Stellungnahme der Google Ireland Ltd. an das Bundesministerium der Justiz und für Verbraucherschutz zum vorgeschlagenen Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (GBRH-E)

Mit dem vorgeschlagenen Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (GBRH-E) sollen das Strafgesetzbuch (StGB-E), die Strafprozessordnung (StPO-E), das Bundeskriminalamt-Gesetz (BKAG-E), das Telemediengesetz (TMG-E) und das Netzwerkdurchsetzungsgesetz (NetzDG-E) erheblich verschärft werden. Grundsätzlich stimmt Google zwar mit der Zielrichtung des Gesetzes überein, die Bekämpfung von Rechtsextremismus und der Verbreitung rechtswidriger Inhalte im Internet zu verbessern. Schon bei der Einführung des NetzDG hat Google darauf hingewiesen, dass eine Eindämmung von Hasskriminalität im Internet ohne ein übergreifendes Gesamtkonzept - zu dem maßgeblich eine effektive Strafverfolgung zählt - nicht erreicht werden kann. Daher ist der Versuch, gemeinsame Bemühungen der Bekämpfung von Hasskriminalität zu verbessern, aus unserer Sicht zu begrüßen. Gleichwohl hält Google Art und Ausmaß der vorgeschlagenen Regelungen für äußerst problematisch.

Die Ausweitung von Straftatbeständen, die umfassende Einräumung neuer Befugnisse und Auskunftsansprüche von Sicherheitsbehörden sowie die Verpflichtungen von Telemedienanbietern (Diensteanbietern) im Allgemeinen und Diensteanbietern sozialer Netzwerke im Speziellen, Nutzerdaten in ganz erheblichem Umfang zu erfassen, zu speichern und teils ohne Beachtung bisher geltender rechtsstaatlicher Schutzmechanismen - wie etwa das Vorliegen eines richterlichen Beschlusses - herausgeben zu müssen, sind rechtlich in höchstem Maße bedenklich.

So wird zum Beispiel durch die erzwungene Ausleitung von Inhalten und IP-Adressen durch Diensteanbieter sozialer Netzwerke an das Bundeskriminalamt (BKA) durch einseitige Verpflichtung Privater eine umfassende Datenbank beim BKA über Nutzer und die von ihnen geposteten Inhalte zum Zwecke der Strafverfolgung aufgebaut, die ihresgleichen sucht: Diensteanbieter sozialer Netzwerke müssten in zigtausenden von Fällen jährlich personenbezogene Daten und Inhalte an das BKA übermitteln, ohne dass vorab eine fallbezogene Prüfung durch das BKA oder eine sonstige staatliche Stelle erfolgt wäre.

Darüber hinaus ermöglicht die Herausgabe von Passwörtern Strafverfolgungsbehörden “Online-Hausdurchsuchungen”. Da unter diversen Landesgesetzen kein Gerichtsbeschluss oder staatsanwaltschaftlicher Beschluss notwendig ist, kann jede Polizeidienststelle auf einfaches Ersuchen hin Passwörter bei den Diensteanbietern erfragen, und das obgleich das Passwort Zugriff auf Bereiche vermitteln kann, die von der polizeilichen Untersuchung nicht umfasst sind.

Auch missachtet die Erweiterung der Definition “Beschwerden über rechtswidrige Inhalte” etablierte und über Jahre hinweg aufgebaute Beschwerdeverfahren der Diensteanbieter und gefährdet damit die umfangreichen Möglichkeiten der Diensteanbieter, Inhalte zu finden, die von der Plattform entfernt werden müssen. Die Diensteanbieter haben erhebliche Anstrengungen unternommen, um die NetzDG-Meldewege einzuführen, die eine klare Methode bieten, Verstöße gegen das deutsche Recht nach dem NetzDG zu melden, während die Nutzer gleichzeitig in der Lage sind, Verstöße gegen die Community-Richtlinien, die nicht unbedingt rechtswidrig sind, in großem Umfang schnell zu melden. Eine Ausdehnung des NetzDG auf alle Meldungen, die zum Ziel eine Inhaltslöschung haben, würde sich nachteilig auf die gesamten Bemühungen der Diensteanbieter zur Bekämpfung von Missbrauch auswirken. Die Anzahl der Beschwerden bzw. der gemeldeten Inhalte würde sich um ein Vielfaches erhöhen, was sich auch entsprechend in der Meldepflicht widerspiegeln würde.

Google erkennt die Notwendigkeit an, gegen Hass und Hetze im Internet weiter vorzugehen und dadurch mittelbar Persönlichkeitsrechte, den öffentlichen Frieden sowie den freien, demokratischen Diskurs zu schützen. Wir haben uns maßgeblich in die Umsetzung des 2017 verabschiedeten NetzDG eingebracht und werden uns auch in Zukunft aktiv und konstruktiv an der wirksamen Bekämpfung von Straftaten im Internet beteiligen. Das schließt im Rahmen des rechtlich Zulässigen die Bereitschaft zur Unterstützung der Strafverfolgungsbehörden bei der Aufklärung von Straftaten ein. Auf Seite 7 erläutert Google seine schon heute effektive Unterstützung der deutschen Strafverfolgungsbehörden. Auf der Herbsttagung des BKA 2019 hat Herr Oberstaatsanwalt Hartmann (Leiter der Zentral- und Ansprechstelle Cybercrime (ZAC) in Nordrhein-Westfalen) ausgeführt, dass Google 100% der Auskunftsersuchen nachgekommen ist und nicht nur formell, sondern auch inhaltlich beauskunftet hat. Diese Statistiken belegen im Übrigen, dass eine Änderung der Rechtspraxis nicht erforderlich ist.

Inhaltsverzeichnis

I. Hauptkritikpunkte

Die von Anfang an gegen das am 1.10.2017 in Kraft getretene NetzDG vorgebrachten Kritikpunkte (vgl. Stellungnahme Google, 2017[1]) haben sich in der bisherigen Praxis und in Bußgeldverfahren bestätigt und werden fortbestehen. Durch die im Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (GBRH-E) vorgesehenen Regelungen würden die Probleme sogar weiter verschärft; neue Probleme kämen hinzu.

1. Der Referentenentwurf verstößt gegen Verfassungsrecht

Die vorgeschlagenen Regelungen gehen weit über die Bekämpfung von Rechtsextremismus und Hasskriminalität hinaus, denn sie beschränken sich eben gerade nicht auf einen konkreten Straftatenkatalog. Das massive Ausleiten von Daten nach §3a NetzDG-E - einschließlich personenbezogener Daten wie IP-Adressen - durch die Diensteanbieter an das Bundeskriminalamt (BKA) ohne eine spezifische Beschränkung der Zeiträume für die Speicherung der abgefragten Daten lassen riesige Datenbanken zu allen möglichen Inhalten beim BKA entstehen, für die kein Kontrollinstrument existiert. Aufgrund der vorgesehenen Stillhaltepflicht für die Diensteanbieter erfahren die Betroffenen nicht einmal, dass ihre Daten an Strafverfolgungsbehörden übergeben wurden. Auf diese Weise würde eine Überwachungsinfrastruktur[2] geschaffen, die zu allen möglichen Zwecken eingesetzt werden könnte. Im Ergebnis würde die Umsetzung des Gesetzgebungsvorhabens einen massiven Eingriff in die Freiheitsrechte der Bürger, nicht zuletzt auch in das Fernmeldegeheimnis, sowie in datenschutzrechtliche Prinzipien bedeuten. Pointiert ausgedrückt, würden zukünftig - vor allem aufgrund neuer und besonders weitreichender Verpflichtungen zur Herausgabe von Passwörtern - “Online-Hausdurchsuchungen” möglich, und zwar ohne weitere Sicherungen wie etwa Richtervorbehalte und zeitlich unbegrenzt. Notwendige rechtliche und selbstverständliche Kontrollmechanismen sind nicht vorgesehen. Dieses Ausmaß ist verfassungsrechtlich nicht nur bedenklich, sondern unverhältnismäßig und nicht zulässig.

Die Pflicht zur Herausgabe von Passwörtern, Nutzungsdaten und IP-Adressen ohne richterliche Anordnung, wie sie durch § 15a TMG-E i.V.m. zahlreichen landesrechtlichen Ermächtigungsnormen ermöglicht werden soll, steht ebenfalls im Konflikt mit verfassungsrechtlichen Normen. Jede Polizeidienststelle kann nach diesen Vorgaben bei Einführung der geplanten Regelungen im Bereich des Gefahrenabwehrrechts auf einfaches Ersuchen hin Passwörter bei den Diensteanbietern erfragen, und das obgleich ein Passwort Zugriff auf Bereiche vermitteln kann, die von der polizeilichen Untersuchung nicht umfasst sind. Ein Passwort erlaubt üblicherweise den Zugriff auf ein Nutzerkonto, einschließlich aller Kommunikationsinhalte wie etwa E-Mails, Postings, Direktnachrichten, in der Cloud hinterlegte Dokumente, private oder berufliche Unterlagen, historische Standortdaten, Suchhistorien etc. Darüber hinaus bestünde bei Besitz von Passwörtern die Möglichkeit, selbst Inhalte aus dem Konto heraus zu veröffentlichen, zu kopieren, zu verändern, zu löschen oder Zugriffsrechte zu ändern bis hin zur Ausschließung des Berechtigten. Zudem eröffnet sie die Möglichkeit der ungehinderten und verdeckten Übernahme des gesamten Nutzerkontos in verfassungsrechtlich höchst problematischer Weise. Der GBRH-E berücksichtigt die Unterschiede zwischen Telekommunikations- und Telemediendiensten weder

[1] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2017/Downloads/03302017_Stellungnahme_google_youTube_RefE_NetzDG.pdf?__blob=publicationFile&v=2

[2] Der Begründung des GBRH-E ist zu entnehmen, "dass vom ersten Halbjahr 2018 bis zum ersten Halbjahr 2019 insgesamt 1.796.046 entsprechende Meldungen [bei den Sozialen Netzwerken] eingingen. Davon haben die sozialen Netzwerke etwa 28 Prozent (Mittelwert) gelöscht." In vielen dieser Fälle bestünde vermutlich eine Meldepflicht, so dass voraussichtlich in mehr als 500.000 Fällen Daten an das BKA ausgeleitet hätten werden müssen.

hinsichtlich der technischen Hintergründe noch der bisherigen rechtlichen Systematik ausreichend, um diese Risiken zu vermeiden.

Schon jetzt ist die Gefahr von Overblocking im Zuge der Umsetzung des geltenden NetzDG groß, da die Möglichkeiten zu einer hinreichend sorgfältigen Abwägung zwischen kontroversen Inhalten und dem Schutz der Meinungsfreiheit aufgrund der Unbestimmtheit der Normen und der kurzen Reaktionsfristen eingeschränkt sind. Durch die nun geplante umfassende Meldepflicht kommt die Gefahr eines Overreportings hinzu, die ebenfalls negative Auswirkungen auf die Meinungsfreiheit, v.a. auf die Meinungsäußerungsfreiheit entfalten kann. Der Grund hierfür ist, dass die geforderte proaktive Einbeziehung staatlicher Behörden "Abschreckungseffekte" erzeugen könnte, die im Ergebnis das bewirken, was der Entwurf ausgehend von der Beschreibung in der Begründung des GBRH-E unter "A. Problem und Ziel" eigentlich verhindern will, nämlich, "d*ass bestimmte Meinungen aus Sorge vor solchen Reaktionen nicht mehr geäußert werden. Dies kann sogar dazu führen, dass sich Menschen vollständig aus dem öffentlichen politischen Diskurs zurückzuziehen*."

2. Der Referentenentwurf verfehlt das Ziel effektiver Strafverfolgung

Google Ireland Ltd. unterstützt das Ziel der EU der Einführung einer E-Evidence Verordnung als europaweites Instrument der transnationalen Datenherausgabe. Die geplanten Gesetzesänderungen des NetzDG durch den GBRH-E würden zu unverhältnismäßigen Einschränkungen von Grundrechten führen sowie die gesetzlichen Bestimmungen und die in der E-Evidence Verordnung vorgeschlagene gerichtliche Überprüfung umgehen. Die geplanten Gesetzesänderungen machen private Unternehmen in noch größerem Umfang als schon heute zu Erfüllungsgehilfen von Strafverfolgungsbehörden. Da die Strafverfolgung jedoch eine ureigene hoheitliche Aufgabe ist, sind die geplanten Regelungen systemfremd und aus Sicht von Google verfassungsrechtlich höchst bedenklich. Die Inpflichtnahme von Diensteanbietern wird nicht nur in quantitativer Hinsicht ausgedehnt, sie ist darüber hinaus eine Abkehr vom (in der Begründung des GBRH-E ausdrücklich erwähnten) Doppeltür-Modell, das das Bundesverfassungsgericht als Leitbild hoheitlicher Auskunftsverlangen geprägt hat (vgl. BVerfGE 130, 151). Die Diensteanbieter müssten in der Folge nicht mehr nur auf ein Auskunftsersuchen reagieren, sondern auch proaktiv Nutzerdaten an staatliche Behörden ausleiten.

Auch wäre das Ziel effektiver Strafverfolgung aufgrund der bloßen Menge der zu erwartenden Ausleitungen von Inhalten verfehlt. Allein YouTube hat im 2. Halbjahr 2019 mehr als 70.000 Inhalte gesperrt oder entfernt, die durch NetzDG Beschwerden gemeldet wurden. Diese Zahl würde sich deutlich erhöhen, wenn potentiell strafrechtsrelevante Inhalte unabhängig vom Meldeweg weitergeleitet werden müssten (vgl. §1 Abs. 4 NetzDG-E sowie §3a Abs. 2 Nr. 1 NetzDG-E). Eine effektive Strafverfolgung scheint bei Millionen von zu bearbeitenden Strafverfahren völlig aussichtslos, es sei denn, nicht nur das BKA würde in erheblichem Maße personell aufgestockt, sondern mindestens im gleichen Umfang auch lokale Polizeibehörden, Staatsanwaltschaften und Gerichte. Sollte dies nicht geschehen, droht eine Paralyse der Strafverfolgung. Um diese gesellschaftlich unerwünschte Situation zu vermeiden, sollte der Fokus zunächst auf die zentralen Strafrechtsparagrafen im demokratieschädlichen Deliktsfeld (z.B. §§ 86, 86a, 130 StGB) gelegt werden.

3. Der Referentenentwurf verstößt gegen europäisches Datenschutzrecht

Der Referentenentwurf widerspricht in mehrfacher Hinsicht der DSGVO und setzt nicht die Vorgaben der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder

Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Richtlinie (EU) 2016/680) um:

Die Rechte der betroffenen Personen werden weitgehend ausgehebelt, da die Informations- und Auskunftspflichten der Diensteanbieter gegenüber ihren Nutzern aufgehoben bzw. über das notwendige Maß hinaus in einer Weise eingeschränkt werden, die mit den Vorgaben der DSGVO nicht mehr im Einklang steht. Dabei ist die Kenntnis der Verarbeitung personenbezogener Daten die Grundvoraussetzung für die Geltendmachung aller Betroffenenrechte. Die betroffenen Personen, die nicht einmal wissen, dass ihre Daten übermittelt werden, sind nach dem GBRH-E im Grunde genommen schutzlos gestellt. Es müssen deshalb jedenfalls wirksame Informationspflichten aufgenommen werden, damit Betroffene über das Verfahren sicher und vollständig aufgeklärt werden und auch im Nachhinein noch ihre Rechte wahrnehmen können. Zudem müssen während der Übermittlung und Verarbeitung bei den Behörden zusätzliche Sicherungspflichten, wie etwa eine strikte Zweckbindung und eine zunächst pseudonyme Verarbeitung sichergestellt werden.

Die Verantwortlichkeit für die Übermittlung der Daten an die Ermittlungsbehörden ist nicht eindeutig geregelt und nach erster Einschätzung von Google ebenfalls nicht DSGVO-konform. Zwar legt der Referentenentwurf fest, dass die Auskunft ersuchende Behörde für die “Zulässigkeit” “verantwortlich” ist. Es ist aber fragwürdig, ob der Entwurf damit tatsächlich vorsieht, dass ausschließlich die Auskunft ersuchenden Behörden auch datenschutzrechtlich für die Verarbeitungen bei den Diensteanbietern Verantwortliche iSv Art. 4 Nr. 7 DSGVO sein sollen. Hier muss zumindest der Wortlaut der Norm und das Verhältnis zu den Regelungen über die datenschutzrechtliche Verantwortlichkeit nach DSGVO klargestellt werden.

Die vorgesehenen Melde- und Auskunftspflichten gegenüber den Ermittlungsbehörden stehen im Widerspruch zu den Pflichten der Diensteanbieter zur Gewährleistung von Datensicherheit und führen demgemäß ebenfalls zu einer Pflichtenkollision. Nach der DSGVO müssen alle personenbezogenen Daten sicher sein; hierzu gehört auch, dass Daten verschlüsselt werden - teilweise sogar so, dass der Verantwortliche sie selbst nicht wieder entschlüsseln kann. Müssen die Daten nun aber in einer Weise gespeichert werden, dass sie nutzbar an die Strafverfolgungsbehörden übermittelt werden können, untergräbt dies die datenschutzrechtlich gebotenen Datensicherheitsmaßnahmen. Es muss hier mindestens klargestellt werden, dass die DSGVO-Vorschriften vorgehen und die eventuelle Entschlüsselung der Daten in der Verantwortung der jeweiligen Behörde liegt.

§ 15a TMG stellt keine hinreichend verlässliche datenschutzrechtliche Erlaubnis für die Diensteanbieter dar. Die DSGVO-Konformität der Regelung - vor allem zur Datenübermittlung - ist äußerst zweifelhaft. Art. 15a TMG-E soll eine weitreichende Übermittlung von Bestands- und Nutzungsdaten unter Berücksichtigung “sämtlicher unternehmensinterner Datenquellen” zulassen. Die Norm ließe somit Datenverarbeitungen zu, die weit über das erforderliche Maß hinausgehen; dies impliziert einen Verstoß gegen den datenschutzrechtlichen Grundsatz der Erforderlichkeit. Auch sind die Befugnisnormen der Behörden so weit gefasst, dass sie gegen die Richtlinie (EU) 2016/680 verstoßen. Die Übermittlung im Rahmen von § 15a TMG-E müsste deshalb auf die erforderlichen Daten eingegrenzt werden, und die Auskunft ersuchende Behörde sollte verpflichtet werden, ihr Ersuchen so weit zu konkretisieren, dass der Diensteanbieter die erforderlichen Daten leicht eingrenzen kann.

Die umfangreiche Datensammlung würde sich auf alle Nutzer international beziehen und nicht auf Nutzer in Deutschland beschränken. In der Folge würden massenhaft personenbezogene Daten aus allen EU-Mitgliedstaaten ohne eine europäische Rechtsgrundlage an deutsche Strafverfolgungsbehörden übermittelt werden. Konflikte mit den europäischen Datenschutzbehörden sind vorprogrammiert. Dieser

Widerspruch ließe sich dadurch lösen, dass die Auskunft ersuchende Behörde verpflichtet wird, alle Daten zu möglichen Straftaten, die nicht in ihre territoriale Zuständigkeit fallen, unverzüglich zu löschen.

4. Der Referentenentwurf führt zu einem nationalen Alleingang in einem allenfalls europarechtlich, ggf. sogar nur global zu harmonisierenden Bereich

Die Harmonisierung des IT-Strafrechts - etwa durch die geplante E-Evidence-Verordnung[3], aber auch die jüngsten Vorstöße in Richtung einer UN-Konvention[4] - steht noch am Anfang. Dennoch greift eine nationale Regelung wegen des grenzüberschreitenden Charakters der Materie in jedem Fall zu kurz.

Dies zeigt sich bereits darin, dass der nationale Gesetzgeber meist lediglich “eine Tür” des Doppeltür-Modells öffnen kann. Ausländische Diensteanbieter können sich nicht auf eine rein deutsche Befugnisnorm verlassen, wie sie §§ 14, 15a TMG-E schaffen soll. Es verbleiben angesichts der mehrpoligen Interessen, denen sich Diensteanbieter verpflichtet sehen, zahlreiche rechtliche Risiken. Diese sind besonders im Bereich des Nutzerdatenschutzes gravierend.

Der Referentenentwurf regelt eine Materie im Überschneidungsbereich zwischen Unionsrecht und nationalem Recht, geht auf die dadurch entstehenden Spannungsverhältnisse aber nicht ein und löst sie schon gar nicht auf. Während die Diensteanbieter der DSGVO unterliegen und entsprechende Pflichten zu erfüllen haben, sind die ihnen gegenüberstehenden Behörden im Bereich der Strafverfolgung dem nationalen Recht unterstellt, welches sich wiederum im Rahmen der Richtlinie (EU) 2016/680 halten muss. Der Referentenentwurf verschiebt den europarechtlichen Rahmen hier unzulässig zu Lasten der Diensteanbieter und auch der betroffenen natürlichen Personen.

Darüber hinaus bestehen die Verstöße gegen das Europarecht, die schon dem NetzDG anhaften, im Referentenentwurf weiter fort. Insbesondere wird das Herkunftslandprinzip des Art. 3 der Richtlinie (EG) 2000/31 über den elektronischen Geschäftsverkehr (ECRL) missachtet, wenn Diensteanbieter, egal in welchem europäischen Land diese niedergelassen sind, Prüfungs- und Meldepflichten nach deutschem Recht haben sollen. Ebenso wird die Bedeutung der Verantwortlichkeitsverteilung nach Art. 14 und 15 ECRL verkannt, indem eine weitgehende Prüfungspflicht nach strafrechtlichen Maßstäben eingeführt wird, ohne dass der Diensteanbieter tatsächlich Kenntnis von der Rechtswidrigkeit von Inhalten hat.

5. Der Referentenentwurf tangiert im Bereich der Kinderpornographie bereits über Jahre etablierte und gut funktionierende Prozesse

Bereits in der geltenden Fassung des NetzDG, besonders aber in dem hier zur Diskussion stehenden Referentenentwurf befremdet, dass in ein Maßnahmenpaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität Regelungen zu kinderpornographischen Inhalten einbezogen werden. Es handelt sich dabei um einen völlig anderen Deliktsbereich. Auch unterscheiden sich Bekämpfungsstrategien der Diensteanbieter gegen Kinderpornographie vom Umgang mit Äußerungsdelikten, die regelmäßig auf Textmaterial basieren. Kinderpornographisches Material enthält in der Regel Bildmaterial, das unverändert weiterverbreitet wird und deshalb beispielsweise der Analyse von Hash-Werten zugänglich ist.

Google arbeitet seit vielen Jahren mit dem amerikanischen National Center for Missing and Exploited Children, kurz NCMEC[5] zusammen. NCMEC ist eine gemeinnützige Organisation mit Sitz in den Vereinigten Staaten von Amerika, die sich der Prävention der sexuellen Ausbeutung von Kindern

[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018PC0225&from=EN
[4] https://www.cyberscoop.com/un-resolution-internet-cybercrime-global-norms/ mit Link auf den Entwurf.
[5] http://www.missingkids.com/

verschrieben hat. NCMEC betreibt die so genannte Cyber-Tipline, das zentrale Meldesystem der USA für die Online-Ausbeutung von Kindern. Google ist nach US-Amerikanischem Recht verpflichtet, Cybertip reports an NCMEC zu melden; NCMEC muss jedem Cybertip Report nachgehen. NCMEC ist ebenfalls verpflichtet, Cybertip Reports an die Stelle weiterzuleiten, die nach Ansicht von NCMEC zuständig ist. Für Deutschland ist die zuständige Stelle das BKA.

Am 28. Oktober 2019 gab das BKA in einer Pressekonferenz bekannt, dass allein im Jahr 2018 rund 70.000 Meldungen von NCMEC bzgl. Kinderpornographie bzw. Missbrauchsdarstellungen im Internet eingegangen sind, die Deutschlandbezüge aufweisen – im Vergleich zu 2017 eine mehr als doppelt so hohe Zahl. Laut BKA gibt es seit nunmehr sechs Jahren einen andauernden rapiden Anstieg der Hinweiszahlen. Für das Jahr 2019 wird eine ähnlich hohe Zahl erwartet.[6]

Darüber hinaus legt das BKA in seinem Bericht über die im Jahr 2018 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedienangeboten mit kinderpornografischem Inhalt[7] ausführlich dar, dass NCMEC "in der Funktion als hinweisentgegennehmende Stelle für US-Provider (...) die Sachverhalte (...) hinsichtlich eines möglichen Tatortes überprüft und anschließend inklusive der durch die Provider zur Verfügung gestellten Beweismittel (IP-Adresse und Zeitstempel zum Verbreitungsvorgang, gegebenenfalls E-Mail-Adresse oder Benutzername, strafrechtlich relevante Dateien, etc.) an den entsprechenden (Tatort-)Staat weitergeleitet. **Für die Bundesrepublik Deutschland bedeutet dies, dass alle Hinweise aus den USA, auf Besitzer und Verbreiter kinderpornografischer Dateien in oder aus Deutschland heraus, über das NCMEC an das BKA als nationale Zentralstelle für diesen Deliktsbereich weitergegeben werden.**" (Hervorhebung diesseits)

Somit wird das BKA bereits umfassend über Missbrauchsdarstellungen im Internet informiert, die von den Diensteanbietern von ihren Diensten entfernt werden. Die im Referentenentwurf vorgeschlagenen Maßnahmen erscheinen daher jedenfalls in diesem Deliktsbereich als eine Doppelung und dürften obsolet sein. Eine Beibehaltung dieser Vorschrift würde daher ohne jeden erkennbaren Zugewinn für Strafverfolgungsbehörden allein ein Mehr an administrativen Prozessen bei Diensteanbietern und Strafverfolgungsbehörden bedeuten, für die kein rechtfertigender Grund ersichtlich ist.

6. Der Referentenentwurf greift der NetzDG Evaluierung vor

Die Begründung zum NetzDG in seiner derzeitigen Fassung sieht eine Evaluierung des Gesetzes binnen drei Jahren nach seinem Inkrafttreten vor. Die Bundesregierung soll umfassend prüfen, ob und inwieweit die beabsichtigten Wirkungen des Gesetzes mit Blick auf den Umgang mit Beschwerden erreicht wurden. Darüber hinaus sollen der Erfüllungsaufwand für Wirtschaft und Verwaltung, unbeabsichtigte Nebenwirkungen sowie die Akzeptanz und Praktikabilität der Regelungen untersucht werden. Sämtliche diesbezüglichen Erkenntnisse sollen durch das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) in einem Gesamtevaluierungsbericht zusammengeführt werden.

Google hat zwei Evaluationsfragebögen (von Prof. Dr. Martin Eifert, LL.M., HU Berlin, der im Auftrag des BMJV eine Evaluierung des Gesetzes durchführt, sowie vom Statistischen Bundesamt) erhalten, deren Antworten Ende 2019 fertiggestellt und an die beiden Stellen versandt wurden. Zu diesem Zeitpunkt war der Referentenentwurf aber bereits geschrieben und veröffentlicht. Es ist aus Sicht von Google nicht nachvollziehbar, warum eine Änderung und sogar Erweiterung des NetzDG vor dessen vorgeschriebener Evaluierung auf den Weg gebracht wird, statt deren Ergebnisse abzuwarten und diese auszuwerten. Die Frage drängt sich auf, ob seitens der Verantwortlichen überhaupt ein ernsthaftes Interesse besteht, das NetzDG sinnvoll nachzubessern. Es ist jedenfalls irritierend, dass eine umfassende Gesetzesänderung

[6] https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2019/pm191028_HandoutPK.pdf
[7] http://dipbt.bundestag.de/dip21/btd/19/127/1912725.pdf

vorgenommen wird, ohne die Gelegenheit zu nutzen, offensichtliche Unzulänglichkeiten des bestehenden Gesetzes zu beheben, zumal auf letztere bereits vielfach hingewiesen wurde. Im Gegenteil würden mit dem vorliegenden Gesetzespaket bei seiner Anwendung neue rechtliche und tatsächliche Probleme geschaffen, ohne die bekannten anzugehen.

II. Bisherige Praxis der Datenbeauskunftung sowie Alternativvorschläge

1. Google unterstützt bereits seit vielen Jahren die mit der Strafverfolgung oder Gefahrenabwehr befassten Behörden

Die Google Ireland Ltd. als Diensteanbieter für Google Dienste und YouTube, die von Nutzern aus dem Europäischen Wirtschaftsraum und der Schweiz in Anspruch genommen werden (bis zum 21.01.2019 die Google LLC und die YouTube LLC), kommt auch als im Ausland ansässiger Diensteanbieter seit vielen Jahren Datenauskunftsersuchen nach, ohne die mit der Strafverfolgung oder Gefahrenabwehr befassten Behörden in Deutschland undifferenziert auf den Rechtshilfeweg zu verweisen. In den vergangenen Jahren ist die Zahl dieser Ersuchen signifikant gestiegen. Allein von Januar bis Juni 2019 hat die Google Ireland Ltd. knapp 10.000 Anfragen von Behörden aus Deutschland erhalten. Im Vergleich dazu hat Google im zweiten Halbjahr 2018 nur knapp 8.500 Anfragen von Behörden aus Deutschland erhalten, was einen Anstieg um 16% ausmacht. Über die letzten zehn Jahre ist die Anzahl der Auskunftsersuchen aus Deutschland um über 2000% gestiegen. Genaue Zahlen für Deutschland (inklusive des prozentualen Anteils, in wie vielen Fällen Daten beauskunftet wurden) sind unter dem nachfolgenden Link online einzusehen:
https://www.google.com/transparencyreport/userdatarequests/DE/.

Eine am 20. Dezember 2019 veröffentlichte Studie von Europol im Rahmen des SIRIUS-Projekts[8] zeigt, dass 38% aller Auskunftsersuchen an Diensteanbieter aus Deutschland erfolgen, gefolgt von Frankreich mit knapp 19%. Betrachtet man die Zahlen der G6-Staaten (Deutschland, Frankreich, Großbritannien, Polen, Spanien und Italien,) so sind ihre Behörden für rund 90% der Überwachungsmaßnahmen in der Europäischen Union verantwortlich. Die Gesamtbeauskunftungsrate für Ersuchen aus Deutschland liegt 2018 laut Studie bei 65%. Die Europol Studie zeigt, dass die Beauskunftung von Bestands- und Nutzungsdaten weitgehend funktioniert. Werden Ersuchen durch die Diensteanbieter abgelehnt, liegt dies in der Regel an den konkreten Anfragen der Behörden (z.B. fehlende Nennung der einschlägigen Ermächtigungsgrundlage, fehlende Identifizierung des in Rede stehenden Benutzerkontos etc.). Nach der Studie ist es für die Ermittlungsbehörden ferner aufgrund mangelnder technische Kenntnis oft schwierig, die beauskunfteten Daten der Diensteanbieter auszuwerten.

Um Auskunftsersuchen der mit der Strafverfolgung oder Gefahrenabwehr befassten Behörden in Deutschland zeitnah und effizient bearbeiten zu können, hat Google 2018 das sog. “Law Enforcement Request System”, kurz “LERS“ entwickelt und Strafverfolgungsbehörden zur Nutzung von konkreten Auskunftsersuchen zur Verfügung gestellt. Über dieses System können verschlüsselt Datenabfragen übermittelt sowie entsprechende Auskünfte abgerufen werden. LERS verfügt über ein Support-Center, über welches Informationen zu Googles Prozessen und Produkten abgerufen werden können. LERS soll die weltweite Plattform von Google zur Einreichung von Auskunftsersuchen und den dazugehörigen Dokumenten werden. Deutschland ist eines der ersten europäischen Länder, in dem Google LERS eingeführt hat. Die Plattform wurde zusammen mit dem BKA und den Landeskriminalämtern vorab ausführlich getestet. In der Praxis hat sich dieses LERS-Angebot bereits als so effektiv erwiesen, dass der Empfangsberechtigte, der “Inlandsbriefkasten”, gem. § 5 Abs. 2 NetzDG von den Behörden faktisch nicht genutzt wird. Dies belegt unseres Erachtens eindrücklich, dass Erfahrung und Kooperationsbereitschaft der Diensteanbieter zu effektiveren Problemlösungen führen können als weitere gesetzliche Verpflichtungen, die in die Grundrechte einer erheblichen Anzahl von Nutzern eingreifen würden.

Die Grenze zwischen Nutzungs- und Inhaltsdaten verläuft oft fließend; im Ausland ansässige Diensteanbieter wie die Google Ireland Ltd. müssen bei Inhaltsdaten aufgrund des mehrseitigen

[8] https://www.europol.europa.eu/newsroom/news/sirius-european-union-digital-evidence-situation-report-2019

Spannungsverhältnisses der betroffenen Rechtsgüter und Interessen auf den Weg der Rechtshilfe verweisen. In der Europol Studie geben 49,7% der Ermittler an, dass dieser Prozess mit durchschnittlich etwa zehn Monaten zu lange dauert. Die anfragenden Behörden können zwar ein Ersuchen zur Datensicherung bei den Diensteanbietern einreichen, bis der Rechtsweg beschritten ist. Dies wird aber häufig vergessen. Die vorgesehenen Regelungen lösen diese Problematik im Spannungsverhältnis zwischen DSGVO, den Grundrechten der betroffenen Nutzer im Kontext internationaler rechtlicher Vorgaben nicht auf.

Bei Gefahr für Leib und Leben kann Google zudem telefonisch rund um die Uhr, auch am Wochenende, erreicht werden. Um einen reibungslosen Ablauf in Notfallsituationen sicherzustellen, hat Google regelmäßig in der Vergangenheit das “Emergency Disclosure Request” Formular an deutsche Behörden versandt und verteilt; im Falle einer Gefahr für Leib und Leben ist es Google möglich, unmittelbar Daten zur Abwendung einer drohenden Lebensgefahr zur Verfügung zu stellen.

2. Alternativvorschläge

Gerade weil die Einführung einer Meldepflicht (vgl. § 3a NetzDG-E) einen weitreichenden Systembruch mit geltendem Recht bedeuten würde (vgl. C.), muss sie mit Augenmaß und mit Blick auf die zentralen rechtsstaatlichen Grundsätze sowie im Einklang mit datenschutzrechtlichen Prinzipien diskutiert und ggf. umgesetzt werden.

Mit dem Ziel der Ermöglichung effektiver Strafverfolgung der Hasskriminalität im Online-Bereich hat sich Google gemeinsam mit der Zentral- und Ansprechstelle Cybercrime (ZAC) in Nordrhein-Westfalen über mögliche praxisnahe Verfahren ausgetauscht, die rechtsstaatlichen Grundsätzen gerecht werden würden.

Es herrschte Einigkeit darüber, dass eine Fokussierung auf bestimmte, besonders demokratieschädliche Tatbestände erfolgen müsse, so z. B. auf §§ 86, 86a und 130 StGB. Die in § 3a NetzDG-E erfassten Straftatbestände sind zu weitreichend bzw. bereits anderweitig Teil einer Zusammenarbeit mit Strafverfolgungsbehörden (vgl. E. Sonderaspekt: Bekämpfung von Kinderpornographie). Ohne eine Einschränkung der Straftatbestände droht ein Kollaps der Strafverfolgung, insbesondere bei den Staatsanwaltschaften mit der Folge gesellschaftlich unerwünschter Konsequenzen.

Da sich manche Erscheinungsformen des Rechtsextremismus und der Hasskriminalität neben der analogen Welt auch im Internet abspielen, müssen Justiz und Strafverfolgung dort ebenfalls präsent sein. Die Erstattung einer Strafanzeige online muss erleichtert werden, z.B. durch die Entwicklung einer Musteranzeige, die digital von Bürgern für individuelle Strafanzeigen genutzt werden kann, die dann wiederum von Seiten der mit der Strafverfolgung befassten Behörden bearbeitet und weiterverfolgt werden können. Aus Sicht von Google sollten Schwerpunkt-Staatsanwaltschaften für solche Online-Anzeigen zuständig sein. Für Betroffene ist es nicht nachvollziehbar, wenn sie Anzeige bei den Strafverfolgungsbehörden erstatten, dann aber keine weitere Verfolgung ihrer Anzeige stattfindet. Es muss demnach auch eine Einbettung weiterer Maßnahmen, wie z. B. Opferschutz und Aufklärung, online stattfinden.

Es gibt unterschiedliche Möglichkeiten, die dazu beitragen könnten, Verfolgung von online begangenen Straftaten durch die Staatsanwaltschaften zu verbessern. So könnten Diensteanbieter beispielsweise Beschwerdeführer und Betroffene von Hasskriminalität auf die Möglichkeit der Erstattung einer Online-Strafanzeige bei den zuständigen Stellen hinweisen und diese mit weiteren hilfreichen Informationen zur Substantiierung einer Anzeige unterstützen. Alternativ, bei Feststellung einer möglichen Strafbarkeit nach §§ 86, 86a und 130 StGB, könnten die Diensteanbieter die Staatsanwaltschaften unterstützen, selbst eine Sicherung öffentlich zugänglicher Inhalte noch vor deren

Entfernung vorzunehmen. Eine Beauskunftung über den Weg der Rechtshilfe, der für bereits entfernte Inhalte eingeschlagen werden müsste, wäre damit nicht nötig. Im Gegensatz zum Referentenentwurf würden IP-Adressen und Portnummern an dieser Stelle ebenfalls noch nicht beauskunftet werden, so dass das derzeit geltende Doppeltürmodell beibehalten werden könnte. Ein solches Verfahren wäre sehr viel weniger grundrechtseinschränkend, aber gleichwohl effizient.

Stellt die Staatsanwaltschaft bei Überprüfung der durch den Beschwerdeführer oder den Betroffenen erstatteten Strafanzeige einen Anfangsverdacht für das Vorliegen einer Straftat fest, können nutzerbezogene Informationen über ein formelles Auskunftsersuchen durch die Strafverfolgungsbehörden bei den Diensteanbietern erfragt werden. Google z.B. hält dafür die zuvor beschriebene Plattform “LERS” vor, welche in Zusammenarbeit mit dem BKA und Vertretern von LKAs in Deutschland eingeführt wurde und zu einer erheblichen Beschleunigung der Beauskunftung geführt hat (vgl. B.I).

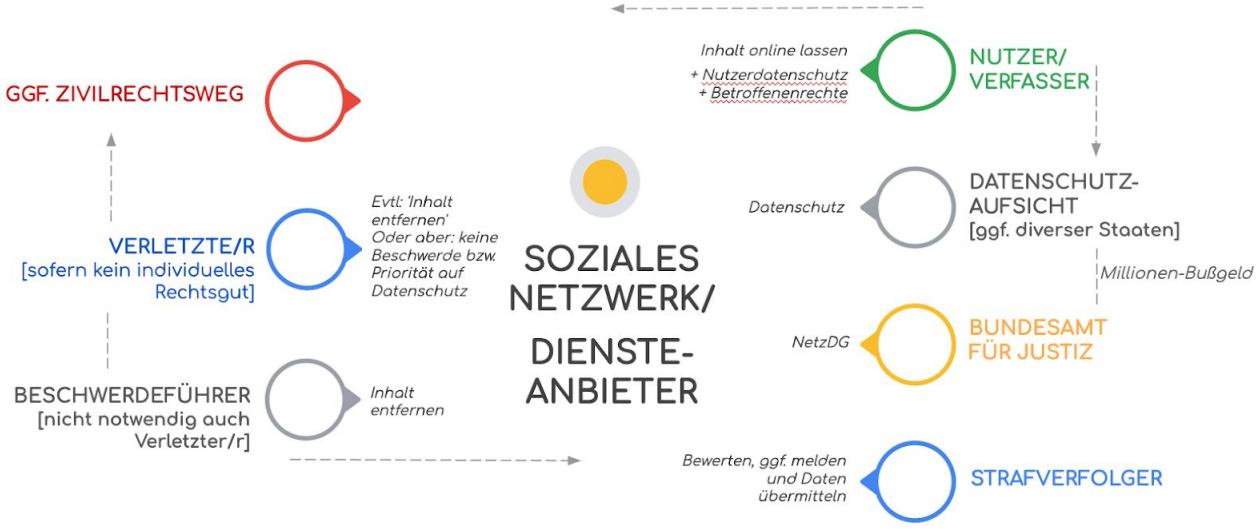
III. Anmerkungen zu einzelnen Artikeln des Referentenentwurfs

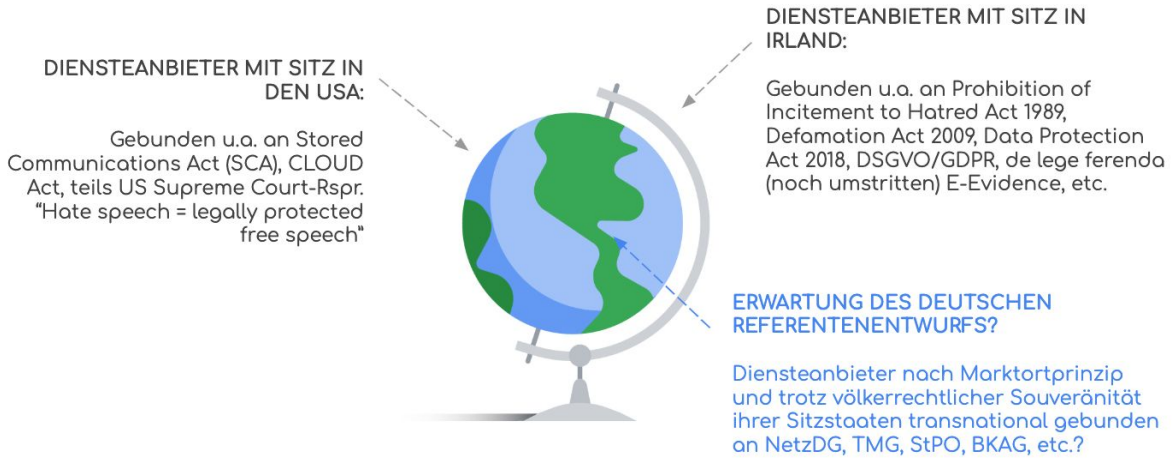
Diensteanbieter von Plattformen wie Google und YouTube sehen sich als Intermediäre divergierenden Interessen und Forderungen verschiedener Beteiligter gegenüber, die sie in einen Ausgleich bringen müssen, oft sogar über verschiedene Staaten hinweg. Anders als der Referentenentwurf suggeriert, entspricht es häufig nicht der Lebensrealität, dass ein selbst betroffener Beschwerdeführer mit einer substantiierten Beanstandung an den Diensteanbieter herantritt. Vielmehr verlangen oft Dritte, nicht selbst Betroffene, die Entfernung und Verfolgung einer für den außenstehenden Diensteanbieter nicht erkennbaren Bedrohung durch einen Nutzer außerhalb derselben Rechtsordnung.

Der Referentenentwurf würde vielmehr erhebliche Anwendungsschwierigkeiten mit sich bringen, weil die Diensteanbieter

- als neutrale Außenstehende “zwischen allen Stühlen” (vgl. nachfolgendes Schaubild) sitzen,
- häufig in unsubstantiierter Form und bisweilen auch nur von unbeteiligten Dritten auf einen Sachverhalt hingewiesen werden, der sich regelmäßig einer Schwarz-Weiß-Betrachtung entzieht,
- dabei zudem als private Laien wie “Hilfssheriffs” eine strafrechtliche Bewertung vornehmen (und nunmehr sogar die Strafverfolgung initiieren) sollen,
- dies tun müssen orientiert an Tatbestandsmerkmalen, die (weit im Vorfeld konkreter Rechtsgutverletzungen) unbestimmt, hoch auslegungsbedürftig und umstritten sind und
- mit Sitz im Ausland dabei oft divergierende Anforderungen aus unterschiedlichen Kulturen und Rechtsordnungen, auch außerhalb der EU, berücksichtigen sollen, die noch nicht einmal ansatzweise harmonisiert sind.

Zwei Skizzen sollen vorab die Komplexität veranschaulichen:





Darüber hinaus will der Referentenentwurf mit der „Bekämpfung von Rechtsextremismus und Hasskriminalität im Internet“ einen Bereich mittels Strafrecht regeln, der vor zentralen grundsätzlichen Fragen und Herausforderungen steht:

- Wie gelingt eine nationale, nach wie vor an Ländergrenzen gebundene Strafverfolgung in globalen sozialen Netzwerken?
- Wie sind Strafverfolgung und Gefahrenabwehr bzw. Repression und Prävention noch voneinander abzugrenzen, wenn die Legislative das Strafrecht immer weiter in das Vorfeld des Anfangsverdachts und der konkreten Rechtsgutsverletzung verlagert?
- Wie sind die verfassungs- und datenschutzrechtlichen Implikationen zu lösen, wenn an dieser Schnittstelle die Privatwirtschaft bei der Initiierung von Strafverfahren in die Pflicht genommen und damit eine genuine Staatsaufgabe ausgelagert wird?
- Wie sind diese schon auf nationaler Ebene hochkomplexen Fragen im grenzüberschreitenden Kontext und gegenüber in einer anderen Rechtsordnung ansässigen Diensteanbietern zu beantworten?

Diese Probleme stehen überdies auch untereinander in Wechselwirkung. Für keine dieser hochkomplexen Grundlagenfragen findet der Entwurf jedoch eine Lösung. Er scheint sich ihrer nicht einmal bewusst. Stattdessen belastet er die Diensteanbieter mit den daraus folgenden Pflichtenkollisionen und zu erwartenden alltäglichen Anwendungsschwierigkeiten.

1. Zur geplanten Änderung des StGB (Art. 1 des Entwurfs)

a. Würden die geplanten Änderungen im Bereich des materiellen Strafrechts in Kraft treten, wären Diensteanbieter sozialer Netzwerke bei der Inhaltskontrolle im Umfang des § 1 Abs. 3 NetzDG zukünftig mit noch größerer Unbestimmtheit konfrontiert.

Folgende Beispiele mögen dies verdeutlichen:

aa. Würde in den Katalog des **§ 126 StGB-E** auch die gefährliche Körperverletzung gem. § 224 StGB aufgenommen, würden die unbestimmten Rechtsbegriffe dieser Norm zu großen

Anwendungsschwierigkeiten führen. Beispielsweise kommt es nach der Rechtsprechung des BGH für die Frage, ob ein Schuh am Fuß als gefährliches Werkzeug i.S.d. § 224 StGB anzusehen ist, auf die Umstände des Einzelfalles an, z.B. auf die Beschaffenheit des Schuhs oder mit welcher Heftigkeit und gegen welchen Körperteil getreten wird. Anbieter sozialer Medien könnten für § 224 StGB maßgebliche Umstände regelmäßig nicht rechtssicher feststellen.
Der Tatbestand des § 224 StGB wird bei der Einbindung in § 126 StGB aber selbst diese durch die Rechtsprechung erarbeiteten Konturierungen verlieren, denn bekanntlich muss bei § 126 StGB die in Aussicht gestellte Tat "nach Zeit, Ort und Opfer" gerade noch nicht näher konkretisiert sein. Zukünftig müssten sich Diensteanbieter z.B. damit befassen, ob ein Kommentar zu einem Video wie "Ich werde [X] richtig heftig vor das Schienbein treten" bereits die Androhung einer gefährlichen Körperverletzung im Sinne der §§ 126, § 224 StGB darstellt und ob der entsprechende Kommentar deshalb entfernt und gemeldet werden muss. Ob der angekündigte Tritt metaphorisch gemeint war oder bei der avisierten Tat im Gegenteil Schuhe getragen werden sollen und ggf. welche, kann sich dem Diensteanbieter nicht erschließen.

bb. Entbehrlich mag die Feststellung konkreter Umstände für die Prüfung sein, ob sich die Äußerung zugleich als Bedrohung i.S.d. **§ 241 StGB-E** darstellt, dessen Erweiterung der Entwurf ebenfalls plant. Für diesen Tatbestand soll es nicht einmal mehr auf die Verwendung eines gefährlichen Werkzeugs ankommen, sondern jede Androhung einer Tat gegen die körperliche Unversehrtheit soll ausreichen. Die Bedrohung kann im Rahmen des § 241 StGB auch über Dritte erfolgen, wenn die Weitergabe an den Adressaten vom Vorsatz des Täters umfasst ist. Die Tatbestände des § 126 StGB-E und des § 241 StGB-E würden somit an Trennschärfe verlieren. Diensteanbieter sozialer Medien können auch deshalb nicht rechtssicher einordnen, ob §§ 241 StGB-E unter Beachtung des Vorsatzes einschlägig ist, weil die Rechtswidrigkeit gem. § 1 Abs. 3 NetzDG allein anhand des objektiven Tatbestands zu prüfen und zu messen ist.

cc. Bis zur Klärung durch die Rechtsprechung muss ein Diensteanbieter im Hinblick auf die Feststellung rechtswidriger Inhalte i.S.d. § 1 Abs. 3 NetzDG ein Sanktionsrisiko gem. § 4 i.V.m. § 3 und § 3a NetzDG wegen struktureller Umsetzungsdefizite eingehen. Zudem bestehen bei unterbliebener Entfernung nach einer substantiierten Beanstandung auch Risiken der Teilnahme an der jeweiligen Haupttat. Alternativ mag der Diensteanbieter jeweils "vorsorglich entfernen und melden" mit allen unerwünschten Konsequenzen eines Overblockings und Overreportings, bis hin zu datenschutzrechtlichen Risiken in Grenzfällen.

b. Ebenso groß wie die absehbaren Anwendungsschwierigkeiten - gerade im Kontext des NetzDG - sind die kriminalpolitischen Bedenken gegen eine Vorverlagerung der Strafbarkeit. Der Tatbestand des § 140 StGB z.B. reicht als abstraktes Gefährdungsdelikt bereits in seiner jetzigen Fassung weit in das Vorfeld konkreter Rechtsgutsverletzungen hinein. Soweit Schutzgut und Normzweck überhaupt erkennbar sind, soll nach der herrschenden Meinung der öffentliche Frieden geschützt werden, in dem ein "psychisches Klima" verhindert wird, in dem bestimmte Straftaten "gedeihen".[9] Die Kommentarliteratur rügt schon heute, dass sich eine solche Zielsetzung jeder validen empirischen Messung entzieht. Für die geplante weitere Ausdehnung der Vorfeldkriminalisierung würden all diese Kritikpunkte erst recht gelten.

Auch ist das Vorfeld konkreter Tatbegehungen ohnehin durch Strafbarkeitsrisiken der Teilnahme erfasst. Als psychische Beihilfe wurde etwa ein "Drängen zur geplanten Tatausführung in vorbereitenden Tatplanungsgesprächen" bewertet (OLG Stuttgart, Urteil vom 06.07.2012 - 6-2 StE 2/10). Die versuchte Anstiftung zu Verbrechen ist über § 30 StGB erfasst. Bei öffentlicher Begehungsweise erfolgt eine noch weitergehende Vorverlagerung durch § 111 StGB.

[9] Schönke/Schröder/Sternberg-Lieben, 30. Aufl. 2019, StGB § 140 Rn. 1; BeckOK StGB/Heuchemer, 44. Ed. Nov. 2019, StGB § 140 Rn. 3.1.

Die gleichzeitig geplante Änderung von § 140 StGB-E, der auf § 126 StGB verweist, führt nun dazu, dass ein “Daumen hoch”-Emoji strafbar sein könnte, das unter die Ankündigung eines geplanten Tritts gesetzt wird. Völlig offen ist auch hier, von welchen konkreten Umständen der angekündigten Tat die Beteiligten dabei jeweils ausgehen müssten.

(Negative) Erfahrungen mit einer noch weitergehenden Vorfeldkriminalisierung eines “Befürwortens geplanter Straftaten” bestehen ohnehin: Mit § 88a StGB a.F. wurde in den 1970er Jahren nicht die allgemeine Befürwortung unter Strafe gestellt, sondern nur die “verfassungsfeindliche Befürwortung”, da das Tatbestandsmerkmal ‘Befürwortung’ als zu weit erkannt wurde (vgl. die Ausführungen des Wissenschaftlichen Dienst des Bundestags). Im damaligen Bericht und Antrag des Sonderausschusses für die Strafrechtsreform heißt es, da “das Tatbestandsmerkmal ‚Befürwortung‘ seinem begrifflichen Inhalt nach sehr weit ist, muss der Tatbestand in verschiedener Hinsicht eingeschränkt werden, um Gefahren für die grundgesetzlich garantierten und geschützten Bereiche der Meinungs- und Pressefreiheit sowie der Freiheit von Kunst, Wissenschaft, Forschung und Lehre zu vermeiden. [...] Die Meinungs- und Pressefreiheit stellen wichtige Elemente des demokratischen Rechtsstaates der Bundesrepublik Deutschland dar. Die Bürger müssen grundsätzlich die Freiheit haben und behalten, sich auch zu dem Problem der Gewaltanwendung frei zu äußern. [...] Diese Frage könne nicht mit Mitteln des Strafrechts gelöst werden.” (Bericht und Antrag des Sonderausschusses für die Strafrechtsreform, BT-Drs. 7/ 4549, S. 7). Trotz der damals in § 88a StGB a.F. umgesetzten tatbestandlichen Begrenzung “verfassungsfeindlicher Befürwortung” wurde die Norm nach wenigen Jahren wieder aufgehoben, da die Beeinträchtigungen der Meinungsfreiheit unverhältnismäßig groß schienen. Bei einer erneuten Beratung eines § 130b StGB-E Ende der 1980er Jahre setzten sich diese Bedenken im Ergebnis erneut durch (BT-Drs. 11/4359, S. 16f).

Vor diesem Hintergrund ist befremdlich, dass sich der Referentenentwurf weder erkennbar mit den Vorerfahrungen der Legislative auseinandersetzt noch mit der erwähnten Ausarbeitung des Wissenschaftlichen Dienstes.

2. Zur geplanten Änderung der StPO (Art. 2 des Entwurfs)

Der Entwurf mag “in Umsetzung des Maßnahmenpakets” das Ziel verfolgen, “eine Auskunftsbefugnis gegenüber den Diensteanbietern zu schaffen, damit die dort noch vorhandenen Daten zu strafrechtlich relevanter Hasskriminalität herausverlangt werden”, wie es im Schreiben des BMJV an die betroffenen Fachkreise und Verbände vom 18.12.2019 heißt.

Die vorgesehenen Neuregelungen der StPO beschränken sich aber gerade nicht auf einen konkreten Straftatenkatalog. Entgegen einer Regelungstechnik wie sie etwa § 100a StPO vorsieht, fehlt in § 100g und § 100j StPO-E eine Beschränkung auf bestimmte Tatbestände, etwa die in § 1 Abs. 3 NetzDG genannten. Daher ist die Reichweite selbst im Bereich der StPO keineswegs auf “Daten zu strafrechtlich relevanter Hasskriminalität” oder jedenfalls zu den von § 1 Abs. 3 NetzDG erfassten Straftatbeständen beschränkt.

Widersprüche ergeben sich zudem spätestens aufgrund der StPO-Bezugnahme des § 46 OWiG für die Verfolgung von Ordnungswidrigkeiten, der den Verfolgungsbehörden im Grundsatz dieselben Rechte und Pflichten wie den Staatsanwaltschaften bei der Verfolgung von Straftaten einräumt. § 46 Abs. 3 OWiG sieht von diesen Befugnissen eine Ausnahme vor für Auskunftsersuchen über Umstände, die dem Post- und Fernmeldegeheimnis unterliegen und daher unzulässig sind. An das Post- und Fernmeldegeheimnis sind gem. § 7 Abs. 3 S. 2 TMG bekanntlich auch Diensteanbieter von Telemedien gebunden. Ob und welche Datenabfragen davon berührt sind (vgl. den BVerfG-Beschluss vom 24. Januar 2012, 1 BvR

1299/05 für die identifizierende Zuordnung dynamischer IP-Adressen[10]), ist jedoch gerade im Bereich der Telemediendienste umstritten.[11]

Entsprechend fraglich ist, ob sich ohne eine Klarstellung im GBRH-E "eine Begrenzung des Eingriffs auf hinreichend gewichtige Rechtsgüter, eine normenklare Ausgestaltung und ein Verfahren, das hinreichende Transparenz und Kontrolle gewährleistet", wie vom Entwurf selbst angestrebt, realisieren lässt. Diese Unklarheit betrifft keineswegs nur Bagatellen, sondern z.B. auch Ermittlungsverfahren im Bereich GWB, DSGVO, NetzDG, etc.

3. Zur geplanten Änderung des BKAG (Art. 3 des Entwurfs)

In Bezug auf das BKAG zeigt sich das gleiche Muster, das auch in Bezug auf das NetzDG insgesamt zu beklagen ist: Die geplanten Änderungen des BKAG vertiefen nochmals systematische Widersprüche, die bereits aus der letzten BKAG-Reform resultieren. Zusätzlich ergeben sich vor allem aufgrund der Gleichstellung von Telekommunikationsdiensten und Telemediendiensten auch neue Kritikpunkte grundsätzlicher Art.

Bemerkenswert ist insbesondere, dass das BMJV noch im Dezember 2016 im Zuge einer Stellungnahme zum BKAG-Referentenentwurf des BMI "*grundsätzliche Erwägungen*" gegen die "*Einbeziehung von Telemedien*" in § 10 BKAG-E erhoben hat, (Anmerkungen zum Referentenentwurf vom 8.12.2016[12], S. 16, dort "*Die Einbeziehung von Telemedien wird aus grundsätzlichen Erwägungen abgelehnt.",* und S. 41, dort "*BMJV fordert Streichung der Verpflichtung von Telemediendienstleistern*"). Dass es heute für Bestandsdatenabfragen bei Diensteanbietern von Telemedien an einer expliziten Befugnisnorm fehlt (so S. 29 des GBRH-E), liegt vermutlich maßgeblich an den Erwägungen, die im Zuge der damaligen BKAG-Reform zur Streichung führten. Sofern für die Abkehr von diesen Grundsätzen heute sachliche Motive bestehen, lassen sich diese dem dem Entwurf nicht entnehmen.

Zudem verwundert die inkonsistente Behandlung von § 10 und § 40 BKAG: Beide Normen regeln die Bestandsdatenauskunft, jedoch für unterschiedliche Aufgaben des BKA: § 10 betrifft die Bereiche "als Zentralstelle nach § 2", "Schutz von Mitgliedern der Verfassungsorgane und der Leitung des BKA nach § 6" und "zum Zeugenschutz nach § 7". § 40 hingegen gehört zum Aufgabenbereich "Abwehr von Gefahren des internationalen Terrorismus" nach § 5 BKAG. Die jüngere Fassung des GBRH-E sieht - anders als eine frühere Version - nur noch eine Änderung des § 10 BKAG, nicht mehr des § 40 BKAG vor. Dies erstaunt, weil die Bundesjustizministerin öffentlich als Hauptziel des Referentenentwurfs gerade den Bereich der Terrorabwehr betont. Die Bestandsdatenauskunft in § 40 BKAG gehört - wie gerade erwähnt - genau zu diesem Aufgabenbereich.

Die Unklarheiten mehren sich noch dadurch, dass § 52 Abs. 2 BKAG schon eine Beauskunftung von *Nutzungsdaten* durch Diensteanbieter von Telemedien vorsieht und zwar *ausschließlich* im genannten Bereich der Terrorabwehr.

Eine "Neuregelung für Bestands- und Nutzungsdaten" gleichermaßen, wie sie im GBRH-E für Telemedien in § 100g StPO-E und § 100j StPO-E angestrebt wird, ergibt sich somit für das BKAG aus dem Entwurf in keiner Weise: Im Bereich der Zentralstellenfunktion wie auch des Schutzes von

---

[10] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2012/01/rs20120124_1bvr129905.html

[11] Differenziert nach Bestands- und Nutzungsdaten etwa Spindler/Schmitz/Schmitz, 2. Aufl. 2018, TMG § 14 Rn. 32

[12] https://fragdenstaat.de/anfrage/stellungnahme-an-bmi-zum-bka-gesetz/64292/anhang/161208_referentenentwurf-bkag-mit-anmerkungen-bmjv.pdf

Mitgliedern der Verfassungsorgane und des Zeugenschutzes (§§ 2, 6 und 7 BKAG) würde es (weiter) an einer Regelung zur Abfrage von Nutzungsdaten fehlen. Im Rahmen der Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus (§ 5 BKAG) hingegen ist eine solche Nutzungsdaten-Regelung in § 52 Abs. 2 schon jetzt vorgesehen, jedoch offensichtlich keine Angleichung des § 40 BKAG-E für Bestandsdaten (mehr) geplant. Eine Begründung für diese Differenzierung fehlt im Entwurf.

Soweit bei Bestandsdatenabfragen des BKA in der Praxis gegenüber Diensteanbietern von Telemedien bislang auf die Generalklausel des § 9 BKAG, auf die Befugnisnorm der Diensteanbieter oder beide Normen in Kombination verwiesen wird, ist für diesen Rückgriff spätestens angesichts der nunmehr ausdrücklich für erforderlich gehaltenen Regelung, der auf S. 28 des Entwurfs klar ausgeführten Bedenken gegen Generalklauseln und der unterschiedlichen Behandlung in § 10 und § 40 BKAG-E kein Raum mehr.

Ein Motiv der intensiven Befassung mit dem Entwurf liegt genau in diesen Erfahrungen: Die Diensteanbieter sind im Bereich der Eingriffsgrundlagen seit Jahren mit inkonsistenter Gesetzgebung konfrontiert. Sie sind zugleich die Anlaufstellen, die sich sodann im Alltag mit konkreten hoheitlichen Ersuchen auseinandersetzen müssen und im Kontakt mit Behördenvertretern stehen. Obwohl die Behörden die Zulässigkeit “in eigener Verantwortung” prüfen müssen, haben sie zur Rechtslage selbst inzwischen oft mehr Fragen als Antworten und versuchen vielfach, auch noch die rechtliche Bewertung auf die Diensteanbieter abzuwälzen, entgegen der auch in § 15a NetzDG-E nochmals “klargestellten” Systematik, dass die Verantwortung für die Zulässigkeit des Auskunftsverlangens die um Auskunft ersuchenden Stellen tragen.

Selbst eine weitreichende Kooperationsbereitschaft der Diensteanbieter kann sich dabei aber nicht über Wortlaut, Gesetzessystematik und/oder in Gesetzgebungsverfahren dokumentierten “grundsätzliche Erwägungen des BMJV” hinwegsetzen.

4. Zur geplanten Änderung des TMG (Art. 4 des Entwurfs)

Der Entwurf des GBRH-E schießt auch aus einem weiteren Grund über den intendierten Regelungsgegenstand “Daten(herausgabe) zu Hasskriminalität” hinaus: Mit dem Referentenentwurf würde auch die “zweite Tür” des im Entwurf erwähnten Doppeltür-Modells weit geöffnet, insbesondere durch den neu vorgesehenen § 15a TMG-E und seine “Dies gilt auch”-Formulierung in Absatz 1. Das Bundesverfassungsgericht hat u.a. im Beschluss vom 24.01.2012 (1 BvR 1299/05[13]) anschaulich ausgeführt, dass “bei der Regelung eines Datenaustauschs zur staatlichen Aufgabenwahrnehmung (...) zwischen der Datenübermittlung seitens der auskunftserteilenden Stelle und dem Datenabruf seitens der auskunftsuchenden Stelle zu unterscheiden [ist]. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. **Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten**.” (Hervorhebungen diesseits) Da der Referentenentwurf die vermeintlich “klarstellende” Legaldefinition des Bestandsdatenbegriffs in der Rechtsgrundlage für die Übermittlung vorsieht, beschränken sich die Auswirkungen bei weitem nicht nur auf Strafverfolgungsmaßnahmen zur Bekämpfung von Hasskriminalität. In der Gesamtbetrachtung ergeben sich daraus weitreichende - möglicherweise gar nicht intendierte - Folgen für das Gesamtgefüge der Eingriffsgrundlagen.

---

13 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2012/01/rs20120124_1bvr129905.html

a. Bezugnahmen anderer Eingriffsgrundlagen auf das TMG

Diensteanbieter sind nicht nur mit Bestandsdatenabfragen nach StPO und BKAG konfrontiert, die durch den Entwurf neu – und (im Ergebnis auch nur scheinbar) mit dem TMG-E abgestimmt – geregelt werden sollen. Übersehen wird im Entwurf, dass viele andere Gesetze – insb. z.B. Landespolizeigesetze – ebenfalls auf § 14 TMG verweisen. Wenn im Referentenentwurf bei den Ausführungen zur Gesetzgebungskompetenz erwähnt wird, dass es gelte, eine föderale "Rechtszersplitterung" durch eine Regelung im TMG zu vermeiden, so gelingt dies angesichts der Vielfalt der Rechtsgrundlagen für die Datenabfragen gerade nicht. In zahlreichen (Bundes- und Landes-)Gesetzen werden das TKG und das TMG systematisch noch sehr unterschiedlich behandelt. Prozedurale Sicherungen für „besondere Bestandsdaten" wie Zugriffskennungen bzw. Passwörter sind in den meisten dieser Gesetze gerade nur für den Bestandsdatenbegriff des TKG vorgesehen.

Für Bestandsdatenabfragen an Diensteanbieter wird hingegen vielfach noch auf die jeweiligen Generalklauseln der Gesetze zurückgegriffen. Der Entwurf problematisiert diese gängige Behördenpraxis bezeichnenderweise für die Ermittlungsgeneralklausel §§ 161, 163 StPO, nicht aber für andere Regelungen, nicht mal andere Bundesgesetze, auf die die in § 15a Abs. 3 TMG-E genannten Stellen regelmäßig zurückgreifen (siehe sogleich).

Vor allem der Umstand, dass durch die vermeintliche „Klarstellung" in § 15a TMG-E nun auch der Bestandsdatenbegriff des § 14 TMG „per Definition" auf Passwörter erstreckt werden soll, hat daher weitreichende Folgen, wenn die Polizei oder andere in § 15a Abs. 3 TMG aufgeführte Stellen durch „anderen Türen" Zugriff auf das TMG nehmen. Diese sehen überwiegend keine prozeduralen Sicherungen vor wie nunmehr etwa in § 100j Abs. 1 S. 2 StPO.

Gleichzeitig wird den Diensteanbietern durch die „Legaldefinition" nunmehr jede Argumentation abgeschnitten, dass der Zugriff auf Passwörter bei einer Bestandsdatenabfrage (u.a. auf Basis von Generalklauseln) unverhältnismäßig ist. Hier liegt das Risiko einer „Online-Hausdurchsuchung" ohne zusätzliche Sicherung. Dieser sicherungslose Zugriff auf Passwörter und damit ganzer Konten kann einer verfassungsrechtlichen Prüfung nicht standhalten.

a. Beispiel eines Bundesgesetzes:

In § 8a BVerfSchG, auf den auch § 4 MADG und § 3 BNDG verweisen, ist eine Bestandsdatenauskunft wie folgt vorgesehen:

> ***§ 8a BVerfSchG Besondere Auskunftsverlangen***
>
> *(1) Das Bundesamt für Verfassungsschutz darf im Einzelfall bei denjenigen, die geschäftsmäßig Teledienste erbringen oder daran mitwirken, Auskunft über Daten einholen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Teledienste (Bestandsdaten) gespeichert worden sind, soweit dies zur Sammlung und Auswertung von Informationen erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 3 Absatz 1 genannten Schutzgüter vorliegen.*

Trotz der Ablösung des Begriffes durch das TMG im Jahr 2007 wird hier noch auf "Teledienste" Bezug genommen. Dies wurde 2011 auch im Zuge einer Überarbeitung "bewusst beibehalten" (vgl. BT-Drs. 17/6925, S. 12). Dieser Befund mag verdeutlichen, dass die Eingriffsgrundlagen bzw. "Türen" vieler in § 15a Abs. 3 TMG-E bezeichneter Stellen auf Jahre hinaus nicht passgenau und widerspruchsfrei als "Doppeltür" mit § 15a Abs. 1 TMG-E korrespondieren werden.

Auch verdeutlicht ein Vergleich dieses auf “Teledienste” bezogenen § 8a BVerfSchG mit dem nachfolgend angeführten § 8d BVerfSchG, dass eine besondere Regelung für verlangte Zugriffskennungen nur bezogen auf Telekommunikationsdienste vorgesehen ist:

> ***§ 8d BVerfSchG Weitere Auskunftsverlangen***
>
> *(1) Soweit dies zur Erfüllung der Aufgaben des Bundesamts für Verfassungsschutz erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.*

Für “Teledienste” fehlt ein solcher Verweis auf die “gesetzlichen Voraussetzungen der Nutzung”. In diesem Bereich drohen zudem Wertungswidersprüche und Unklarheiten der jeweiligen Bestandsdaten-”Legaldefinitionen”, die bei den jeweiligen Türen des Doppeltür-Modells nicht deckungsgleich sind.

> b. Beispiel eines Landesgesetzes (Polizeirecht in Hessen statt vieler vergleichbarer Regelungen, vgl. etwa auch Niedersachsen und Brandenburg):
>
> ***§ 15a Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG)***
>
> *[...]*
>
> *(2) […] Auskunft über Bestandsdaten nach den §§ 95 und 111 des Telekommunikationsgesetzes können die Polizeibehörden von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, unter den Voraussetzungen des § 12 Abs. 1 Satz 1, Abs. 3 und 4 verlangen (§ 113 Abs. 1 Satz 1 und 3 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 3 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Die Auskunft über Bestandsdaten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse darf nur zur Abwehr einer erheblichen Gefahr verlangt werden.*

In Abs. 2a HSOG fehlt hingegen - letztlich vergleichbar der Situation des BVerfSchG - wiederum eine solche Sicherung für das TMG. Es findet sich nur eine allgemein gehaltene Bezugnahme auf § 14 TMG:

> *(2a) Unter den Voraussetzungen des Abs. 1 können die Polizeibehörden von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, Auskunft über Nutzungsdaten nach § 15 Abs. 1 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 28. September 2017 (BGBl. I S. 3530), verlangen. Die Auskunft kann auch über zukünftige Nutzungsdaten verlangt werden. Unter den Voraussetzungen des § 12 Abs. 1 Satz 1, Abs. 3 und 4 können die Polizeibehörden Auskunft über Bestandsdaten nach § 14 Abs. 1 des Telemediengesetzes*

verlangen. Der Diensteanbieter hat die Daten unverzüglich auf dem von der Polizeibehörde bestimmten Weg zu übermitteln.

Jede Polizeidienststelle kann nach diesen Vorgaben bei Einführung der geplanten Regelungen im Bereich des Gefahrenabwehrrechts auf einfaches Ersuchen hin Passwörter bei den Diensteanbietern erfragen, und das obgleich das Passwort Zugriff auf Bereiche vermitteln kann, die von der polizeilichen Untersuchung nicht umfasst sind. Ein Passwort erlaubt üblicherweise den Zugriff auf ein Nutzerkonto, einschließlich aller Kommunikationsinhalte wie etwa E-Mails, Postings, Direktnachrichten, in der Cloud hinterlegte Dokumente, private oder berufliche Unterlagen, historische Standortdaten, Suchhistorien etc. Darüber hinaus bestünde bei Besitz von Passwörtern die Möglichkeit, selbst Inhalte aus dem Konto heraus zu veröffentlichen, zu kopieren, zu verändern, zu löschen oder Zugriffsrechte zu ändern bis hin zur Ausschließung des Berechtigten.

Im Ergebnis würde die Umsetzung des Gesetzgebungsvorhabens einen massiven Eingriff in die Freiheitsrechte der Bürger, nicht zuletzt auch in das Fernmeldegeheimnis, sowie in datenschutzrechtliche Prinzipien bedeuten. Pointiert ausgedrückt, würden zukünftig “Online-Hausdurchsuchungen” möglich, und zwar ohne weitere Sicherungen wie etwa Richtervorbehalte und zudem zeitlich unbegrenzt. Da die Diensteanbieter die Nutzer selbst nach dem Referentenentwurf über die Herausgabe der relevanten Daten einschließlich Passwörtern nicht in Kenntnis setzen dürften, würde den betroffenen Nutzern faktisch die Möglichkeit genommen, die Datenverarbeitung durch die Ermittlungsbehörden überprüfen zu lassen.

Die vorgeschlagenen Regelungen gehen daher weit über die Bekämpfung von Rechtsextremismus und Hasskriminalität hinaus. Es würde eine rechtlich abgesicherte Überwachungsinfrastruktur geschaffen, die - mangels im Gesetz verankerter strenger Zweckbindung und zeitlicher Beschränkungen - zu allen möglichen Zwecken eingesetzt werden könnte, und damit auch zu Zwecken, die die Freiheitsrechte der Bürger erheblich beeinträchtigen, ohne dass die notwendigen und selbstverständlichen Sicherungsmechanismen der Justiz eingebaut sind. Dieses Ausmaß ist verfassungsrechtlich nicht nur bedenklich, sondern unverhältnismäßig und mithin nicht zulässig.

Ein bemerkenswerter Punkt des Referentenentwurfs ist zudem, dass für Diensteanbieter nicht einmal sicher ist, ob sie auf Grundlage von § 15a TMG-E überhaupt Daten an das BKA herausgeben dürfen, da das BKA selbst nicht in § 15 Abs. 3 TMG-E als Behörde aufgeführt ist. Dementsprechend könnte es sich allenfalls um eine Behörde im Sinne von § 15a Abs. 3 Nr. 1 TMG-E handeln, die also in diesem Fall für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständig ist. Um dies zu beurteilen, müsste der Diensteanbieter also die Zuständigkeit des BKA für den einzelnen Fall nach § 4 BKAG bewerten. Die Unzumutbarkeit liegt auf der Hand.

b. Widerspruch mit Verschlüsselungstechniken

Zusätzlich sieht sich der Diensteanbieter einem Konflikt zwischen dem Datenschutzrecht und den Anforderungen nach § 15a TMG-E ausgesetzt, der erhebliche Rechtsunsicherheit erzeugt. Viele Diensteanbieter speichern Passwörter verschlüsselt, eine Dechiffrierung ist nicht möglich (sog. one-way hash). Dies entspricht der Vorgabe des Art. 32 Abs. 1 lit. a DSGVO, der verlangt, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten. Hierbei werden gerade auch “Pseudonymisierung und Verschlüsselung personenbezogener Daten” als geeignete Maßnahmen explizit benannt. Teils wird sogar bereits eine entsprechende datenschutzrechtliche Verpflichtung zur Verschlüsselung bejaht. Gerade Passwörter werden deshalb regelmäßig so verschlüsselt, dass auch der jeweilige Dienstleister nicht oder nicht ohne weiteres auf diese zugreifen kann. Dies sieht z.B. auch der “Anforderungskatalog

Cloud Computing“ des Bundesamtes für Sicherheit in der Informationstechnik[14] vor. Das Ziel des § 15a TMG-E setzt aber logisch voraus, dass auch Zugriffskennungen einschließlich Passwörtern so übermittelt werden, dass diese durch die anfragenden Behörden genutzt werden können. Der Diensteanbieter wird also vor die Wahl gestellt, entweder auf eine auch nach der DSGVO wesentliche Sicherheitsmaßnahme zu verzichten und damit datenschutzwidrig zu handeln, oder aber eine Herausgabe i.S.d. § 15a Abs. 1 TMG-E tatsächlich unmöglich zu machen und damit im Fall eines konkreten Herausgabeverlangens aufgrund der bereits jetzt absehbar sinnwidrigen Regelung mindestens Erklärungsbedarf zu riskieren, obwohl er nur seine - anderweitigen - Pflichten erfüllt.

Für die Diensteanbieter ergibt sich somit auch hier eine Pflichtenkollision gem. NetzDG und DSGVO und somit das Risiko eines unvermeidlichen Verstoßes gegen eines der Regelwerke.

c. Verstoß gegen das Prinzip der Datenminimierung

§ 15a Abs. 1 TMG-E soll augenscheinlich als mitgliedstaatliche datenschutzrechtliche Erlaubnisvorschrift i.S.d. Art. 6 Abs. 1 c) DSGVO fungieren, die für die Rechtmäßigkeit der Datenverarbeitungen durch die Diensteanbieter im Zusammenhang mit den Auskunftsverfahren sorgen soll. Als solche müsste § 15a Abs. 1 TMG-E den verbindlichen Anforderungen aus Art. 6 Abs. 3b DSGVO genügen.

Die Pflicht des Diensteanbieters aus § 15a Abs. 1 S. 4 TMG-E, bei einer Auskunftserteilung sämtliche unternehmensinterne Datenquellen zu berücksichtigen, verstößt gegen den datenschutzrechtlichen “Grundsatz der Datenminimierung”, verankert in Art. 5 Abs. 1 lit. c DSGVO. Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Speziell für den Bereich der Strafverfolgung legt dies auch Art. 4 Abs. 1 lit. c der Richtlinie (EU) 2016/680 fest.

Diesen Anforderungen genügt es nicht, wenn nach dem Gesetzesentwurf “sämtliche unternehmensinternen Datenquellen” zu berücksichtigen sind. Dies schließt regelmäßig auch solche personenbezogenen Daten mit ein, die für die Aufklärung einer bestimmten Straftat nicht erforderlich sind. Zu denken ist hierbei insbesondere an Nutzungsdaten, die das Verhalten einer Person innerhalb eines Telemediendienstes kleinteilig nachvollziehbar machen, selbst wenn dieses mit einem etwaigen Verstoß nicht in Beziehung steht. Ein Mechanismus, wonach nur die für den Zweck maßgeblichen Daten übermittelt beziehungsweise verarbeitet werden, sieht der Referentenentwurf hingegen nicht vor.

§ 15a Abs. 1 TMG-E wird außerdem von umfangreichen Auskunftsansprüchen der Strafverfolgungsbehörden gespiegelt (§ 100j Abs. 1 S. 1 StPO-E sowie § 1 Abs. 1 BKAG-E). Zusätzlich bestehen auf Grundlage des Referentenentwurfs umfangreiche Berichtspflichten von Diensteanbietern sozialer Netzwerke gegenüber dem BKA (§ 3a NetzDG-E). Im Ergebnis wird eine umfangreiche Datenbank für tatsächliche oder vermeintliche Straftaten und Täter erstellt, die den Charakter einer (unzulässigen) Vorratsdatenspeicherung erreichen kann. Dies gilt insbesondere, wenn an das BKA gemeldete Inhalte und IP-Adressen über entsprechende Auskunftsersuchen mit einer Fülle an Bestands- und Nutzungsdaten angereichert werden, zu denen sogar Passwörter und alle anderen Daten aus den unternehmensinternen Datenquellen gehören. Insofern wird auch gegen Art. 4 Abs. 1 lit. c der Richtlinie (EU) 2016/680 verstoßen, der vorschreibt, dass personenbezogene Daten dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie erhoben werden, nicht übermäßig sind. Dies beachtet der Referentenentwurf offensichtlich nicht.

---

14 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf?__blob=publicationFile&v=4, S.54

d. Verstoß gegen den datenschutzrechtlichen Grundsatz der Transparenz

Weiter widerspricht §15a Abs. 4 S. 2 TMG-E dem in Art. 5 Abs. 1 lit. a DSGVO festgelegten Grundsatz der Transparenz, da der Diensteanbieter über ein Auskunftsersuchen und die erteilte Auskunft gegenüber den "Betroffenen sowie Dritten Stillschweigen zu wahren" hat; Ausnahmen sind nicht vorgesehen. Nach der DSGVO sind personenbezogene Daten aber stets in einer für die betroffene Person nachvollziehbaren Art und Weise zu verarbeiten. Entsprechend legen Art. 13 und 14 DSGVO konkrete Informationspflichten für Verantwortliche gegenüber allen Betroffenen fest. Für die Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung sieht Art. 13 RL (EU) 2016/680 entsprechende Informationspflichten vor. Dadurch ergibt sich für die Diensteanbieter eine unzumutbare Pflichtenkollision, die entweder ihrer Verschwiegenheitspflicht oder ihren Informationspflichten hinsichtlich der Auskunftserteilung nachkommen können.

Ausnahmen zu diesen Informationspflichten sind eng begrenzt und nur dann zulässig, wenn andere Maßnahmen vom Verantwortlichen getroffen werden, die die Rechte, Freiheiten sowie die berechtigten Interessen der betroffenen Personen schützen (s. z.B. Art. 14 DSGVO, Art. 13 Abs. 3 RL (EU) 2016/680). Insbesondere die Voraussetzungen des Art. 14 Abs. 5 DSGVO sind hier aber nicht erfüllt. Auch die Anforderungen an eine Ausnahme nach nationalem Recht gemäß § 33 Abs. 1 Nr. 1 lit. a und lit. b des deutschen Bundesdatenschutzgesetzes (BDSG) i.V.m. Art. 23 DSGVO, die hier dem Grunde nach gleich laufen und die einzige Rechtsgrundlage dafür bieten können, dass auf die an sich notwendige Information verzichtet wird, liegen nicht vor. Die Regelung sieht entsprechende Ausnahmen nur für die Fälle vor, dass die Erfüllung der Aufgaben der jeweiligen Stelle durch die Information gefährdet würde (lit. a) oder die öffentliche Sicherheit oder Ordnung gefährdet werden würde oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde (lit. b). Die Öffnungsklausel in Art. 23 DSGVO verlangt dabei, dass die nationalen Gesetze, die von dieser Gebrauch machen, eine Reihe von Absicherungen der Rechte der Betroffenen vorsehen. Gerade dies wird aber schon für § 33 BDSG in der Literatur in Zweifel gezogen.

§ 15a Abs. 4 S. 2 TMG-E soll es den Diensteanbietern generell, dauerhaft und ausnahmslos untersagen, die betroffenen Personen über das Auskunftsersuchen und die Auskunftserteilung zu informieren; Kompensationsmaßnahmen sind nicht vorgesehen. Die Norm soll also augenscheinlich die Rechte der betroffenen Personen gegenüber den Diensteanbietern nach Art. 13. 14 und 15 DSGVO im Hinblick auf die Verarbeitung der Bestands- und Nutzungsdaten zu Zwecken der Auskunftserteilung vollständig ausschließen. Das geht über das erforderliche Maß der Einschränkung hinaus und ist nach den Vorgaben der DSGVO unzulässig. In der Folge bestehen durchgreifende Zweifel über die Vereinbarkeit dieses nationalen Rechts mit Unionsrecht und damit über die Anwendbarkeit der nationalen Regelung.

Konkret geht § 15a TMG-E über das von Art. 23 DSGVO erlaubte Maß hinaus, indem es die Auskunft auch im Fall der Verfolgung von Ordnungswidrigkeiten erlaubt. Art. 23 DSGVO erlaubt eine Ausnahme von Informationspflichten allgemein nur bei wichtigen Zielen des allgemeinen öffentlichen Interesses (s. Abs. 1 lit. e), sowie anderer ebenso gewichtiger Ziele, die aber konkret benannt werden müssen. Dass die Anforderungen an diese Ziele hoch sind, ergibt sich aus den anderen, explizit genannten Zielen wie der nationalen Sicherheit (Abs. 1 lit. a), die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Abs. 1 lit. c) oder auch der öffentlichen Sicherheit (Abs. 1 lit. b), die nach dem EuGH erst dann bedroht ist, wenn eine tatsächliche und hinreichend schwere Gefährdung vorliegt, die ein Grundinteresse der Gesellschaft berührt (EuGH, 14.03.2000 - C-54/99, Rn. 17 - "Meilicke"; es darf hier gerade nicht der Begriff der öffentlichen Sicherheit aus dem deutschen Verwaltungsrecht herangezogen werden). Dieser Maßstab zeigt, dass eine Ausnahme von der Informationspflicht bei der bloßen Verfolgung einer Ordnungswidrigkeit jedenfalls nicht gerechtfertigt werden kann.

Im Übrigen erkennt auch das deutsche Recht diesen Maßstab ausdrücklich an, indem es in § 46 Abs. 3 OwiG Auskunftsersuchen über Umstände, die dem Post- und Fernmeldegeheimnis unterliegen, ausschließt (s.o. B II).

Dabei ist zu beachten, dass Transparenzpflichten und Informationsrechte den betroffenen Personen stets dazu dienen, ihre weiteren Rechte geltend zu machen. Ohne über die Datenverarbeitung überhaupt Kenntnis zu haben, werden die betroffenen Personen daher von der Ausübung ihrer Rechte gegenüber den auskunftsersuchenden Stellen effektiv ausgeschlossen. Dies gilt indes auch bei der Verarbeitung von personenbezogenen Daten durch die Strafverfolgungsbehörden auf Grundlage von nationalem Recht sowie der Richtlinie (EU) 2016/680. Letztere gibt den Mitgliedstaaten eindeutig auf, auch in diesem Zusammenhang die Betroffenenrechte einschließlich der Informationspflichten zu wahren.

Die geplanten Änderungen sind daher nicht mit den Vorgaben der DSGVO und Richtlinie (EU) 2016/680 in Einklang zu bringen und folglich europarechtswidrig.

e. Rechtsrisiken sind systemwidrig vom Diensteanbieter zu tragen

§ 15a Abs. 5 S. 3 TMG-E beschränkt die Prüfungskompetenz der Diensteanbieter auf die formalen Voraussetzungen. Dies steht aber gerade im Widerspruch zur Verteilung der datenschutzrechtlichen Verantwortung. Auch der Verantwortliche, der personenbezogene Daten übermittelt, muss die Rechtmäßigkeit dieser Datenübermittlung sicherstellen (s. Art. 24 DSGVO). Dabei ist die Verantwortung gerade nicht auf formelle Aspekte der Übermittlung beschränkt, sondern betrifft die Rechtmäßigkeit der Übermittlung insgesamt.

Der Diensteanbieter, der sich einem Auskunftsersuchen ausgesetzt sieht, muss daher eine umfassende datenschutzrechtliche Prüfung durchführen, ohne tatsächlich in der Lage zu sein, die Rechtmäßigkeit vollumfänglich beurteilen zu können. Der Diensteanbieter muss sich deshalb entscheiden, ob er einem gegebenenfalls rechtmäßigem Auskunftsersuchen nicht nachkommt, oder möglicherweise gegen das Datenschutzrecht verstößt. Dies ist unzumutbar.

Diesem Konflikt wird im Gesetzentwurf nicht ausreichend Rechnung getragen, auch nicht durch § 15a Abs. 2 S. 4 TMG-E, wonach die um Auskunft ersuchende Stelle die “Verantwortung” für die “Zulässigkeit” des Auskunftsverlangens trägt. Die von der DSGVO abweichenden Rechtsbegriffe können auch so verstanden werden, dass die datenschutzrechtliche Verantwortlichkeit für die Rechtmäßigkeit der Übermittlung gerade beim Diensteanbieter verbleibt. Weiter zeigt § 15a Abs. 5 S. 4 TMG-E gerade, dass in jedem Fall eine zumindest teilweise Verantwortlichkeit beim Diensteanbieter verbleiben soll.

f. Nationale Strafverfolgung im globalen Cyberspace, insb. im NetzDG-Umfeld

Der Referentenentwurf verhält sich nicht hinreichend zur Anwendbarkeit des deutschen Strafrechts und zur Strafverfolgung in grenzüberschreitenden Fällen.

Materiellrechtlich müssen die Diensteanbieter bei der Inhaltsbewertung weiterhin selbst beurteilen, ob sich ein hinreichender Inlandsbezug erschließt, obwohl in Kommentarliteratur und Rechtsprechung weiter umstritten ist, welche Parameter dabei den Ausschlag geben sollen. Die Rechtsanwendung hängt dabei maßgeblich auch davon ab, ob von abstrakten oder abstrakt-konkreten Gefährdungsdelikten oder ggf. auch von Erfolgsdelikten auszugehen ist. Im Katalog des § 1 Abs. 3 NetzDG finden sich die unterschiedlichsten Deliktstypen.

Die vermeintliche im Sinne des Doppeltüren-Modells korrespondierende Regelung in StPO/BKAG und TMG greift - wie mit Blick auf die datenschutzrechtlichen Implikationen bereits aufgezeigt - bei

ausländischen Diensteanbietern zu kurz. Im Sinne des erwähnten Doppeltür-Modells des BVerfG gilt dies für beide Türen: Die Eingriffsgrundlage würde einer nationalen Behörde nicht die zwangsweise Durchsetzung eines Auskunftsverlangens gegenüber ausländischen Diensteanbietern erlauben (können). Ohne kooperative Mitwirkung der Diensteanbieter, deren rechtliche Zulässigkeit gerade bei Inhaltsdaten Grenzen hat, müssten die Behörden auf komplexe Verfahren nach dem IRG / Mutual Legal Assistance (MLAT) ausweichen.

Die Umgehung des völkerrechtlichen Souveränitätsgebots durch die Pflicht zur Einrichtung eines "Inlandsbriefkastens" gem. § 5 Abs. 2 NetzDG in der gültigen Fassung des NetzDG ist schon problematisch. Die Auferlegung proaktiver Datenherausgaben im Vorfeld von hoheitlichen Auskunftsersuchen geht darüber hinaus. Denn die transnationale Inpflichtnahme der Privatwirtschaft in grenzüberschreitenden Fällen zu Zwecken der Strafverfolgung unter Umgehung des Souveränitätsgebots stellt einen Systembruch und Fremdkörper im Bereich der Internationalen Rechtshilfe dar. Dass z.B. Teil 5 des irischen Data Protection Act 2018 auch "Processing of Personal Data for Law Enforcement Purposes" ausländischer Behörden umfasst, kann deshalb keineswegs als selbstverständlich unterstellt werden.

Die nationale Betrachtungsweise wird in beiderlei Hinsicht der Komplexität der heutigen Lebensrealität nicht gerecht: Ein in Irland ansässiger Diensteanbieter sieht sich nach einer Beschwerde i.S.d. NetzDG-E ggf. mit einer Meldepflicht gegenüber deutschen Strafverfolgungsbehörden konfrontiert, wobei er auf eigene Sanktionsrisiken hin beurteilen muss, ob deutsches Strafrecht anwendbar ist oder nicht. Ein Beispiel verdeutlicht dies: ein in Irland ansässiger Diensteanbieter muss prüfen, ob die Einbeziehung einer SS-Rune auf einem wenigen Sekunden zu sehenden Requisit in einem türkischsprachigen Musikvideo ggf. schon den Schutzzweck der Norm des § 86a StGB tangiert oder ob ein fremdsprachiges Interview mit einem Machthaber der Junud al-Sham als Propaganda gegen § 129 bzw. § 129a StGB verstößt. Derartige Fallgestaltungen gibt es vielfach.

Gerade der Umgang mit "Hate Speech" ist weltweit umstritten[15]. Die an das Legalitätsprinzip gebundenen deutschen Strafverfolgungsbehörden stoßen voraussichtlich bei weiteren Ermittlungen ohnehin an diese Grenzen und Erfordernisse der Internationalen Rechtshilfe/Mutual Legal Assistance, einschließlich des Erfordernisses beiderseitiger Strafbarkeit. Es erscheint daher fragwürdig und unverhältnismäßig, die Diensteanbieter mit einem Vorfilter zu belasten, der die Herausforderungen einer transnationalen Lebensrealität ausblendet.

Die vorgeschlagene Regelung würde ebenfalls der Zwecksetzung des Clarifying Lawful Overseas Use of Data Act (CLOUD Act) entgegenstehen, nämlich den effizienten, grenzüberschreitenden Datenaustausch über digitale Beweise hinsichtlich Terrorismus und ähnlichen Straftaten zu ermöglichen. Mit dieser Regelung wird der schnelle Austausch von Informationen zwischen Diensteanbietern und ausländischen Strafverfolgungsbehörden ermöglicht, jedoch unter der Voraussetzung, dass die jeweilige Strafverfolgungsbehörde *eine Anfrage* im Einklang mit den jeweiligen landesrechtlichen Voraussetzungen stellt, und dass diese ein entsprechend hohes rechtliches Niveau haben. Nur unter diesen Voraussetzungen würde das schwergängige Verfahren gem. Mutual Legal Assistance Treaty (MLAT) abgelöst und Diensteanbieter wie Google würden von Verpflichtungen gem. dem Stored Communications Act (SCA) freigestellt, die einer solchen Informationsweitergabe an die ausländischen Partnerstaaten der Vereinigten Staaten sonst im Wege stünden.

Die Europäische Kommission hat einen Vorschlag für eine "e-Evidence"-Richtlinie unterbreitet, mit welcher der Prozess harmonisiert werden soll, mit dem EU-Mitgliedsstaaten digitale Beweise unmittelbar und in einem einheitlichen Verfahren von ISPs anfragen können. Weitreichende proaktive

[15] vgl. für Irland: www.justice.ie/en/JELR/Pages/Hate_Speech_Public_Consultation

Offenlegungspflichten bereits im Vorfeld hoheitlicher Auskunftsersuchen sind geeignet, auch das e-Evidence-System zu umgehen und kommen zu einem Zeitpunkt, in dem die EU und die Vereinigten Staaten gerade mit den Vorbereitungen für eine Harmonisierung der Regeln für die Übertragung von Beweismitteln begonnen haben.

5. Zur geplanten Änderung des NetzDG (Art. 5 des Entwurfs)

a. Begriffsbestimmung: Beschwerde (§ 1 Absatz 4 NetzDG-E)

Die vorgesehen Erweiterung der Definition von "Beschwerden über rechtswidrige Inhalte" auf jede Beanstandung eines Inhaltes mit dem Begehren der Entfernung des Inhaltes oder der Sperrung des Zugangs zum Inhalt missachtet etablierte und über Jahre hinweg aufgebaute Beschwerdeverfahren und gefährdet damit die umfangreichen Möglichkeiten der Diensteanbieter sozialer Netzwerke, Inhalte jenseits rechtlicher Verpflichtungen zu finden, die von der Plattform entfernt werden. Darüber hinaus würde diese Erweiterung auf jedwede Meldungen im Zusammenhang mit den vorgesehenen Regelungen zur Auskunftserteilung zu einer Ausleitung von Daten in wahrscheinlich hunderttausenden von Fällen führen, bei denen keine klare Rechtsverletzung und Straftaten vorliegen, die in § 1 Abs. 3 NetzDG aufgelistet sind.

Diensteanbieter sozialer Netzwerke haben erhebliche Anstrengungen unternommen, um dedizierte NetzDG-Meldewege einzuführen, die eine klare Methode bieten, Verstöße gegen das deutsche Recht nach dem NetzDG zu melden, während den Nutzern gleichzeitig bereits seit Jahren ermöglicht wird, Verstöße gegen die Community-Richtlinien in großem Umfang schnell mitzuteilen. Diese für die Nutzer klar erkennbare Trennung ermöglicht es Diensteanbietern, die Verfahrensanforderungen nach dem NetzDG zu erfüllen und den Nutzern gleichzeitig eine einfache Möglichkeit zu bieten, eine breite Palette von Inhalte zu melden, die nicht unbedingt rechtswidrig sind, jedoch möglicherweise gegen die eigenen öffentlich zugänglichen Richtlinien verstoßen (z.B. Spam-Inhalte).

Wie aus den öffentlich zugänglichen Transparenzberichten hervorgeht, werden die neu eingeführten NetzDG-Meldewege vielfach genutzt, allein bei YouTube über 300.000 Mal in der ersten Jahreshälfte 2019[16]. Ebenfalls in der ersten Jahreshälfte 2019 erreichten YouTube weltweit fast 23 Millionen Meldungen wegen Verstößen gegen die Community Richtlinien.[17]

Eine Ausdehnung des Begriffs einer “Beschwerde über rechtswidrige Inhalte i.S.d. NetzDG” auf jegliche Meldungen, die eine Inhaltslöschung zum Ziel haben, würde sich nachteilig auf die gesamten Bemühungen der Diensteanbieter zur Durchsetzung ihrer eigenen Richtlinien und zur Bekämpfung von Missbrauch in großem Umfang auswirken:

Über einfache “Flagging” Möglichkeiten für Nutzer erhalten Diensteanbieter sozialer Medien in großem Umfang Hinweise der Community zu potenziell problematischen Inhalten. Die Schlichtheit des Beschwerdeverfahrens erlaubt die Prüfung unterschiedlichster Inhalte, wobei ein “Flag” als ein Signal gilt, dass mit dem Inhalt etwas nicht stimmen könnte. Zudem hilft ein schlicht gestaltetes Flagging-Verfahren in solchen Fällen, in denen die Inhalte sich plötzlich viral ausbreiten. Hier kann eine vermehrte Anzahl von Flags darauf hinweisen, dass ein Inhalt problematisch ist. Ein derart einfaches Flagging-System ist jedoch auch anfällig für Missbrauch durch Dritte, die Inhalte weder aus rechtlichen Gründen, noch wegen einer Richtlinienverletzung, sondern rein aus persönlichen Gründen entfernt haben möchten. Hervorzuheben ist daher, dass ein nicht unerheblicher Teil von Flags ungenau ist und nicht zu einer Entfernung führt. Sogar im Rahmen der Meldungen unter NetzDG wurden 76,62% der gemeldeten

[16] https://transparencyreport.google.com/netzdg/overview?hl=de
[17] https://transparencyreport.google.com/youtube-policy/removals?hl=de

Inhalte in der zweiten Jahreshälfte 2019 nicht entfernt, da sie weder gegen YouTube Community Richtlinien noch gegen deutsches Recht verstoßen haben.[18] Auswertungen der UC Berkley von Unterlassungs- und Löschungsaufforderungen, die an Diensteanbieter gerichtet waren, zeigen, dass viele Beschwerdeführer rechtmäßige und unter die Meinungsfreiheit fallende Inhalte entfernt haben möchten.[19]

Ein flexibles Flagging-System erlaubt es YouTube, schnell zu handeln und einen möglichen Missbrauch des Systems zu verhindern. Die Einführung zusätzlicher verfahrenstechnischer Anforderungen für das Flagging würde die beiden oben beschriebenen Ziele gefährden und ein gut funktionierendes System, das von Millionen von Nutzern auf der ganzen Welt genutzt wird, erheblich verkomplizieren.

b. Hinweispflicht gegenüber dem Beschwerdeführer in Bezug auf die Möglichkeit eines Strafantrags (§ 3 Absatz 2 Nummer 5 NetzDG-E)

Grundsätzlich ist eine Hinweispflicht in Bezug auf die Möglichkeit eines Strafantrags an Beschwerdeführer durch die Diensteanbieter als sinnvoll anzusehen. Allerdings kann so eine Hinweispflicht die Diensteanbieter dann vor Schwierigkeiten stellen, wenn der Beschwerdeführer und der Verletzte nicht dieselbe Person sind. §3 Abs. 2 Nr. 5 NetzDG-E setzt den Beschwerdeführer offensichtlich mit dem (vermeintlichen) Verletzten i.S.d. § 406d StPO gleich, obwohl diese nach den bisherigen Erfahrungen mit den NetzDG-Beschwerden nicht selten, sondern in den meisten Fällen auseinanderfallen. Denn Beanstandungen gehen oft nur von Dritten aus, nicht von den selbst unmittelbar durch die Inhalte Betroffenen bzw. Verletzten (sog. “third party complaints”).

Schon bisher griff das NetzDG zu kurz, indem es terminologisch ungenau nur “Beschwerdeführer und Nutzer” als Gegensatzpaar gegenüber stellte. Die Beteiligten, denen sich die Diensteanbieter gegenüber sehen, können sich gerade im Falle der eben genannten third party complaints vervielfachen, mit allen Konsequenzen für die gleichzeitige Potenzierung etwaiger Hinweis- und Informationspflichten, wie sie der Referentenentwurf vorsieht.

Beispielsweise wurde im vergangenen Jahr im Zuge der Auseinandersetzung um den umstrittenen Artikel 13 der EU-Urheberrechtsreform (“Upload-Filter”-Debatte) ein dem Politiker Axel Voss gewidmetes Rap-Video vielfach als vermeintliche Beleidigung gemeldet. Der Betroffene selbst hat nach unserer Information jedoch weder gegen die Veröffentlichung interveniert noch Strafanzeige oder Strafantrag gestellt, obwohl auch ihm das sehr breit rezipierte Video sicher zur Kenntnis gelangt sein dürfte.

Eine derartige Konstellation ist keine Seltenheit. Allerdings sind nur in Ausnahmefällen Personen betroffen, die als Personen des öffentlichen Lebens von den Diensteanbietern unabhängig von einer Beschwerde identifizierbar und ggf. erreichbar sind. In dieser Konstellation kann durch bloße Hinweise an den oder die “Beschwerdeführer” das mit § 3 Abs. 2 Nr. 5 NetzDG-E offenbar verfolgte Ziel, dass der vermeintlich Verletzte einen ggf. erforderlichen Strafantrag stellt, ohnehin nicht erreicht werden. Ob und ggf. wem gegenüber in einer solchen Konstellation gleichwohl ein Hinweis erfolgen soll, stellt der Entwurf nicht klar.

Eine Informationspflicht gegenüber dem Beschwerdeführer, “auf welchen Internetseiten er hierüber weitere Informationen erhalten kann”, ist unbestimmt und ist zu konkretisieren. Ansonsten wären die Dienstleister mit der Rechtsunsicherheit belastet, auf welche Informationen rechtssicher zu verweisen ist. Insbesondere die sachliche und örtliche Zuständigkeit der Behörden lassen sich für die Diensteanbieter regelmäßig nicht beurteilen. Auch sind die Möglichkeiten einer Online-Strafanzeige föderal sehr unterschiedlich geregelt. Teilweise bestehen z.B. auch Kooperationen mit dem Business Keeper

[18] https://transparencyreport.google.com/netzdg/youtube?hl=de
[19] vgl. z.B. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628

Monitoring System (BKMS®), um anonyme Strafanzeigen gerade auch bei “rechtsmotivierten Straftaten” zu ermöglichen.[20]

Dies verhindert auch die Erfüllung der datenschutzrechtlichen Betroffenenrechte (Art. 12 ff. DSGVO), insbesondere wenn Dritte betroffen sind, die weder (meldende) Nutzer noch Täter eines möglichen Verstoßes sind (sondern zum Beispiel selbst Opfer oder sonstige Dritte). Über die entsprechende Datenweitergabe ist nämlich der jeweilige Betroffene zu informieren, auch wenn er nicht Nutzer oder Beschwerdeführer ist. Dies verstößt ebenso gegen Art. 6 RL (EU) 2016/680, der ausdrücklich festlegt, dass das nationale Recht vorsehen muss, “dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet,...”. Mögliche Kategorien, nach denen der Verantwortliche gem. Art. 6 dabei unterscheiden soll, sind ausdrücklich Verdächtige, verurteilte Straftäter, Opfer und mögliche Opfer und weitere Parteien wie zum Beispiel (mögliche) Zeugen. Dies tut der Referentenentwurf eindeutig nicht, obwohl dies in der zu regelnden Situation klar geboten wäre, da jede der beispielhaft aufgezählten und schon von der Richtlinie antizipierten Personengruppen auch hier Teil des Verfahrens sein kann.

Es sollte folglich eine zentrale Meldestelle durch die Staatsanwaltschaften ggf. mit einer eigenen Homepage eingerichtet werden, an und auf die die sozialen Netzwerke verweisen können, um das Verfahren für die Beschwerdeführer und/oder die Verletzten überschaubar und einfach handhabbar auszugestalten. Die Diensteanbieter könnten dann in den nunmehr vorgesehenen Benachrichtigungen auf diese Homepage verweisen.
Außerdem sollte der Entwurf den Kreis der zu informierenden Personen erweitern, so dass alle betroffenen Personen zu informieren sind.

c. Meldepflicht gegenüber dem BKA (§ 3a Abs. 6 NetzDG-E)

aa. Allgemeine Ausführungen zur Meldepflicht

Die geplante Einführung einer Meldepflicht für soziale Netzwerke stellt einen Systembruch mit dem geltenden Recht dar, jedenfalls soweit die Meldepflichten über § 138 StGB hinausgehen.

Soweit hingegen Deckungsgleichheit mit § 138 StGB besteht (etwa bei der Meldepflicht von ernstlichen Mordankündigungen i.S.d. § 241 StGB), ergibt sich schon keine Regelungslücke: Schon bisher besteht eine Anzeigepflicht, wenn jemand “zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann”, von bestimmten Katalogtaten (u.a. Totschlag/Mord) “glaubhaft erfährt und es unterläßt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen”. Das Verhältnis der geplanten Meldepflicht zu dieser Norm wird bisher nicht hinreichend diskutiert. Das erscheint aber notwendig, wenn hoheitliche Aufgaben an private Akteure delegiert werden sollen.

Zudem sah sich der Gesetzgeber bezogen auf die aus § 138 StGB folgende Meldepflicht veranlasst, das Verhältnis zum Fernmeldegeheimnis ausdrücklich klarzustellen. Insoweit sei verwiesen auf § 88 Abs. 3 Satz 4 TKG, der ausdrücklich einen Vorrang von § 138 StGB vorsieht.

Aus übergeordneten rechtspolitischen Gründen sei an dieser Stelle erwähnt, dass Diensteanbieter, die an das Fernmeldegeheimnis gebunden sind, wenn also private Kommunikation über ein soziales Netzwerk läuft, Kenntnisse des Inhalts oder der näheren Umstände der Telekommunikation nur verwenden dürfen, soweit dies für die geschäftsmäßige Diensteerbringung erforderlich ist. Eine Verwendung für *andere* Zwecke, insbesondere die Weitergabe an Dritte, ist nur zulässig, soweit eine gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht (sog. Kleines Zitiergebot iSd § 88 Abs. 3 Satz 3 TKG).

[20] vgl. https://www.polizei-bw.de/anonymes-hinweisgebersystem/

bb. Inhaltsdaten

Diensteanbieter sozialer Netzwerke sollen nach § 3a Abs. 4 Nr. 1, 2 NetzDG-E Inhalte und IP-Adressen (inkl. Portnummern) über eine eigens einzurichtende technische Schnittstelle an das BKA übermitteln, wenn Inhalte nach Auffassung des Diensteanbieters gegen bestimmte StGB-Straftatbestände verstoßen.

Durch diese erzwungene Ausleitung von Inhalten und IP-Adressen durch Diensteanbieter an das BKA würde durch eine einseitige Verpflichtung Privater eine Datenbank ganz erheblichen, bisher noch nicht bekannten Umfangs beim BKA über Nutzer und die von ihnen geposteten Inhalte angelegt, die nach Auffassung der Diensteanbieter nach kursorischer Prüfung möglicherweise einen der in § 3a Abs. 3 Nr. 3 NetzDG-E aufgezählten Straftatbestände erfüllen. Konkret bedeutet dies, dass Diensteanbieter sozialer Netzwerke in zigtausend Fällen jährlich personenbezogene Daten und Inhalte an das BKA übermitteln müssen, ohne dass vorab eine fallbezogenen Prüfung im Hinblick auf einen möglichen Anfangsverdacht durch das BKA oder eine sonstige staatliche Stelle erfolgt wäre.

Die erhebliche Grundrechtsrelevanz dieser Regelung ist evident. Im Zuge der BVerfG-Entscheidung über die Vorratsdatenspeicherung wurde eine Milderung des Grundrechtseingriffs noch darin gesehen, dass "sich die Verpflichtung zur Speicherung [...] auf die Verkehrsdaten beschränkt [...] und weil sie dezentral bei den privaten Diensteanbietern erfolgt" (Abweichende Meinung des Richters Eichberger, NJW 2010, 833). Bei der nun vorgesehenen Datenbank fehlt es selbst an diesen Sicherungen.

Diensteanbieter bekommen zudem keinerlei Rückmeldung des BKAs über den Verbleib der Daten sowie über den Stand des Verfahrens. Es ist unklar, wie das Verfahren weitergeht und an wen die Daten in welchem Zeitraum übergeben werden, wenn das BKA die Einschätzung des Diensteanbieters teilt. Kommt das BKA zu dem Schluss, dass ausgeleitete Inhalte strafrechtlich nicht einschlägig sind, so liegen personenbezogene Daten der Betroffenen den Strafverfolgungsbehörden sogar vor, obwohl sich die Betroffenen rechtmäßig verhalten haben. Hinzu kommt, dass die durch das BKA als rechtmäßig befundenen Inhalte gesperrt bleiben, und die Diensteanbieter die Prüfkriterien und Entscheidungen des BKAs nicht in ihre zukünftige Prüfpraxis mit aufnehmen können. Die vorgesehenen Regelungen sind daher verfassungsrechtlich höchst bedenklich.

Ebenfalls unklar ist, was mit Inhalten passiert, die von nicht in Deutschland ansässigen Nutzern eingestellt wurden.

cc. IP-Adresse und Portnummer

Zur Übermittlungspflicht von IP-Adresse und Portnummer enthält das Gesetz in § 3a Abs. 4 NetzDG-E die Einschränkung "soweit vorhanden". Der Entwurf geht in seiner ganzen Systematik und Zielsetzung jedoch wie selbstverständlich davon aus, dass "die IP-Adresse einschließlich der Portnummer, die der Nutzer verwendet hat, als er den Inhalt mit anderen Nutzern geteilt oder der Öffentlichkeit zugänglich gemacht hat", vorgehalten werden. Allein dies stelle eine "effektive Strafverfolgung" sicher.

Der Bestandsdatenbegriff des § 14 TMG orientiert sich aber nicht daran, was für die Strafverfolgung erforderlich wäre, sondern daran, was "für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich" ist.

Die "Erforderlichkeit" hinsichtlich eines Vertragsverhältnisses einerseits und hinsichtlich der Strafverfolgung andererseits fallen bei sozialen Netzwerken regelmäßig auseinander. Erst recht stellt sich aber die Frage, wie im weiteren Verlauf bei den Access Providern anhand von wechselnd zugeordneten IP-Adressen, vor allem aber anhand der bei jeder Nutzung, Browser-Öffnung, etc. wechselnd zugeteilten Portnummern eine Identifizierung der Nutzer gelingen soll.

Insgesamt müssten für die Möglichkeit einer Identifizierung in ganz erheblichem Umfang Daten gespeichert werden, die zur jeweiligen Diensteerbringung nicht (mehr) erforderlich sind. Dies gilt erst recht bei Berücksichtigung des zu erwartenden Fallaufkommens, auf dass die Strafverfolgungsbehörden personell bei weitem nicht eingerichtet sind und das realistisch kaum binnen weniger Tage abgearbeitet werden kann.

Sofern kein abweichendes technisches Verständnis zugrunde liegt, dürfte die Übermittlungspflicht regelmäßig ins Leere laufen, sofern der Entwurf nicht bereits von einer bevorstehenden, noch wesentlich extensiveren Pflicht zur Vorratsdatenspeicherung und ggf. auch zur Identifizierung der Nutzer seitens der Telemediendienste ausgeht.

dd. Pflicht zur Nutzung einer vom BKA bereitgestellten Schnittstelle

Die im Referentenentwurf vorgesehenen Regelungen zur Übermittlung von herauszugebenden Daten über eine Schnittstelle sind widersprüchlich. Die Übermittlung der geforderten Informationen i.S.d. § 3a NetzDG-E an das BKA soll elektronisch an eine vom BKA zur Verfügung gestellte Schnittstelle erfolgen. Ausweislich § 15a Abs. 5 TMG-E soll hingegen "für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte" eine Schnittstelle durch den Diensteanbieter selbst eingerichtet werden. Das Verhältnis dieser beiden Regelungen ist unklar. Sollten tatsächlich parallele Verfahren mit unterschiedlichen Schnittstellen für Meldungen und Auskunft vorgesehen sein, würde dies nicht nur zu einer erhöhten Komplexität und Fehleranfälligkeit der Prozesse führen, sondern auch zu Datenverarbeitungen, die dem Prinzip der Datenminimierung widersprechen.

d. Informationspflicht gegenüber dem Nutzer (frühestens) nach 14 Tagen (§ 3a Abs. 6 NetzDG-E)

Der Umstand, dass der betroffene Nutzer nach § 3 Abs. 6 NetzDG-E frühestens nach 14 Tagen über die Übermittlung an das BKA zu informieren ist, intensiviert den Eingriff in seine Interessen durch die heimliche Vorgehensweise, die den Diensteanbietern abverlangt wird. Wie bereits an anderer Stelle (Seite 10) erörtert, können sich auch im Verhältnis zwischen Diensteanbieter und betroffenem Nutzer Pflichtenkollisionen ergeben, insbesondere in transnationalen Sachverhalten, in denen lokale Beschränkungen der Betroffenenrechte zu kurz greifen.

Die in § 3a Abs. 6 NetzDG-E vorgesehene Informationspflicht geht zu Lasten des Diensteanbieters, der nicht nur die Information des betroffenen Nutzers übernehmen muss, sondern auch genau beobachten muss, wann diese (abhängig von der ursprünglichen) Meldung zu erfolgen hat und ob diese (abhängig von einer Aufforderung des BKA) dann überhaupt noch erfolgen darf. Dies ist auch deshalb überraschend, da die Richtlinie (EU) 2016/680 in ihrem Art. 12 Abs. 1 vorsieht, dass der jeweilige Verantwortliche die betroffenen Personen informiert.

Zudem stellt der Entwurf das Verhältnis von § 3 Abs. 6 NetzDG-E zu dem Verbot der Benachrichtigung nach § 15a TMG-E nicht klar.

e. Verarbeitung personenbezogener Daten europäischer Nutzer aufgrund deutscher Rechtsgrundlage

Ein besonderer Widerspruch zum europäischen Recht besteht, da auf Grundlage deutschen Rechts personenbezogene Daten von Nutzern auch aus dem europäischen Ausland übermittelt werden sollen. Die Vorschriften des Referentenentwurfs betreffen nämlich nicht nur deutsche Bürger und andere

Personen, die sich in Deutschland aufhalten, sondern jeden Nutzer, dessen Inhalt Gegenstand des Meldeverfahrens nach § 3a NetzDG-E wird.

Im Ergebnis werden auch Inhalte, IP-Adressen und ggf. die Portnummern von betroffenen Personen außerhalb Deutschlands übermittelt werden. Die Folge werden massenhafte Übermittlungen von personenbezogenen Daten aus dem (EU-)Ausland an deutsche Strafverfolgungsbehörden sein, die nicht von einer europäischen Rechtsgrundlage gedeckt sind.

Hier sind bereits Konflikte mit den europäischen Datenschutzbehörden vorprogrammiert, die die deutschen Strafverfolgungsbehörden auffordern werden, die Nutzerdaten zu löschen.

6. Zur Regelung des Inkrafttretens (Art. 6 des Entwurfs)

Selbst wenn die zahlreichen inhaltlichen Defizite, die der Entwurf aufweist, bereinigt würden: Die im Entwurf vorgesehene Frist zur Umsetzung von drei Monaten ist angesichts der Vielzahl der mit dem Entwurf neu auferlegten Pflichten in jedem Fall viel zu kurz bemessen, um die erforderliche Implementierung der erforderlichen Infrastruktur und Umstellung der internen Verfahren zu gewährleisten.

IV. Verfassungsrechtliche Einordnung

1. Grundrechtseingriffe

Dass der Referentenentwurf in Grundrechte der Bürgerinnen und Bürger eingreift, liegt auf der Hand. Zu nennen sind hier insbesondere das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet hat (s. u.A. NJW 2012, 1419, 1442, Rn. 122 mwN.), sowie ein Eingriff in das Fernmeldegeheimnis aus Art. 10 GG.

Offensichtlich greift der Referentenentwurf in das Recht auf informationelle Selbstbestimmung ein, wenn er es erlaubt, dass den staatlichen Behörden massenhaft personenbezogene Daten übermittelt werden, ohne dass dies den Betroffenen bewusst ist noch überschaubar oder beherrschbar erscheint. Zwar unterliegen dem Fernmeldegeheimnis nur solche Vorgänge, die nicht an die Allgemeinheit, also einem unbestimmten Personenkreis, gerichtet sind. Hier geht es aber auch um Inhalte, die in einer privaten Gruppe und anderen geschützten Bereichen geteilt werden, also an einen bestimmten Personenkreis gerichtet sind. In dieser Hinsicht sowie auch mit Blick auf eine etwaige Herausgabe von Passwörtern liegt ein Eingriff in das Fernmeldegeheimnis nahe.

Mit Blick auf die Erforderlichkeit des Referentenentwurfs ist übergreifend darauf hinzuweisen, dass Google im engen Austausch mit einer Schwerpunktstaatsanwaltschaft bereits ein praxisnahes Alternativmodell entwickelt hat, das sich - nicht nur mit Blick auf die erforderliche "Überwachungsgesamtrechnung"[21] - als milderes, aber dessen ungeachtet mindestens gleich wirksames Mittel darstellt. Auch vor diesem Hintergrund ergeben sich durchgreifende Zweifel an der Verhältnismäßigkeit.

Auch die Angemessenheit des Referentenentwurfs im Sinne einer Zweck-Mittel-Relation ist äußerst fraglich. Erlaubt der Entwurf massenhafte Übermittlungen personenbezogener Daten an Strafverfolgungsbehörden, die darüber hinaus weitgehend im Verborgenen geschehen (s.o.# sowie unten C II), um schon geringste Verstöße wie Ordnungswidrigkeiten repressiv zu verfolgen, spricht dies für die Unangemessenheit dieser massenhaften und vorratsmäßigen Datensammlung und Überwachung. Hinzu kommen die bereits an vielen Stellen angesprochenen und noch anzusprechenden Punkte, dass Privatunternehmen zum Erfüllungsgehilfen der Strafverfolgungsbehörden gemacht werden, die betroffenen Nutzer sich also gar nicht mehr sicher sein können, ob sie sich noch in einem normalen Nutzungsverhältnis mit dem Diensteanbieter befinden, oder bereits Gegenstand eines von diesem zwangsweise in Gang gesetzten Ermittlungsverfahrens sind. Zu berücksichtigen ist in dieser Hinsicht auch, dass der Diensteanbieter schon durch die enorme Bußgeldandrohung von bis zu 50 Millionen Euro regelmäßig eher zu einer Meldung neigen dürfte.

2. Funktionsvorbehalt, Art. 33 Abs. 4 GG

Dem geltenden Recht liegt zugrunde, dass Strafverfolgung ureigene hoheitliche Aufgabe (genuine Staatsaufgabe) ist. Jede Zuweisung an Private ist am sog. Funktionsträgervorbehalt des Art. 33 Abs. 4 GG zu messen: Aufgabenbereiche, deren Erfüllung strukturell die Ausübung hoheitlicher Befugnisse erfordert, sind durch Beamte wahrzunehmen. Funktionale Privatisierung von Hoheitsaufgaben muss durch zwingende sachliche Gründe gerechtfertigt sein. Zudem ist bei entsprechenden Aufgabenübertragungen die Kostentragung stets ein Diskussionspunkt (Problem der Sonderabgaben).

Wg. eines Verstoßes gegen den Funktionsvorbehalt wurde z.B. die selbstständige Geschwindigkeitsüberwachung durch Private für unzulässig erklärt (NJW 2016, 3318). Eine solche

[21] Zum BVerfG-Urteil vom 02.03.2010 - Vorratsdatenspeicherung - Roßnagel, NJW 2010, 1238.

Unterstützung sei nur für Tätigkeiten zulässig, die die Herrschaft über die Messung nicht betreffen. Als Verwaltungshelfer dürfen Private lediglich im Auftrag und nach Weisung für staatliche Behörden tätig werden, nicht hingegen eigenverantwortlich und mit eigener Entscheidungsmacht.

Für die Bejahung einer rein „untergeordneten und unselbstständigen Hilfsfunktion“ ist weder das NetzDG selbst noch der Katalog der in § 1 Abs. 3 Bezug genommenen Tatbestände des StGB hinreichend bestimmt. Der Referentenentwurf konstruiert mit der Verpflichtung zur massenhaften Übermittlung von Inhalten und Nutzerdaten an das BKA vielmehr gezielt einen Vorfilter in privater Hand.

Die vorgesehenen Melde-/Offenlegungspflichten im GBRH-E setzen die ohnehin bedenkliche Entwicklung einer Privatisierung der Strafverfolgung bzw. der Strafverfolgungsvorsorge (u.a. Verdachtsgewinnung) durch Spezialgesetze fort, z.B. im GwG und im SGB V.

Dass Diensteanbieter i.S.d NetzDG nun ebenfalls so umfassend zur Erfüllung einer Staatsaufgabe herangezogen werden sollen wie z.B. die Banken im Bereich der Geldwäsche, ist problematisch. Selbst im Finanzsektor ist von jeher umstritten, die Banken zu Hilfssheriffs gegen ihre eigenen Kunden zu machen.

Aufgrund der allgemein zugänglichen Inhalte und der damit sichergestellten Transparenz der (vermeintlichen) Deliktsbegehung in sozialen Netzwerken besteht aber vorliegend sogar noch ein zentraler Unterschied zu den Meldepflichten z.B. nach dem GwG. Anders als der dezentrale bargeldlose Zahlungsverkehr, Abrechnungen im Gesundheitswesen oder Insiderverstöße sind die am NetzDG/StGB zu messenden Inhalte in der Regel für alle sichtbar und ließen sich auch durch die Behörden kontrollieren, etwa durch intensivere „virtuelle Streifenfahrten“ mit staatlichem Personal. Ein sachlich zwingender Grund für die Inpflichtnahme Privater besteht daher, anders als ggf. im Bereich der Geldwäsche, nicht.

Es gibt überdies nicht einmal eine Verfahrensordnung für das Vorgehen der Diensteanbieter, das z.B. bestimmten Beweisregeln unterliegen würde. Der Vergleich mit den Regelungen im GwG ist zudem deswegen irreführend, da dortige Anbieter - anders als im aktuellen NetzDG-Entwurf - eine Haftungsprivilegierung für die entsprechende Meldepflicht erhalten. Beides wäre jedenfalls im Entwurf zu ergänzen.

V. Bisherige Umsetzung / Beleg milderer, genauso wirksamer Maßnahmen

In einer Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages hat Google ausführlich das von YouTube vorgehaltene Beschwerdemanagement dargelegt, darauf wird an dieser Stelle verwiesen.[22]

[22] https://www.bundestag.de/resource/blob/642500/f7cbbae5c4c97e6c601049d4182e7eca/frank-data.pdf

VI. Sonderaspekt: Bekämpfung von Kinderpornographie

Google engagiert sich seit vielen Jahren, um missbräuchliche Inhalte so schnell wie möglich aufzuspüren und sofort zu entfernen.

Google setzt umfangreiche technologische, personelle und zeitliche Ressourcen ein, um explizite Inhalte zu erkennen, zu verhindern, zu entfernen und natürlich auch zu melden. Außerdem gehen wir ungewöhnlichem Verhalten von Nutzern nach, das auf sexuellen Missbrauch von Kindern hindeuten könnte. Bereits seit 2008 verwenden wir zusätzlich die sogenannte "Hash-Technologie" für Pilot-Verfahren in diesem besonderen Deliktsbereich: Das bedeutet, dass jedem uns bekannten Inhalt, der sexuellen Missbrauch von Kindern abbildet, eine eindeutige ID zugeordnet wird. Dadurch können wir Kopien dieser Inhalte direkt aufspüren und entfernen, sollten sie noch an anderer Stelle in unseren Diensten vorhanden sein.

Google hat darüber hinaus eine branchenweit genutzte Datenbank von Video-Hashwerten erstellt, mit deren Hilfe bereits bekannte Videos, die sexuellen Missbrauch von Kindern zeigen, identifiziert und gesperrt werden können. So können auch andere Unternehmen diese Inhalte direkt erkennen und von ihren Plattformen entfernen.

Im Jahr 2013 haben wir unsere Suchalgorithmen angepasst, um - so effizient wie technische Neuentwicklungen es jeweils zulassen - zu verhindern, dass Bilder, Videos und Links zu Missbrauchsdarstellungen von Kindern in den Suchergebnissen erscheinen. Diese Änderung wurde weltweit umgesetzt, so dass Millionen von Suchanfragen heutzutage automatisch geprüft werden.

Bei Google und YouTube kommen Werkzeuge wie CSAI Match und die Content Safety API zusammen mit weiteren internen Tools zum Einsatz – denn der Kampf gegen missbräuchliche Inhalte hat für uns absolute Priorität. Wir arbeiten ständig daran, diese Verfahren zu verbessern, und setzen zu diesem Zweck die neuesten Entwicklungen im Bereich der neuronalen Deep-Learning-Netzwerke und des maschinellen Lernens in diesem in mehrfacher Hinsicht besonderen Deliktsbereich um.

Außerdem entwickeln wir Technologien, die wir auch anderen Organisationen kostenlos zur Verfügung stellen. Wir wollen sie auf diese Weise dabei unterstützen, Missbrauchsdarstellungen aufzuspüren und zu entfernen. Zusätzlich haben wir spezielle Initiativen ins Leben gerufen, um unsere technische Expertise mit Nichtregierungsorganisationen, anderen Unternehmen der Branche und vielen weiteren Akteuren zu teilen.

Seit mehr als einem Jahrzehnt sind wir zudem Mitglied verschiedener öffentlich-privater Zusammenschlüsse. Dazu gehören u.a. die Technology Coalition, die ICT Coalition, die WeProtect Global Alliance und die Finanzkoalition gegen sexuelle Ausbeutung von Kindern im Internet von Europol. In diesen Zusammenschlüssen entwickeln Unternehmen gemeinsam technologische Lösungen, um den Austausch von Missbrauchsdarstellungen von Kindern im Internet zu unterbinden und die sexuelle Ausbeutung von Kindern zu verhindern.

Darüber hinaus arbeiten wir eng mit NCMEC zusammen, wie bereits dargestellt wurde.

Googles Spenden an NCMEC seit 2009 belaufen sich auf insgesamt 3,7 Mio. USD und unterstützen den Kampf gegen Missbrauchsdarstellungen von Kindern, indem sie NCMEC dabei helfen, seine technischen Kapazitäten zu verbessern, z.B. durch die Einstellung von technischem Personal und die Entwicklung technischer Lösungen, die Missbrauchsdarstellungen identifizieren und diese entfernen. Zusätzlich zu den regelmäßigen Spenden leistet Google auch einmalige Spenden an das NCMEC, um maßgeschneiderte Projekte zu finanzieren. So hat Google beispielsweise im November 2015 zur Erstellung einer technischen Umfrage unter 50 Organisationen auf der ganzen Welt beigetragen, die

Missbrauchsdarstellungen bekämpfen, wobei der Schwerpunkt auf der Identifizierung gemeinsamer Herausforderungen und möglicher technischer Lösungen lag.

Zudem hat Google:

- NCMEC einen "Googler in Residence", einen Google Mitarbeiter, Vollzeit zur Verfügung gestellt (ähnlich wie bei der IWF-Vereinbarung), um NCMECs technische Kapazitäten zu stärken und neue Tools und Ressourcen zu entwickeln;
- 2017 ein einjähriges technisches Stipendium für einen Softwareentwickler finanziert;
- Googles Ingenieurs- und Produktteams für tausende Arbeitsstunden freigestellt, um ein innovatives, Cloud-basiertes visuelles Suchtool zu entwickeln, das NCMEC dabei unterstützt, Missbrauchsdarstellungen schneller zu identifizieren, um sie schneller und effizienter bekämpfen zu können;
- Mithilfe dieser Suchtool-Software konnten NCMEC-Analysten die umfangreichen Informationssysteme und Millionen von NCMEC-Berichten schnell durchsuchen und Dateien, die Missbrauchsdarstellungen enthalten, effektiver analysieren.

Außerdem arbeiten Google und NCMEC daran, die Hash-Datenbank von NCMEC in Googles Content Safety API zu integrieren, wodurch es für NCMEC einfacher wird, ihre Datenbank breiter zugänglich zu machen und gleichzeitig den Zugang zu den neuesten Informationen zu erleichtern, die im Kampf gegen Missbrauchsdarstellungen verfügbar sind.