

Schriftliche Stellungnahme im Rahmen der öffentlichen Anhörung zu

a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/17741)

b) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/18470)

Vorbemerkungen

Das NetzDG aus dem Jahr 2017 war zweifellos ein richtiger Ansatz zur Bekämpfung der Hasskriminalität im Internet. Gleichwohl hat sich gezeigt, dass die Löschung rechtswidriger Inhalte allein nicht ausreichend ist, um der zunehmenden Verrohung durch Hass und Hetze wirksam zu begegnen. Kernpunkt der nunmehr vorliegenden, umfassenden Gesetzentwürfe ist daher, die Voraussetzungen für eine effektive Strafverfolgung zu schaffen.

Die gesetzgeberische Zielsetzung der Ermöglichung einer effektiven Strafverfolgung wird die beteiligten (Ermittlungs-) Behörden vor eine beispiellose Mammutaufgabe im Bereich der Bekämpfung der Massenkriminalität stellen. Denn es ist nicht nur die immense Anzahl der zu erwartenden Meldungen, sondern insbesondere die Flüchtigkeit der zur Verfügung stehenden Daten, die – im Gegensatz zur „Offline-Massenkriminalität“ – die Ermittlung der Verantwortlichen erheblich erschweren wird.

Massenkriminalität erfolgreich zu bekämpfen setzt aus unserer langjährigen Erfahrung bei der Bekämpfung der Verbreitung der Kinderpornographie zunächst insbesondere voraus, dass der Rechtsrahmen, in dem die Beteiligten tätig werden, klar definiert ist.

Ferner müssen die einzelnen Abläufe organisiert, strukturiert und – jedenfalls soweit möglich – automatisiert sein.

Dies mag banal bzw. selbstverständlich klingen. Gleichwohl hat das bisherige Gesetzgebungsverfahren gezeigt, dass auch grundsätzliche Fragestellungen jedenfalls noch nicht abschließend geklärt sind, die für das Ziel der Ermöglichung einer effektiven Strafverfolgung von wesentlicher Bedeutung sein dürften.

Als Vertreter einer Strafverfolgungsbehörde möchte ich in diesem fortgeschrittenen Stadium des Gesetzgebungsverfahrens und aufgrund der Vielzahl bereits vorliegender Stellungnahmen das Augenmerk ganz bewusst nur auf wenige, für die Effizienz der Strafverfolgung jedoch immens wichtige Punkte lenken, auf die der bisherige Diskurs noch nicht oder jedenfalls nicht primär gerichtet war.

I. Klarstellung der Aufgaben des Bundeskriminalamts

Auf eine wesentliche, sich im Kern nicht einmal aus dem Text des Gesetzentwurfs selbst, sondern vielmehr aus der Gesetzesbegründung ergebende Problemstellung hat der Bundesrat in seiner Stellungnahme vom 27.03.2020 (Drs. 87/20, S. 13 f.) hingewiesen. § 3a Absatz 2 NetzDG-E sieht vor, dass das Bundeskriminalamt (BKA) die Meldungen als Zentralstelle zum Zwecke der „Ermöglichung der Verfolgung von Straftaten“ entgegennimmt. Eine eindeutige Bestimmung, welche Aufgaben das BKA als Zentralstelle wahrnimmt, ergibt sich – wie der Bundesrat zu Recht feststellt – hieraus nicht.

Die sich aus der Gesetzesbegründung ergebende Aufgabenbeschreibung dagegen erscheint bislang zumindest missverständlich, wenn sie einerseits feststellt, dass sich die Tätigkeit des BKA im Rahmen der Zentralstellenfunktion auf die Maßnahmen beschränkt, die erforderlich sind, um die zuständige Strafverfolgungsbehörde auf Landesebene festzustellen andererseits aber davon ausgeht, dass das BKA „...nach Einschätzung, ob es sich um einen strafbaren Inhalt handelt, die beim sozialen Netzwerk gespeicherten Daten, soweit sie zur Identifizierung des Verfassers erforderlich sind, anfordern und diese Daten der zuständigen Strafverfolgungsbehörde in den Ländern übermitteln...“ wird.

Im Kern geht es darum, ob das BKA zunächst eine Bewertung der Meldung auf strafrechtliche Relevanz vornehmen darf oder muss, bevor es die übermittelte IP-Adresse

beim Access-Provider abfragt. Nach hiesiger Einschätzung ist das BKA hierzu sogar gesetzlich verpflichtet.

Der Bundesrat weist in diesem Zusammenhang zu Recht darauf hin, dass auch in der analogen Welt die Polizei nicht sämtliche ihr zugetragenen Erkenntnisse ungefiltert der Staatsanwaltschaft übermittelt werden. Die Vorlagepflicht der Polizeibehörden des § 163 Abs. 2 StPO besteht nämlich gerade nicht, wenn bereits der Anfangsverdacht einer Straftat, die Voraussetzung für den sog. „ersten Zugriff“ – also die beweissichernden Erstmaßnahmen – nicht vorliegt.

Hinzu kommt, dass die qualifizierte Bestandsdatenabfrage des § 10 Abs. 2 BKAG zumindest „einen hinreichenden Anfangsverdacht gemäß den §§ 161, 163 StPO oder eine konkrete Gefahr im Sinne der polizeilichen Generalklausel“ voraussetzt (*Schenke/Graulich/Ruthig*, Sicherheitsrecht des Bundes, § 10 BKAG, Rn. 19) voraussetzt. Eine Abfrage gem. § 10 Abs. 2 BKAG ohne jegliche Prüfung, ob die Meldung überhaupt einen strafrechtlich relevanten Inhalt aufweist, wäre daher nicht rechtmäßig und würde, wie der Bundesrat feststellt, eine Vertiefung des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung der Nutzer zur Folge haben, die mangels Erforderlichkeit auch datenschutzrechtlich bedenklich wäre.

Das mögliche (Gegen-) Argument, es habe bereits eine Prüfung auf strafrechtliche Relevanz durch die sozialen Netzwerke stattgefunden, verkennt, dass es sich bei den Tatbeständen des § 3 Abs. 2 Nr. 3. NetzDG-E überwiegend um komplexe Vorschriften handelt, deren Bewertung vertiefte juristische Kenntnisse voraussetzt. Die Erfahrungen, die meine Zentralstelle in Zusammenarbeit mit Nichtregierungsorganisationen im Zuge des Aktionsprogramms der hessischen Landesregierung unter dem Schlagwort #HessengegenHetze gemacht hat, zeigen, dass von den übermittelten Meldungen – obgleich die Kooperationspartner teils juristisch geschult waren – über 60 Prozent als strafrechtlich nicht relevant eingestuft werden mussten. Es wäre also zu befürchten, dass – ohne jegliche Prüfung durch das BKA – in vielen tausend Fällen zu Unrecht Bestandsdatenabfragen erfolgen und strafrechtlich irrelevante Sachverhalte an die Strafverfolgungsbehörden übermittelt würden.

Eine weitere Problemstellung, die sich unmittelbar an die Frage der Aufgaben des BKA als Zentralstelle anschließt und die bislang noch nicht explizit behandelt wurde, ist die

Frage, ob mit der Bejahung des Anfangsverdacht und der Bestandsdatenabfrage bereits die Phase des strafrechtlichen Ermittlungsverfahrens begründet ist.

Der Bundesrat hat in diesem Zusammenhang zu Recht darauf hingewiesen, dass mit der Implementierung der Meldepflicht für Plattformbetreiber verhindert werden soll, dass strafbare Inhalte im Netz gelöscht und damit der strafrechtlichen Würdigung und gegebenenfalls Verfolgung entzogen werden. Die Meldung ist damit gerade keine das Ermittlungsverfahren auslösende Strafanzeige gemäß § 158 StPO, denn sie enthält kein eigenes Prüfungsbegehren des Plattformbetreibers. Vielmehr erfolgt sie gleichsam „neutral“ in Erfüllung einer dem Plattformbetreiber auferlegten gesetzlichen Pflicht. Schließlich spricht auch der Wortlaut des § 3a Absatz 2 NetzDG-E, dass die Meldepflicht den Zweck verfolge, den zuständigen Behörden die Verfolgung etwaiger Straftaten zu „ermöglichen“, dafür, dass die Tätigkeit des BKA in dieser Phase reine Zentralstellentätigkeit im Sinne des § 2 BKAG mit der Folge darstellt, dass Sachverhalte, die als strafrechtlich irrelevant bewertet wurden, weder bei einer Staatsanwaltschaft erfasst, noch von dieser „zweitbewertet“ und auch keiner förmlichen Einstellung zugeführt werden müssen.

Der Befürchtung, dass durch das BKA aufgrund der Komplexität der Tatbestände Sachverhalte ausgeschieden werden, die mglw. durch Staatsanwaltschaften für strafrechtlich relevant erachtet werden könnten, ist durch umfangreiche Schulungsmaßnahmen zu begegnen. So hat sich die in diesem Bereich langjährig tätige und mit besonderer Expertise ausgestattete Zentral- und Ansprechstelle Cybercrime NRW (ZAC) der Staatsanwaltschaft Köln, die sich gemeinsam mit meiner Zentralstelle bereits zu Beginn des Gesetzgebungsverfahrens mit dem BKA ins Benehmen gesetzt hat, um eine möglichst reibungslose Umsetzung des Gesetzes zu gewährleisten bereit erklärt, durch umfassende und fortlaufende Aus- und Fortbildungsmaßnahmen unterstützend tätig zu werden.

II. Klarstellung der (unmöglichen) Effizienz der Strafverfolgung

Im Gegensatz zu der Auffassung der Bundesregierung, die davon auszugehen scheint, dass mit den dem BKA übermittelten Daten und der im Rahmen der Zentralstellenfunktion zulässigen Abfragemöglichkeiten ein hoher Prozentsatz der Poster rechtswidriger Inhalte identifizierbar sein wird, ist aus der hiesigen, langjährigen Praxis davon auszugehen, dass lediglich ein relativ geringer Anteil derjenigen Personen, die für solche

rechtswidrigen Inhalte verantwortlich sind, allein durch (qualifizierte) Bestandsdatenabfragen ermittelbar sein wird.

Die unter Artikel 5 Ziffer 3 vorgeschlagene Vorschrift des § 3a Abs. 4 Nr. 2 NetzDG-E, welche die Übermittlung von „vorhandenen“ IP-Adressen und Portnummern an das BKA vorsieht und die zur Identifizierung der Verantwortlichen führen soll, wird in der Praxis weitgehend leerlaufen.

Obwohl Telemediendiensteanbieter bereits bisher IP-Adressen grundsätzlich auch über das Ende des Nutzungsvorgangs hinaus speichern dürfen (vgl. BGH NJW 2017, 2416), wird jedenfalls die für die Zuordnung zu einem Anschluss so wichtige Portnummer nach hiesiger Kenntnis von den Telemediendiensten derzeit mangels gesetzlicher Verpflichtung auch nicht gespeichert, sodass aufgrund der Tatsache, dass die Telekommunikationsdienste bei mobilen Endgerätenutzung durch Nutzung des sog. NAT-Verfahrens eine IP-Adresse vielfach vergeben, eine Zuordnung zum Anschlussinhaber allein aufgrund der gem. § 3a Abs. 4 Nr. 1 NetzDG-E übermittelten IP-Adresse ohne Portnummer nicht möglich sein wird. Aber selbst, wenn Portnummern erhoben und übermittelt werden würden, wäre eine Zuordnung schon deshalb nicht möglich, da die deutschen Telekommunikationsdiensteanbieter aufgrund mangelnder gesetzlicher Verpflichtung eine Speicherung von Portnummern nicht vornehmen. Schließlich besteht auch für den Fall, dass bei der Nutzung von Desktop-PCs vereinzelt Diensteanbieter kein Carrier-grade NAT verwenden, grundsätzlich die Problematik, dass aufgrund nicht erfolgter Umsetzung des § 100g Abs. 2 StPO, der aber ohnehin viele Tatbestände des § 3a Abs. 2 Nr. 3 NetzDG-E nicht enthält, eine Speicherung von IP-Adressen auf der Grundlage des § 100 TKG für höchstens 6 Tage vorgenommen wird, wobei viele Diensteanbieter die Verkehrsdaten unmittelbar nach Beendigung der Telekommunikationsverbindung löschen.

Diese rechtliche Einschätzung wird untermauert durch die Erkenntnisse aus den sog. „NCMEC-Verfahren“, in denen – sehr vergleichbar mit dem hiesigen Gesetzesvorhaben - durch amerikanische Diensteanbieter (u.a. auch soziale Netzwerke wie Facebook oder WhatsApp) nicht nur Login-IP-Adressen, sondern darüber hinaus gehend auch die Bestandsdaten von Nutzern, die für die Verbreitung von Kinderpornographie verantwortlich sind, über die private, gemeinnützige Organisation NCMEC dem BKA stellt zur Verfügung gestellt werden. Obgleich mangels umgesetzter Vorratsdatenspeicherung dem BKA als einziger Polizeibehörde weltweit der unmittelbare Zugriff auf die Datenbank von NCMEC zusteht, scheitert in über der Hälfte der Fälle die Identifizierung bereits von

vornherein daran, dass die IP-Adresse durch Zeitablauf nicht mehr zuzuordnen ist oder mobile Endgeräte genutzt wurden.

Um eine solch hohe Quote an nichtidentifizierten Postern zu vermeiden und dem Legalitätsprinzip zu entsprechen, wird daher in einem zweiten Schritt das BKA die strafrechtlich relevanten, aber nicht ermittelbaren Sachverhalten „von Amts wegen“ einer oder mehrerer Staatsanwaltschaften vorlegen müssen, damit diese eine Identifizierung mit den über die Möglichkeiten des BKAG hinausgehenden Ermittlungsinstrumentarien der Strafprozessordnung versuchen.

Da zu diesem Zeitpunkt weder Täter noch Tatort feststehen, besteht gem. § 143 I 2 GVG die Möglichkeit, dass das BKA eine Staatsanwaltschaft „erstbefasst“, die in diesen Fällen als „Identifizierungsstaatsanwaltschaft“ tätig wird und nach erfolgreicher Ermittlung das Verfahren an die örtlich zuständige Staatsanwaltschaft abgibt.

Meine Zentralstelle, die diese Funktion in unterschiedlichsten Kriminalitätsfeldern seit vielen Jahren in enger Zusammenarbeit mit dem BKA ausfüllt und die Verfahrensabläufe im Bereich der Massenkriminalität strukturiert und automatisiert hat, hat sich auch in den Fällen der Hasskriminalität bereit erklärt, identifizierend tätig zu werden.

Allerdings – und insoweit muss eindringlich gewarnt werden – wird eine Identifizierung auch mit den Mitteln der Strafprozessordnung weder flächendeckend oder auch nur überwiegend möglich sein.

Zwar könnten sich weitere Ermittlungsansätze aus den bei den sozialen Netzwerken hinterlegten Bestandsdaten ergeben. § 15a TMG-E schafft auch die Voraussetzung für die Beauskunftung von Bestands- und Nutzungsdaten gegenüber Telemediendiensteanbietern. Im Gegensatz zu den Anbietern von Telekommunikationsdienstleistungen, die gemäß § 111 TKG verpflichtet sind, Kundendaten zu erheben und diese bei Prepaid-Produkten auf ihre Richtigkeit hin zu überprüfen, findet sich eine solche Datenspeicherungs- und Überprüfungsverpflichtung in den Gesetzentwürfen betreffend das TMG jedoch nicht vor. Im Ergebnis bedeutet dies, dass bei Telemediendiensten, die von einer Erhebung von Bestands- und Nutzungsdaten absehen, eine Zuordnung der Beweismittel (bspw. der Screenshots der strafrechtlich relevanten Postings) zu einem Tatverdächtigen von vornherein ausgeschlossen sein wird. Erhebt der Telemediendienst zwar Bestandsdaten, sieht aber – zulässigerweise und wie derzeit üblich – von einer Identitätsprüfung des Nutzers ab, ist auch der Auskunftsanspruch gemäß § 100j Abs. 1 Satz 1 Nr.2 TMG-E nicht zielführend, denn der Tatverdächtige, der seinen Ac-

count nutzt, um strafbare Inhalte zu posten, wird diesen in aller Regel unter Falschpersonalien anlegen.

Zudem ist zu berücksichtigen, dass die NetzDG-relevanten Anbieter sozialer Netzwerke diese Bestandsdaten jeweils im Ausland vorhalten, so dass eine unmittelbare Beaufskunftung an das BKA oder andere Strafverfolgungsbehörden ausschließlich im Rahmen einer freiwilligen Kooperation erfolgen kann. Aus den Erfahrungen meiner Zentralstelle bei der Verfolgung von Hasskommentaren im Internet ist dabei allerdings festzustellen, dass die Anbieter Sozialer Netzwerke nur in wenigen Ausnahmefällen Bestandsdaten ihrer Kunden freiwillig herausgeben. Anderenfalls müsste die Erhebung der Bestandsdaten bei den Anbietern sozialer Netzwerke im Wege der förmlichen internationalen Rechtshilfe erfolgen, was in vielen Fällen der Massenkriminalität kaum verhältnismäßig sein dürfte.

Da sich aus der hiesigen Praxis im Rahmen der NCMEC-Verfahren jedoch gezeigt hat, dass sich aus den hinterlegten Bestandsdaten immer wieder Ermittlungsansätze zur Identifizierung der Nutzer (bspw. Kontakt-E-Mail-Adressen; hinterlegte Telefonnummern) ergeben haben, wäre es absolut wünschenswert, wenn diese Daten neben den Inhalten und der IP-Adresse mit ausgeleitet werden würden. Durch das BKA könnten diese Datenabfragen dann aufgrund der Erweiterung des § 10 BKAG auf Telemediendienste dann auch im Rahmen der Zentralstellentätigkeit erfolgen. Eine Abfrage der Nutzungsdaten durch Staatsanwaltschaften wäre durch die beabsichtigte Änderung des § 100g StPO, die einen Richtervorbehalt vorsieht, erheblich erschwert und verzögert.

Andere grundsätzlich denkbare Ermittlungsmaßnahmen, insbesondere verdeckte technische oder personale Ermittlungshandlungen sind bereits wegen des damit verbundenen Aufwandes zur Bekämpfung der Massenkriminalität ungeeignet und allenfalls bei herausragenden Fällen einsetzbar.

Es wird daher – zusammenfassend – gebeten,

a) zu Klarstellungszwecken im weiteren Gesetzgebungsvorhaben festzustellen, dass das BKA nach den Vorgaben des NetzDG-E im Rahmen der sich aus § 2 BKAG ergebenden Zentralstellenfunktion tätig wird, die auch eine Bewertung der übermittelten Inhalte auf deren strafrechtliche Relevanz umfasst.

Die vom Bundeskriminalamt als nicht strafbar bewerteten Inhalte, sind - da die Phase des Ermittlungsverfahrens nicht eröffnet ist - weder einer Staatsanwalt-

schaft zur Prüfung oder Erfassung vorzulegen und auch keiner förmlichen Einstellung zuzuführen

b) zu prüfen, ob § 3a Abs. 4 NetzDG-E um eine Verpflichtung der Sozialen Netzwerke zur Übermittlung der dort hinterlegten Bestandsdaten erweitert werden könnte.

Frankfurt am Main, den 05.05.2020

gez. May

Leitender Oberstaatsanwalt