vgl. Kapitel 2.3). Letztlich kann zudem festgehalten werden, dass bereits die von Verrohung und Enthemmung gekennzeichneten medialen Diskurse zu den dargelegten Auswirkungen beitragen, sodass die politisch motivierte Hasskriminalität im Internet auf Basis des soziologischen Verbrechensbegriffs zu betrachten ist.

Das zweite Element ist ein die kriminologischen Implikationen integrierender Erklärungsansatz politisch motivierender Hasskriminalität im Internet. Gleichwohl eine solche Theorie einer empirischen Validierung bedarf, kann sie entlang der literaturtheoretisch-analytischen Betrachtungen skizziert werden. Unter Bezugnahme auf die bisherigen Ausführungen, liegen die Gründe für die Entstehung und das hohe Aufkommen des Phänomens in einem in der gesamtgesellschaftlichen Situation, Struktur und Entwicklung begründeten, multifaktoriellen Ursachenbündel.

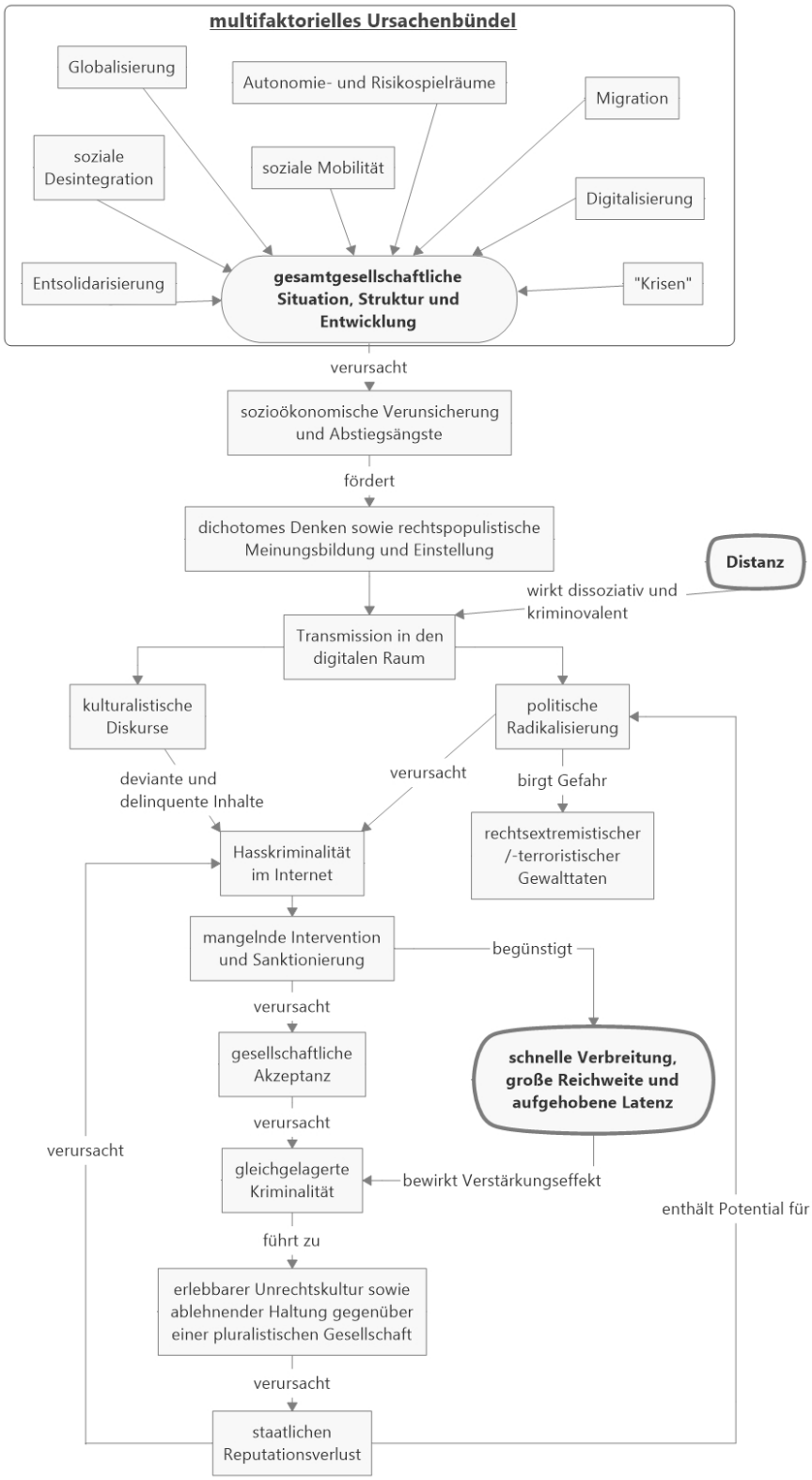

Abbildung 2: Erklärungsansatz „politisch motivierte Hasskriminalität im Internet“

Dieses verursacht sozioökonomische Verunsicherungen und Abstiegsängste, welche wiederrum eine rechtspopulistische Meinungsbildung und Einstellung bei einem breiten gesellschaftlichen Personenkreis sowie in geringer

Zahl rechtsextremistische Gesinnungen bewirken. Es findet eine Transmission in das Internet statt, wobei dem Aspekt der Distanz eine dissoziative und kriminovalente Wirkung zukommt, sodass vor dem Hintergrund ethnozentrischer Weltbilder unter beispielhaftem Verweis auf die Fallvignette Lübcke kulturalistische Diskurse geführt werden, denen einerseits eine Sozialschädlichkeit inhärent ist und bei welchen andererseits die Grenzen zwischen deviantem und delinquentem Verhalten schwinden oder ganz aufgehoben werden. In homogenen Echokammern besteht zudem die Gefahr der politischen Radikalisierung und die Fallvignette Halle zeigt, dass es in virtuellen Gemeinschaften zur Aufhebung des Unterschieds zwischen digitaler und analoger Gewalt kommen kann (vgl. Albrecht und Fielitz 2019: 185). Die mangelnde Intervention und Durchsetzung rechtsstaatlicher Normen fördert unter Bezugnahme auf die dargelegten Aspekte des Broken-Web-Phänomens und der Space Transition Theory die gesellschaftliche Akzeptanz politisch motivierter Hasskriminalität sowie die Nachahmung gleichgelagerter Kriminalität und führt sowohl zu einer erlebbaren Unrechtskultur mit Einschüchterungseffekten im digitalen Raum, als auch zu einer ablehnenden Haltung gegenüber einer pluralistischen Gesellschaft. Hierdurch werden ganze Bevölkerungsgruppen geschädigt (vgl. Ceffinato 2020: 546), es kommt zur Polarisierung zwischen Bevölkerungsgruppen und der Staat sowie seine Institutionen erleiden in letzter Konsequenz einen Reputationsverlust (vgl. Valerius 2020: 673 m. w. N.). Diese Umstände fordern zum Einen weitere Kriminalität heraus und zum Anderen liegt in ihnen erneut das Potential für eine politische Radikalisierung. Das der Fallvignette Lübcke zugrundeliegende vollendete Tötungsdelikt verdeutlicht hierbei, dass politische Entscheidungsträger, denen aus rechtsextremistischen Kreisen die Verantwortung für die gesamtgesellschaftliche Entwicklung zugeschrieben wird, zum Feindbild werden (vgl. Backes 2020: 10 f.). Darüber hinaus besteht im virtuellen Raum einen Verstärkungseffekt. Für die analoge Kriminalität kann zwischen den kognitiven und den tatsächlichen Geltungsstrukturen eine Differenz angenommen werden (vgl. Popitz 1968: 15) und eine totale Verhaltenstransparenz im Sinne der Entdeckung aller Normbrüche erscheint nicht möglich (vgl. ebd.: 18). Während hierbei der im Dunkelfeld verbleibenden Kriminalität eine normstabilisierende Wirkung zukommt, führen die schnelle Verbreitung, die große

Reichweite und insbesondere die aufgehobene Latenz politisch motivierter Hasskriminalität im digitalen Raum in Verbindung mit einer mangelnden Intervention und Sanktionierung zur Akzeleration der beschriebenen Effekte in einem Kreislauf.

Auf dieser Basis können Aussagen zur Präventabilität des Phänomens getroffen werden, wobei analoge Maßnahmen, zum Beispiel das Einwirken auf die Ursachen auf sozialpolitischem Wege, nicht betrachtet werden, sondern eine Fokussierung auf digitale Interventionsmöglichkeiten erfolgt. Unter Bezugnahme auf die Ausführungen zum Routine Activity Approach und Broken-Web-Phänomen bestehen insbesondere im Hinblick auf potentielle Täter und die Schutzmechanismen präventive Ansatzpunkte. In Bezug auf potentielle Täter ist die Gültigkeit von Normen im digitalen Raum zu vermitteln, um die Hemmschwelle hinsichtlich krimineller Handlungen im Internet zu erhöhen (vgl. Rüdiger 2017: 52; Rüdiger 2019: 38). Es handelt sich hierbei um eine wesentliche Säule von Medienkompetenz. Hinsichtlich der Schutzmechanismen besteht zur Steigerung der Verfolgungswahrscheinlichkeit die Möglichkeit einer Verstärkung der Normenkontrolle im Internet (vgl. Rüdiger 2017: 52; Rüdiger 2019: 39). Eine solche Intervention, welche auch die Interdependenz zur Hemmschwelle und somit zum Element des Täters verdeutlicht, kann sowohl durch die Verbesserung der Sichtbarkeit des Rechtsstaats (vgl. Rüdiger 2018: 283 f.; Rüdiger 2019: 39), als auch durch die Inanspruchnahme von Plattformbetreibern[43] (vgl. Rüdiger 2018: 281 ff.), erreicht werden. Für den ersten Aspekt skizzieren Bayerl und Rüdiger (2017: 921) die Möglichkeit eines „Digital Community Policing“. Für den zweiten Aspekt wird in der Literatur auf Ansätze der städtebaulichen Kriminalprävention Bezug genommen. Hiernach ist ein gegen Normbrüche wehrhafter Raum „a surrogate term for the range of mechanisms - real and symbolic barriers, strongly defined areas of influence, and improved opportunities for surveillance - that combine to bring an environment under the control of its residents“ (Newman 1973: 3). Bei diesem sozio-physischen Ansatz sind die Elemente der Territorialität und natürlichen Überwachung sowie des Images und Milieus von Bedeutung (vgl. ebd.: 50). Übertragen auf das Internet können territoriale Hal-

[43] Diesbezüglich wird als Vorgriff auch auf das fünfte Kapitel und die dortigen Ausführungen zum Netzwerkdurchsetzungsgesetz verwiesen.

tungen und Vorrechte von sich normenkonform verhaltenden Personen und die natürliche Überwachung im Sinne einer Kontrollierbarkeit bereits durch die digitale Konstruktion verbessert werden (vgl. Ehlert und Rüdiger 2020: 165, 167). Exemplifizierend wird eine Klarnamenpflicht in sozialen Netzwerken angeführt.[44] Auch die aktive Positionierung und Gegenmaßnahmen können Normbrüchen entgegenwirken. Aufgezeigt wird beispielhaft die Möglichkeit der Gegenrede[45], um dem Normbruch durch eine Reaktion die Normalität zu nehmen und auf die Hemmschwelle des Täters einzuwirken, um hierdurch ein positives Milieu und gutes Image der Plattform zu schaffen (vgl. ebd.: 163 f.). Insbesondere der Sichtbarkeit etwaiger Reaktionen, zum Beispiel durch einen expliziten Hinweis auf entfernte Inhalte wegen Normverstößen, kommt eine hohe Bedeutung zu, da diese sowohl auf die Täter, Opfer und den gesamten Nutzerkreis wirkt sowie die Existenz und Funktionsfähigkeit von Schutzmechanismen verdeutlicht (vgl. ebd.: 166).

Als Fazit der kriminologischen Implikationen ist festzuhalten, dass der Erkenntnisstand zur politisch motivierten Hasskriminalität im Internet weder in phänomenologischer, noch in ätiologischer Hinsicht als ausreichend erachtet werden kann. In Bezug auf die Phänomenologie besteht zur Beschreibung der tatsächlichen Kriminalitätslage der Bedarf an einer verbindlichen Definition und in Ergänzung der PKS sowie über die benannten amtlichen Lagebilder hinaus, an einer empirischen Aufhellung des Dunkelfeldes durch eine profunde Sicherheitsberichterstattung unter Einbezug von Viktimisierungssurveys (vgl. Plank 2020: 57).[46] Hieraus könnten nicht zuletzt Rückschlüsse darauf gezogen werden, ob das Phänomen im Spannungsverhältnis von

[44] Nach § 13 Abs. 6 S. 1 TMG sind die Dienstanbieter von Telemedien in Abhängigkeit der technischen Möglichkeit und Zumutbarkeit grundsätzlich verpflichtet, die Nutzung anonym oder unter einem Pseudonym zu ermöglichen. In Abweichung hierzu entschied das OLG München (vgl. Urteile vom 8. Dezember 2020, Az. 18 U 2822/19 Pre sowie 18 U 5493/19 Pre), dass aufgrund des inzwischen weitverbreiteten sozialschädlichen Verhaltens im Internet ein legitimes Interesse an der präventiven Einwirkung auf die Nutzer zu bejahen und eine Klarnamenpflicht grundsätzlich geeignet sei, rechtswidriges Verhalten im virtuellen Raum einzudämmen, wohingegen die Nutzung eines Pseudonyms die Hemmschwelle senke. Hierbei wurden das supranationale Recht der Datenschutzgrundverordnung und ihre Entstehungsgeschichte, aus welcher sich gerade kein Recht auf eine pseudonyme Nutzung ergibt, für eine europarechtskonforme Auslegung des TMG herangezogen und hierüber wurde eine Begründung für die Dienstanbieter ermöglicht, dass die Nutzung unter einem Pseudonym im Sinne des § 13 Abs. 6 S. 1 TMG unzumutbar sei.

[45] Vertiefend hierzu siehe Fn. 61.

[46] Diese Forderung wurde in Bezug auf Hasskriminalität bereits im Bericht der Agentur der Europäischen Union für Grundrechte (vgl. 2012: 10 f.) formuliert.

Meinungsfreiheit und betroffenen Rechtsgütern strafrechtlich hinreichend erfasst ist. Die Dunkelfeldstudie „Sicherheit und Kriminalität in Deutschland 2020“ des Bundeskriminalamts und der Polizeien der Länder erscheint grundsätzlich als geeigneter Ansatz, wobei die politisch motivierte Hasskriminalität im Internet kein expliziter Gegenstand der Befragung ist, aber Fragestellungen zum subjektiven Sicherheitsgefühl beinhaltet sind und hierbei zumindest auch die Thematik der vorurteilsgeleiteten Kriminalität in der affektiven Dimension behandelt wird (vgl. Bundeskriminalamt 2020b). Während die in der analogen Welt begründeten, sozioökonomischen Ursachen nachvollziehbar erscheinen, ergibt sich bereits hinsichtlich der Transmission in das Internet und den dortigen Einflussfaktoren die Notwendigkeit einer empirischen Validierung. Gleiches gilt für die tatsächliche Vulnerabilität des virtuellen Raumes und der dort agierenden Personen sowie für die Auswirkungen dieser Kriminalitätsform und die zumindest aufgrund der beschriebenen Indizien zu vermutenden Wechselwirkungen zwischen dem analogen und digitalen Raum. Das Forschungsprojekt „Der strafrechtliche Umgang mit Hate Speech im Internet“ der Universität Leipzig stellt hierbei einen vielversprechenden Ansatz dar. Auf Grundlage entsprechender Erkenntnisse besteht die Möglichkeit, eine belastbare Kriminalitätstheorie zu entwickeln und dazu korrespondierende Präventionsmaßnahmen umzusetzen. Nach der eingehenden empirischen Untersuchung des Phänomens bedarf der dargelegte ätiologische Erklärungsansatz sicherlich einer Modifikation, insbesondere in Bezug auf die Interdependenz zwischen dem analogen und digitalen Raum, beziehungsweise hinsichtlich der Fusion dieser beiden Welten. Der Ansatz ist lediglich als theoretischer Ausgangspunkt dazu geeignet, bestehende Fragmentierungen in der Erkenntnislage zu beheben. Erst auf Basis eines durch kriminologische Forschung verbesserten Erkenntnisstandes und systematisierten Gegenstandsbereichs können legislative und organisationale Maßnahmen ergriffen werden, um dem Phänomen evidenzbasiert zu begegnen (vgl. Plank 2020: 64 f.). Vor dem Hintergrund der bisherigen empirischen Erkenntnisse zur politisch motivierten Hasskriminalität im Internet und ihres demokratiegefährdenden Potentials ist dies rechtsstaatlich dringend geboten.

4. Kriminalistische Implikationen

> *„In IT-Systemen zu ermitteln ist häufig alternativlos, da im Netzwerk der international verbundenen Informations- und Telekommunikationstechnik ein wachsender Teil menschlichen Verhaltens rein virtuell stattfindet. Viele menschliche Handlungen bleiben allein auf elektronischem Wege nachweisbar.“* (Heinson 2015: 1)

Wie in der Einleitung beschrieben, beschäftigt sich die Kriminalistik mit den Mitteln, Methoden und Verfahren zur Aufdeckung, Untersuchung, Aufklärung und Verhütung von Straftaten und kriminalistisch relevanten Sachverhalten. In Bezug auf den Gegenstandsbereich, das Erkenntnisinteresse und die Methoden unterscheidet sie sich elementar von der Kriminologie. Der Gegenstand der Kriminalistik „sind die Gesetzmäßigkeiten und Erscheinungen des Entstehens von Informationen (Spuren/Beweisen) bei der Straftatenbegehung sowie die Methoden ihres Auffindens, Sicherns und Bewertens für Ermittlungs- und Beweiszwecke. Ihre Aufgabe ist, Ereignisse mit strafrechtlicher und kriminalistischer Relevanz aufzudecken, deren Ablauf zu untersuchen, den Täter zu ermitteln und mit hinreichender Sicherheit zu überführen (Repression). Sie entwickelt aus Erkenntnissen zur Straftatenuntersuchung Verfahren zu Verhütung künftiger Straftaten (Prävention) und gibt kriminalstrategische Empfehlungen zur Kriminalitätskontrolle und Bekämpfung von Straftaten“ (Ackermann 2019: 18). Ein wesentliches Unterscheidungsmerkmal ergibt sich daraus, dass der Kriminalistik der formelle, beziehungsweise legalistische Verbrechensbegriff zu Grunde liegt, sodass alle von strafrechtlichen Normen pönalisierten Verhaltensweisen von Bedeutung sind und eine Abhängigkeit zu den in einer Gesellschaft geltenden Strafgesetzten (lex lata) besteht (vgl. Kunz und Singelnstein 2016: 10).

Die Kriminalistik kann in drei Subkategorien unterteilt werden. Hierbei handelt es sich erstens um die Kriminaltechnik als Lehre der naturwissenschaftlichen und technischen Möglichkeiten der Beweisführung (vgl. Ackermann et al. 2000a: 733). Als zweites ist die Kriminaltaktik als Lehre von den auf den Einzelfall ausgerichteten Maßnahmen und Ermittlungshandlungen zur Erhebung und Nutzung von beweisrelevanten Erkenntnissen zu nennen (vgl.

ebd.: 732 f.). Neben dem Ziel der Ermittlung des wahren Sachverhalts[47] (vgl. BVerfGE 57, 250, 275; 70, 297, 308) sind im Rahmen der kriminalistischen Untersuchungsplanung auch der polizeiliche Ressourceneinsatz und dessen Organisation in das Blickfeld zu nehmen, da für eine effektive und effiziente Zielerreichung die Vorbereitung, Planung, Organisation und Koordination der Aufklärungs- und Ermittlungstätigkeiten erforderlich sind (vgl. Ackermann 2019a: 221). Bei der dritten Teildisziplin handelt es sich um die Kriminalstrategie als „Lehre von der Verwirklichung des politisch und rechtlich bestimmten Auftrags zur präventiven und repressiven Verbrechensbekämpfung durch umfassend geplante, intern und extern koordinierte mittel- oder langfristig zu realisierende Maßnahmen, die den Gesichtspunkt der Effizienz zu berücksichtigen haben“ (Klink und Kordus 1986: 23 f.).

Vor dem Hintergrund einer auf diese Weise angelegten Kriminalistik werden in Bezug auf politisch motivierte Hasskriminalität im Internet in diesem Kapitel zunächst die kriminaltechnischen Aspekte digitaler Spuren erörtert, um darauf aufbauend anhand kriminaltaktischer Überlegungen die Bedarfe an die Ablauforganisation und aus kriminalstrategischer Perspektive die Anforderungen an die behördliche Aufbauorganisation zur Bekämpfung des Phänomens zu betrachten, wobei auch auf die Erkenntnisse zur Präventabilität des Phänomens rekurriert wird. Anschließend werden die Möglichkeiten und Grenzen der automatisierten Erkennung entsprechender Inhalte erörtert, ehe die kriminalistischen Implikationen in einem Zwischenfazit bilanziert werden. Die Ausführungen dieses Kapitels beschränken sich auf den Bereich der Polizei, wobei unbestritten bleibt, dass die Kriminalistik das „Instrument aller an der Strafverfolgung beteiligten Organe der Rechtspflege“ (Ackermann 2013: 25) ist, die daher zu ihren Bedarfsträgern zählen.

4.1 Forensische Aspekte digitaler Spuren

Bei Spuren handelt es sich um „sichtbare oder latente materielle Veränderungen, die im Zusammenhang mit einem kriminalistisch relevanten Ereignis entstanden sind und [die] zu dessen Aufklärung beitragen können“ (Keller 2019: 181). Bei analogen Delikten entstehen kriminalistisch relevante Spuren

[47] Im Sinne des erkenntnistheoretischen Realismus handelt es sich dabei „um eine Sachverhaltsschilderung, die möglichst weitgehend mit dem tatsächlichen Geschehen übereinstimmt“ (de Vries 2015: 253).

in der Regel durch die Handlungen des Täters am Tatort und gegebenenfalls an der geschädigten Person. Hierbei kommt es zur Entstehung von Spuren und zusätzlich besteht die Möglichkeit der wechselseitigen Übertragung solcher Spuren vom Täter an den Tatort oder auf die geschädigte Person sowie vom Tatort oder der geschädigten Person auf den Täter. Diese klassische Spurenlage findet sich nicht bei computerbasierten Delikten, bei welchen die digitalen Spuren jedoch Ermittlungsansätze bieten (vgl. Kunze 2018: 163). Diese gilt es zu nutzen, um bevorstehende Straftaten unter dem Gesichtspunkt der Prävention zu verhindern und um bei begangenen Taten die Täter im Sinne der Repression zu identifizieren und deren Täterschaft nachzuweisen.

Digitale Spuren weisen hierbei verschiedene technische Besonderheiten auf, die sich auf die inhaltlichen Anforderungen und somit auch auf ihren Beweiswert auswirken. Diese Charakteristiken werden nachfolgend vor dem Hintergrund der politisch motivierten Hasskriminalität im Internet betrachtet und anhand der in den vorherigen Kapiteln bereits thematisierten Fallvignetten verdeutlicht.

Der erste Aspekt ist die Datenmenge, welche sowohl im Hinblick auf die Datenbreite, also nach der Zahl der Quellen und Datensätze zu verschiedenen Sachverhalten oder Personen, als auch hinsichtlich der Datentiefe, mithin der Anzahl der Einzeldaten zu einem Sachverhalt oder einer Person sowie der auszuwertenden Eigenschaften, betrachtet werden kann (vgl. Riedmüller 2018: 10 f.). Die Fallvignette Lübcke, bei welcher davon ausgegangen wurde, dass tausende Ermittlungsverfahren wegen Delikten der Hassrede zu führen sein werden (vgl. Zeit online 2019), macht deutlich, dass aufgrund eines singulären Ereignisses eine hohe Datenbreite entstehen kann. Die Fallvignette Halle, bei welcher im Rahmen der Ermittlungen die digitale Radikalisierung nachzuzeichnen ist, veranschaulicht, dass dies gleichfalls auf anfallende Einzeldaten, also eine große Datentiefe, zutreffen kann. Diese Datenmengen müssen im Rahmen der kriminalpolizeilichen Ermittlungen abgearbeitet werden und stellen somit eine Herausforderung dar.

Der zweite Aspekt ist die Datengeschwindigkeit. Diese kann einerseits als Flüchtigkeit verstanden werden und meint die Art der Speicherung (vgl. De-

wald und Freiling 2015: 37) und damit verbunden die Möglichkeit ihrer Wahrnehmung und Sicherung. Bei entsprechenden Inhalten, beispielsweise in sozialen Medien, besteht regelmäßig die Möglichkeit, die Aussagen zu verändern oder Inhalte ganz oder teilweise zu löschen. Es handelt sich somit zunächst nicht um persistente Spuren, sodass das Erfordernis einer zeitnahen Datensicherung besteht. Andererseits kann auch auf die Verarbeitungsgeschwindigkeit abgestellt werden (vgl. Riedmüller 2018: 11). So enthält der in Frage kommende strafrechtliche Deliktskatalog (vgl. Kapitel 2.2.2) auch die Tatbestände der öffentlichen Aufforderung zu Straftaten gemäß § 111 StGB, der Störung des öffentlichen Friedens durch Androhung von Straftaten gemäß § 126 StGB und der Anleitung zu Straftaten gemäß § 130a StGB. Es handelt sich hierbei um die Aufforderung, das In-Aussicht-Stellen und die Förderung von analog noch nicht verwirklichten Straftaten, die jedoch eine schwerwiegende Rechtsgutverletzung bedeuten würden. Aus rechtsstaatlicher Perspektive ergibt sich damit ein Gefahrenüberhang, der eine umgehende Intervention zur Verhinderung von Straftaten und damit eine schnelle Verarbeitungsgeschwindigkeit der digitalen Spuren erforderlich macht. Auch im Hinblick auf die Auswertung von digitalen Spuren und Asservaten im Ermittlungsverfahren besteht verfahrensrechtlich das Bedürfnis an einer entsprechenden Verarbeitungsgeschwindigkeit. In Betracht kommt hier beispielhaft schon die Frage, über welchen Zeitraum die Sicherstellung oder Beschlagnahme technischer Gegenstände zu Auswertezwecken verhältnismäßig sein kann.[48] Die Verarbeitungsgeschwindigkeit kann weiterhin die Entscheidung über die Fortdauer von Untersuchungshaft nach sechs Monaten durch die Haftprüfung des OLG gemäß §§ 121, 122 Strafprozessordnung (StPO) beeinflussen, da das Ergebnis der Datenauswertung den für Untersuchungshaft erforderlichen dringenden Tatverdacht weiter stützen kann. Mithin ergeben sich auch aus der Datengeschwindigkeit mit ihren Elementen der Flüchtigkeit und Verarbeitungsgeschwindigkeit Herausforderungen für die Ermittlungsbehörden.

[48] Das Landgericht (LG) Cottbus (vgl. Beschluss vom 10. April 2019, Az. 22 Qs 1/19) entschied beispielsweise, dass die vorläufige Sicherstellung elektronischer Speichermedien zur Auswertung über einen Zeitraum von 14 Monaten verfassungsrechtlich nicht mit der mangelnden personellen Ausstattung der Ermittlungsbehörden gerechtfertigt werden kann.

Bei dem dritten Aspekt handelt es sich um die Datenvielfältigkeit, die nach Datenherkunft und Datenabbildung betrachtet werden kann (vgl. Riedmüller 2018: 13). Politisch motivierte Hasskriminalität tritt im Internet an einer Vielzahl von Örtlichkeiten auf, sodass als virtuelle Tatorte zum Beispiel Foren, soziale Netzwerke sowie Foto- und Videoportale in Betracht kommen. Auch in Bezug auf die Abbildung der Daten kommen verschiedene Formate in Betracht. Zu denken ist zunächst an Texte, Bilder sowie Audio- und Videoaufnahmen, durch deren Inhalt beziehungsweise Verbreitung der jeweilige Tatbestand erfüllt wird. Ermittlungsansätze zur Identifizierung der Täter und Beweisführung ergeben sich darüber hinaus aus Daten in weiteren Formaten, welche bei Plattformbetreibern und Providern zu erheben sind.[49] In Betracht kommen insbesondere die gemäß §§ 3 Nr. 3, 95, 111, 112, 113 Telekommunikationsgesetz (TKG) in Verbindung mit § 100j StPO zu erhebenden Bestandsdaten oder die Verkehrsdaten gemäß §§ 3 Nr. 30, 96, 113b TKG, welche unter den Voraussetzungen des § 100g StPO erhoben werden können.[50] Sofern das Telemediengesetz (TMG) einschlägig ist, können Bestands- und Nutzungsdaten auf Grundlage der dortigen §§ 14 und 15 übermittelt und gemäß §§ 161, 161a, 163 StPO erhoben werden. Im Ergebnis bleibt festzuhalten, dass Daten aus vielfältigen Quellen und in verschiedensten Formaten durch die Ermittlungsbehörden zu erheben und zu verarbeiten sind, worin eine weitere Herausforderung liegt.

An die in ein Ermittlungsverfahren eingebrachten Daten besteht der Anspruch der Glaubwürdigkeit, wobei sich die Qualität an der Vollständigkeit und Fehlerfreiheit der Daten bemisst (vgl. Riedmüller 2018: 15). Aus rechtsstaatlicher Perspektive ergibt sich für die Beweisführung das Erfordernis, die Ermittlungsergebnisse zu digitalen Spuren begründet und nachvollziehbar darzustellen. Hierbei kommt den Begrifflichkeiten der Integrität und Authentizität eine besondere Bedeutung zu. So ergibt sich ein hoher Integritätsgrad, wenn die Daten über den gesamten Verfahrens- und Bearbeitungslauf un-

[49] Hierbei bedarf es zum Austausch personenbezogener Daten im Sinne eines Doppeltürenmodells sowohl einer Rechtsgrundlage für die Datenübermittlung durch die auskunftserteilende Stelle, als auch für die Datenabfrage und -erhebung durch die auskunftssuchende Stelle (vgl. BVerfGE 130, 151, 184).

[50] Aufgrund ihrer Bedeutung bezeichnet Wernert (vgl. 2017: 49 f.) die Bestands- und Verkehrsdaten zutreffend als ermittlungsrelevante Daten.

verändert geblieben sind (vgl. Momsen 2015: 81). Da die ursprünglichen Daten, sogenannte Rohdaten, im Rahmen der Ermittlungen regelmäßig aufbereitet und ausgewertet werden, sind die Bearbeitungsschritte für den Authentizitätsnachweis darzustellen und die Rohdaten vorzuhalten, damit die Ermittlungsschritte wiederholt werden können (vgl. ebd.: 77 f.). Nur durch die Gewährleistung der Integrität und Authentizität kann es gelingen, „dem beurteilenden Gericht einen Sachverhalt durch jedermann überzeugende und beliebig oft reproduzierbare Fakten so darzustellen, dass ein vernünftiger Zweifel an dem von den Strafverfolgungsorganen [...] bei vorläufiger Tatbewertung angenommenen Tatgeschehen nicht möglich ist“ (Clages 2017c: 47) und somit einen Beweis zu führen. Generell gilt für im Internet begangene Delikte, dass durch die Täter verschiedene Möglichkeit zur Verschleierung der eigenen Identität oder zur Täuschung über diese genutzt werden können. Zudem sind die Ermittlungsbehörden in Bezug auf zugelieferte Bestands-, Verkehrs- und Nutzungsdaten auf die Korrektheit der Erkenntnisse angewiesen, da die Daten nicht selbst gesichert, sondern von einem verpflichteten Dritten übermittelt werden. Auch diese Aspekte müssen somit Beachtung finden.

Über die Glaubwürdigkeit hinaus, muss den digitalen Daten für das Ermittlungsverfahren ein Wert zukommen. Bei dem gegenständlichen Phänomen liegt dieser darin, wenn die Spur dazu geeignet ist oder beiträgt, eine zunächst unbekannte Person zu identifizieren und deren Täterschaft nachzuweisen. In Betracht kommt einerseits die Eignung einer Spur als Beweis, wenn sie auf den nachzuweisenden Sachverhalt direkt hindeutet (vgl. Clages 2017c: 54) oder als Indiz, wenn aus ihr als mittelbare Tatsache „unter Anwendung von Denkgesetzen und Erfahrungssätzen auf eine unmittelbar entscheidungserhebliche Tatsache geschlossen werden muss“ (ebd.: 54). So wird allein vor den Hintergründen der Verschleierung und Täuschung über die Identität die Bestandsdatenauskunft zu einem Nutzerprofil in einem sozialen Netzwerk, über welches ein Delikt der politisch motivierten Hasskriminalität verwirklicht wurde, nicht dazu geeignet sein, den Beweis der Täterschaft einer konkreten Person zu führen. Das Ergebnis der Bestandsdatenauskunft stellt zunächst ein Indiz dar und erst weitere Ermittlungen zu den in

der Bestandsdatenauskunft hinterlegten, ergänzenden Informationen[51] oder Auskünften zu Verkehrs- und Nutzungsdaten, die auf die vom Täter genutzten Endgeräte hinweisen, können eine Beweiskette bilden.[52] Die Bedeutung der Bestandsdatenauskunft liegt also nicht in ihrer Indiztatsache, sondern in dem sich daran anschließenden Denkprozess, durch welchen auf das Vorhandensein weiterer rechtserheblicher Tatsachen geschlossen werden kann (vgl. BGHZ 53, 245, 260). Hieraus wird deutlich, dass zur Beweisführung regelmäßig mehrere Beweismittel (Indizien und Beweise) heranzuziehen sein werden, die in logischem Zusammenhang stehen und unterschiedliche Beweiswerte haben können (vgl. Clages 2017c: 47).

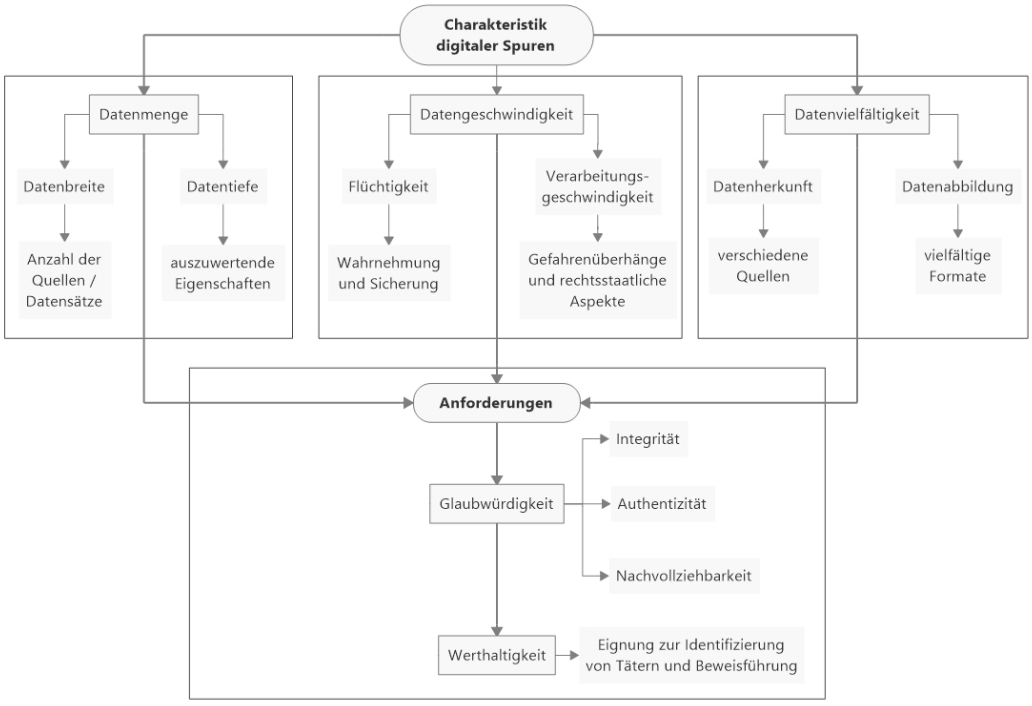

Abbildung 3: Charakteristiken und Anforderungen digitaler Spuren

Die skizzierten technischen Besonderheiten sowie die sich daraus ergebenden Herausforderungen und inhaltlichen Ansprüche digitaler Spuren an den Beweiswert stellen Anforderungen an die Ablauf- und Aufbauorganisation, die nachfolgend betrachtet werden.

[51] In Betracht kommen beispielsweise E-Mail Adressen, Mobilfunknummern sowie Zahlungsinformationen, wie Bankverbindungen oder Kreditkartendaten.

[52] Für die Möglichkeiten des Zusammenwirkens von Indizien siehe Clages 2019: 68 ff.; Keller 2019: 154 ff.

4.2 Anforderungen an die Ablauf- und Aufbauorganisation

Die polizeiliche Ablauforganisation wird durch das zusammenwirkende Ordnen von Arbeitsabläufen beschrieben (vgl. Keller 2019: 239). Das strafrechtliche Ermittlungsverfahren kann kriminaltaktisch in mehrere Prozessschritte unterteilt werden, deren differenzierende Betrachtung die verschiedenen Anforderungen verdeutlicht, welche die politisch motivierte Hasskriminalität im Internet an die polizeiliche Ablauforganisation stellt. Auf Basis des Ergebnisses werden anschließend die kriminalstrategischen Anforderungen an die polizeiliche Aufbauorganisation abgeleitet, ehe die Möglichkeiten präventiver Maßnahmen erörtert werden. Die Exemplifizierung erfolgt dabei jeweils anhand der beiden Fallvignetten Lübcke und Halle.

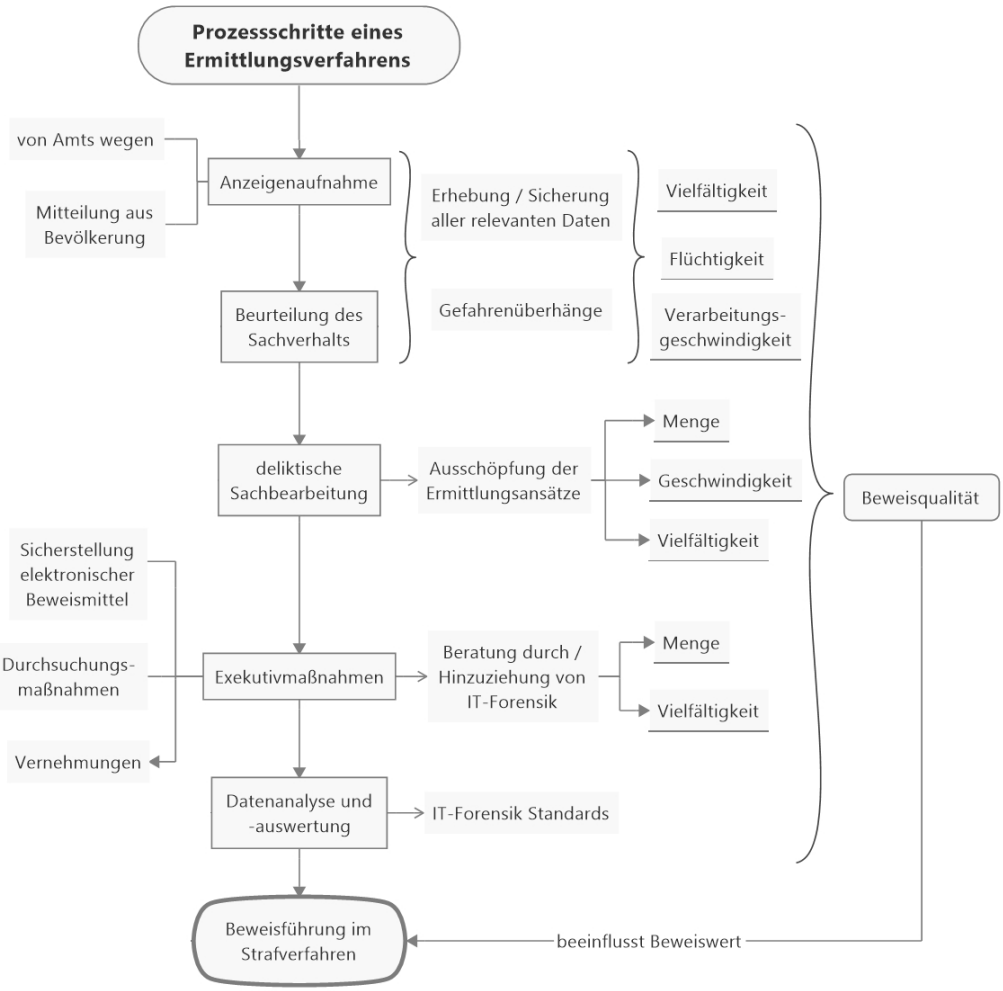

Abbildung 4: Prozessschritte eines strafrechtlichen Ermittlungsverfahrens

Der erste Prozessschritt eines polizeilichen Ermittlungsverfahrens ist die Einleitung des Verfahrens durch die Anzeigenaufnahme. Dies kann einerseits infolge der behördlichen Wahrnehmungen geschehen, wenn im Rahmen einer anlassunabhängigen polizeilichen Internetrecherche der Verdacht der Strafbarkeit eines Sachverhalts anzunehmen ist oder andererseits durch die Mitteilung eines strafrechtlich relevanten Sachverhalts an die Polizeibehörden erfolgen (vgl. Clages 2017b: 30 f.).[53] In einem zweiten Schritt erfolgt die umfassende Beurteilung des Sachverhalts, wobei verschiedene Aspekte von Relevanz sind. Einerseits ist es in Bezug auf die Vielfältigkeit digitaler Spuren und der damit verbundenen Ermittlungsansätze erforderlich, alle benötigten Daten zu (er-)kennen und zu erheben sowie die Maßnahmen zu deren Sicherung durchzuführen oder zu veranlassen, wobei unter Verweis auf die Datengeschwindigkeit den flüchtigen Daten eine besondere Bedeutung zukommt (vgl. Kunze 2018: 174 f). Die Geschwindigkeit von Daten in Form ihrer Verarbeitung bezieht sich andererseits auch auf präventive Gesichtspunkte, da bei Gefahrenüberhängen eine umgehende Intervention zur Verhinderung eines Schadenseintritts erforderlich ist (vgl. Kapitel 4.1). Im nächsten Prozessschritt erfolgen Ermittlungen im Rahmen der deliktischen Sachbearbeitung. Aufgrund des Umstands, dass es sich um politisch motivierte Kriminalität handelt, obliegt die Bearbeitung im Regelfall den örtlich zuständigen Staatsschutzdienststellen der Länder[54] (vgl. Keller 2019: 759). Die Kenntnis der Ermittlungsansätze und die Durchführung der entsprechend erforderlichen Ermittlungen sind hierbei für das weitere Verfahren wesentlich (vgl. Kunze 2018: 164 f.), wobei die Datenvielfalt mit ihren Aspekten der Herkunft und Abbildung eine Herausforderung darstellt und verfahrensabhängig große Datenmengen analysiert und ausgewertet werden müssen. In Abhän-

[53] Für Maßnahmen zur positiven Beeinflussung der Anzeigewahrscheinlichkeit und Erhöhung der Anzeigequote (vgl. Kapitel 3.2) kann die Meldeplattform „Hessen gegen Hetze“ als Vorbild dienen, da hierdurch nicht nur der zeitliche und logistische Aufwand zur Anzeigenerstattung für die Bevölkerung verringert wird, sondern über das Meldeformular bei korrekter Anwendung auch alle verfahrensrelevanten Daten, wie die betreffende Internetadresse sowie eine Dokumentation des entsprechenden Inhalts durch Screenshots, erhoben werden (vgl. Hessisches Ministerium des Innern und für Sport 2020). Eine solche Plattform mit Medienredaktionen als Zielgruppe existiert in Bayern (vgl. Bayerische Landeszentrale für neue Medien 2020).

[54] Die organisationale Gestaltung der Polizeibehörden sowie die Angliederung und Denomination der zuständigen Organisationseinheiten, zum Beispiel als (Kriminal-)Kommissariat oder Dezernat, variiert in den Ländern infolge des Föderalismus.

gigkeit des Einzelfalls und des Zwischenergebnisses der Ermittlungen kommen zur weiteren Beweisführung offene Ermittlungsmaßnahmen in Betracht. Hierbei ist, insbesondere im Rahmen von Durchsuchungsmaßnahmen gemäß §§ 102 ff. StPO, die Sicherstellung, respektive Beschlagnahme von Daten, Datenträgern und elektronischen Geräten ein wesentlicher Bestandteil der polizeilichen Ermittlungstätigkeit (vgl. ebd.: 175). Hierbei ist zu berücksichtigen, dass es bei einer (Spuren-)Sicherung durch Ermittlungskräfte zu Defiziten in Bezug auf die kriminaltechnischen Notwendigkeiten der IT-Forensik kommen kann (vgl. Burba 2019: 154), weswegen die Hinzuziehung von kriminaltechnischen Fachkräften aus dem Bereich der IT-Forensik angezeigt sein kann.[55] Diese besitzen häufig keine ausreichenden Kenntnisse über die kriminalistischen Fragestellungen des Einzelfalles, weshalb für eine gleichermaßen zielführende, wie effiziente Datenerhebung ein enger Abstimmungsbedarf besteht (vgl. ebd.: 154 f.). Für die sich als weiteren Prozessschritt anschließende Datenanalyse und -auswertung sowie die damit verbundene Beweisführung spielen die dargestellten Aspekte der Beweiseignung und der Beweisqualität[56] eine herausragende Rolle, weswegen Standards der IT-Forensik[57] einzuhalten sind, um digitale Daten in einen Strafprozess einbringen zu können sowie die Überprüfung der Daten und Ermittlungsschritte zu ermöglichen (vgl. Momsen 2015: 78 ff.). Die Beweisqualität digitaler Spuren, welche sich wiederum auf den Beweiswert auswirkt, steht maßgeblich mit der Berücksichtigung ihrer Charakteristiken und Anforderungen über das gesamte Verfahren hinweg in Zusammenhang.

Auf Basis dieser Überlegungen ergeben sich die nachfolgenden kriminalstrategischen Anforderungen an die polizeiliche Aufbauorganisation. Hierbei ist zu berücksichtigen, dass es sich bei politisch motivierter Hasskriminalität im Internet zwar um ein konkretes Kriminalitätsphänomen handelt, jedoch geht es bei den nachfolgenden Ausführungen primär nicht um eine Deliktsstrategie zur Kontrolle dieses Deliktsbereichs. Vielmehr stehen deliktsübergreifend die mit den digitalen Spuren einhergehenden Herausforderungen und somit

[55] Für die wesentlichen Aspekte bei der Sicherstellung von elektronischen Beweismitteln im Rahmen von Durchsuchungen siehe Wernert 2017: 109 ff.

[56] Casey (vgl. 2011: 69 ff.) definiert hierfür sieben „Levels of Certainty“.

[57] Beispielhaft wird auf den Prozess einer forensischen Untersuchung des Bundesamts für Sicherheit in der Informationstechnik (vgl. 2011: 86 ff.) verwiesen.

eine diesbezügliche organisationale Fachstrategie zu digitalen Spuren im Zentrum der Betrachtung (vgl. Ackermann et al. 2000: 657). Unter Verweis auf die von Wernert (vgl. 2017: 38 ff.) skizzierten Ebenen der IT-Sachbearbeitung, verdeutlichen die beiden Fallvignetten die Notwendigkeit der nachfolgend dargelegten Komponenten.[58]

Wie bereits dargelegt, repräsentiert die Fallvignette Lübcke Delikte der politisch motivierten Hasskriminalität, welche im Internet an unterschiedlichen Orten begangen werden und dort für einen großen Personenkreis wahrnehmbar sind. Bemerkenswert ist, dass diese virtuellen Delikte der Fallvignette als Reaktionen auf eine analoge Straftat, nämlich das zugrunde liegende vollendete Tötungsdelikt, erfolgten. Unerheblich des Umstandes, ob entsprechende Inhalte durch eine anlassunabhängige Internetrecherche im Rahmen einer sogenannten virtuellen Streife festgestellt werden oder ob die Polizei eine Mitteilung durch die Bevölkerung erhält, müssen alle Polizeibediensteten in die Lage versetzt werden, den Sachverhalt adäquat bewerten und die Maßnahmen des Ersten Angriffs treffen zu können (vgl. Wernert 2017: 39; Fauth 2015: 150). Vor dem Hintergrund der Ausführungen zur Datengeschwindigkeit und -vielfältigkeit bedarf es hierfür der Aus- und Fortbildung sowie der Informationsbereitstellung zu entsprechendem Grundlagenwissen sowie den Möglichkeiten und Notwendigkeiten der erforderlichen Sicherungsmaßnahmen. Auf Basis der Überlegungen zu den praktischen Bedürfnissen gehören hierzu in besonderem Maße das Vorhalten von Vorlagen für Ermittlungen bei den Dienstanbietern im elektronischen Vorgangsbearbeitungssystem, die Anlage und Pflege einer Datenbank mit den Kontakten der Provider und Dienstleister sowie eine Übersicht zu den rechtlichen und besonderen Voraussetzungen bei der Datenerhebung.

Die weitere Betrachtung zielt auf die Erfordernisse im Rahmen der deliktischen Sachbearbeitung in den Staatsschutzdienststellen der Behörden.[59] Die mit der Sachbearbeitung dieses Phänomens befassten Bediensteten müssen dahingehend qualifiziert werden, dass sie die verschiedenen, mit der Daten-

[58] Die Ebene der Sachbearbeitung für Cybercrime im engeren Sinne (vgl. Wernert 2017: 39) findet hier keine Berücksichtigung.

[59] Diese Komponente gilt auch für die deliktische Sachbearbeitung anderer Kriminalitätsphänomene mit dem Tatmittel Internet, woraus erneut deutlich wird, dass es sich um eine Fachstrategie handelt.

menge, -geschwindigkeit und -vielfältigkeit einhergehenden Herausforderungen kennen und bewältigen können und unter Verweis auf die Anforderungen digitaler Spuren die Ermittlungsansätze ausschöpfen und das Ergebnis in das Verfahren einbringen können. Hierzu gehören neben der Verfolgung der allgemeinen digitalen Ermittlungsansätze[60] auch die Nutzung der Möglichkeiten der Ermittlung in sozialen Netzwerken sowie die Durchführung von Ermittlungen in sonstigen, frei verfügbaren und offenen Quellen (vgl. Keller 2019: 743 ff. m. w. N.). Hierbei verdeutlicht die Fallvignette Halle, bei welcher die digitale Radikalisierung einen wesentlichen Ermittlungsansatz darstellte, dass digitale Spuren auch bei analogen Straftaten von großer Bedeutung sein können und dass das Ausmaß der diesbezüglichen Ermittlungen immens sein kann. Aus der Presseberichterstattung zu dieser Fallvignette ergibt sich, dass weder Kommunikation des Täters, noch Reaktionen anderer Personen auf die in Echtzeit in das Internet übertragene Tat gesichert wurden, sodass diese digitalen Spuren für die Ermittlungen nicht zur Verfügung standen (vgl. Quack 2020; Rietzschel 2020). Im konkreten Fall muss daher von einer mangelnden Sensibilität im Hinblick auf die Notwendigkeit ausgegangen werden, dass die digitalen Ermittlungsansätze von derart wesentlicher Bedeutung für das Verfahren sein werden. Dies wiederrum dürfte dazu geführt haben, dass mutmaßlich zu wenige Ressourcen eingesetzt wurden und keine ausreichende Fachlichkeit vorhanden war. Im Rahmen einer entsprechenden Fachstrategie zu Cyberkriminalität oder digitalen Spuren ist also zu berücksichtigen, dass sowohl in personeller, als auch in fachlicher Hinsicht ausreichende Ressourcen in den Polizeibehörden geschaffen werden und dass insbesondere ein höheres Bewusstsein für die Bedeutung digitaler Spuren entsteht. Ferner bedarf es einer entsprechenden technischen Ausstattung zur sachgerechten Aufgabenwahrnehmung. Nur hierdurch wird es möglich, entsprechende Ermittlungsansätze in großen Ermittlungsverfahren, wie der Fallvignette Halle, im Rahmen der kriminalistischen Untersuchungsplanung ausreichend verfolgen zu können (vgl. Ackermann 2019a: 232). Digitale Spuren spielen in nahezu allen strafrechtlichen Ermittlungsverfahren

[60] Hiermit sind beispielsweise Ermittlungen zu IP-Adressen und Domains gemeint. Einige Möglichkeiten der Ermittlungsführung sind bei Wernert (vgl. 2017: 95 ff.) dargestellt.

eine Rolle und sind daher aus kriminalistischer Perspektive nicht zuletzt aufgrund des ihnen innewohnenden Potentials von großer Bedeutung.

Unter Bezugnahme auf die Ausführungen zur IT-Forensik im Rahmen von Sicherstellungen bei Durchsuchungen sowie der Auswertung und Analyse von Daten bedarf es weiterhin einer technisch und personell ausgestatteten, behördlichen Komponente zur IT-Beweissicherung, die neben der praktischen Durchführung der Maßnahmen auch beratend und unterstützend tätig ist (vgl. Wernert 2017: 39 f.).

Neben den Möglichkeiten und Maßnahmen im Rahmen der Strafverfolgung beschäftigt sich die Kriminalistik auch mit der Prävention und bei der Gefahrenabwehr handelt es sich um den zweiten gesetzlichen Auftrag der Polizei. In Bezug auf die Präventabilität des Phänomens der politisch motivierten Hasskriminalität im Internet müssen zwei Aspekte nochmals herausgegriffen werden, um ihre kriminalstrategische Bedeutung zu verdeutlichen. Hierbei handelt es sich einerseits um das Internet als präventivpolizeilicher Einsatzraum. Rüdiger (vgl. 2018: 264 ff.; 2019: 40) stellt heraus, dass das Nutzungsverhalten der deutschen Polizei im internationalen Vergleich gering ist und attestiert eine ausbaufähige Sichtbarkeit im digitalen Raum. Eine sichtbare Präsenz führt zu einer diesbezüglichen gesellschaftlichen Wahrnehmung und kann einen generalpräventiven Beitrag dazu leisten, die Gültigkeit von Normen im virtuellen Raum zu verdeutlichen und die gefühlte und tatsächliche Verfolgungswahrscheinlichkeit zu erhöhen, weshalb ein solcher Ressourceneinsatz sinnvoll erscheint. Die sodann im Rahmen einer virtuellen polizeilichen Streifentätigkeit als strafbar festgestellten Inhalte sollten nicht nur entfernt und entsprechende Ermittlungsverfahren eingeleitet werden, sondern durch die Strafverfolgungsbehörden muss zur Erreichung der präventiven Ziele wahrnehmbar und explizit auf das Vorliegen eines Straftatbestandes hingewiesen werden. Im Sinne eines ganzheitlichen Präventionsansatzes kann die polizeiliche Präsenz auch dazu genutzt werden, um die Bevölkerung zu ermutigen, bei entsprechenden Feststellungen mit der Polizei Kontakt aufzunehmen, eine Anzeige zu erstatten sowie das sich anschließende behördliche Vorgehen darzustellen, um Transparenz zu schaffen, realistische Erwartungen an das Verfahren zu wecken und das Vertrauen in die Polizei auszubauen (vgl. Brand und Materni 2020: 267).

Andererseits kommt auch dem Aspekt der Gegenrede eine präventive Bedeutung zu, da hierdurch der Normbruch verdeutlicht wird und gleichsam auf die Hemmschwelle der Täter eingewirkt werden kann (vgl. Kapitel 3.5). Aus kriminalstrategischer Perspektive sind daher Kooperationen mit zivilgesellschaftlichen Akteuren in diesem Feld durch die Sicherheitsbehörden zu prüfen und anzustreben.[61]

Zusammenfassend ist festzuhalten, dass der Umgang mit digitalen Spuren umfassende Anforderungen an die Aufbau- und Ablauforganisation stellt und dass diese Ansprüche daher in die kriminaltaktischen und -strategischen Maßnahmen einzubeziehen sind. Nicht zuletzt ist die Kontrolle des Ermittlungserfolgs, also die Frage der kriminalistischen Zielerreichung und der Effektivität, Teil der kriminaltaktischen Methodik (vgl. Clages 2017a: 17). Die Ergebnisse müssen Einfluss in die kriminalstrategische Planung finden[62], um identifizierte Abweichungen von Zielvorstellungen und -vorgaben bei der Steuerung des Gesamtprozesses und der Fachstrategie berücksichtigen zu können.

4.3 Möglichkeiten und Grenzen der automatisierten Detektion

Angesichts der weiten Verbreitung von politisch motivierter Hasskriminalität im Internet und im Hinblick auf die großen Datenmengen, welche in strafrechtlichen Ermittlungsverfahren ausgewertet werden müssen, erscheint die Anwendung automatisierter Detektionsverfahren als vielversprechender Ansatz[63]. Das Potential und die Limitierungen der bestehenden Möglichkeiten werden nachfolgend für diese beiden Anwendungsgebiete betrachtet.

---

[61] Beispielweise hat die bereits erwähnte Initiative „Hessen gegen Hetze“ mit dem gemeinnützigen Verein „ichbinhier“ die größte Counterspeech-Initiative im deutschsprachigen Raum als Bündnispartner, welcher durch sachliche und konstruktive Kommentare im sozialen Netzwerk Facebook ein Gegenwicht zu Hasskriminalität herzustellen versucht (vgl. Hessisches Ministerium des Innern und für Sport 2020a). Auch die Initiative „Zivile Helden“ (vgl. 2020) als Projektpartner der polizeilichen Kriminalprävention des Bundes und der Länder bietet ein interaktives präventives Angebot zur Thematik Hass im Netz.

[62] Hierzu sind Maßnahmen des Controllings und der Evaluation erforderlich (vgl. Keller 2019: 837).

[63] Für die Identifizierung von sinngleichen Inhalten zu bereits als relevant festgestellten Beiträgen in sozialen Netzwerken stellte bereits der Gerichtshof der Europäischen Union (EuGH) fest, dass der Hosting-Anbieter nicht zu einer autonomen Beurteilung verpflichtet ist, sodass „auf automatisierte Techniken und Mittel zur Nachforschung“ (EuGH, Urteil vom 3. Oktober 2019, Az. C-18/18, Rn. 46) zurückgegriffen werden kann.

Die Verbreitung von politisch motivierter Hasskriminalität im Internet in Form strafrechtlich relevanter Inhalte, insbesondere in sozialen Medien, erfolgt überwiegend im Textformat. Für diese sprachlich manifestierten Delikte besteht die Möglichkeit, auf Algorithmen basierende Klassifikationsverfahren zu entwickeln,[64] wobei der Erfolg dieses maschinellen Lernens von der zugrundeliegenden Datenbasis abhängig ist (vgl. Mandl 2020: 215 f.). Am Beispiel des vom Bundesministerium für Bildung und Forschung finanziell geförderten und an der Freien Universität Berlin mit Verbundpartnern durchgeführten Projektes „NOHATE“ wird deutlich, dass gut ausgearbeitete und breit angelegte Datensätze sowie das Zusammenwirken zwischen der Informatik und den Sozialwissenschaften für das maschinelle Deep-Learning-Verfahren essentiell sind (vgl. Yücel 2017). In diesem Projekt wurde ein Datenbestand von circa 225.000 Onlinekommentaren in englischer Sprache mit unterschiedlichen technischen Ansätzen analysiert, wobei ein kombinierter Einsatz der Algorithmen vorgeschlagen wurde, um zu entscheiden, welches Modell für den spezifischen zu untersuchenden Kommentar am besten geeignet ist und um individuelle Modellfehler auszugleichen (vgl. van Aken et al. 2018: 5). Unabhängig vom genutzten algorithmischen Modell und der Kombination, ergab sich die Problemstellung von falsch negativen und falsch positiven Detektionen[65] und es bleibt festzuhalten, dass rein deutschsprachige Datensätze bislang zu klein und damit fehleranfälliger sind (vgl. Gleiß 2019).

Die Gründe für falsch negative und falsch positive Detektionen ergeben sich bei einer Betrachtung der Thematik aus linguistischer Perspektive. So können Phrasen, die an der sprachlichen Oberfläche in Ermangelung von diskriminierenden, rechtextremistischen, volksverhetzenden oder beleidigenden Inhalten zunächst keine Auffälligkeiten zeigen für automatische Detektions-

[64] Hierbei können künstliche neuronale Netze mit verschiedenen technischen Ansätzen zur Anwendung kommen. Beispielhaft wird für einen Überblick, die Forschungsergebnisse und die Genauigkeit von bis zu 80 Prozent bei der Zuordnung zum „Word Embedding“ und dem „Sentence Encoding“ auf Mandl 2020: 217 ff. sowie für den „k-Nearest-Neighbor-Algorithmus“ auf Vogel, Regev und Steinebach 2019: 241 ff. verwiesen.

[65] Bei einem Inhalt, der aufgrund der verwendeten Sprache nicht als Hasskriminalität identifiziert wird, es aber bei Berücksichtigung des Kontexts hätte erfolgen müssen, handelt es sich um eine falsch negative Detektion. Ein Inhalt, der sprachliche Merkmale von Hasskriminalität enthält und deshalb identifiziert wird, bei Bewertung des Kontexts jedoch auszufiltern wäre, stellt eine falsch positive Detektion dar.

verfahren unauffällig sein, obwohl die Identifikation als Hasskriminalität über den Kontext der Aussage oder durch Inferenzen erfolgen kann (vgl. Marx 2020: 715 f.). Ebenso können, beispielsweise bei Statusverhandlungen innerhalb einer Peergroup jenseits von Tabugrenzen, inhaltlich Beschimpfungen und dehumanisierende Metaphern genutzt worden oder die Degradierung einer Person kann erfolgt sein, ohne dass es sich um Hasskriminalität handeln muss, weswegen die Beziehung der Interagierenden bei der Bewertung zu berücksichtigen ist (vgl. ebd.: 718). Im Ergebnis ist eine ausschließlich lexikalische Suche nach Begrifflichkeiten ungeeignet, da hierbei der Textzusammenhang keinen Einfluss in die Bewertung findet und empirische Studien belegen, dass sich relevante Inhalte insbesondere auch durch sprachliche Kreativität und indirekte Angriffe in Form von Methapern oder phraseologischen Modifizierungen auszeichnen (vgl. Jaki und De Smedt 2018: 24). An das zur Detektion genutzte System besteht daher die komplexe Anforderung, dass über das Vokabular hinaus die Semantik berücksichtigt wird, um über lexikographische und emotive Muster den Gesamtzusammenhang zu erfassen (vgl. Hartung et al. 2017: 322) und dass der unmittelbare und mittelbare Kontext sowie diskursives Wissen im Rahmen der Bewertung analysiert werden (vgl. Marx 2020: 717).

Es ist darauf hinzuweisen, dass ein Großteil der bestehenden Verfahren auf die automatisierte Detektion von Inhalten in den sozialen Netzwerken ausgelegt ist. Unter Verweis auf die Fallvignette Lübcke ist dies ein wichtiger Anwendungsbereich, wobei zu beachten ist, dass relevante Inhalte auch auf vielen weiteren Plattformen mit Potential zu homogenen Echokammern sowie in Onlinespielen auftreten. Für den Bereich der Computerspielkultur kann unter Bezugnahme auf Gabriel (vgl. 2020: 272 ff.) festgehalten werden, dass sich Formen der politisch motivierten Hasskriminalität dort bereits bei der Benennung von Spielerprofilen und -gruppen manifestieren und dass sich während des Spielens freigesetzt Emotionen über die integrierten Kommunikationsmöglichkeiten in Form von entsprechenden verbalen und textlichen Äußerungen entladen. Wie für die sozialen Netzwerke gelten auch an diesen virtuellen Orten die Mechanismen der Distanz und der scheinbaren Anonymität (vgl. Kapitel 3), sodass maschinelle Detektionsverfahren auch in diesen

Bereichen des Internets zur Erkennung von politisch motivierter Hasskriminalität eingesetzt werden könnten.

Neben dem Umgang mit Textformaten in strafrechtlichen Ermittlungsverfahren erfolgt, insbesondere bei der Auswertung elektronischer Beweismittel, auch eine Befassung mit Mediendaten, wie Bildern sowie Audio- und Videoaufnahmen. Da auch hier regelmäßig große Datenmengen im Rahmen der Auswertung zu bewältigen sind, kommt die visuelle Erkennung von Objekten und Personen, aber auch von Aktionen und Interaktionen als weiteres Anwendungsgebiet für die automatisierte Detektion in strafrechtlichen Ermittlungsverfahren in Betracht und es existieren diesbezüglich bereits verschiedene Verfahren und Forschungsprojekte (vgl. Burkhardt 2020: 337 f.). Analog zu Textformaten gilt für diese Ansätze, dass die Qualität von der zugrundeliegenden Datenbasis abhängig ist.

Im Ergebnis bleibt zur automatisierten Detektion von politisch motivierter Hasskriminalität im Internet dreierlei festzuhalten: Erstens sind softwaregestützte Verfahren in Bezug auf die verschiedenen Anwendungsgebiete ein vielversprechender Ansatz, um der Charakteristik der Datenmenge zu begegnen, wodurch wiederum personelle Ressourcen freigesetzt oder geschont werden können. Die Möglichkeiten der automatisierten Detektion können hierbei Auswerteprozesse beschleunigen, indem eine Relevanzbewertung, Vorselektion und Priorisierung von Mediendaten erfolgt und neue Ermittlungsansätze schnell generiert werden können (vgl. Burkhardt 2020: 340). Zweitens verdeutlicht wiederum die Gefahr der falsch negativen und falsch positiven Detektionen die Grenzen solcher Verfahren und zeigt, dass eine Ergänzung um qualitative Analysen erfolgen muss. Drittens machen die vorstehenden Ausführungen deutlich, dass bei der Forschung zu und der Arbeit mit automatisierten Detektionsverfahren ein interdisziplinärer Ansatz verschiedener Wissenschaften geboten ist. Hierzu gehören neben den Sozialwissenschaften, der Informatik und der Linguistik auch die Kriminologie und die Kriminalistik. Entsprechende Kooperationen, wie die des BKA und des Landeskriminalamts (LKA) Rheinland-Pfalz mit dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI), welche nicht auf das Phänomen der politisch motivierten Kriminalität im Internet beschränkt ist, sondern verschiedene Anwendungsszenarien für Künstliche Intelligenz in der polizeili-

chen Ermittlungsarbeit berücksichtigt, sind zu begrüßen und zeigen, dass die relevanten Institutionen der Strafverfolgungsbehörden sowie der Wissenschaft und Forschung die diesbezüglichen Notwendigkeiten erkannt haben (vgl. Bundeskriminalamt 2020c).[66]

4.4 Zwischenfazit

Die Charakteristiken digitaler Spuren und die damit einhergehenden Anforderungen in strafrechtlichen Ermittlungsverfahren stellen verschiedene Herausforderungen dar. Diesen ist kriminaltaktisch und -technisch im Einzelfall zu begegnen und die dargelegten Zusammenhänge mit den beiden Fallvignetten zeigen, welche unterschiedlichen Aspekte von Bedeutung sein können. Da die Herausforderungen nicht auf das Phänomen der politisch motivierten Hasskriminalität im Internet beschränkt bleiben, sondern die weiteren Delikte mit Tatmittel Internet gleichermaßen betroffen sind, bedarf es in der kriminalstrategischen Gesamtschau einer Fachstrategie, welche die personalen, organisationalen und technischen Anforderungen der IT-basierten Delikte berücksichtigt.

Die Polizeien des Bundes und der Länder verfolgen unterschiedliche Ansätze bei der Aus- und Fortbildung und Schaffung der erforderlichen personellen Ressourcen für Straftaten im Internet und in Zusammenhang mit digitalen Spuren. Zwei Herangehensweisen werden als Beispiel dargestellt. Das BKA bietet für Absolventen eines Hochschulstudiums der Informatik, eines technisch oder naturwissenschaftlichen Studiums mit IT-bezogener Schwerpunktsetzung eine cyberkriminalistische Qualifizierungsmaßnahme mit anschließender Verwendung in der kriminalpolizeilichen Sachbearbeitung in den Bereichen der Ermittlung, Auswertung und Analyse (vgl. Bundeskriminalamt 2020d). Die hessische Polizei hingegen hat im regulären Studiengang Kriminalpolizei die Vertiefungsrichtung Cyberkriminalistik geplant, um dort Inhalte der Informatik und Informationstechnik vertiefend zu behandeln (vgl.

[66] Ebenfalls sei auf das auf drei Jahre angelegte, interdisziplinäre Forschungsprojekt „KISTRA“ (Einsatz von KI zur Früherkennung von Straftaten) unter Einbindung von Wissenschaft, Wirtschaft und dem BKA hingewiesen, welches unter anderem „die Erkennung und sozialwissenschaftliche Betrachtung politisch motivierter Hassreden und ‚Hasskriminalität' im Internet“ sowie „die Erarbeitung und Implementierung von adaptiven KI-Methoden zur Unterstützung der polizeilichen strafrechtlichen Bewertung von Vorgängen, die Hasskriminalität betreffen“ (Zentrale Stelle für Informationstechnik im Sicherheitsbereich 2020) zum Ziel hat.

Klein 2020). Aufgrund einer zu geringen Bewerberlage wurde der Studienbeginn vom Wintersemester 2020/21 in das Sommersemester 2021 verlegt (vgl. Perske 2020). Unabhängig davon, ob Cyberkriminalistik im originären Studium der Fachhochschulen der Polizei gelehrt wird, ob IT-Kräfte im Bereich der Kriminalistik qualifiziert werden oder ob IT-Fachkräfte in ihrer Profession beschäftigt werden, wird sich der Erfolg des jeweiligen Ansatzes insbesondere an den Verdienstmöglichkeiten und Aufstiegschancen im Vergleich zu Privatunternehmen der freien Wirtschaft bemessen. Auch zu große monetäre Unterschiede bei den polizeilichen Ansätzen könnten für ein Gefälle in der Interessenlage sorgen, woraus sich Abstimmungs- und Anpassungsbedarfe auch im Vergleich zu anderen Sicherheitsbehörden ergeben.

Im BKA als Zentralstelle der deutschen Polizei erfolgte zum 1. April 2020 eine Organisationsveränderung zur Optimierung der Bekämpfung von Cyberkriminalität, indem diese vormals als Gruppe in der Abteilung Schwere und Organisierte Kriminalität verortete Thematik nunmehr durch eine eigenständige Abteilung Cybercrime bearbeitet wird (vgl. Bundeskriminalamt 2020e). Auch wenn die Schwerpunktsetzung im Bereich Cyberkriminalität im engeren Sinne erfolgt, wird auch „die Bereitstellung sowohl querschnittlicher Beratungsleistungen und erweiterter Ermittlungsservices für BKA-interne und -externe Bedarfsträger“ (ebd.) durch Ermittlungsunterstützungen und Internetrecherchen in anderen Kriminalitätsphänomenen ermöglicht. Für den Bereich der Strafverfolgung existiert mit der ZIT bei der Generalstaatsanwaltschaft Frankfurt am Main in der Justiz der entsprechende „Ansprechpartner des Bundeskriminalamtes für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland oder bei Massenverfahren gegen eine Vielzahl von Tatverdächtigen bundesweit“ (Hessisches Ministerium der Justiz 2020), sodass elementare Strukturen der Aufbau- und Ablauforganisation sowie technische Ressourcen existent sind, die entsprechend der jeweiligen Bedarfe auch in den Polizeien und Staatsanwaltschaften der Länder[67] abgebildet werden müssen.

[67] Beispielsweise erfolgten zur Optimierung der Ermittlungsstrukturen in Bayern die Ansiedlung eines Hate-Speech-Beauftragten bei der Zentralstelle zur Bekämpfung von Extremismus und Terrorismus (ZET) bei der Generalstaatsanwalt München und die Einrichtung von Sonderdezernaten zur Bekämpfung des Phänomens bei den 22 bayerischen Staatsanwaltschaften (vgl. Bayerisches Staatsministerium der Justiz 2020).

Die Möglichkeiten der automatisierten Detektionsverfahren sind ein wertvoller Ansatz zur Bewältigung großer Datenmengen durch Vorselektion und Relevanzbewertung und sie müssen sodann durch qualitative Analysen ergänzt werden. Die dargestellten Forschungsprojekte und Verfahren beziehen sich vornehmlich auf den Bereich der sozialen Netzwerke, sodass die weiteren Bereiche des virtuellen Raums keine Berücksichtigung finden, obwohl dort entsprechende Inhalte auftreten. Da personelle Ressourcen geschont und Auswertedauern verkürzt werden können, sind entsprechende Initiativen zu verfolgen. Der Kooperation des BKA und des LKA Rheinland-Pfalz mit dem DFKI sowie dem Forschungsprojekt „KISTRA“ kommt hierbei eine wegweisende Bedeutung zu und sie verdeutlichen besser als jeder andere Aspekt in diesem Kapitel, dass es sich bei der Kriminalistik um eine interdisziplinäre Wissenschaft handelt. Die Kritik an entsprechenden Verfahren wird mit Einschnitten in die Meinungsfreiheit bis hin zur Zensur begründet. Zur Schaffung der gesellschaftlichen Akzeptanz ist entsprechenden Vorbehalten mit einem Mindestmaß an Transparenz zu begegnen (vgl. Mandl 2020: 224 f.), da die Zielrichtung nicht die Beschränkung der Meinungsfreiheit, sondern ihre verfassungsmäßige Gewährleistung für jedermann und die Durchsetzung der geltenden Rechtsordnung ist.

Im Kern geht es im Spannungsverhältnis zwischen Freiheit und Sicherheit also um die Gewährleistung, dass es sich im Internet nicht um einen rechtsfreien Raum handelt (vgl. Münch 2020: 5). Unstrittig ist, dass die Strafrechtspflege nur selektiv ist und sein kann,[68] jedoch erfordert ihre gesellschaftliche Stabilisierungsfunktion keine allumfassende Aufklärung und Verfolgung, da verletzte Normen „auch dann hinreichende soziale Bestätigung erfahren [können], wenn nur regelmäßig sanktioniert wird und die Kriterien der Verfahrenseinstellung sachgerechten, transparenten Erwägungen folgen“ (Gärditz 2020).[69] Erforderlich ist mithin eine hinreichende Wahrscheinlichkeit für eine Rechtsdurchsetzung im virtuellen Raum.

[68] Siehe hierzu auch Popitz (1968: 18), der von der Unmöglichkeit ausgeht, dass „ein Sanktionssystem, [...] seine Schutzfunktion bewahren könnte, wenn es mit allen Normbrüchen, die passieren, fertig werden müsste“.

[69] Diesbezüglich abweichend ein Beschluss der Innenministerkonferenz (vgl. 2019: 4), wonach von Opportunitätseinstellungen gem. §§ 153, 153a StPO und der Verweisung auf den Privatklageweg kein Gebrauch gemacht werden sollte. Zudem können nach Nr. 86 Abs. 2 S 1 der Richtlinien für das Strafverfahren und das Bußgeldverfahren rassistische,

Unter Bezugnahme auf die dargestellten Ansätze besteht insbesondere hinsichtlich der Vereinfachung der Möglichkeiten zur Anzeigeerstattung sowie im Bereich der anlassunabhängigen Internetrecherche und einer darauf aufbauenden gefahrenabwehrrechtlichen oder strafrechtlichen Intervention im Bedarfsfall ein nicht unerhebliches Optimierungspotential. Letzteres will das BKA durch die Erhöhung dieser Ressourcen und durch Maßnahmen gegen technische Strukturen zur automatisierten Verbreitung ausschöpfen (vgl. Münch 2020: 5). Ferner erscheinen Präventionskampagnen gegen entsprechende Inhalte und die anlassbezogene Presse- und Öffentlichkeitsarbeit zu gefahrenabwehrrechtlichen und repressiven Maßnahmen geeignet, um die sicherheitsbehördlichen Initiativen und Ermittlungserfolge medial und gesellschaftlich in den Fokus zu rücken und hierüber einen Beitrag dazu zu leisten, die Gültigkeit der Rechtsordnung im digitalen Raum zu verdeutlichen.[70]

Aus der globalen Vernetzung und der damit verbundenen territorialen Schrankenlosigkeit des Internets wird darüber hinaus deutlich, dass nationale Lösungen zur Gewährleistung der öffentlichen Sicherheit und bei der Bekämpfung dieser Kriminalitätsphänomene zu kurz greifen. Dies gilt über die strafprozessrechtlichen Möglichkeiten zur Rechtsdurchsetzung hinaus auch für „die Einführung der wirksamsten Methoden, Verfahren und Mittel zur Verbrechensbekämpfung, der neuesten Errungenschaften in der Ermittlungstätigkeit und [...] in der forensischen Forschung“ (Ackermann et al. 2020: 360), weswegen eine europäische und transnationale kriminalistische Forschung und Wissenschaft anzustreben ist.

Für die kriminalistischen Implikationen ist daher zu bilanzieren, dass organisationale Handlungsnotwendigkeiten erkannt und Maßnahmen in Teilen bereits umgesetzt wurden oder sich in der sicherheitsbehördlichen Befassung befinden. Gleichwohl dürften diese Aktivitäten erst den Anfang darstellen, da

---

fremdenfeindliche oder sonstige menschenverachtende Beweggründe des Täters ein öffentliches Interesse an der Strafverfolgung begründen. Insgesamt kritisch hierzu Singelnstein und Stolle (vgl. 2012: 119), die darstellen, dass zwar der Mechanismus der Disziplinierung nicht verschwunden ist, sich jedoch die dieses Konzept der sozialen Kontrolle tragenden gesellschaftlichen Bedingungen infolge der gesamtgesellschaftlichen Prozesses (vgl. Kapitel 3) auflösen.

[70] Beispielhaft wird auf die Pressemitteilung zum europaweiten Aktionstag gegen Hasspostings am 3. November 2020 verwiesen, in welcher über koordinierte Exekutivmaßnahmen in sieben europäischen Staaten berichtet wird (vgl. Bundeskriminalamt 2020f).

sie - sicherlich auch im Kontext der beiden hier genutzten Fallvignetten[71] - teilweise erst kürzlich initiiert wurden, sich aus den hiesigen Ausführungen weitere Handlungsfelder und -möglichkeiten ergeben und mit der fortschreitenden Digitalisierung weitere Anpassungs- und Ergänzungsbedürfnisse entstehen werden. Im Ergebnis ist eine bislang nur selektive Befassung mit dem Phänomen festzustellen, weshalb eine Ausweitung für einen ganzheitlichen Ansatz geboten ist. Als erfolgskritische Faktoren sind hierbei insbesondere die Einhaltung von Standards der IT-Forensik im Zusammenwirken mit den klassischen kriminalistischen Mitteln, Methoden und Verfahren sowie die Vermittlung der Kompetenzen zum Umgang mit Cyberkriminalität und digitalen Spuren durch die institutionelle Verankerung in der Aus- und Fortbildung zu nennen. Ferner erscheint die Erhöhung der sichtbaren Präsenz der Strafverfolgungsbehörden im digitalen Raum sowie der Ausbau intuitiver Kommunikations- und Anzeigemöglichkeiten erforderlich (vgl. Hoheisel-Gruler 2020: 103 f.).

Im Rahmen der bisherigen Ausführungen erfolgte bislang keine Befassung mit legislativen Aktivitäten, die in Zusammenhang mit dem gegenständlichen Phänomen stehen. Diese werden daher nachfolgend einer kritischen Analyse unterzogen.

5. Kriminalpolitische Aktivitäten

> *„Verantwortungsbewusste Kriminalpolitik in einem pluralistischen, freiheitlich-demokratischen Rechtsstaat sollte (im Kern) in ihrem (Ideal-)Anspruch versuchen, möglichst wissenschaftlich-rational gesamtgesellschaftliche Problemstellungen abweichenden Verhaltens zweckgerichtet, gleichermaßen verfassungsgemäß wie sozialadäquat, legislativ aufzulösen."* (Plank 2017: 293)

Eine Sentenz aus dem Koalitionsvertrag zur 19. Legislaturperiode verdeutlicht - bereits mit einem speziellen Kriminalitätsphänomen kontextualisiert und einer Zielsetzung versehen - den Gegenstandsbereich kriminalpoliti-

[71] So auch Valerius (vgl. 2020: 666 f.), der davon ausgeht, dass das Phänomen aufgrund der beiden hier genutzten Fallvignetten in der öffentlichen und politischen Betrachtung kontinuierlich an Bedeutung gewonnen hat.

scher Maßnahmen: „Wir wollen die Sicherheitsbehörden bei der Verfolgung und Prävention von Cyberkriminalität durch die Schaffung notwendiger rechtlicher, organisatorischer sowie technischer Rahmenbedingungen stärken“ (Bundesregierung 2018: 128). Durch legislative Aktivitäten werden für die Institutionen der Kriminalitätskontrolle unter dem Gebot der Rechtsstaatlichkeit als verfassungsmäßige Beschränkung die präventiven und repressiven Voraussetzungen und Vorgaben geschaffen, welche wiederum von „der sich ständig in Umfang, Art und Schwere verändernden Kriminalität, dem sich wandelnden Normenverständnis der Gesellschaft sowie dem Sicherheitsbedürfnis bzw. der Verbrechensfurcht“ (Clages 2017: 2 f.) abhängig sind. Da zur Kriminalitätsverhütung und -bekämpfung die Gesamtheit der staatlichen Maßnahmen einzubeziehen ist, bleibt Kriminalpolitik nicht nur auf die Wirksamkeit des Strafrechts beschränkt. Im Sinne des Diktums, dass eine gute „Sozialpolitik zugleich auch die beste und wirksamste Kriminalpolitik darstellt“ (von Liszt 1898: 246), wird daher in der Literatur auch von ressortübergreifender Kriminalpolitik oder Rechtsgüterpolitik mit weitreichenden gesellschaftlichen Zielen gesprochen (vgl. Feltes 2006: 160 m. w. N.).

Es bestehen neben sozial- und gesellschaftspolitischen Einflüssen verschiedene Anknüpfungspunkte zur Kriminologie und Kriminalistik. Für erstere ergibt sich der Bezug aufgrund der empirischen Befassung mit dem Gegenstandsbereich des abweichenden Verhaltens und der gesellschaftlichen Reaktionen. Die kriminologische Forschung zu entsprechenden Erkenntnissen über die Ursachen, Wirkungen sowie Präventions- und Interventionsmöglichkeiten der politisch motivierten Hasskriminalität im Internet (vgl. Kapitel 3) sind für auf das Phänomen bezogene rechtsstaatliche legislative Aktivitäten erforderlich, wobei die an der Wirkung orientierte Kriminologie hierbei beratend bis kritisch wirken kann. Für letztere sind die Bezüge zwingend, da es sich per definitionem bei der Kriminalistik um die Wissenschaft handelt, die sich mit der Straftatenaufdeckung, -untersuchung, -aufklärung und -verhütung befasst und mithin das Zentrum einer effektiven Strafrechtspflege darstellt, welches somit der Betrachtung und Entscheidungsfindung durch die

Kriminalpolitik als einem Teilbereich des Gewaltmonopols bedarf.[72] Die Berührungspunkte der Kriminalistik zur Kriminalpolitik bestehen für alle Teilbereiche. Am offensichtlichsten ist die Verbindung zur Kriminalstrategie, da hier der institutionalisierte Austausch über Vorgaben sowie Vorschläge und Bedürfnisse durch Einbindung in die Gremienstruktur der IMK erfolgt (Innenministerkonferenz 2020; Münch 2020a: 580 f.). Auch die Kriminaltechnik erzeugt eine diesbezügliche Wirkung, da beispielsweise der Einsatz automatisierter Detektionsverfahren (vgl. Kapitel 4.3) rechtlich legitimiert und gleichzeitig reguliert werden muss, wobei dieses Ergebnis wiederum unmittelbaren Einfluss auf die kriminaltaktischen Anwendungsmöglichkeiten nimmt.

Auf diese Prolegomena aufbauend, werden nachfolgend wesentliche, mit der politisch motivierten Hasskriminalität im Internet in Zusammenhang stehende legislative Aktivitäten de lege lata und de lege ferenda auf Basis der vorstehenden kriminologischen und kriminalistischen Implikationen sowie aus telemedien- und verfassungsrechtlicher Perspektive analysiert. Hierzu gehören die Regelungen des seit dem 1. Oktober 2017 gültigen Netzwerkdurchsetzungsgesetzes, das inzwischen beschlossene Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität sowie der in der Befassung befindliche Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes. Als Datum des verbindlichen Rechtsstandes für die nachfolgenden Ausführungen gilt hierbei der 31. Januar 2021. Aufgrund der Umstände, dass die aktuelle Regierungskoalition die Bedeutung der kriminologischen Forschung hervorhebt und sich einer evidenzbasierten Kriminalpolitik bei der Erarbeitung von Gesetzesentwürfen und der Evaluation verschrieben hat (vgl. Bundesregierung 2018: 133), müssen sich die Ergebnisse hieran messen lassen.[73]

[72] Siehe hierzu bereits Weber (1972: 29), wonach „Staat […] ein politischer Anstaltsbetrieb heißen [soll], wenn und insoweit sein Verwaltungsstab erfolgreich das Monopol legitimen physischen Zwanges für die Durchführung der Ordnungen in Anspruch nimmt."

[73] Kriminalpolitische Entscheidungen werden neben der Berücksichtigung kriminologischer Befunde auch zukünftig durch weitere Parameter und gesellschaftliche, wirtschaftliche und mediale Einflüsse geprägt sein, sodass das Rollengefüge nicht neu geordnet wird und die Politik unabhängig bleibt (vgl. Meier 2020: 1 f. m. w. N.; Kinzig 2020: 9). Dies gilt umso mehr, da verschiedene rechtliche Hemmnisse einer empirischen kriminologischen Forschung entgegenstehen (vgl. Meier 2020: 5 f.).

5.1 Netzwerkdurchsetzungsgesetz ab 1. Oktober 2017

Das am 1. Oktober 2017 in Kraft getretene Netzwerkdurchsetzungsgesetz (NetzDG) richtet sich gem. § 1 Abs. 1 und 2 an die Telemediendienstanbieter sozialer Netzwerke mit mehr als zwei Millionen registrierten Nutzern im Inland.[74] Diese sind gem. § 3 Abs. 1 NetzDG verpflichtet, ein Verfahren zum Umgang mit Beschwerden vorzuhalten, dass den Elementen der Erkennbarkeit, Erreichbarkeit und Verfügbarkeit für die Nutzer genügt. Eingehende Beschwerden sind gem. § 3 Abs. 2 Nr. 1 NetzDG unverzüglich dahingehend zu prüfen, ob ein rechtswidriger Inhalt im Sinne des § 1 Abs. 3 NetzDG vorliegt, wozu der Tatbestand einer dort genannten Katalogtat[75] erfüllt sein muss und der Inhalt nicht gerechtfertigt sein darf. Liegen diese Voraussetzungen vor, sind gem. § 3 Abs. 2 Nr. 2 NetzDG offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden und gem. § 3 Abs. 2 Nr. 3 NetzDG jeder rechtswidrige Inhalt in der Regel innerhalb von sieben Tagen zu entfernen oder der Zugang zu ihm ist zu sperren. Im Falle einer Entfernung ist der Inhalt gem. § 3 Abs. 2 Nr. 4 NetzDG für einen Zeitraum von zehn Wochen zu Beweiszwecken zu sichern und nach § 5 Abs. 2 NetzDG ist eine empfangsberechtigte Person im Inland für Auskunftsersuchen inländischer Strafverfolgungsbehörden zu benennen, wobei diese Ersuchen innerhalb von 48 Stunden zu beantworten sind. Der Beschwerdeführer sowie der Nutzer sind gem. § 3 Abs. 2 Nr. 5 NetzDG über jede Entscheidung unverzüglich mit einer Begründung zu informieren. Gem. § 3 Abs. 4 NetzDG ist der gesamte Prozess zu überwachen und im Falle von organisatorischen Unzulänglichkeiten ist unverzüglich Abhilfe zu schaffen. Gemäß § 2 NetzDG obliegt denjenigen Anbietern, welche pro Kalenderjahr mehr als 100 Beschwerden erhalten, zudem beginnend seit dem ersten Halbjahr 2018 eine umfassende halbjährliche Berichtspflicht zum Beschwerdeverfahren und den Umgang mit Beschwerden. Verstöße gegen die Verpflichtungen können nach § 4 Abs. 1 NetzDG Ord-

[74] Telemedienrechtlich sind die Anbieter sozialer Netzwerke als Host-Service-Provider einzustufen, da sie die Inhalte und Informationen ihrer Nutzer auf ihren Servern speichern und diese zur Verfügung stellen (vgl. Hilgendorf und Valerius 2012: 58, Rn. 180). Andere Host-Provider, insbesondere solche, die zur Individualkommunikation genutzt werden, sind von den Regelungen des NetzDG ausgenommen. Hierzu zählen beispielsweise E-Mail- und Messenger-Dienstanbieter.

[75] Aus dem Tatbestandskatalog können für die politisch motivierte Hasskriminalität im Internet die §§ 86, 86a, 91, 100a, 111, 126, 130, 131, 140, 166, 185-187 und 241 StGB relevant sein.

nungswidrigkeiten darstellen, die mit bis zu fünf Millionen Euro bußgeldbewährt sind.

Telemedienrechtlich sind Unterschiede zwischen den Regelungen des TMG und des NetzDG festzustellen. Nach § 10 TMG sind Host-Provider für die Inhalte ihrer Nutzer nicht verantwortlich, sofern sie keine Kenntnis von rechtswidrigen Handlungen oder Informationen haben[76] und diese Privilegierung besteht fort, sofern der Provider tätig wird, um entsprechende Inhalte im Falle einer Kenntniserlangung zu entfernen oder den Zugang hierzu zu sperren.[77] § 7 Abs. 2 TMG sieht für Host-Provider explizit keine Überwachungs- oder Prüfpflicht auf rechtswidrige Tätigkeiten in Zusammenhang mit den übermittelten oder gespeicherten Informationen vor, zumal der Gesetzgeber keine Garantenstellung der Provider begründen wollte (vgl. BT-Drs. 14/6098, S. 37; BT-Drs. 16/3078, S. 15). Dies steht einer bußgeld- oder strafrechtlichen Verantwortung der Anbieter aufgrund von Unterlassungsdelikten gem. § 8 Gesetz über Ordnungswidrigkeiten (OWiG) und § 13 StGB entgegen. Die in § 3 Abs. 2 Nr. 1 NetzDG statuierte Prüfpflicht steht zunächst im Widerspruch zu der in § 7 Abs. 2 TMG nicht vorgesehenen proaktiven Kontrolle (vgl. Altenhain 2019: § 7 TMG, Rn. 6) und sie kann zudem eine Kenntnis gem. § 10 TMG begründen, was vor dem Hintergrund des Konzepts des TMG mit einer beschränkten strafrechtlichen Verantwortung der Host-Provider und der Gefahr, dass eine solche quasi als Nebenwirkung durch das NetzDG entsteht, problematisch erscheint.

In der Literatur werden verschiedene verfassungsrechtliche Einwände gegen das NetzDG geäußert (vgl. nur Liesching 2018: 26 ff.), von welchen drei exemplifizierend dargestellt werden: Erstens werden aufgrund des Umstandes, dass die Normadressaten gem. § 1 Abs. 2 NetzDG auf soziale Netzwerke mit mehr als zwei Millionen registrierten Nutzern im Inland beschränkt und kleinere Netzwerke sowie solche ohne Registrierungsmöglichkeit nicht umfasst sind, Bedenken in Bezug auf das Gleichheitsgebot erhoben, wobei die Zahl der Nutzer als sachlicher Anknüpfungspunkt folglich abgelehnt wird (vgl.

[76] Erforderlich ist eine positive Kenntnis über die Fundstelle des Inhalts und der Rechtswidrigkeit (vgl. Hilgendorf und Valerius 2012: 64, Rn. 208; BT-Drs. 14/6098, S. 25).

[77] Das Tätigwerden des Providers meint hierbei den ernsthaften Versuch, weshalb der tatsächliche Erfolg der Entfernung oder Sperrung zur Aufrechterhaltung der Privilegierung nicht erforderlich ist (vgl. Hilgendorf und Valerius 2012: 64, Rn. 207 m. w. N.).

ebd.: 28). Zweitens bestehen in Bezug auf die Kernthemen des NetzDG - die Prüfpflicht der Anbieter zu rechtswidrigen Inhalten, der Umgang mit den Beschwerden sowie das Beschwerdeverfahren - Zweifel hinsichtlich des rechtsstaatlichen Gebots der Normenklarheit im Allgemeinen und aufgrund der bestehenden Bußgeldvorschriften hinsichtlich des gem. Art. 103 Abs. 2 GG und § 3 OWiG strengeren Maßstabs hinsichtlich des Bestimmtheitsgebots[78]. Hierzu wird ausgeführt, dass unklar sei, ob sich die Prüfpflicht der Telemediendienstanbieter nur auf die objektiven Tatobjektsmerkmale in Form des Inhalts erstrecke oder ob kumulativ oder alternativ weitere Aspekte, wie die konkrete Tathandlung, der Vorsatz, die Sozialadäquanzklauseln[79] sowie die Geltung des deutschen Strafrechts, zu prüfen seien (vgl. Liesching 2018: 26 f.). Drittens wird angeführt, dass das NetzDG ungerechtfertigte Eingriffe in die Meinungs- und Informationsfreiheit aus Art. 5 GG verursache.[80] Da das NetzDG Bußgelder in Zusammenhang mit den Verpflichtungen der Normadressaten vorsieht, würde die Wahrscheinlichkeit gefördert, dass es auf Beschwerden vielfach zur Löschung oder Sperrung eigentlich legitimer Kommunikationsinhalte komme (vgl. ebd.: 27). Der Gesetzgeber wollte einen solchen Effekt explizit vermeiden (vgl. BT-Drs. 18/12356, S. 23), jedoch würde das System mit der Tendenz zur Löschung durch ökonomische Risikoabwägungen hervorgerufen, da personal- und kostenintensive inhaltliche Prüfungen, öffentlichkeitswirksame Aufsichtsmaßnahmen mit Imageschäden sowie

[78] Der Gesetzgeber ist hiernach verpflichtet, die Voraussetzungen für eine Strafbarkeit „so konkret zu umschreiben, daß [sic!] Tragweite und Anwendungsbereich […] zu erkennen sind und sich durch Auslegung ermitteln lassen“ (BVerfGE 25, 269, 285, stRspr. seither), sodass „der Einzelne die Möglichkeit hat, das durch die Strafnorm ausgesprochene Verbot eines bestimmten Verhaltens zu erkennen und die staatliche Sanktion im Falle der Übertretung vorherzusehen“ (BVerfGE 87, 363, 391).

[79] Die Strafnormen des Deliktskatalogs in § 1 Abs. 3 NetzDG enthalten solche in §§ 86 Abs. 3, 86a Abs. 3, 91 Abs. 2 Nr. 1, 130 Abs. 7, 131 Abs. 2 StGB.

[80] Die mit Verstößen gegen Nutzungsbedingungen begründete, durch Nutzer jedoch auf das NetzDG zurückgeführte Löschung von Inhalten und zumindest zeitweise Sperrung von Nutzerprofilen führte bereits zu einer Verfassungsbeschwerde. Diese wurde durch das Bundesverfassungsgericht mit der Begründung nicht zur Entscheidung genommen, dass es an der gegenwärtigen Selbstbetroffenheit gefehlt habe und der fachgerichtliche Rechtsweg nicht ausgeschöpft worden sei, über welchen inzidenter auch die Überprüfung der Verfassungsmäßigkeit des NetzDG habe veranlasst werden können (vgl. BVerfG, Nichtannahmebeschluss vom 23.04.2019, Az. 1 BvR 2314/18). Neben weiteren Verfassungsbeschwerden nach Art. 93 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG kommen zur Überprüfung der Verfassungsmäßigkeit des NetzDG gem. Art. 100 Abs. 1 GG, § 80 Abs. 1 BVerfGG ein Vorlageverfahren eines Gerichts sowie nach Art. 93 Abs. 1 Nr. 2 GG, § 76 Abs. 1 BVerfGG oder Art. 93 Abs. 1 Nr. 2a GG, § 76 Abs. 2 BVerfGG ein Normenkontrollverfahren in Betracht.

potentielle Bußgeldzahlungen lediglich geringen wirtschaftlichen Folgen bei unberechtigten Löschungen gegenüberstehen (vgl. Liesching 2018: 27). Zudem könne sich der Anbieter bei Kritik an der Löschpraxis auf die Regelungen des NetzDG und den Gesetzgeber berufen (vgl. ebd.: 30).

Halbjahr	Inhalte	Facebook	Twitter	YouTube	Google+	Instagram
1/2018	gemeldet	1.704	264.818	214.827	2.769	-
	gelöscht	362	28.645	58.297	1.277	-
2/2018	gemeldet	1.048	256.462	250.957	2.835	-
	gelöscht	369	23.165	54.644	1.502	-
1/2019	gemeldet	1.050	503.464	304.425	547	252
	gelöscht	349	46.702	71.168	285	116
2/2019	gemeldet	4.274	843.527	277.478	-	468
	gelöscht	1.043	137.171	71.907	-	221
1/2020	gemeldet	6.038	765.715	388.824	-	3.458
	gelöscht	2.308	122.302	90.814	-	1.067
2/2020	gemeldet	4.401	811.469	323.792	-	5.570
	gelöscht	1.276	118.797	73.477	-	884

Abbildung 5: Daten ausgewählter Transparenzberichte von Telemediendienstanbietern

Die Transparenzberichte ausgewählter Dienstanbieter (vgl. Facebook 2018; 2019; 2019a; 2020a; 2020b; 2021; Twitter 2018; 2019; 2019a; 2020a; 2020b; 2021; Google 2018; 2018a; 2019; 2019a; 2019b; 2019c; 2020a; 2020b; 2021; Instagram 2019; 2020; 2020a; 2021) machen, bezogen auf die Meldung-Löschung-Relation, in quantitativer Hinsicht zumindest deutlich, dass eine inhaltliche Befassung und Prüfung für eine Entscheidung über die Löschung oder Sperrung eines Inhalts stattfindet, wobei die Berichterstattung keine qualitative Aussage zu den gelöschten Inhalten zulässt. Im Längsvergleich ist tendenziell sowohl eine Zunahme der gemeldeten, als auch der gelöschten und gesperrten Inhalte festzustellen. Der Quervergleich der Dienstanbieter ist nicht aussagekräftig, da die Anzahl der gemeldeten Inhalte stark voneinander abweicht und die zugrunde gelegten Bewertungsmaßstäbe unklar sind.

Im Hinblick auf die kriminologischen Implikationen (vgl. Kapitel 3.5) ist zunächst festzuhalten, dass das NetzDG in dieser Form nicht die Verbreitung und Kenntnisnahme entsprechender Inhalte verhindert und ihrer großen Reichweite nicht entgegenwirkt. Aufgrund der Normadressaten aus § 1 Abs.1 NetzDG bleibt es zudem auf den Bereich sozialer Netzwerke beschränkt und erfasst solche gem. § 1 Abs. 2 NetzDG auch erst ab einer Zahl von zwei Millionen Nutzern im Inland, sodass weite Teile des Internets von den Regelungen nicht erfasst werden. Die dargestellten Prüf- und Löschpflichten der An-

bieter sorgen weiterhin nicht für eine staatliche Intervention und Sanktionierung von Rechtsverstößen und die bloße Löschung oder Sperrung von Inhalten bewirkt die kriminologisch indizierte soziale Sichtbarkeit des Rechtsstaats im Internet und der Reaktionen auf Normverletzungen nicht. Im Ergebnis bleibt die Verdeutlichung der Gültigkeit von Normen sowie der Existenz und Funktionsfähigkeit von Schutzmechanismen im virtuellen Raum aus. Die Regelungen zielen vielmehr auf eine Selbstregulierung durch die Anbieter der verpflichteten sozialen Netzwerke und die Verwaltung von politisch motivierter Hasskriminalität im Internet (vgl. Ceffinato 2020: 560 f.). Das NetzDG steht hiermit im Widerspruch zu seinen Prämissen der Notwendigkeit einer effektiven Bekämpfung und Verfolgung des Phänomens sowie einer verbesserten Rechtsdurchsetzung in sozialen Netzwerken aufgrund der „große[n] Gefahr für das friedliche Zusammenleben einer freien, offenen und demokratischen Gesellschaft (BT-Drs. 18/12356, S. 1). Das NetzDG bestätigt jedoch die zunehmende Bedeutung neuer Formen der sozialen Kontrolle (vgl. Fn. 69), da es die formelle Sozialkontrolle in sozialen Medien an private Wirtschaftsunternehmen delegiert (vgl. Singelnstein 2018: 736).[81]

Bezogen auf die kriminalistischen Implikationen sind zwar gem. § 3 Abs. 2 Nr. 4 NetzDG eine Sicherung inkriminierter Inhalte zu Beweiszwecken sowie gem. § 5 Abs. 2 NetzDG eine Stelle für Auskunftsersuchen von Strafverfolgungsbehörden vorgesehen. Eine Verpflichtung zur Übermittlung dieser Inhalte an die Strafverfolgungsbehörden gibt es jedoch nicht, sodass die Einleitung eines strafrechtlichen Ermittlungsverfahrens weiterhin vor allem von einer Anzeigenerstattung abhängig ist. In Ermangelung einer Verpflichtung der Dienstanbieter zur Speicherung der dazugehörigen Bestands- und Nutzungsdaten sowie aufgrund einer nicht existenten Vorratsdatenspeicherung,[82] liegen die ermittlungsrelevanten Verkehrsdaten (vgl. Fn. 50) zudem

[81] Diesen fallen ohnehin bereits weitreichende Kompetenzen zum Umgang mit der Meinungsfreiheit zu. Während das NetzDG in Deutschland zwar dafür sorgt, dass gemeldete Inhalte zur Leugnung des Holocaust gelöscht oder der Zugang zu ihnen gesperrt wird, entscheiden die Anbieter in Bezug auf die Gesamtheit des Internets. So legte der Anbieter Facebook erst im Jahr 2020 fest, die Einstellung dieser Inhalte auf der Plattform weltweit zu unterbinden (vgl. Zeit online 2020).

[82] Die nach derzeitiger Rechtslage vorgesehene Vorratsdatenspeicherung wurde infolge einer Entscheidung des Oberverwaltungsgerichts (OVG) des Landes Nordrhein-Westfalen (vgl. Beschluss vom 22. Juni 2017, Az. 13 B 238/17) aufgrund der Unvereinbarkeit mit dem Recht der Europäischen Union (vgl. EuGH, Urteil vom 21. Dezember 2016, Az. C-203/15 und C-698/15) von der Bundesnetzagentur ausgesetzt. Nach neuester Unions-

regelmäßig nach bereits kurzer Zeit nicht mehr vor. Der Ansatz des NetzDG greift also auch aus kriminalistischer Perspektive zu kurz.

5.2 Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

Der von den Fraktionen der CDU/CSU und SPD in das legislative Verfahren eingebrachte Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (vgl. BT-Drs. 19/17741) wurde im Juni 2020 auf Empfehlung des Rechtsausschusses (vgl. BT-Drs. 19/20163) durch den Bundestag beschlossen.[83] Materiell-strafrechtlich erfolgten hierdurch die Konkretisierung von Grundsätzen der Strafzumessung, eine Anpassung von Straftatbeständen für „eine effektive Strafverfolgung insbesondere von Hasskriminalität mit rechtsextremistischem Hintergrund, nicht nur, aber gerade auch bei Tatbegehungen im Internet“ (vgl. BT-Drs. 19/17741, S. 1) sowie die Verschärfung von Strafandrohungen. Strafverfahrensrechtlich wurden Änderungen der StPO, des Bundeskriminalamtgesetzes (BKAG) und des TMG vorgenommen, um die bestehenden Regelungen der Bestands- und Verkehrsdatenerhebung gegenüber Telekommunikationsdienstanbietern auch auf Telemediendienstanbieter auszurichten. Zudem wurde in das NetzDG eine Meldepflicht für die nach dieser Norm verpflichteten Dienstanbieter bezogen auf bestimmte, strafrechtlich relevante Inhalte implementiert. Die Gesetzesinitiative ist nicht unwesentlich auf die beiden hier genutzten Fallvignetten zurückzuführen, da diese unter den Ausführungen zur Notwendigkeit der Regelungen explizit genannt werden. Hierbei wird neben der Verrohung der Kommunikation im Internet und ihrer einschüchternden Wirkung auf das Risiko Bezug genommen, „dass öffentlich ausgesprochene Drohungen dazu beitragen, dass die Hemmschwelle zur Tatausführung beim Verfasser des Inhalts oder bei Dritten, die die Drohung wahrnehmen, sinkt“ (BT-Drs.

---

rechtsprechung sind unter strengen Voraussetzungen und Garantien „[a]ngesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte[...] neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen“ (EuGH, Urteil vom 6. Oktober 2020, Az. C-511/18, C-512/18 und C-520/18, Rn. 156). Ein diese Kautelen berücksichtigender nationaler Gesetzesentwurf zur Neufassung der Vorratsdatenspeicherung ist zu erwarten.

[83] Ein wortgleicher Gesetzesentwurf der Bundesregierung (vgl. BT-Drs. 19/18470) wurde hierdurch für erledigt erklärt.

19/17741, S. 15). Die für die politisch motivierte Hasskriminalität im Internet wesentlichen Neuerungen werden nachfolgend analysiert.

5.2.1 Änderungen des Strafgesetzbuchs

Durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität werden die Strafzumessungsgrundsätze des § 46 Abs. 2 StGB um antisemitische Bewegründe erweitert. Auf der Rechtsfolgenseite erscheinen eine vereinfachte Subsumtion antisemitisch motivierter Straftaten[84] und hierdurch eine Strafverschärfung möglich. Es ist jedoch zu berücksichtigen, dass eine solche Erweiterung des Katalogs strafschärfender Umstände nach umfassender Prüfung „weder grammatisch, systematisch, historisch-genetisch noch teleologisch erforderlich [ist]“ (Gerson 2020: 36), da entsprechende Beweggründe bereits unter den genannten Tatmotiven des § 46 StGB erfasst sind. Die Erweiterung ist, da sie keine Strafbarkeitslücke schließt, nicht nur redundant, sondern zudem auch selektiv, da sie lediglich eine von vorurteilsgeleiteten Straftaten geschädigte Personengruppe herausstellt (vgl. ebd.: 37). Bedenkt man weiterhin, dass bereits die explizite Aufnahme rassistischer, fremdenfeindlicher oder sonstiger menschenverachtender Beweggründe in den § 46 StGB[85] im Jahr 2015 von der Bundesregierung als Maßnahme mit vorrangig symbolischem Charakter beschrieben wurde (vgl. BT-Drs. 17/9345, S. 7), drängt sich hier der Verdacht einer symbolischen Kriminalpolitik auf. Durch dieses Wertbekenntnis beabsichtigt der Gesetzgeber, im Sinne einer positiven Generalprävention auf das allgemeine Rechtsbewusstsein einzuwirken und perhorresziert hierdurch entsprechende Tatmotive (vgl. Roxin und Greco 2020: 46, Rn. 37 f.), wie sie beispielsweise bei der Fallvignette Halle zugrunde lagen. Bemisst man „Legitimität und Illegitimität ‚symbolischer’ Gesetzgebungstendenzen [entlang der Frage], ob eine Vorschrift neben ihren bewusstseinsbildenden Zielen und der bekenntnishaften Demonstration von Werthaltungen auch zum realen Schutz eines friedlichen Zusammenlebens wirklich nötig ist“ (ebd.: 46, Rn. 39), ist die explizite Aufnahme antisemitischer Beweggründe in den Katalog des § 46

[84] Dies war Zielsetzung des Gesetzgebers, da es sich um eine „Klarstellung und Bekräftigung der bereits jetzt geltenden Rechtslage“ (BT-Drs. 19/17741, S. 18) handelt.

[85] Die Aufnahme erfolgte durch das Gesetz zur Umsetzung von Empfehlungen des NSU-Untersuchungsausschusses des Deutschen Bundestages, veröffentlicht im Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 23, ausgegeben zu Bonn am 19. Juni 2015, S. 925.

Abs. 2 StGB abzulehnen, da hierdurch nicht „mit Änderungen der Rechtsprechung im Rahmen der Strafzumessungspraxis [...] zu rechnen ist“ (Schiemann 2020: 271).

Weiterhin werden durch das Gesetz mehrere Äußerungsdelikte und in Teilen deren Strafandrohungen angepasst. Die kriminalistische Bedeutung dieser Änderungen kann damit zusammengefasst werden, dass die Ausweitung der Tatbestände grundsätzlich zu einer steigenden Anzahl von Ermittlungsverfahren führen wird.

Der Katalog des § 126 Abs. 1 StGB wird durch die Androhung von Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 177 Absatz 4 bis 8 oder des § 178 sowie die gefährliche Körperverletzung gem. § 224 StGB erweitert. Während die erstgenannten Straftaten zum bisherigen Deliktskatalog von Verbrechenstatbeständen passen, führt die Aufnahme der gefährlichen Körperverletzung als Vergehen zu einem Bruch in diesem System. Die Ausweitung wird kritisiert, da bezweifelt wird, dass Ankündigungen von Straftaten mittlerer Kriminalität das öffentliche Gewaltmonopol in Frage stellen (vgl. Schiemann 2020: 272). Da kumulativ zur Katalogtat die Eignung zur Friedensstörung erforderlich ist (vgl. Fischer 2020: § 126 StGB, Rn. 9), wird von einer geringen praktischen Bedeutung ausgegangen, jedoch werden weitere Maßnahmen nach dem NetzDG hervorgerufen und die Eingriffsschwelle für Ermittlungen im Internet gesenkt (vgl. Bundesrechtsanwaltskammer 2020: 7).

Die Billigung von Straftaten gem. § 140 StGB erstreckt sich durch die Novellierung nicht mehr wie bisher auf bereits begangene oder strafbar versuchte Taten, sondern wird unabhängig von einer konkreten Tatbegehung in das Vorfeld verlagert, während sich die Belohnung nach wie vor auf eine begangene oder strafbar versuchte Tat beziehen muss. Nach Auffassung des Gesetzgebers soll in Bezug auf die Tatbegehungsweise der Billigung bereits die Zustimmung oder das Gutheißen einer entsprechenden Tat genügen, „wenn der Täter die Katalogtat in ihren wesentlichen Merkmalen umreißt, ohne die Einzelheiten der Katalogtat zu kennen“ (BT-Drs. 19/17741, S. 34). An der Vorverlagerung wird kritisiert, dass das Problem eines bereits konturlosen Tatbestands hinsichtlich der tatbestandlichen Unbestimmtheit und Weite ver-

schärft würde und die vagen Anforderungen eine Eignung zur Störung des öffentlichen Friedens nicht begründen würden (vgl. Schiemann 2020: 272 f.).

Weitere Änderungen betreffen die Ehrverletzungsdelikte. So wird die Strafandrohung der Beleidigung gem. § 185 StGB erhöht, sofern diese öffentlich, in einer Versammlung oder durch das Verbreiten von Schriften[86] begangen wird. Während diese Taten bislang mit einer Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bedroht waren, besteht forthin ein Strafrahmen einer Freiheitsstrafe bis zu zwei Jahren oder eine Geldstrafe. Die Üble Nachrede und Verleumdung gegen Personen des politischen Lebens gem. § 188 StGB wird um das Delikt der Beleidigung ergänzt und für die enthaltenen Tatbegehungsweisen wird die Strafandrohung erhöht. Zudem wird ergänzt, dass sich das politische Leben des Volkes bis auf die kommunale Ebene erstreckt. Ferner wird das absolute Strafantragserfordernis des § 194 StGB relativiert, sodass ein Strafantrag für Taten nach § 188 StGB nicht erforderlich ist, wenn die Strafverfolgungsbehörde ein öffentliches Interesse bejaht. Die Änderungen tragen den aktuellen Entwicklungen, insbesondere belegt durch die Fallvignette Lübcke, Rechnung und gewichten den größeren Unrechtsgehalt dieser Delikte im virtuellen Raum stärker. Eine Fokussierung auf Rechtsextremismus und Hasskriminalität erfolgt jedoch nicht, denn das Gesetz spricht in dieser Ausgestaltung „privaten, aber in einem öffentlichen Forum ausgetragenen ehrverletzenden Auseinandersetzungen unter Nachbarn oder Kollegen einen ebenso unterschiedslos erhöhten Unrechtsgehalt zu[,] wie zutiefst rassistischen Äußerungen auf einer Webseite gegen ein nur aufgrund seiner Zugehörigkeit zu einer vom Täter verhassten Gruppe ausgewähltes Opfer“ (Valerius 2020: 688 f.).

Schließlich wird die Bedrohung gem. § 241 StGB in einem neuen Abs. 1 dahingehend ergänzt, dass nunmehr auch die Drohung mit einer Straftat gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert ausreicht. Er-

[86] Vor dem Hintergrund der Weiterentwicklung des Schriftenbegriffs zu einem Inhaltsbegriff in § 11 Abs. 3 StGB (vgl. Kapitel 2.2.2) ist eine Anpassung dieser Formulierung über den Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 (vgl. BT-Drs. 19/25294, S. 31) vorgesehen. Vertiefend zu diesem Gesetzentwurf siehe Kapitel 5.2.3.

folgt die Tathandlung öffentlich, in einer Versammlung oder durch das Verbreiten von Schriften[87] besteht für Taten nach dem neuen Abs. 1 die Strafandrohung von bis zu zwei Jahren Freiheitsstrafe oder einer Geldstrafe und in den Fällen der neuen Absätze zwei und drei, welche die bisherige Bedrohung mit einem Verbrechen und die Drohung wider besseres Wissen beinhalten, nunmehr eine erhöhte Strafandrohung von bis zu drei Jahren Freiheitsstrafe oder einer Geldstrafe. Wie bei § 126 StGB wird die Ausweitung auf Straftaten der mittleren Kriminalität kritisiert (vgl. Schiemann 2020: 275), jedoch enthält zumindest Abs. 1 keine im Mindestmaß erhöhte Strafandrohung und auch die Qualifizierung durch eine Tatbegehung, die öffentlich oder durch das Verbreiten von Inhalten erfolgt, enthält entsprechende Abstufungen. Ein Bezug zu Rechtsextremismus und Hasskriminalität muss jedoch nicht zwingend gegeben sein.

5.2.2 Änderungen des NetzDG

In einem neuen § 1 Abs. 4 NetzDG wird zunächst definiert, dass es sich um Beschwerden im Sinne des Gesetzes handelt, wenn ein Inhalt beanstandet und die Entfernung des Inhalts oder die Sperrung des Zugangs hierzu begehrt wird, es sei denn, es wird mit der Beanstandung erkennbar nicht geltend gemacht, dass ein rechtswidriger Inhalt vorliegt.

Die bereits bestehende Informationspflicht nach § 3 Abs. 2 Nr. 5 NetzDG wird in Bezug auf den Beschwerdeführer um eine Hinweispflicht auf die Möglichkeit einer Strafanzeige, einen gegebenenfalls erforderlichen Strafantrag sowie auf Internetseiten mit weiteren Informationen hierzu erweitert.

Als zentrale Maßnahme des Gesetzes wird für die verpflichteten Dienstanbieter durch einen neuen § 3a NetzDG eine Meldepflicht an das BKA statuiert. Die Meldepflicht bezieht sich nach § 3a Abs. 2 NetzDG auf Inhalte, die dem Anbieter als Beschwerde über rechtswidrige Inhalte gemeldet und daraufhin entfernt wurden oder deren Zugang gesperrt wurde, sofern konkrete Anhaltspunkte vorliegen, dass der Tatbestand eines vorgegebenen Delikts-

[87] Vor dem Hintergrund der Weiterentwicklung des Schriftenbegriffs zu einem Inhaltsbegriff in § 11 Abs. 3 StGB (vgl. Kapitel 2.2.2) ist eine Anpassung dieser Formulierung über den Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 (vgl. BT-Drs. 19/25294, S. 31) vorgesehen. Vertiefend zu diesem Gesetzentwurf siehe Kapitel 5.2.3.

katalogs erfüllt ist.[88] Sie umfasst nach § 3a Abs. 4 NetzDG neben dem Inhalt auch die IP-Adresse und Portnummer des Nutzers. Die Übermittlung an das BKA hat gem. § 3a Abs. 3 NetzDG unverzüglich nach Prüfung durch den Dienstanbieter zu erfolgen. Nach § 3a Abs. 6 NetzDG informiert der Dienstanbieter den Nutzer nach Ablauf von vier Wochen über diese Maßnahme, sofern das BKA in diesem Zeitraum keine Zurückstellung anordnet.

Im Hinblick auf die kriminologischen Implikationen bestehen die Aspekte der weiten Verbreitung und großen Reichweite entsprechender Inhalte, die fehlende soziale Sichtbarkeit des Rechtsstaats im Internet und der Reaktionen auf Normverletzungen fort und der beschränkte Kreis der verpflichteten Dienstanbieter sorgt dafür, dass weite Teile des virtuellen Raums nicht berücksichtigt werden. Die Wirkung der Hinweispflicht auf die strafrechtlichen Möglichkeiten ändert in Bezug auf die Sichtbarkeit des Rechtsstaats nichts, da der Hinweis erst nach einer nutzerseitigen Beschwerde erfolgt. Unter den Voraussetzungen des § 3a NetzDG wird lediglich bei Vorliegen der beschriebenen Voraussetzungen eine staatliche Intervention und Sanktionierung ermöglicht. Zumindest in Teilbereichen erfolgt hierdurch die Rückkehr einer staatlichen Verantwortlichkeit im Umgang mit rechtswidrigen Handlungen im Internet.

Vor dem Hintergrund der kriminalistischen Implikationen kann festgestellt werden, dass mit der Meldung an das BKA, der dortigen Einrichtung einer Zentralstelle zur Erstbewertung, Prüfung der strafrechtlichen Relevanz, Durchführung erster Schritte zur Erhebung von Bestands- und Nutzungsdaten sowie der Übermittlung an die zuständige Strafverfolgungsbehörde (vgl. BT-Drs. 19/17741, S. 16) Grundzüge einer Aufbau- und Ablauforganisation (vgl. Kapitel 4.2) beschrieben werden. Hierdurch wird nur die Bearbeitung solcher Verfahren an die Länder übertragen, bei welchen belastbare Ermitt-

[88] Aus dem Tatbestandskatalog können für die politisch motivierte Hasskriminalität im Internet die §§ 86, 86a, 91, 126, 130, 131 und 140 StGB sowie die Bedrohung gem. § 241 StGB relevant sein, sofern hierbei mit einem Verbrechen gegen das Leben, die sexuelle Selbstbestimmung, die körperliche Unversehrtheit oder die persönliche Freiheit gedroht wird. Hierdurch beschränkt der Gesetzgeber die Meldepflicht auf ausgewählte rechtswidrige Inhalte im Sinne des § 1 Abs. 3 NetzDG, welche nach seiner Auffassung „eine gefährliche Wirkung auf das demokratische System und die öffentliche Ordnung haben können“ (BT-Drs. 19/17741, S. 45).

lungsansätze bestehen oder beschuldigte Personen benannt werden können.

Aus kriminalistischer Perspektive greifen diese jedoch aus verschiedenen Gesichtspunkten heraus zu kurz. Beispielsweise werden Inhalte, die der Dienstanbieter ohne eine Beschwerde im Sinne des NetzDG aufgrund eines Verstoßes gegen die Nutzungsbedingungen (vgl. Facebook 2020; Twitter 2020; Google 2020) oder im Falle einer Beschwerde unter Verweis auf diese löscht oder den Zugang zu ihnen sperrt, nicht gemeldet und potentielle Straftaten verbleiben im Dunkelfeld. Der Umfang der meldepflichtigen Daten umfasst die Nutzungsdaten, jedoch nicht die Bestandsdaten. Hieran wird kritisiert, dass „die für die Zuordnung zu einem Anschluss so wichtige Portnummer [...] von den Telemediendiensten derzeit mangels gesetzlicher Verpflichtung auch nicht gespeichert [wird]“ (May 2020: 5), weshalb der Ermittlungsansatz der IP-Adressen nicht ausreichend erscheint. Auch das Auskunftsverhalten zu den von den verpflichteten Dienstanbietern im Ausland vorgehaltenen ermittlungsrelevanten Daten steht einer effektiven Strafverfolgung entgegen, da in Ermangelung einer umfassenden inhaltlichen Auskunftspflicht eine Datenerhebung auf dem langwierigen Weg der förmlichen internationalen Rechtshilfe erfolgen muss (vgl. ebd.: 7; Hartmann 2020: 13). Insgesamt steht daher zu besorgen, dass bei einer Vielzahl von Straftaten der Täter über die bestehenden Ermittlungsansätze nicht identifiziert werden kann. Für die Verfahren, bei welcher im Zuge der ersten Maßnahmen keine Identifizierung und damit Feststellung der örtlichen Zuständigkeit einer Strafverfolgungsbehörde erfolgen kann, erfolgt die weitere Befassung für diese Maßnahmen durch die ZIT bei der Generalstaatsanwaltschaft Frankfurt am Main (vgl. May 2020: 6).

Trotz dieser aus kriminalistischer Perspektive bestehenden Einschränkungen werden die Polizeien und Staatsanwaltschaften der Länder ihre Aufbau- und Ablauforganisationen im Hinblick auf eine steigende Anzahl von Ermittlungsverfahren durch Umsetzung der Meldepflicht anpassen müssen. Legt man die Zahlen der bisherigen Transparenzberichte (vgl. Kapitel 5.1) sowie die Schätzungen und Berechnungen des Deutschen Richterbundes (vgl. Spiegel 2020) und im Gesetzentwurf (vgl. BT-Drs. 19/17741, S. 25, 31; BT-Drs. 19/18470, S. 15 f.) zugrunde, ist bundesweit mit einem groben Mengenraster

zwischen 150.000 und 275.000 zusätzlichen strafrechtlichen Ermittlungsverfahren zu rechnen. Die Erwartung eines solchen zusätzlichen Arbeitsaufkommens und der Umstand, dass das Internet als Tatmittel genutzt wird, lassen zunächst eine umfassende Zentralisierung von Kompetenzen und Zuständigkeiten innerhalb der Strafverfolgungsbehörden als einen Lösungsansatz erscheinen (vgl. Hoheisel-Gruler 2020: 104 f.). In der Praxis dürften weitreichenden strukturellen Änderungen jedoch insbesondere beschränkte personelle Ressourcen gegenüberstehen, sodass im Regelfall von einer Bearbeitung im Rahmen bisheriger deliktischer Zuständigkeiten auszugehen sein wird.

Weiterhin stellt neben der frühzeitigen Erkennung von Gefahrenüberhängen zur umgehenden Intervention sicherlich die Identifizierung von identischen Meldungen zur Vermeidung einer Doppelbefassung eine wesentliche Herausforderung dar. Hierdurch spielen die Implementierung einer Zentraldatenbank und das Einsatzgebiet automatisierter Detektionsverfahren (vgl. Kapitel 4.3) eine wesentliche Rolle.

5.2.3 Strafverfahrensrechtliche Änderungen

Wie bereits ausgeführt, werden durch das Gesetz die Auskunftspflichten zu Bestands- und Nutzungsdaten in der StPO, dem TMG und dem BKAG auf die Telemediendienstanbieter ausgerichtet (vgl. Wissenschaftliche Dienste Deutscher Bundestag 2020: 12 ff.). Hierzu werden zunächst die Vorschrift des § 100g StPO um die Erhebung von Nutzungsdaten ergänzt und die Vorschrift des § 100j StPO im Hinblick auf die Reglungen zur Bestandsdatenauskunft des TMG abgestimmt. Das Auskunftsverfahren zu Bestands- und Nutzungsdaten wird im TMG in einem neu eingefügten § 15a geregelt und der ebenfalls neu eingefügte § 15b TMG regelt das Auskunftsverfahren zu Passwörtern und anderen Zugangsdaten. Zudem erfolgt eine entsprechende Anpassung des BKAG zur Wahrnehmung der dortigen Zentralstellenfunktion (vgl. Kapitel 5.2.2).

Aus kriminalistischer Perspektive handelt es sich zunächst um eine Harmonisierung der strafverfahrensrechtlichen Auskunftsbefugnisse gegenüber Telekommunikations- und Telemediendienstanbietern. Diese weitergehenden Möglichkeiten bewirken eine Zunahme der Ermittlungsansätze und der Aus-

kunftsersuchen an die Dienstanbieter und haben hierüber einen kriminalistischen Mehrwert.

Problematische Auswirkungen auf das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität hatte ein Beschluss des BVerfG vom 27. Mai 2020 (vgl. Az. 1 BvR 1873/13 sowie 1 BvR 2618/13). Mit dieser Entscheidung wurden die manuelle Bestandsdatenauskunft gem. § 113 TKG sowie die Entsprechungen in verschiedenen Fachgesetzen des Bundes für zu weit gehend und damit verfassungswidrig erklärt.[89] Im Sinne des Doppeltürenmodells (vgl. Fn. 49) muss bereits die Übermittlungsbefugnis die Zweckbindung, die tatbestandliche Eingriffsschwelle und einen hinreichend gewichtigen Rechtsgüterschutz im Hinblick auf verfassungsrechtliche Anforderungen begrenzen (vgl. BVerfG, Beschluss vom 27. Mai 2020, Az. 1 BvR 1873/13 sowie 1 BvR 2618/13, Rn. 130). Die Verfassungswidrigkeit der bisherigen Regelungen begründet sich in der Unverhältnismäßigkeit der Übermittlungsbefugnis, welche keine begrenzenden Eingriffsschwellen im Sinne eines auf tatsächliche Anhaltspunkte gestützten Eingriffsanlass enthält (vgl. ebd., Rn. 144 f.). Für die allgemeine Bestandsdatenauskunft nach § 113 Abs. 1 S. 1 TKG ist für die Gefahrenabwehr eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht erforderlich (vgl. ebd., Rn. 146). Der individualisierten Zuordnung einer dynamischen IP-Adresse als qualifizierte Bestandsdatenauskunft gem. § 113 Abs. 1 S. 3 TKG kommt ein erhöhtes Eingriffsgewicht zu, weshalb diese einem Rechtsgüterschutz von hervorgehobenen Gewicht dienen muss, wozu auch die durch das Strafrecht geschützten Rechtsgüter zählen (vgl. ebd., Rn. 175, 178). Im Ergebnis ist nicht nur eine Anpassung der bestehenden und nunmehr für verfassungswidrig erklärten Regelungen erforderlich, sondern auch eine Folgewirkung auf das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität festzustellen. Denn dort wurde die Bestandsdatenauskunft zu Telemediendaten gemessen an der Entscheidung des BVerfG gleichsam unzureichend geregelt, weshalb evidente verfassungsrechtliche Bedenken an diesem Gesetz bestehen (vgl. Wissenschaftliche Dienste Deutscher Bundestag 2020: 28 ff.; Bäcker 2020: 3 ff.), die wiederum dazu führten, dass eine Ausfertigung des

[89] Vertiefend siehe Bundesverfassungsgericht 2020a. Zu dem Umstand, dass der Beschluss zunächst keine Auswirkungen auf die Verfolgung von Straftaten hat, vgl. Krause 2020.

Gesetzes durch den Bundespräsidenten bislang nicht erfolgte. Die Fraktionen der CDU/CSU und SPD haben am 15. Dezember 2020 den Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 (vgl. BT-Drs. 19/25294) vorgelegt. Hiermit soll eine Novellierung der Übermittlungsbefugnisse im TKG und TMG sowie der Abrufbefugnisse in der StPO und der Entsprechungen in verschiedenen Fachgesetzen des Bundes zur manuellen Bestandsdatenauskunft zur Harmonisierung dieser Regelungen an die Vorgaben des BVerfG erfolgen. Ausweislich des stenografischen Berichts zur 206. Sitzung des Deutschen Bundestags wurde der Gesetzentwurf am 28. Januar 2021 in der Fassung des Ausschusses für Inneres und Heimat (vgl. BT-Drs. 19/26267) mit den Stimmen der Koalitionsfraktionen angenommen (Plenarprotokoll 19/206, 25998 C – 25998 D).[90] Im Ergebnis ist eine zeitnahe, gegebenenfalls auch gemeinsame Ausfertigung beider Gesetze durch den Bundespräsidenten und eine parallele Veröffentlichung im Bundesgesetzblatt zu erwarten (vgl. Sehl 2020; Kaufmann und Suliak 2020). Ein solches Vorgehen erscheint zumindest ungewöhnlich und der weitere Verlauf bleibt im Hinblick auf die bisherige Qualität bei der inhaltlichen Ausgestaltung abzuwarten.

5.3 Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes

Mit diesem von der Bundesregierung eingebrachten Gesetzentwurf (vgl. BT-Drs. 19/18792) sind Modifizierungen des NetzDG vorgesehen, deren wesentlicher Regelungsgehalt nachfolgend kursorisch betrachtet wird.

Die Berichtspflichten der Dienstanbieter in § 2 Abs. 2 NetzDG sollen um Informationen über den Einsatz von automatisierten Detektionsverfahren sowie die technischen und wissenschaftlichen Hintergründe dieser Maßnahmen ergänzt werden. Ferner erfolgen Konkretisierungen zu den Berichtspflichten der Prüfverfahren und zum Umgang mit Nutzerbeschwerden, um den Informationsgehalt und die Vergleichbarkeit der Transparenzberichte zu erhöhen (vgl. ebd., S. 2).

[90] In diesem Zusammenhang wurde der Antrag der Fraktion Bündnis 90 / Die Grünen abgelehnt, das Gesetz zur Bekämpfung von Rechtsextremismus und Hasskriminalität unverzüglich verfassungskonform auszugestalten (vgl. BT-Drs. 19/22888).

Die Nutzerrechte von Beschwerdeführern sollen gestärkt werden, indem das in § 3 Abs. 1 NetzDG statuierte Verfahren zur Übermittlung von Beschwerden über rechtswidrige Inhalte durch eine verbesserte Erkennbarkeit und leichtere Bedienbarkeit nutzerfreundlicher gestaltet werden soll und Nutzer über eine Erweiterung des § 3 Abs. 2 NetzDG weitreichendere Informationen zum Verfahren und ihren Möglichkeiten erhalten sollen. Durch die Integrierung eines Gegenvorstellungsverfahrens gegen die Entfernung von Inhalten oder die Sperrung ihres Zugangs in einem neuen § 3b NetzDG sollen die Rechte von betroffenen Nutzern zum Schutz vor unberechtigten Löschungen oder Sperrungen gestärkt werden.

Über den Gesetzentwurf wird weiterhin der Kreis der verpflichteten Dienstanbieter erweitert, indem zur Umsetzung europarechtlicher Vorgaben[91] über die §§ 3d ff. NetzDG Videosharingplattform-Dienste in den Anwendungsbereich des NetzDG einbezogen werden sollen. Als Ausnahme von § 1 Abs. 2 NetzDG werden auch grundlegende Anforderungen an Videosharingplattform-Dienste gestellt, die im Inland weniger als zwei Millionen Nutzer haben, wenn die Bundesrepublik Deutschland das Sitzland des Anbieters ist oder sie als solches gilt. Für diese kleineren Dienstanbieter bestehen die Verpflichtungen nur, wenn aus dem Deliktskatalog des § 1 Abs. 3 NetzDG audiovisuelle Inhalte ausgewählte Tatbestände erfüllen. Bezogen auf politisch motivierte Hasskriminalität sind dies die §§ 111, 130 Absatz 1 oder 2, 131, 140 und 166 StGB. Die umfassenden Berichtspflichten des § 2 NetzDG sowie die über das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität in § 3a NetzDG vorgesehene Meldepflicht der Dienstanbieter an das BKA sind von diesen grundlegenden Anforderungen ausgenommen.

Durch die Einfügung eines § 4a NetzDG wird ferner eine Aufsichts- und Anordnungskompetenz des Bundesamts für Justiz implementiert, um festge-

[91] Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste, veröffentlicht im Amtsblatt der Europäischen Union vom 15. April 2010, L 95/1 ff. sowie Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste im Hinblick auf sich verändernde Marktgegebenheiten, veröffentlicht im Amtsblatt der Europäischen Union vom 28. November 2018, L 303/69 ff.

stellten Verstößen der verpflichteten Dienstanbieter abzuhelfen (vgl. BT-Drs. 19/18792, S. 53). In § 5 NetzDG sind zudem Klarstellungen zu den Pflichten der Zustellungsbevollmächtigen des Dienstanbieter vorgesehen.

Der Gesetzentwurf sieht vor allem eine Stärkung der Nutzerrechte, Ausweitung der Auskunftsmöglichkeiten sowie die Schärfung der staatlichen Aufsicht über die Einhaltung der Vorgaben durch die verpflichteten Dienstanbieter und Ausweitung ihrer Berichtspflichten vor. Während die vorgesehene Ausweitung des Kreises der Verpflichteten auf Videosharingplattform-Dienste eine steigende Anzahl von Ermittlungsverfahren haben dürfte, ist eine solche Steigerung vor allem auch durch eine vermehrte Anzeigenerstattung von Nutzern außerhalb der zukünftigen Meldeverpflichtungen der Dienstanbieter über den § 3a NetzDG zu erwarten.

6. Fazit

> *„Eigentlich ist ja alles ganz einfach [...]: der Traum von einer ‚Gesamten Strafrechtswissenschaft', die alle, wie im Paradies, zusammenbringt: [...] die Kriminalisten mit den Kriminologen, die Substantialisten mit den Prozeduralisten, die Theoretiker mit den Praktikern – in Friede und Fruchtbarkeit."* (Hassemer 2008: 116)

Die kriminalpolitischen Aktivitäten de lege lata und de lege ferenda sind wie folgt zusammenzufassen: Der Gesetzgeber hat sich durch die Ausgestaltung des NetzDG dazu entschieden, strafrechtlichen Inhalten im Internet und somit auch ausgewählten Delikten der politisch motivierten Hasskriminalität insbesondere durch die Inanspruchnahme der jeweiligen Dienstanbieter zu begegnen. Bezogen auf die forschungsleitende Fragestellung zu den kriminalpolitischen Aktivitäten werden diese Maßnahmen im aufgezeigten Rahmen einen Beitrag zur Bekämpfung des Phänomens leisten. Im Hinblick auf die Gesamtproblematik greift dieser Ansatz jedoch zu kurz und die konkreten Interventionsmöglichkeiten der Strafverfolgungsbehörden wurden bislang nicht zielgerichtet ausgestaltet. Die kriminologischen und kriminalistischen Implikationen wurden im jeweiligen Zwischenfazit bereits zusammengeführt und ihre Essentials herausgearbeitet. Bezieht man diese auf die legislativen Aktivitäten, ist zu bilanzieren, dass das NetzDG nur selektiv wirkt, da nur die

verpflichteten Dienstanbieter sozialer Medien sowie Videosharingplattformen vom Regelungsinhalt umfasst sind und andere Teile des Internets unberücksichtigt bleiben. Eine Strafverfolgung wird nur bei ausgewählten Tatbeständen initiiert. Die bloße Löschung eines Inhalts oder die Sperrung des Zugangs hierzu führt – selbst wenn die Voraussetzungen zur Übermittlung an das BKA gegeben sind und diese erfolgt – dazu, dass die soziale Sichtbarkeit des Rechtsstaats, welcher eine kriminoresistente Wirkung zugeschrieben wird, als wesentliches Element einer generalpräventiven Intervention ausbleibt. Diese „Abwesenheit staatlicher und damit demokratisch legitimierter Gewalt“ (Hoheisel-Gruler 2020: 92) stellt eine unüberbrückbare Schwäche des Bekämpfungsansatzes dar, da das NetzDG die Dienstanbieter zur Rechtsdurchsetzung initial in Anspruch nimmt. Und auch wenn über den Regelungsinhalt des NetzDG Ermittlungsansätze geschaffen werden, stellt dies die Strafverfolgungsbehörden vor die dargelegten, immensen Herausforderungen und es steht zu besorgen, dass diese Ermittlungsmöglichkeiten oftmals nicht zur Identifizierung und Beweisführung ausreichen (vgl. Kapitel 5.2.2).[92]

Die kriminalpolitischen Aktivitäten machen zudem deutlich, dass eine systematische Rahmung zur Bekämpfung der politisch motivierten Hasskriminalität im Internet noch nicht gefunden ist. Dies mag daran liegen, dass die entsprechende Gesetzgebung sowie entsprechende Initiativen vor allem durch jüngere Ereignisse, wie die beiden genutzten Fallvignetten, geprägt sind und Grundlagen sowie generelle Herausforderungen nachrangig berücksichtigt wurden (vgl. Valerius 2020: 687 f.). Dies betrifft bereits eine fehlende verbindliche Definition und manifestiert sich zudem in dem Umstand, dass innerhalb weniger Jahre umfassende Änderungen und Weiterentwicklungen vorgenommen wurden und solche perspektivisch auch weiterhin zu erwarten sind. Dies könnte zwar dahingehend positiv ausgelegt werden, dass erkannte Problemstellungen und Durchsetzungsdefizite zeitnah behoben werden sollen. Gegen eine solche Deutung sprechen jedoch die grundsätzlichen ver-

[92] Dies bestätigt sich in den Erfahrungen zur Fallvignette Lübcke, da bei den diesbezüglichen Ermittlungsverfahren der Anteil der identifizierten Täter durch die ZIT auf ungefähr zehn Prozent geschätzt wird (vgl. Lang 2021). Diese niedrige Quote der identifizierten, ermittelten Täter offenbart Durchsetzungsdefizite im Hinblick auf Ermittlung der verfahrensrelevanten Daten bei den Telemediendienstanbietern.

fassungsrechtlichen Einwände gegen das NetzDG (vgl. Kapitel 5.1) sowie die bisweilen mangelhafte Qualität bei der inhaltlichen Ausgestaltung spezifischer Regelungen (vgl. Kapitel 5.2.3).

Das NetzDG ist in der Literatur insbesondere auch der Kritik ausgesetzt, dass es „die staatliche Regulierung im Wesentlichen auf die Überwachung der den Unternehmen übertragenen Überwachungs- und Löschpflichten [reduziere]“ (Hoheisel-Gruler 2020: 103). Als Alternative werden eine Garantenstellung der Dienstanbieter und folglich ihre strafrechtliche Verantwortung ins Feld geführt, da sie das wesentliche Tatmittel zur Verfügung stellten, dessen Ausgestaltung als Verbreitungsmedium auch der wesentliche Faktor zur Tatbegehung sei (vgl. Ceffinato 2020: 555 ff.). Alleine zur Sicherstellung eines freien Zugangs zu den digitalen Informations- und Kommunikationsdiensten und zum Schutz der Meinungsfreiheit ist ein solcher Ansatz, der mit einer deutlich erheblicheren Gefahr einer weitreichenderen Löschung und Sperrung verbunden ist, abzulehnen. Darüber hinaus stellen abweichendes Verhalten von gesellschaftlich mehrheitlich anerkannten Normen und Werten und somit auch Verstöße gegen die geltende Rechtsordnung eine normale und ubiquitäre Erscheinung dar. Wie für die analoge Welt kann es in Bezug auf den virtuellen Raum mithin gar nicht darum gehen, die Begehung von Straftaten komplett zu verhindern. Vielmehr muss die Zielsetzung eine Regulierung von Devianz und Delinquenz auf ein Maß sein, das mit der Unsicherheitserwartung demokratischer Staaten einhergeht. Dies bekräftigt sich nicht zuletzt in dem Umstand, dass mit den Mitteln des Straf- und Strafprozessrechts stets nur Symptome und keine Ursachen bekämpft werden können.

Als legislative Maßnahmen sind der Literatur insbesondere zwei Vorschläge zur Zielerreichung zu entnehmen. Einerseits wird ein digitales Gewaltschutzgesetz[93] benannt, womit die Einführung eines zivilgerichtlichen Verfahrens zur zeitweisen oder dauerhaften Sperrung von Nutzerprofilen im Falle von rechtswidrigen Äußerungen beabsichtigt ist (vgl. Buermeyer 2019). Dieser Vorschlag sieht vor, dass bei einem noch nicht bekannten oder dauerhaft anonymen Profilinhaber der Dienstanbieter als Antragsgegner fungieren könnte, welcher den Nutzer über zu hinterlegende Kontaktdaten informieren

[93] Dieser Ansatz wird auch im spezifischen Kontext von digitaler Gewalt an Frauen thematisiert (vgl. Hecht 2020: passim).

sollte, damit dieser darüber entscheiden kann, ob er selbst in das Verfahren eintritt (vgl. ebd.). Ein solcher Ansatz erscheint unter Inanspruchnahme des gem. § 5 Abs. 2 NetzDG bereits vorgesehenen inländischen Empfangsberechtigten auch vor dem Hintergrund der territorialen Schrankenlosigkeit des Internets geeignet und praktikabel. Der elementare Unterschied zwischen der Löschung oder Sperrung eines Inhalts und eines Nutzerprofils ist die Möglichkeit der Teilhabe und damit der Gewährleistung des Grundrechts der Meinungsfreiheit. Die Entscheidung über die Sperrung eines Profils kann in einem freiheitlich demokratischen Rechtsstaat nicht ökonomisch handelnden Unternehmen überlassen werden und bedarf stattdessen einer gerichtlichen Entscheidung oder einer Entscheidung entlang staatlich legitimierter Vorgaben.[94] Im Rahmen von Strafverfahren wäre die Möglichkeit zu prüfen, auf der Rechtsfolgenseite die Einziehung von zur Tatbegehung genutzten Profilen als Tatmittel gem. § 74 Abs. 1 StGB angeordnet werden kann.

Andererseits stellt sich die Frage nach dem Umfang einer Klarnamenpflicht im digitalen Raum. Die Rechtsprechung zur Löschung oder Sperrung von Profilen im Falle der pseudonymen Nutzung wurde bereits thematisiert (vgl. Fn. 44). Auch wenn die Frage einer Verpflichtung zur Verwendung des Klarnamens höchstrichterlich noch nicht entschieden ist (vgl. OLG München, Urteil vom 8. Dezember 2020, Az. 18 U 2822/19 Pre, Rn. 90), werden bereits dieser Entscheidung weitreichende Konsequenzen zukommen. Eine tatsächliche Klarnamenpflicht auf lediglich nationaler Ebene erscheint vor dem Hintergrund der territorialen Schrankenlosigkeit des Internets und der mit dieser Pflicht eigentlich verfolgten Absicht problematisch und nicht zielgerichtet. Sie stünde weiterhin einem bisherigen Grundsatz des Telemedienrechts diametral gegenüber und zudem wären verschiedenste Folgewirkungen zu bedenken. So würden beispielsweise Personen, die sich bislang anonym oder pseudonym im digitalen Raum gegen politisch motivierte Hasskriminalität positionieren, durch eine Klarnamenpflicht der Möglichkeit persönlicher Anfeindungen ausgesetzt (vgl. Buermeyer 2019). Unabhängig von einer Klarnamenpflicht käme als weiterer Ansatz auch die Authentifizierung der Nut-

[94] Während der Entstehung dieses Fazits wird die dauerhafte Sperrung des Twitter-Accounts des inzwischen ehemaligen US-amerikanischen Präsidenten Trump gesellschaftlich, medial und politisch thematisiert (vgl. nur Freidel 2021).

zerdaten bereits bei der Registrierung in Betracht. Eine solche Identifizierungspflicht für soziale Netzwerke und Spieleplattformen sieht der Gesetzesantrag der Länder Niedersachsen und Mecklenburg-Vorpommern vor (vgl. BR-Drs. 70/20).[95] Aus kriminalistischer Perspektive würde eine solche Ausgestaltung eine Zunahme der Ermittlungsansätze bedeuten und hierüber die Zahl der geklärten Ermittlungsverfahren erhöhen.

Ein weiterer Ansatz zur Regulierung des Phänomenbereichs ergibt sich aus der Anwendungsmöglichkeit eines auf Künstlicher Intelligenz basierenden Moderators für virtuelle Diskussionen. Ein auf vier Jahre angelegtes Forschungsprojekt unter Leitung der Universität Göttingen und Beteiligung der Technischen Universität Warschau und der Universitäten Konstanz, Maastricht und Dundee soll im April 2021 beginnen und hierbei sollen verschiedene Deeskalationsstrategien zur Intervention bei destruktiver Kommunikation in sozialen Medien entwickelt werden (vgl. Georg-August-Universität Göttingen 2020). Hierzu soll ausweislich der Pressemeldung ein interdisziplinärer Ansatz aus „Philosophie, Ethik, Politikwissenschaft, Sprachwissenschaft und Technikwissenschaft“ (ebd.) verfolgt werden. Hinsichtlich der Möglichkeiten und Grenzen beim Einsatz von Künstlicher Intelligenz wird auf die Ausführungen in Kapitel 4.3 verwiesen.

Im jeweiligen Zwischenfazit zu den kriminologischen und kriminalistischen Implikationen wurden diverse noch offene Fragestellungen und Handlungsmöglichkeiten aufgezeigt. Diese sind nicht abschließend und könnten fortgeführt werden. In Bezug auf eine Identifizierungs- oder Klarnamenpflicht wäre beispielsweise zu klären, wie viele Delikte tatsächlich anonym oder pseudonym begangen werden. Die Antwort hätte maßgeblichen Einfluss auf eine diesbezügliche Entscheidung. Hinsichtlich der dargestellten legislativen Aktivitäten stellt sich weiterhin die Frage der Wirksamkeit ihres Regelungsgehalts. Ferner limitiert die territoriale Schrankenlosigkeit des Internets die nationalstaatlichen Maßnahmen von Beginn an. Der Vorschlag des „Digital Services Act“ der EU-Kommission (2020/0361 vom 15.12.2020) könnte – im Fal-

[95] Dieser Gesetzesantrag sieht ferner die Ergänzung des Anwendungsbereichs des NetzDG auf Spieleanbieter vor. Eine solche Ausweitung der verpflichteten Dienstanbieter hätte aus kriminalistischer Perspektive unter Einbeziehung der im fünften Kapitel dargestellten legislativen Maßnahmen eine Steigerung der Anzahl von Ermittlungsverfahren zur Folge.

le der Umsetzung im Rahmen des ordentlichen Gesetzgebungsverfahrens – eine europaweit einheitliche Plattformregulierung bewirken.

Eine endgültige Antwort, durch welche Maßnahmen bestehende Defizite beseitigt werden sollten, kann infolge des unzureichenden Erkenntnisstandes nicht gegeben werden. Es stellt sich daher zum Abschluss die Frage, woher der Impetus für eine systematische Rahmung kommen und auf welchem Wege zielgerichtet, evidenzbasiert und verfassungsgemäß Remedur geschaffen werden kann. Im Rahmen der Arbeit wurden mehrere Forschungsprojekte dargestellt, die sich aus verschiedenen Perspektiven und mit unterschiedlichen Zielsetzungen mit dem Phänomenbereich beschäftigen. Die bestehenden Fragestellungen und die unterschiedlichen Handlungsmöglichkeiten sowie gesellschaftliche Entwicklungen und der stetige Fortschritt der Digitalisierung zeigen deutlich das Erfordernis einer weiteren empirischen und interdisziplinären Forschung zu politisch motivierter Hasskriminalität im Internet. Aufgrund der gegebenen Komplexität erscheint es zwingend, hierfür einen integrativen Ansatz zu wählen, bei welchem alle wesentlichen Wissenschaftsdisziplinen bei gegenseitiger Anerkennung vernetzt und beteiligt werden. Bei der Umsetzung legislativer Maßnahmen sollten die hervorgebrachten empirischen Erkenntnisse maßvoll „zur Modifizierung der Zielrichtung und des Zweckgedankens [der] Regelungsmaterie“ (Plank 2017: 329) genutzt werden. Bezugnehmend auf das einleitende Zitat dieses Kapitels, könnte hieraus die erforderliche Steuerungskraft erwachsen, welche eine die Würde des Menschen achtende, digitale Kommunikationskultur fördert und hierdurch fundamentale Bedingungen einer freiheitlichen Demokratie gewährleistet.

Literaturverzeichnis

Ackermann, Rolf; Koristka, Christian; Leonhardt, Rainer; Nisse, Reingard; Wirth, Ingo (2000): Zum Stellenwert der Kriminalistik. Teil 2. In: Kriminalistik, Ausgabe 10/2000. S. 655-660.

Ackermann, Rolf; Koristka, Christian; Leonhardt, Rainer; Nisse, Reingard; Wirth, Ingo (2000a): Zum Stellenwert der Kriminalistik. Teil 3. In: Kriminalistik, Ausgabe 11/2000. S. 731-736.

Ackermann, Rolf (2013): Zur Entwicklung der Kriminalistik in Deutschland. In: der kriminalist, Ausgabe 9/2013. S. 18-25.

Ackermann, Rolf (2019): Einführung in die Kriminalistik. In: Ackermann, Rolf; Clages, Horst; Roll, Holger (Hrsg.), Handbuch der Kriminalistik. Kriminaltaktik für Praxis und Ausbildung. 5. Auflage. Boorberg Verlag, Stuttgart. S. 1-54.

Ackermann, Rolf (2019a): Fallanalyse, Versions-/Hypothesenbildung, Untersuchungsplanung. In: Ackermann, Rolf; Clages, Horst; Roll, Holger (Hrsg.), Handbuch der Kriminalistik. Kriminaltaktik für Praxis und Ausbildung. 5. Auflage. Boorberg Verlag, Stuttgart. S. 169-248.

Ackermann, Rolf; Kurapka, Vidmantas; Malewski, Henryk; Shepitko, Valery (2020): Schaffung eines einheitlichen europäischen kriminalistischen Raumes. Die Tätigkeit öffentlicher Organisationen zur Stärkung der internationalen Beziehungen. In: Kriminalistik, Ausgabe 6/2020. S. 355-363.

Agentur der Europäischen Union für Grundrechte (2012): Hasskriminalität in der Europäischen Union sichtbar machen: die Rechte der Opfer anerkennen [online] https://fra.europa.eu/sites/default/files/fra-2012_hate-crime-de.pdf [03.12.2020].

Albrecht, Stephen; Fielitz, Maik (2019): Rechtsterrorismus im digitalen Zeitalter. In: Wissen schafft Demokratie. Schriftenreihe des Instituts für Demokratie und Zivilgesellschaft, Ausgabe 6/2019. S. 176-187.

Altenhain, Karsten (2019): Münchener Kommentar zum StGB, Band 7, Nebenstrafrecht II. 3. Auflage. Verlag C. H. Beck, München.

Apostel, Christoph (2019): Hate Speech - zur Relevanz und den Folgen eines Massenphänomens. In: KriPoZ, Ausgabe 5/2019. S. 287-292.

Bäcker, Matthias (2020): Folgerungen aus dem zweiten Bestandsdatenbeschluss des BVerfG für die durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität geschaffenen Datenverarbeitungsregelungen. Rechtsgutachten im Auftrag der Bundestagsfraktion Bündnis 90/Die Grünen [online] https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/rechtspolitik/PDF/200917-Baecker-Gutachten-Gesetz_zur_Bekaempfung_des_Rechtsextremismus_und_der_Hasskriminalitaet.pdf [27.12.2020].

Backes, Uwe (2020): Zur Dynamik der Radikalisierung. Feindbildwandel und reziproke Legitimierung in interagierenden extremistischen Gewaltszenen. In: Kriminalistik, Ausgabe 1/2020. S. 9-14.

Bauman, Zygmunt (2016): Die Welt in Panik. Wie die Angst vor Migranten geschürt wird [online] https://www.blaetter.de/ausgabe/2016/oktober/die-welt-in-panik [14.09.2020].

Bayerische Landeszentrale für neue Medien (2020): Justiz und Medien – Konsequent gegen Hass [online] https://www.blm.de/konsequent-gegen-hass.cfm [06.12.2020].

Bayerisches Staatsministerium der Justiz (2020): Pressemitteilung vom 12. Februar 2020. Bayerns Justizminister Eisenreich stellt den neuen Hate-Speech-Beauftragten der bayerischen Justiz und die Sonderdezernenten für die Bekämpfung von Hate-Speech vor [online] https://www.justiz.bayern.de/presse-und-medien/pressemitteilungen/archiv/2020/13.php [18.12.2020].

Bayerl, Petra Saskia; Rüdiger, Thomas-Gabriel (2017): Die polizeiliche Nutzung sozialer Medien in Deutschland: Die Polizei im digitalen Neuland. In: Stierle, Jürgen; Wehe, Dieter; Siller, Helmut (Hrsg.), Handbuch Polizeimanagement. Polizeipolitik - Polizeiwissenschaft - Polizeipraxis. Springer Gabler, Wiesbaden. S. 919-943.

Brand, Laura; Materni, Simona (2020): Auf Social Media zur Zivilcourage anleiten. Die Polizei in der Schweiz erklärt der Bevölkerung auf Facebook, Twitter und YouTube, wie sie Zivilcourage zeigen kann. In: Kriminalistik, Ausgabe 4/2020. S. 266-269.

Brodowski, Dominik; Freiling, Felix (2011): Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Schriftenreihe Forschungsforum Öffentliche Sicherheit [online] https://www.sicherheit-forschung.de/forschungsforum/schriftenreihe_neu/sr_v_v/SchriftenreiheSicherheit_04.pdf [26.08.2020].

Buermeyer, Ulf (2019): Statt Klarnamen: Digitales Gewaltschutzgesetz [online] https://background.tagesspiegel.de/digitalisierung/statt-klarnamen-digitales-gewaltschutzgesetz [14.01.2021].

Bundesamt für Sicherheit in der Informationstechnik (2011): Leitfaden „IT-Forensik“ [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 [01.11.2020].

Bundeskriminalamt (2019): Polizeiliche Kriminalstatistik. Richtlinien für die Führung der Polizeilichen Kriminalstatistik in der Fassung vom 01.02.2019. Anlage 3 – Definitionskatalog [online] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2019/Interpretation/02_Rili/Anlage-3-Definitionskatalog.pdf?__blob=publicationFile&v=3 [15.09.2020].

Bundeskriminalamt (2019a): Polizeiliche Kriminalstatistik. Richtlinien für die Führung der Polizeilichen Kriminalstatistik in der Fassung vom 01.02.2019 [online] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2019/Interpretation/02_Rili/Richtlinien.pdf?__blob=publicationFile&v=3 [26.09.2020].

Bundeskriminalamt (2020): Politisch motivierte Kriminalität -rechts. Lage. Hassposting [online] https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/PMKrechts/PMKrechts_node.html;jsessionid=9A3CF9B874EFA20D2B08BB3AC500362B.live2291#doc121714bodyText1 [26.08.2020].

Bundeskriminalamt (2020a): T05 Grundtabelle - Straftaten mit Tatmittel „Internet“ – Fallentwicklung [online] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2019/Bund/Faelle/BU-F-13-T05-TM-Internet-Fallentw_xls.xlsx?__blob=publicationFile&v=6 [26.09.2020].

Bundeskriminalamt (2020b): Sicherheit und Kriminalität in Deutschland 2020. Projektbeschreibung. Inhalte der Befragung. Ziffer 3: Generierung von Erkenntnissen über das Sicherheitsgefühl und die Kriminalitätsfurcht in der Bevölkerung [online] https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Dunkelfeldforschung/SKiD/Projektbeschreibung/projektbeschreibung_node.html [19.11.2020].

Bundeskriminalamt (2020c): Künstliche Intelligenz gegen das Verbrechen: Kooperation gestartet [online] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/201027_pmForschungskoop.html [16.11.2020].

Bundeskriminalamt (2020d): Qualifizierungsmaßnahme zur Cyber-Kriminalistin / zum Cyber-Kriminalisten [online] https://www.bka.de/DE/KarriereBeruf/Stellenangebote/Beamte/CyberKriminalist/cyberkriminalist.html [22.11.2020].

Bundeskriminalamt (2020e): Unsere Aufgaben. Deliktsbereiche. Cybercrime. Bekämpfung von Cybercrime durch das BKA [online] https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html [25.11.2020].

Bundeskriminalamt (2020f): Pressemitteilung zum europaweiten Aktionstag gegen Hasspostings [online] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/201103_Hasspostings.html?fbclid=IwAR29oP3G313EiQZYi5gLBDKM6-oHd6xbkt-HZzj33XMlEMNEqmHBE9KSNo4 [19.11.2020].

Bundesministerium des Innern, für Bau und Heimat (2019): Politisch motivierte Kriminalität im Jahr 2018. Bundesweite Fallzahlen [online] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2019/pmk-2018.pdf;jsessionid=B0C9C804B5CA915FCBD43F6FDCEF1705.1_cid364?__blob=publicationFile&v=4 [15.09.2020].

Bundesministerium des Innern, für Bau und Heimat (2020): Verfassungsschutzbericht 2019 [online] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/vsb-2019-gesamt.pdf;jsessionid=A32B40E908DB907A04172D3AC88077EF.2_cid287?__blob=publicationFile&v=5 [26.08.2020].

Bundesministerium des Innern, für Bau und Heimat (2020a): Politisch motivierte Kriminalität im Jahr 2019. Bundesweite Fallzahlen [online] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2020/pmk-2019.pdf?__blob=publicationFile&v=6 [26.08.2020].

Bundesrechtsanwaltskammer (2020): Stellungnahme zum Regierungsentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität i. d. F. 18.02.2020 [online] https://brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2020/maerz/stellungnahme-der-brak-2020-12.pdf [20.12.2020].

Bundesregierung (2018): Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode [online] https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1 [29.11.2020].

Bundesverfassungsgericht (2020): Klarstellung verfassungsrechtlicher Maßgaben für strafrechtliche Verurteilungen wegen ehrbeeinträchtigender Äußerungen. Pressemitteilung Nr. 49/2020 vom 19. Juni 2020 [online] https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-049.html [26.08.2020].

Bundesverfassungsgericht (2020a): Regelungen zur Bestandsdatenauskunft verfassungswidrig. Pressemitteilung Nr. 61/2020 vom 17. Juli 2020 [online] https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-061.html [27.12.2020].

Bundeszentrale für politische Bildung (2017): Was ist Hate Speech? [online] https://www.bpb.de/252396/was-ist-hate-speech [26.08.2020].

Burba, Matthias (2019): Zukünftige Anforderungen an Polizeivollzugsbeamte aus kriminaltechnischer Sicht. In: Lange, Hans-Jürgen; Model, Thomas; Wendekamm, Michaela (Hrsg.), Zukunft der Polizei. Trends und Strategien. Springer VS, Wiesbaden. S. 153-160.

Burger, Reiner; Iskandar, Katharina (2020): Razzia wegen Hetze im Netz. Mord an Walter Lübcke [online] https://www.faz.net/2.1844/mord-an-walter-luebcke-razzia-wegen-hetze-im-netz-16799836.html [14.09.2020].

Burkhardt, Lukas (2020): Künstliche Intelligenz in der Strafverfolgung. Potential und Limitierung von Anwendungen des maschinellen Lernens zur Unterstützung von Ermittlern bei der Bewältigung von Massen-Mediendaten. In: Kriminalistik, Ausgabe 5/2020. S. 336-340.

Busching, Michael (2015): Der Begehungsort von Äußerungsdelikten im Internet. Grenzüberschreitende Sachverhalte und Zuständigkeitsprobleme. In: MMR Multimedia und Recht, Ausgabe 5/2015. S. 295-299.

Camus, Renaud (2016): Revolte gegen den großen Austausch. Verlag Antaios, Schnellroda.

Casey, Eoghan (2011): Digital Evidence in the Courtroom. In: Ders. Hrsg., Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. 3. Auflage. Academic Press, Cambridge. S. 49-83.

Ceffinato, Tobias (2020): Zur Regulierung des Internets durch Strafrecht bei Hass und Hetze auf Onlineplattformen. In: ZStW, Ausgabe 3/2020. S. 544-563.

Clages, Horst (2017): Kriminalwissenschaften. In: Clages, Horst; Ackermann, Rolf (Hrsg.), Der rote Faden. Grundsätze der Kriminalpraxis. 13. Auflage. C. F. Müller, Heidelberg. S. 1-7.

Clages, Horst (2017a): Kriminalistische Methodik. In: Clages, Horst; Ackermann, Rolf (Hrsg.), Der rote Faden. Grundsätze der Kriminalpraxis. 13. Auflage. C. F. Müller, Heidelberg. S. 8-22.

Clages, Horst (2017b): Strafanzeige. In: Clages, Horst; Ackermann, Rolf (Hrsg.), Der rote Faden. Grundsätze der Kriminalpraxis. 13. Auflage. C. F. Müller, Heidelberg. S. 30-46.

Clages, Horst (2017c): Beweis- und Verdachtslehre. In: Clages, Horst; Ackermann, Rolf (Hrsg.), Der rote Faden. Grundsätze der Kriminalpraxis. 13. Auflage. C. F. Müller, Heidelberg. S. 47-62.

Clages, Horst (2019): Beweislehre, Beweisführung. In: Ackermann, Rolf; Clages, Horst; Roll, Holger (Hrsg.), Handbuch der Kriminalistik. Kriminaltaktik für Praxis und Ausbildung. 5. Auflage. Boorberg Verlag, Stuttgart. S. 55-74.

Cohen, Lawrence; Felson, Marcus (1979): Social Change and Crime Rate Trends: A Routine Activity Approach. In: American Sociological Review, Ausgabe 4/1979. S. 588-608.

Dachsel, Felix (2018): Das geheime Dahinter. Verschwörungstheorien [online] https://www.zeit.de/kultur/2018-06/verschwoerungstheorien-politik-israel-afd/komplettansicht [20.09.2020].

Danwitz, Thomas von (2008): Europäisches Verwaltungsrecht. Springer-Verlag, Berlin und Heidelberg.

Dewald, Andreas; Freiling, Felix (2015): Digitale Spuren. In: Dies. Hrsg., Forensische Informatik. 2. Auflage. Books on Demand, Norderstedt. S. 29-61.

Dieckmann, Janine; Geschke, Daniel; Braune, Ina (2017): Diskriminierung und ihre Auswirkungen für Betroffene und die Gesellschaft. In: Wissen schafft Demokratie. Schriftenreihe des Instituts für Demokratie und Zivilgesellschaft, Ausgabe 2/2017. S. 18-37.

Eckert, Roland (2020): Radikalisierung in konflikttheoretischer Perspektive. In: Ben Slama, Brahim; Kemmesies, Uwe (Hrsg.), Handbuch Extremismusprävention - Gesamtgesellschaftlich. Phänomenübergreifend. Bundeskriminalamt, Wiesbaden. S. 213-267.

Ehlert, Cindy; Rüdiger, Thomas-Gabriel (2020): Defensible Digital Space. In: Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hrsg.), Cyberkriminologie. Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden. S. 151-171.

Europäische Kommission gegen Rassismus und Intoleranz (2016): Allgemeine Politik-Empfehlung Nr. 15 der ECRI über die Bekämpfung von Hassrede [online] https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-combating-hate-speech-germ/16808b5b00 [26.08.2020].

Europarat (1997): Empfehlung Nr. R (97) 20 des Ministerkomitees an die Mitgliedsstaaten über die „Hassrede“ [online] http://www.egmr.org/minkom/ch/rec1997-20.pdf [26.08.2020].

Europarat (2003): Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art. SEV Nr. 189 [online] https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/189 [26.08.2020].

European Criminal Policy Initiative (2013): Manifest zum Europäischen Strafverfahrensrecht. In: ZIS, Ausgabe 11/2013. S. 412-429.

Facebook (2018): Facebook veröffentlicht NetzDG-Transparenzbericht [online] https://about.fb.com/de/news/2018/07/facebook-veroeffentlicht-netzdg-transparenzbericht/ [16.12.2020].

Facebook (2019): Facebook veröffentlicht zweiten NetzDG-Transparenzbericht [online] https://about.fb.com/de/news/2019/01/facebook-veroeffentlicht-zweiten-netzdg-transparenzbericht/ [16.12.2020].

Facebook (2019a): Facebook veröffentlicht dritten NetzDG-Transparenzbericht [online] https://about.fb.com/de/news/2019/07/dritter-netzdg-transparenzbericht/ [16.12.2020].

Facebook (2020): Gemeinschaftsstandards. III: Anstößige Inhalte. 12. Hassrede [online] https://de-de.facebook.com/communitystandards/hate_speech [26.08.2020].

Facebook (2020a): Facebook veröffentlicht vierten NetzDG-Transparenzbericht [online] https://about.fb.com/de/news/2020/01/facebook-veroeffentlicht-vierten-netzdg-transparenzbericht/ [16.12.2020].

Facebook (2020b): Facebook veröffentlicht fünften NetzDG-Transparenzbericht [online] https://about.fb.com/de/news/2020/07/facebook-veroeffentlicht-fuenften-netzdg-transparenzbericht/ [16.12.2020].

Facebook (2021): Facebook veröffentlicht sechsten NetzDG-Transparenzbericht [online] https://about.fb.com/de/news/2021/01/facebook-veroeffentlicht-sechsten-netzdg-transparenzbericht/ [30.01.2021].

Fauth, Jürgen (2015): Veränderungen polizeilicher Alltagsarbeit durch die Entwicklung der IT und die Auswirkungen auf das Berufsbild des Polizeibeamten. In: Lange, Hans-Jürgen; Bötticher, Astrid (Hrsg.), Cyber-Sicherheit. Springer VS, Wiesbaden. S. 147-159.

Feltes, Thomas (2006): Kriminalpolitik. In: Lange, Hans-Jürgen (Hrsg.), Wörterbuch zur Inneren Sicherheit. Springer VS, Wiesbaden. S. 160-165.

Fischer, Thomas (2020): Strafgesetzbuch. 67. Auflage. Verlag C. H. Beck, München.

Frankfurter Allgemeine Zeitung (2016): Gaulands Rede im Wortlaut. Zum Nachlesen [online] https://www.faz.net/aktuell/politik/inland/zum-nachlesen-gaulands-rede-im-wortlaut-14269861.html?printPagedArticle=true#pageIndex_2 [20.09.2020].

Freidel, Morten (2021): Soll der Staat über Löschungen bestimmen? [online] https://www.faz.net/aktuell/politik/twitter-ohne-trump-soll-der-staat-ueber-sperren-bestimmen-17149634.html [23.01.2021].

Gabriel, Sonja (2020): Hate Speech in der Computerspielkultur. Affinitätsräume als Ort der Diskriminierung und Ausgrenzung? In: Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hrsg.), Cyberkriminologie. Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden. S. 269-287.

Gärditz, Klaus (2020): Die Grenze des Sagbaren. BVerfG zu Meinungsäußerung und Menschenwürde [online] https://www.lto.de/recht/hintergruende/h/bverfg-beschluss-1-bvr-2459-19-grundrechte-meinungsfreiheit-beleidigung-grenze/ [26.11.2020].

Georg-August-Universität Göttingen (2020): Presseinformation: Diskussion und Deeskalation in den sozialen Medien [online] https://www.uni-goettingen.de/de/3240.html?id=6118 [14.01.2021].

Gerson, Oliver (2020): Fauler (Wort-)Zauber im Strafzumessungsrecht. Plädoyer gegen die ausdrückliche Einfügung „antisemitischer Beweggründe“ als Strafzumessungstatsache in § 46 Abs. 2 S. 2 (1. Gruppe) StGB. In: KriPoZ, Ausgabe 1/2020. S. 22-37.

Geschke, Daniel; Klaßen, Anja; Quent, Matthias; Richter, Christoph (2019): #Hass im Netz: Der schleichende Angriff auf unsere Demokratie. Eine bundesweite repräsentative Untersuchung. Institut für Demokratie und Zivilgesellschaft [online] https://www.idz-jena.de/fileadmin/user_upload/_Hass_im_Netz_-_Der_schleichende_Angriff.pdf?bcsi_scan_e09ff2199bb3916e=0&bcsi_scan_filename=_Hass_im_Netz_-_Der_schleichende_Angriff.pdf [26.08.2020].

Gleiß, Hanna (2019): Deep Learning zur Klassifizierung von Hate Speech: Zwischenergebnisse des NOHATE Forschungsprojekts [online] https://www.das-nettz.de/deep-learning-zur-klassifizierung-von-hate-speech-zwischenergebnisse-des-nohate-forschungsprojekts [09.11.2020].

Google (2018): YouTube. Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz 01. Januar 2018 - 30. Juni 2018 [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/YT-NetzDG-TR-Bundesanzeiger-2018-06.pdf [16.12.2020].

Google (2018a): Google+. Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz 01. Januar 2018 - 30. Juni 2018 [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/G%2B_NetzDG-TR-Bundesanzeiger-2018-06.pdf [16.12.2020].

Google (2019): YouTube. Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz 01. Juli 2018 - 31. Dezember 2018 [online] http://storage.googleapis.com/transparencyreport/legal/netzdg/YT-NetzDG-TR-Bundesanzeiger-2018-12.pdf [16.12.2020].

Google (2019a): Google+. Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz 01. Juli 2018 - 31. Dezember 2018 [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/G%2B_NetzDG-TR-Bundesanzeiger-2018-12.pdf [16.12.2020].

Google (2019b): YouTube. Entfernungen von Inhalten aus YouTube auf der Grundlage des NetzDG 01. Januar 2019 – 30. Juni 2019 [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/YT-NetzDG-TR-Bundesanzeiger-2019-06.pdf [16.12.2020].

Google (2019c): Google+. Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz 01. Januar 2019 - 02. April 2019 [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/G%2B_NetzDG-TR-Bundesanzeiger-latest.pdf [16.12.2020].

Google (2020): YouTube-Richtlinien zu Hassrede [online] https://support.google.com/youtube/answer/2801939?hl=de [26.08.2020].

Google (2020a): YouTube. Entfernungen von Inhalten aus YouTube auf der Grundlage des NetzDG 01. Juli 2019 – 31. Dezember 2019 [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/YT-NetzDG-TR-Bundesanzeiger-2019-12.pdf [16.12.2020].

Google (2020b): YouTube. Entfernungen von Inhalten aus YouTube auf der Grundlage des NetzDG 01. Januar 2020 – 30. Juni 2020 [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/YT-NetzDG-TR-Bundesanzeiger-latest.pdf [16.12.2020].

Google (2021): Transparenzbericht YouTube. Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz [online] https://storage.googleapis.com/transparencyreport/legal/netzdg/YT-NetzDG-TR-Bundesanzeiger-latest.pdf [30.01.2021].

Haase, Adrian (2017): Computerkriminalität im Europäischen Strafrecht. Kompetenzverteilung, Harmonisierungen und Kooperationsperspektiven. Mohr Siebeck, Tübingen.

Hartleb, Florian (2020): Die Manifeste rechtsterroristischer Einzeltäter. Eine vergleichende Analyse. In: Kriminalistik, Ausgabe 5/2020. S. 313-318.

Hartmann, Markus (2020): Stellungnahme zum Entwurf der Fraktionen der CDU/CSU und SPD eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/17741) und zu dem Entwurf der Bundesregierung eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/18470) [online] https://www.bundestag.de/resource/blob/694016/f5454d834ec71ed26574e4af0516bd1f/hartmann-data.pdf [20.12.2020].

Hartung, Matthias; Klinger, Roman; Schmidtke, Franziska; Vogel, Lars (2017): Identifying Right-Wing Extremism in German Twitter Profiles: A Classification Approach. In: Frasincar, Flavius; Ittoo, Ashwin; Nguyen, Le Minh; Métais, Elisabeth (Hrsg.), Natural Language Processing and Information Systems. 22nd International Conference on Applications of Natural Language to Information Systems, NLDB 2017, Liège, Belgium, June 21-23, 2017, Proceedings. Springer International Publishing, Cham. S. 320-325.

Hassemer, Winfried (2008): Strafrecht. Sein Selbstverständnis, seine Welt. Berliner Wissenschafts-Verlag, Berlin.

Hecht, Dorothea (2020): Digitales Gewaltschutzgesetz? Ein Beitrag aus der Perspektive der Frauenhauskoordinierung. In: BdW Blätter der Wohlfahrtspflege, Ausgabe 4/2020. S. 127-129.

Heinson, Dennis (2015): IT-Forensik. Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen. Mohr Siebeck, Tübingen.

Heinze, Rolf (2019): Sozioökonomische Zersplitterung und Digitalisierung: Auf dem Weg zur granularen Gesellschaft? In: Lange, Hans-Jürgen; Model, Thomas; Wendekamm, Michaela (Hrsg.), Zukunft der Polizei. Trends und Strategien. Springer VS, Wiesbaden. S. 11-33.

Heitmeyer, Wilhelm (2020): "In der Krise wächst das Autoritäre". Interview von Christian Bangel [online] https://www.zeit.de/gesellschaft/zeitgeschehen/2020-04/wilhelm-heitmeyer-coronavirus-verschwoerungstheorien-finanzmarkt-rechtsradikalismus/komplettansicht [14.09.2020].

Hessisches Ministerium der Justiz (2020): Generalstaatsanwaltschaft Frankfurt am Main. Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität [online] https://staatsanwaltschaften.hessen.de/staatsanwaltschaften/gsta-frankfurt-am-main/aufgabengebiete/zentralstelle-zur-bekämpfung-der [25.11.2020].

Hessisches Ministerium des Innern und für Sport (2020): Hessen gegen Hetze. Meldeformular [online] https://hessengegenhetze.de/hasskommentare-melden [16.11.2020].

Hessisches Ministerium des Innern und für Sport (2020a): Hessen gegen Hetze. Vorstellung unserer Partner [online] https://hessengegenhetze.de/partner [16.11.2020].

Hilgendorf, Eric; Valerius, Brian (2012): Computer- und Internetstrafrecht. Ein Grundriss. 2. Auflage. Springer-Verlag, Berlin und Heidelberg.

Hirschi, Travis (1969): Causes of Delinquency. University of California Press, Berkeley and Los Angeles.

Hoffmann-Riem, Wolfgang (2018): Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data. In: Ders. Hrsg., Big Data – Regulative Herausforderungen. 1. Auflage. Nomos-Verlag, Baden-Baden. S. 11-78.

Höft, Regine (2020): Hate Speech. Ergebnisse einer repräsentativen Bevölkerungsumfrage [online] https://medienstrafrecht.jura.uni-leipzig.de/download/0/0/1912772142/eea569cd9e06640156bb3d6678181b53a48c570f/fileadmin/medienstrafrecht.jura.uni-leipzig.de/uploads/Veroeffentlichungen/gdp_Ergebnisse_HateSpeech_Kurzbericht.pdf [16.09.2020].

Hoheisel-Gruler, Roland (2020): Der digitale Raum ist kein (grund-)rechtsfreier Raum. In: Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hrsg.), Cyberkriminologie. Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden. S. 71-108.

Holscher, Max; Schneider, Anna-Sophie (2019): Ein Satz - und der Hass danach. Rekonstruktion der Bürgerversammlung in Kassel [online] https://www.spiegel.de/politik/deutschland/walter-luebcke-was-geschah-bei-der-buergerversammlung-2015-in-kassel-a-1274434.html [15.09.2020].

Innenministerkonferenz (2019): Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 211. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 04. bis 06. Dezember 2019 in Lübeck [online] https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2019-12-04_06/beschluesse.pdf?__blob=publicationFile&v=2 [06.12.2020].

Innenministerkonferenz (2020): Aufgaben und Arbeitsweise [online] https://www.innenministerkonferenz.de/IMK/DE/aufgaben/aufgaben-node.html [26.08.2020].

Instagram (2019): NetzDG – Transparenzbericht Juli 2019 [online] https://instagram-press.com/de/wp-content/uploads/sites/2/2019/07/instagram_netzdg_July_2019_deutsch.pdf [16.12.2020].

Instagram (2020): NetzDG – Transparenzbericht Januar 2020 [online] https://scontent-frt3-1.xx.fbcdn.net/v/t39.8562-6/103350018_565433014163676_6978092986598451203_n.pdf?_nc_cat=106&ccb=2&_nc_sid=ae5e01&_nc_ohc=QkephCqALPoAX8Yb9Lz&_nc_ht=scontent-frt3-1.xx&oh=3f1cc38ce0f4a67e259ad0005c90ea8e&oe=5FFE98AF [16.12.2020].

Instagram (2020a): NetzDG - Transparenzbericht Juli 2020 [online] https://scontent-frt3-1.xx.fbcdn.net/v/t39.8562-6/116715787_2373553682941263_6359719088636124711_n.pdf?_nc_cat=109&ccb=2&_nc_sid=ae5e01&_nc_ohc=KixGQ2txd4UAX9i-mqW&_nc_ht=scontent-frt3-1.xx&oh=d64fe403089549fb475163332359cb27&oe=60011F43 [16.12.2020].

Instagram (2021): NetzDG Transparenzbericht Januar 2021 [online] https://scontent-ham3-1.xx.fbcdn.net/v/t39.8562-6/143798695_2387152677248_816206035702077565_n.pdf?_nc_cat=103&ccb=2&_nc_sid=ae5e01&_nc_ohc=GmnhR7usRc8AX8l7QRa&_nc_ht=scontent-ham3-1.xx&oh=e6c3b9182e6f2790842972c961705c92&oe=603AFA84 [30.01.2021].

Institut für Demoskopie Allensbach (2019): Erosion des Vertrauens. Eine Dokumentation des Beitrags von Prof. Dr. Renate Köcher in der Frankfurter Allgemeinen Zeitung Nr. 270 vom 20. November 2019 [online] https://www.ifd-allensbach.de/fileadmin/IfD/sonstige_pdfs/FAZ_November2019_Vertrauen.pdf [17.09.2020].

Jaeger, Mona (2020): Höchststrafe für Halle-Attentäter gefordert [online] https://www.faz.net/aktuell/politik/inland/prozess-zum-anschlag-in-halle-hoechststrafe-gefordert-17058932.html?fbclid=IwAR1WIB3C5RPyRHI6ceMzJkQes7OAM59ku_se8d-LW2PdcfiE_Sgm6al8Ch8&utm_campaign=GEPC%253Ds6&utm_content=buffer196d7&utm_medium=social&utm_source=facebook.com [19.11.2020].

Jaishankar, Karuppannan (2007): Establishing a Theory of Cyber Crimes. In: International Journal of Cyber Criminology, Ausgabe 2/2007. S. 7-9.

Jaishankar, Karuppannan (2008): Space transition theory of cyber crimes. In: Schmalleger, Frank; Pittaro, Michael (Hrsg.), Crimes of the Internet. Prentice Hall, Upper Saddle River. S. 283-301.

Jaki, Sylvia; De Smedt, Tom (2018): Right-wing German Hate Speech on Twitter: Analysis and Automatic Detection [online] https://arxiv.org/pdf/1910.07518.pdf [14.11.2020].

Kaufmann, Annelie; Suliak, Hasso (2020): Kann das Gesetz gegen Hasskriminalität bald in Kraft treten? BMI legt Reparaturgesetz vor [online] https://www.lto.de/recht/hintergruende/h/gesetz-hasskriminalitaet-verfassungswidrig-reparatur-bestandsdatenauskunft-ausfertigung-bundespraesident/ [01.01.2021].

Keller, Christoph (2019): Basislehrbuch Kriminalistik. Strategien und Techniken der Verbrechensaufklärung und -bekämpfung. 1. Auflage. Verlag Deutsche Polizeiliteratur, Hilden.

Kelling, George; Wilson, James (1982): Broken Windows. The police and neighborhood safety. In: The Atlantic, Ausgabe März 1982.

Kinzig, Jörg (2020): Der Einfluss der Kriminologie auf die Strafgesetzgebung. In: KriPoZ, Ausgabe 1/2020, S. 8-13.

Klein, Manfred (2020): Hessen startet Kriminalpolizei-Studium mit Vertiefungsrichtung „Cyberkriminalistik“ [online] https://www.egovernment-computing.de/hessen-startet-kriminalpolizei-studium-mit-vertiefungsrichtung-cyberkriminalistik-a-925307/ [22.11.2020].

Klink, Manfred; Kordus, Siegfried (1986): Kriminalstrategie. Grundlagen polizeilicher Verbrechensbekämpfung. Boorberg Verlag, Stuttgart.

Koreng, Ansgar (2017): Hate-Speech im Internet: Eine rechtliche Annäherung. In: KriPoZ, Ausgabe 3/2017. S. 151-159.

Krause, Benjamin (2019): „Hate Speech“ im Internet. Ein Überblick zur strafrechtlichen Einordnung. In: Kriminalistik, Ausgabe 12/2019. S. 751-754.

Krause, Benjamin (2020): Regelungen zu Bestandsdatenabfragen verfassungswidrig – und nun? Eine Einordnung für Strafverfolgungsbehörden. In: Kriminalistik, Ausgabe 8-9/2020. S. 546-547.

Kunz, Karl-Ludwig; Singelnstein, Tobias (2016): Kriminologie. Eine Grundlegung. 7. Auflage. Haupt Verlag, Bern.

Kunze, Dirk (2018): Basiskompetenzen im Bereich Cybercrime und digitale Spuren. In: Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hrsg.), Digitale Polizeiarbeit. Herausforderungen und Chancen. Springer VS, Wiesbaden. S. 161-181.

Küpper, Beate (2017): Rechtspopulistische Einstellungen und der Einfluss der Medien. In: Interventionen. Zeitschrift für Verantwortungspädagogik, Ausgabe 09-10/2017. S. 26-35.

Landesanstalt für Medien NRW (2018): Ergebnisbericht Hassrede [online] https://www.medienanstalt-nrw.de/fileadmin/user_upload/lfm-nrw/Foerderung/Forschung/Dateien_Forschung/forsaHate_Speech_2018_Ergebnisbericht_LFM_NRW.PDF [16.09.2020].

Lang, Anna-Sophia (2021): Wenn Rentner zum Mord aufrufen [online] https://zeitung.faz.net/faz/rhein-main/2021-01-28/2e9c672a07522042be311cbb32a2ce06/?GEPC=s9 [30.01.2021].

Leets, Laura (2002): Experiencing Hate Speech: Perceptions and Responses to Anti-Semitism and Antigay Speech. In: Journal of Social Issues, Ausgabe 2/2002, S. 341-361.

Liesching, Marc (2018): Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG. Überblick über die wesentlichen Kritikpunkte. In: MMR Multimedia und Recht, Ausgabe 1/2018. S. 26-30.

Liszt, Franz von (1898): Das Verbrechen als sozial-pathologische Erscheinung. Vortrag, gehalten in der Gehe-Stiftung zu Dresden am 10. Dezember 1898. In: Ders. Hrsg. (1905), Strafrechtliche Aufsätze und Vorträge. Zweiter Band. 1892-1904. J. Guttentag Verlagsbuchhandlung, Berlin. S. 230-250.

Lüdemann, Christian; Ohlemacher, Thomas (2002): Soziologie der Kriminalität. Theoretische und empirische Perspektiven. Juventa Verlag, Weinheim und München.

Mandl, Thomas (2020): Die Erkennung unangemessener Inhalte im Internet: KI-Verfahren, Evaluierung und Herausforderungen. In: Bibliotheksdienst, Ausgabe 3-4/2020. S. 214-226.

Marx, Konstanze (2020): Warum automatische Verfahren bei der Detektion von Hate Speech nur die halbe Miete sind. In: Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hrsg.), Cyberkriminologie. Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden. S. 707-725.

May, Andreas (2020): Schriftliche Stellungnahme im Rahmen der öffentlichen Anhörung zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität [online] https://www.bundestag.de/resource/blob/694250/4959dbfa32486a45263036901dd04134/may-data.pdf [20.12.2020].

Meier, Bernd-Dieter (2015): Kriminologie und Internet: ein ungeklärtes Verhältnis. In: Beck, Susanne; Meier, Bernd-Dieter; Momsen, Carsten (Hrsg.), Cybercrime und Cyberinvestigations. Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie. 1. Auflage. Nomos-Verlag, Baden-Baden. S. 93-118.

Meier, Bernd-Dieter (2020): Herausforderungen und Hindernisse einer evidenzbasierten Kriminalpolitik. In: KriPoZ, Ausgabe 1/2020. S. 1-7.

Miliopoulos, Lazaros (2018): Ursachen für politischen Extremismus. In: Jesse, Eckhard; Mannewitz, Tom (Hrsg.), Extremismusforschung. Handbuch für Wissenschaft und Praxis. 1. Auflage. Nomos-Verlag, Baden-Baden. S. 205-243.

Momsen, Carsten (2015): Digitale Beweismittel aus Sicht der Strafverteidigung. In: Beck, Susanne; Meier, Bernd-Dieter; Momsen, Carsten (Hrsg.), Cybercrime und Cyberinvestigations. Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie. 1. Auflage. Nomos-Verlag, Baden-Baden. S. 67-91.

Münch, Holger (2020): Innere Sicherheit weiterdenken. Ausgrenzung, Hass und Gewalt - Herausforderungen für den Rechtsstaat und die Sicherheitsbehörden. In: Kriminalistik, Ausgabe 1/2020. S. 3-8.

Münch, Holger (2020a): 70 Jahre AG Kripo. Paradebeispiel für gelebten Föderalismus. In: Kriminalistik, Ausgabe 10/2020. S. 579-583.

Musyal, Sören (2018): Rechtspopulistische Einstellung als Kompensationsleistung von Souveränitätskrisen? In: Interventionen. Zeitschrift für Verantwortungspädagogik, Ausgabe 11/2018. S. 32-40.

Nachtwey, Oliver (2016): Die Abstiegsgesellschaft. Über das Aufbegehren in der regressiven Moderne. Suhrkamp Verlag, Berlin.

Neubacher, Frank (2020): Kriminologie. 4. Auflage. Nomos-Verlag, Baden-Baden.

Newman, Oscar (1973): Defensible Space. Crime Prevention Through Urban Design. Macmillan, New York.

Papendick, Michael; Rees, Yann; Wäschle, Franziska; Zick, Andreas (2020): Hass und Angriffe auf Medienschaffende. Eine Studie zur Wahrnehmung von und Erfahrungen mit Angriffen auf Journalist*innen [online] https://mediendienst-integration.de/fileadmin/Dateien/Studie_Hass_und_Angriffe_auf_Medie nschaffende.pdf [16.09.2020].

Perske, Jörn (2020): Polizei-Nachwuchs hat wenig Interesse an Cyberkriminalistik. Studiengang mangels Bewerber verschoben [online] https://www.hessenschau.de/panorama/studiengang-verschoben-polizei-nachwuchs-hat-wenig-interesse-an-cyberkriminalistik,polizei-cyberkriminalistik-100.html?fbclid=IwAR3tHqMuLLH8u70Bl5h3rh7tk_deGKi-nTdNGUCksBj4UqsQKMCOJucxNKs [22.11.2020].

Pfahl-Traughber, Armin (2020): Der Einzeltäter ist ein einzelner Täter. In: Kriminalistik, Ausgabe 2/2020. S. 74-80.

Plank, Holger (2017): "Gesamte Strafrechtswissenschaft" - Ein fallanalytischer Diskurs am Beispiel eines Kriminalromans. Bochumer Schriften zur Rechtsdogmatik und Kriminalpolitik, Band 40. Felix-Verlag, Holzkirchen.

Plank, Holger (2020): Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich? In: Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hrsg.), Cyberkriminologie. Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden. S. 13-70.

Popitz, Heinrich (1968): Über die Präventivwirkung des Nichtwissens. Dunkelziffer, Norm und Strafe. Mohr, Tübingen.

Prätor, Susann (2014): Ziele und Methoden der Dunkelfeldforschung. Ein Überblick mit Schwerpunkt auf Dunkelfeldbefragungen im Bereich der Jugenddelinquenz. In: Eifler, Stefanie; Pollich, Daniela (Hrsg.), Empirische Forschung über Kriminalität. Methodologische und methodische Grundlagen. Springer VS, Wiesbaden. S. 31-65.

Preglau, Max (1997): Postmoderne Soziologie. In: Morel, Julius; Bauer, Eva; Meleghy, Tamas; Niedenzu, Heinz-Jürgen; Preglau, Max; Staubmann, Helmut (Hrsg.), Soziologische Theorie. Abriß der Ansätze ihrer Hauptvertreter. 5. Auflage. Oldenbourg Verlag, München. S. 265-288.

Quack, Gregor (2020): Die Kunst der Spurensicherung. „NSU-Watch“ [online] https://www.faz.net/aktuell/feuilleton/nsu-watch-spuren-und-hintergruende-zum-halle-attentat-16950608.html?printPagedArticle=true#pageIndex_2 [18.09.2020].

Reinemann, Carsten; Nienierza, Angela; Fawzi, Nayla; Riesmeyer, Claudia; Neumann, Katharina (2019): Jugend - Medien - Extremismus. Wo Jugendliche mit Extremismus in Kontakt kommen und wie sie ihn erkennen. Springer VS, Wiesbaden.

Riedmüller, Kay (2018): Big Data in Ermittlungsverfahren - Grundlagen und Entwicklung eines Auswertungszyklus. Felix-Verlag, Holzkirchen.

Rieger, Diana (2019): Diskussionsräume und Radikalisierungsprozesse in sozialen Medien [online] https://www.bpb.de/politik/extremismus/rechtspopulismus/290851/diskussionsraeume-in-sozialen-medien [14.09.2020].

Rieger, Diana; Frischlich, Lena; Rack, Stefanie; Bente, Gary (2020): Digitaler Wandel, Radikalisierungsprozesse und Extremismusprävention im Internet. In: Ben Slama, Brahim; Kemmesies, Uwe (Hrsg.), Handbuch Extremismusprävention - Gesamtgesellschaftlich. Phänomenübergreifend. Bundeskriminalamt, Wiesbaden. S. 351-386.

Rietzschel, Antonie (2020): Halle-Attentäter zu lebenslanger Haft und anschließender Sicherungsverwahrung verurteilt [online] https://www.sueddeutsche.de/politik/halle-anschlag-synagoge-urteil-1.5154249 [26.12.2020].

Rosa, Hartmut (2016): Resonanz. Eine Soziologie der Weltbeziehung. 2. Auflage. Suhrkamp Verlag, Berlin.

Roxin, Claus; Greco, Luis (2020): Strafrecht Allgemeiner Teil, Band I: Grundlagen. Der Aufbau der Verbrechenslehre. 5., vollständig neu bearbeitete Auflage. Verlag C. H. Beck, München.

Rüdiger, Thomas-Gabriel (2017): Das Broken-Web-Phänomen. In: Der Wirtschaftsführer, Ausgabe 2017-2018. S. 50-53.

Rüdiger, Thomas-Gabriel (2018): Das Broken Web: Herausforderung für die Polizeipräsenz im digitalen Raum. In: Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hrsg.), Digitale Polizeiarbeit. Herausforderungen und Chancen. Springer VS, Wiesbaden. S. 259-299.

Rüdiger, Thomas-Gabriel (2019): Haben wir eine Unrechtskultur im digitalen Raum? In: Kriminalistik, Ausgabe 1/2019. S. 37-41.

Sampson, Robert; Raudenbush, Stephen (1999): Systematic Social Observation of Public Spaces: A New Look at Disorder in Urban Neighborhoods. In: American Journal of Sociology, Ausgabe November 1999. S. 603-651.

Saurwein, Florian; Just, Natascha; Latzer, Michael (2017): Algorithmische Selektion im Internet: Risiken und Governance automatisierter Auswahlprozesse. In: kommunikation @ gesellschaft, Jg. 18, Beitrag 3. S. 1-22.

Schiemann, Anja (2018): Volksverhetzende Inhalte im Internet – Ausweitung der Strafbarkeit auf Handlungen im Ausland zur Bekämpfung des sog. Propagandatourismus. In: KriPoZ, Ausgabe 3/2018. S. 152-155.

Schiemann, Anja (2020): Änderungen im Strafgesetzbuch durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität. In: KriPoZ, Ausgabe 5/2020. S. 269-276.

Schindler, Frederik (2020): So verbreiten Höcke und Co. antisemitische Verschwörungstheorien [online] https://www.welt.de/politik/deutschland/article213254624/Lagebild-zum-Judenhass-So-verbreiten-Hoecke-und-Co-antisemitische-Verschwoerungstheorien.html [20.09.2020].

Sehl, Markus (2020): 5 wichtige BVerfG-Entscheidungen 2020. 5/5: Bestandsdatenauskunft und eine verfassungsrechtliche Stunt-Einlage [online] https://www.lto.de/recht/hintergruende/h/wichtige-bverfg-urteile-2020-sterbehilfe-suizid-ezb-eugh-urteil-eu-bnd-auslands-ueberwachung/6/ [01.01.2020].

Séville, Astrid (2019): Vom Sagbaren zum Machbaren? Rechtspopulistische Sprache und Gewalt. In: APuZ, Ausgabe 49-50/2019. S. 33-38.

Singelnstein, Tobias; Stolle, Peer (2012): Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert. 3. Auflage. Springer VS, Wiesbaden.

Singelnstein, Tobias (2018): Digitalisierung, Big Data und das Strafverfahren. In: Stein, Ulrich; Greco, Luís; Jäger, Christian; Wolter, Jürgen (Hrsg.), Systematik in Strafrechtswissenschaft und Gesetzgebung. Festschrift für Klaus Rogall zum 70. Geburtstag am 10. August 2018. Duncker & Humblot, Berlin. S. 725-738.

Sinus Markt- und Sozialforschung GmbH (2018): Informationen zu den Sinus - Milieus® 2018 [online] https://www.sinus-institut.de/fileadmin/user_data/sinus-institut/Bilder/Sinus-Milieus_092018/2018-09-18_Informationen_zu_den_Sinus-Milieus.pdf [14.09.2020].

Spiegel (2020): Gesetz gegen Hasskriminalität. Richterbund fordert Hunderte neue Richter und Staatsanwälte [online] https://www.spiegel.de/panorama/justiz/hasskriminalitaet-im-internet-richterbund-fordert-hunderte-neue-juristen-a-3856459c-3cd5-4e84-891f-83c455fb6db4 [20.12.2020].

Spoo, Georg (2017): Wie weiter gegen Rechts? Der Erfolg der AfD und die Strategien der Linken [online] https://www.blaetter.de/ausgabe/2017/dezember/wie-weiter-gegen-rechts [14.09.2020].

Steinke, Ronen (2020): Klick, dann Strafbefehl [online] https://www.sueddeutsche.de/digital/facebook-twitter-likes-strafbar-1.5148806 [20.12.2020].

Stöss, Richard (2010): Rechtsextremismus im Wandel. 3. Auflage. Friedrich-Ebert-Stiftung, Berlin.

Sykes, Gresham; Matza, David (1957): Techniques of Neutralization: A Theory of Delinquency. In: American Sociological Review, Ausgabe 6/1957. S. 664-670.

Tagesspiegel (2017): "Gemütszustand eines total besiegten Volkes". Höcke-Rede im Wortlaut [online] https://www.tagesspiegel.de/politik/hoecke-rede-im-wortlaut-diese-regierung-ist-zu-einem-regime-mutiert/19273518-2.html [20.09.2020].

Twitter (2018): Netzwerkdurchsetzungsgesetzbericht: Januar - Juni 2018 [online] https://cdn.cms-twdigitalassets.com/content/dam/transparency-twitter/data/download-netzdg-report/netzdg-jan-jun-2018.pdf [16.12.2020].

Twitter (2019): Netzwerkdurchsetzungsgesetzbericht: Juli - Dezember 2018 [online] https://cdn.cms-twdigitalassets.com/content/dam/transparency-twitter/data/download-netzdg-report/netzdg-jul-dec-2018.pdf [16.12.2020].

Twitter (2019a): Netzwerkdurchsetzungsgesetzbericht: Januar - Juni 2019 [online] https://cdn.cms-twdigitalassets.com/content/dam/transparency-twitter/data/download-netzdg-report/netzdg-jan-jun-2019.pdf [16.12.2020].

Twitter (2020): Richtlinie zu hassschürendem Verhalten [online] https://help.twitter.com/de/rules-and-policies/hateful-conduct-policy [26.08.2020].

Twitter (2020a): Netzwerkdurchsetzungsgesetzbericht: Juli - Dezember 2019 [online] https://cdn.cms-twdigitalassets.com/content/dam/transparency-twitter/data/download-netzdg-report/netzdg-jul-dec-2019.pdf [16.12.2020].

Twitter (2020b): Netzwerkdurchsetzungsgesetzbericht: Januar - Juni 2020 [online] https://transparency.twitter.com/content/dam/transparency-twitter/archive/data/download-netzdg-report/netzdg-jan-jun-2020.pdf [16.12.2020].

Twitter (2021): Netzwerkdurchsetzungsgesetzbericht: Juli - Dezember 2020 [online] https://transparency.twitter.com/content/dam/transparency-twitter/netzdg/NetzDGJul-Dec2020.pdf [30.01.2021].

Valerius, Brian (2020): Hasskriminalität – Vergleichende Analyse unter Einschluss der deutschen Rechtslage. In: ZStW, Ausgabe 3/2020. S. 666-689.

Van Aken, Betty; Risch, Julian; Krestel, Ralf; Löser, Alexander (2018): Challenges for Toxic Comment Classification: An In-Depth Error Analysis [online] https://arxiv.org/pdf/1809.07572.pdf [09.11.2020].

Vogel, Inna; Regev, Roey; Steinebach, Martin (2019): Automatisierte Analyse Radikaler Inhalte im Internet. In: David, Klaus; Geihs, Kurt; Lange, Martin; Stumme, Gerd (Hrsg.), Informatik 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft. Gesellschaft für Informatik e.V., Bonn. S. 233-245.

Voigts, Hanning (2019): Rechter Terror: Die deutsche Blindheit [online] https://www.fr.de/meinung/rechter-terror-halle-deutsche-blindheit-13101424.html [15.09.2020].

Vries, Hinrich de (2015): Einführung in die Kriminalistik für die Strafrechtspraxis. Kohlhammer Verlag, Stuttgart.

Weber, Max (1972): Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie. 5., revidierte Auflage. Besorgt von Johannes Winckelmann. Studienausgabe. Mohr Siebeck, Tübingen.

Welsch, Wolfgang (2008): Unsere postmoderne Moderne. 7. Auflage. Akademie Verlag, Berlin.

Wendekamm, Michaela; Model, Thomas (2019): Arbeitskultur und Berufsbilder der Polizei. Zwischen gesellschaftlichen Megatrends und Herausforderungen der Inneren Sicherheit. In: Lange, Hans-Jürgen; Model, Thomas; Wendekamm, Michaela (Hrsg.), Zukunft der Polizei. Trends und Strategien. Springer VS, Wiesbaden. S. 261-279.

Wernert, Manfred (2017): Internetkriminalität. Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen. 3. Auflage. Boorberg Verlag, Stuttgart.

Wissenschaftliche Dienste Deutscher Bundestag (2016): Aktueller Begriff: Hass und Hetze im Strafrecht [online] https://www.bundestag.de/resource/blob/483584/1ccf107faf0d0f8a98de634009cf33b6/hass-und-hetze-im-strafrecht-data.pdf [03.12.2020].

Wissenschaftliche Dienste Deutscher Bundestag (2020): Verfassungsrechtliche Aspekte der Übermittlung von gelöschten Inhalten und IP-Adressen an das Bundeskriminalamt nach dem Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drs. 19/17741 und 19/20163) [online] https://www.bundestag.de/resource/blob/803144/f83da25e745ffcb2743dc40138e1e29f/WD-10-030-20-pdf-data.pdf [27.12.2020].

Yücel, Dennis (2017): Eine Maschine gegen den Hass. Wissenschaftler entwickeln eine Software, um sogenannte Hate Speech im Internet aufzuspüren [online] https://www.tagesspiegel.de/themen/freie-universitaet-berlin/hate-speech-im-netz-eine-maschine-gegen-den-hass/20659376.html [09.11.2020].

Zeit online (2019): LKA erwartet Tausende Verfahren wegen Hasskommentaren im Fall Lübcke [online] https://www.zeit.de/politik/2019-07/hassrede-tausende-strafverfahren-mordfall-walter-luebcke [15.09.2020].

Zeit online (2020): Facebook verbietet Holocaust-Leugnung weltweit [online] https://www.zeit.de/digital/internet/2020-10/antisemitismus-facebook-verbot-holocaust-leugnung [13.12.2020].

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (2020): KISTRA [online] https://www.zitis.bund.de/DE/ZITiS/Forschungsprojekte/forschungsprojekte_node.html [18.12.2020].

Zivile Helden (2020): Zivile Helden gegen Hass im Netz. Handeln gegen Hass im Netz [online] https://www.zivile-helden.de/hass-im-netz/zivile-helden-gegen-hass-im-netz/ [23.11.2020].

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen, als die angegebenen Quellen und Hilfsmittel benutzt habe, alle Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, kenntlich gemacht sind und die Masterarbeit in gleicher oder ähnlicher Fassung noch nicht Bestandteil einer Studien- oder Prüfungsleistung war.

_____

Offenbach am Main, 31.01.2021