Sehr geehrte Mitglieder des Ausschusses für Recht und Verbraucherschutz,
sehr geehrte Mitglieder des Bundestags,

mit den Entwürfen für ein *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität* sowie für ein *Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG)* will das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) Hasskriminalität bekämpfen und Betroffene unterstützen. Die Gesetzesvorhaben sollen den freien Meinungsaustausch im Netz sichern, die Persönlichkeitsrechte schützen und die Grundwerte der freiheitlich-demokratischen Grundordnung unserer Verfassung verteidigen. Diese wichtigen Ziele finden unsere Anerkennung und Unterstützung, wenn wir auch einige Punkte in den Entwürfen, insbesondere hinsichtlich der Einschränkung von Privatsphäre und Datenschutz, aber auch mit Blick auf die Verkürzungen rechtsstaatlicher Absicherungen und Prinzipien, riskant finden.

Unsere Kritik und ausführlichen Anmerkungen bezüglich beider Entwürfe haben wir in zwei Stellungnahmen aus der Zivilgesellschaft veröffentlicht; unsere Stellungnahme zum Entwurf eines G*esetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität* finden Sie hier, die Stellungnahme zum zweiten Gesetzesentwurf hier.

Mit diesem Brief möchten wir die Möglichkeit nutzen, als Bündnis ergänzende Forderungen einzubringen und Sie bitten, diese bei der weiteren Bearbeitung der Entwürfe zu berücksichtigen - um zu gewährleisten, dass die Gesetzesentwürfe nicht nur Symbolpolitik sind, sondern das Netz nachhaltig zu einem inklusiven Raum für alle machen.

(1) Nachvollziehbarkeit der Transparenzberichte

Wir begrüßen die Bestrebungen zur Ausweitung und Vereinheitlichung der Anforderungen an die Transparenzberichte, die die vom NetzDG umfassten Diensteanbieter halbjährlich veröffentlichen müssen.

Die „EU High-Level Expert Group on AI" betont die Bedeutung von Transparenz und Erklärbarkeit von automatisierten Entscheidungssystemen (ADM), die erhebliche Auswirkungen auf das Leben von Menschen haben. Eine tatsächliche Transparenz schaffende Berichterstattung muss daher nachvollziehbare Erläuterungen zum Content-Moderationssystem als Ganzes, den einzelnen ADM-Instrumenten sowie der praktischen Umsetzung von Moderationsrichtlinien beinhalten. Nur wenn Diensteanbieter hier nach klaren Standards und Leitlinien Rechenschaft ablegen, können notwendige Erkenntnisse über Umsetzung und Funktionsweise der NetzDG-Reformansätze gewonnen werden.

Jedoch empfehlen wir, dass die Berichte mit Informationen zu eingesetzter Technologie und Moderationsrichtlinien nicht der breiten Öffentlichkeit zur Verfügung gestellt werden sollten, um einen weiteren Missbrauch der Plattformen zu vermeiden. Wir schließen uns hier dem Policy Brief des Counter Extremism Projects an, welcher u.a. empfiehlt: "Die mit der Aufsicht beauftragte Institution kann den Detaillierungsgrad der veröffentlichten Berichte einschränken, um Geschäftsgeheimnisse zu schützen oder den Missbrauch zu verhindern." (CEP, 2020). Auf die Daten und Informationen sollten diejenigen Zugriff haben, die ein berechtigtes Interesse an deren Nutzung haben, etwa Forschungsinstitute, aber auch Politik und ausgewählte Organisationen der Zivilgesellschaft, die diese Informationen in ihre praktischen Arbeit aufnehmen können.

(2) Bedenken bezüglich Privatsphäre und Datenschutz - Quick Freeze als Lösung

Der Gesetzesentwurf zur Bekämpfung des Rechtsextremismus und der Hasskriminalität sieht gemäß §3 NetzDG n.F. eine Meldepflicht der Diensteanbieter an das BKA vor, was zwangsläufig zu einer flächendeckenden Speicherung personenbezogener Daten beim BKA

führt, insbesondere da die Speicherung allein aufgrund der Einschätzung der Diensteanbieter erfolgt. Dieses Vorhaben wird von Datenschützer*innen wie auch der Zivilgesellschaft scharf kritisiert; die Vereinbarkeit eines solchen Ansatzes mit den Grundsätzen der Meinungsäußerungs-, Medien- und Informationsfreiheiten ist nicht vorauszusetzen.

Um das Risiko einer "Verdachtsdatenbank" und der damit einhergehenden Konsequenzen zu umgehen, empfehlen wir den Einsatz des sogenannten Quick Freeze-Prinzips, das bereits im Urheberrecht genutzt wird. Diese ergänzende Maßnahme kann sicherstellen, dass die Ausleitung von IP-Adressen trotz überlasteter Strafermittlungsbehörden nutzbringend ist. Darüber hinaus wird ein Datenverlust verhindert, Persönlichkeitsrechte werden jedoch nicht unverhältnismäßig eingeschränkt: Die Nutzer*innendaten können bei den Providern vorgehalten werden, bis ein Anfangsverdacht durch eine Staatsanwaltschaft bestätigt oder verneint werden kann. Hier liegt die einzige Schwachstelle (weil Mehraufwand im Vergleich zur aktuell geplanten Meldung ans BKA) des Quick Freeze: In der Regel wird es nicht eine zuständige Staatsanwaltschaft geben. Es müsste also, wenn der Wohnsitz des*der Verfasser*in unbekannt ist, erst einmal eine zufällig ausgewählte Staatsanwaltschaft einen Anfangsverdacht prüfen – dies erscheint unserer Ansicht nach jedoch ein machbarer und vertretbarer Mehraufwand zu sein. In diesem Kontext ist auch die hinreichende personelle und finanzielle Ausstattung der Justiz in Anbetracht steigender Fallzahlen von zentraler Bedeutung.

(3) Rechtsdurchsetzung im Netz – Marktortprinzip

Insgesamt braucht es dringend eine Verbesserung der Rechtsdurchsetzung im Netz. Dazu zählt auch eine Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden und den Diensteanbietern – denn bislang scheitert die Rechtsdurchsetzung häufig daran, dass die Diensteanbieter Auskunftsersuchen nicht nachkommen. Vielmehr werden Ermittlungsbehörden an ausländische Stellen verwiesen, mit dem Verweis, dass die angeforderten Daten im Ausland liegen. Es ist anzunehmen, dass diese Handhabung auch mit einer national geregelten Auskunftspflicht beibehalten wird[1].

Aus diesem Grund empfehlen wir für Telemedien die Einführung des Marktortprinzips, um die Beantwortung von Anfragen der Ermittlungsbehörden, unabhängig vom Speicherort der Daten, zu garantieren: "Unter Geltung des Marktortprinzips könnten sich Plattformen nicht länger auf eine Datenspeicherung im Ausland berufen, da sie verpflichtet wären, Daten im Inland vorzuhalten." (HateAid, 2020). Auch der Antrag zur "Effektivierung von Auskunftserteilungen durch ausländische Anbieter sozialer Netzwerke" der Bundesländer Bremen und Hamburg zur Entschließung des Bundesrats von Februar 2020 hat sich für ein solches Vorgehen ausgesprochen.

In der Hoffnung, dass unsere ergänzenden Forderungen Eingang in Ihre Beratungen finden, verbleiben wir mit freundlichen Grüßen.

Unterzeichner*innen

Das NETTZ - Vernetzungsstelle gegen Hate Speech
No Hate Speech Movement
Amadeu Antonio Stiftung
Campact
Counter Extremism Project (CEP)

[1] Hierzu empfiehlt auch der Bundesrat in seiner Stellungnahme vom 15. Mai die Überprüfung des Herkunftslandprinzips: https://www.bundesrat.de/DE/plenum/bundesrat-kompakt/20/989/22.html#top-22