Chaos Computer Club

Stellungnahme

zum Eckpunkte-Papier zum Gesetz gegen digitale Gewalt

26. Mai 2023

Einleitung

Die vom BMJ veröffentlichten Eckpunkte zu einem Gesetz gegen digitale Gewalt weisen eine Reihe von problematischen Ansätzen und Annahmen auf, die in der Praxis ein hohes Missbrauchspotenzial sowie diverse Probleme mit sich bringen.

Der Chaos Computer Club (CCC) betont ausdrücklich, dass ein effektiver und praktikabler Schutz der Betroffenen nötig und wünschenswert ist. Ähnlich wie beispielsweise bei der parallelen Diskussion um die Chatkontrolle[1] ist der vorliegende Entwurf dafür jedoch nicht oder nur sehr partiell geeignet.

Die technischen und praktischen Implikationen des vorliegenden Entwurfs sind in der öffentlichen Diskussion bisher zu wenig beleuchtet. Es muss vermieden werden, dass sich im geplanten Gesetz die Fehler des Netzwerkdurchsetzungsgesetzes (NetzDG) wiederholen.[2] Hierzu ist auch eine umfangreiche Evaluierung der praktischen Auswirkungen des Netzwerkdurchsetzungsgesetzes nötig. Nur so können zukünftige Fehlentwicklungen und negative Auswirkungen auf die Meinungsfreiheit und andere Grundrechte verhindert werden.

Die im Entwurf vorgeschlagenen Maßnahmen führen zu einem Verlust an informationeller Selbstbestimmung mit potentiell katastrophalen Folgen für zu Unrecht Beschuldigte. Die Probleme der „digitalen Gewalt" werden zudem im Entwurf ausschließlich in den Bereich der Hassrede verschoben. „Digitale Gewalt" ist jedoch komplexer und weitreichender als Hassrede. Diese einseitige Fokussierung von Aufmerksamkeit und Ressourcen sorgt sogar dafür, dass Maßnahmen, die Betroffenen von digitaler Gewalt wirklich helfen würden, nicht debattiert und angegangen werden.

Unzureichende Begriffsdefinition „digitale Gewalt"

Ein gravierender Mangel des Eckpunktepapiers ist die fehlende präzise und abschließende Begriffsdefinition von „digitaler Gewalt". Die Ausweitung des Begriffs auf alle Fälle der Verletzung absoluter Rechte droht in der Praxis dazu zu führen, dass das Gesetz beispielsweise zur Durchsetzung von Urheberrechtsansprüchen, als Informationsbeschaffungsmittel für Stalking und die Bekämpfung politischer Gegner genutzt wird.

Am vom BMJ selbst aufgeführten Beispiel der „verleumderischen Restaurantkritik" lässt sich das Problemfeld gut ersehen: Nehmen wir an, ein Gast beschwert sich in einem Nutzerkommentar zu Recht über unhygienische Zustände in der Küche oder über unhöflichen Service. Der Restaurant-

---

[1] Vgl. Positionspapier: Alle gegen Chatkontrolle, https://www.ccc.de/de/updates/2022/positionspapier-alle-gegen-chatkontrolle vom 19. Oktober 2022.

[2] Siehe https://www.ccc.de/de/updates/2017/netzdg vom 10. April 2017. In dieser breit getragenen Deklaration für die Meinungsfreiheit erkennen die Unterzeichnenden an, dass Handlungsbedarf besteht, aber der Gesetzentwurf nicht dem Anspruch genügt, die Meinungsfreiheit adäquat zu wahren.

besitzer bestreitet dies aber. Der Gast wird per Gerichtsanordnung deanonymisiert, auf Schadenersatz in Anspruch genommen und sein Google-Account gesperrt. Er verliert den Zugang zu seinen Fotos, seiner E-Mail-adresse, seinem Kalender und seinen Dokumenten. Um sich zu wehren, müsste er eine umfangreiche Tatsachendokumentation beibringen, die er wahrscheinlich beim Restaurantbesuch gar nicht vorgenommen hat. Vielleicht hatte er Glück und das Gericht urteilt in der Folge, dass die Kritik berechtigt war. Jedoch ist der Schaden durch die Accountsperre bereits eingetreten, und es besteht durch die Offenlegung seiner Identität kein Schutz mehr vor informellem Mobbing und Gängelung durch den Gastwirt. Dieses Szenario ist mitnichten theoretisch.

Nötig ist eine klare und saubere Begriffsdefinition von „digitaler Gewalt". Eine Verbesserung wäre, wenn diese nur für natürliche Personen gelten sollte und unter eng gefassten Voraussetzungen Anwendung findet. Eine Differenzierung zwischen dem öffentlichen Raum und dem digitalen Nahfeld ist hierbei unerlässlich, um einen angemessenen Schutz der Betroffenen unter Wahrung der informationellen Selbstbestimmung zu gewährleisten.

Je weiter der Begriff „digitale Gewalt" auslegbar ist, desto größer werden alle im folgenden erläuterten Risiken. Die ausufernde und unbestimmte Begriffsdefinition wirkt als Brandbeschleuniger für alle negativen Effekte und Nebenwirkungen einer Regelung.

Speicher- und Identifikationspflicht

Die im Entwurf vorgesehenen Speicher- und Identifikationspflichten sind eine potenzielle Gefahr für die Grundrechte der Betroffenen. Insbesondere im Hinblick auf die Ausgestaltung des Auskunftsverfahrens und die Beweissicherungsanordnung muss die tatsächliche Rechtspraxis der Gerichte und die resultierende Auskunftspraxis der Netzanbieter in Urheberrechtsfragen als warnendes Beispiel in Betracht gezogen werden. Die aus der vorgeschlagenen Regelung zu erwartende Rechtspraxis ist, dass Beklagte regelmäßig deanonymisiert werden, auch wenn in späteren Verfahren keine strafbare „digitale Gewalt" festgestellt wird.

Die Erläuterung zum Eckpunktepapier postuliert: „Nur wenn es zu dem Ergebnis kommt, dass eine Rechtsverletzung vorliegt, gibt das Gericht dem Auskunftsanspruch statt." Die Erfahrung aus der Urheberrechts-Praxis zeigt jedoch, dass die Gerichte angesichts der Fülle von Begehren und dem aus ihrer Sicht bestehenden Rechtsschutz durch nachgelagerte Verfahren einem Auskunftsersuchen regelmäßig stattgeben, teilweise im Widerspruch zur Intention des Gesetzgebers.

Es gibt derzeit praktisch keine Fälle, in denen ein Gericht in Urheberrechtssachen einen Auskunftsanspruch verweigert, weil regelmäßig keine ernsthafte Prüfung des Sachverhaltes stattfindet. Auskunftsersuchen werden schlicht „durchgestempelt". In der Folge werden massenweise automatisiert Abmahnungen generiert, an denen sich spezialisierte Anwaltskanzleien bereichern.

Es ist zu erwarten, dass eine praktische Anwendung des Gesetzes gegen digitale Gewalt ähnlich ausfallen wird. Dass Missbrauchspotential für ein solches Modell wird insbesondere durch die Forderung nach möglichst kleinen Hürden sowie die Automatisierung von Auskunftsverfahren gestützt.

Die vorgeschlagenen Auskunftsverfahren sowie Beweissicherungsanordnung (Kapitel II, 1. b) wirken als indirekte Vorratsdatenspeicherung. Durch die im Eckpunktepapier vorgesehenen Maßnahmen wird verstärkt Druck auf die Telekommunikationsanbieter ausgeübt, im Falle einer Beweissicherungsanordnung die Zuordnung von IP-Adresse und Nutzerdaten für den unbestimmten Zeitraum des gesamten Verfahren umfangreicher zu speichern oder durch einstweilige Anordnung frühzeitig offenzulegen. Die unscharfe Regelung, dass die Speicherfrist dem Anbieter obliegt, ist in der Realität nicht hilfreich, da insbesondere große Unternehmen anfällig für Reputationsschäden durch Boulevard-Medien sind, die Einzelfälle aufbauschen. „Dieser miese Hetzer konnte nicht enttarnt werden, weil die Telekom nicht lange genug speichert“, ist sicher keine Schlagzeile, die ein Telekommunikationsanbieter lesen möchte. Entsprechend groß wird der Druck auf die Anbieter.

Eine Herausgabe von Nutzungsdaten und die Ausweitung auf Messenger- und Internetzugangsdienste bergen besondere Risiken für anonyme oder pseudonyme Kommunikation. Zudem könnten die technischen Implikationen für Ende-zu-Ende-Verschlüsselung (E2EE) und weitere Werkzeuge der Informationssicherheit verheerend sein. Es muss hier eine Einschränkung auf öffentlich zugängliche Kommunikation verankert werden. Für Fälle „digitaler Gewalt“ in nicht öffentlich sichtbaren Kommunikationskanälen müssen differenziertere Regeln gefunden werden, die nicht zu einer Schwächung oder dem Bruch von E2EE führen.

Weiter muss klargestellt werden, dass eine solche Regelung nicht dazu führt, besonders datensparsame Anbieter dazu zu verpflichten, mehr Daten als nötig zu erheben.

Ein besonderer Konflikt besteht in der hier neuen Form der Profilbildung unter dem Mantel der Strafverfolgung. Einerseits tritt der Digital Services Act (DSA) der Profilbildung klar entgegen, andererseits werden jedoch vor dem Hintergrund dieses Gesetzesentwurfs immer mehr Daten eingefordert. Diese Gegenläufigkeit erzeugt einen Konflikt, der dringend adressiert werden muss, um die Grundrechte der Betroffenen zu schützen.

Accountsperren-Regelung kann Strafe ohne Urteil sein

Die vorgeschlagenen Regeln für Accountsperren gehen von Annahmen aus, die fern der heutigen digitalen Praxis sind und offenbar auf sehr selektiv gewählten Szenarien beruhen. Daraus entstehen mehrere Problemfelder.

Die Schwere der faktischen Auswirkungen einer Accountsperre für Betroffene variiert erheblich. Während sie für jemanden mit fünfzig Troll-Accounts kaum relevant ist, werden Menschen mit einer großen Anhängerschaft, Monetarisierung ihrer Inhaltsproduktion (etwa Youtube-Kanäle oder Podcasts) und einem umfangreichen sozialen Netzwerk

überproportional stark getroffen. Viele Accounts dienen nicht nur einem einzigen Zweck, sondern werden in vielfältiger Weise verwendet. Google-Accounts werden beispielsweise nicht nur für Restaurantkritiken, sondern parallel auch für Dokumentenbearbeitung, Kalender, Bilder-Archivierung, Backups und via „Login with Google“ für eine unabsehbar große Zahl von anderen Online-Accounts verwendet.

Beim Beispiel der oben erwähnten Restaurantkritik wären die Folgen erheblich. Denn die großen Plattformen agieren erfahrungsgemäß nach einer sog. „Hammer Gottes“-Methode, wenn sie eine Accountsperre durchführen: Es wird nicht nur die Möglichkeit des Abgebens von Restaurantkritiken gesperrt, sondern das gesamt Online-Leben des Betroffenen de facto beendet.

Im Bereich von Youtube und anderen Medienplattformen, die eine Monetarisierung erlauben, ist nicht selten ein erheblicher Teil des Lebensunterhalts von einer Accountsperre betroffen. Auch wenn Accountsperren stets mit einer zeitlichen Begrenzung vorgesehen sind, wird sie zu einem kurzen bzw. langfristigen Ausfall des Lebensunterhalts führen. Diese erhebliche Strafe tritt ein, bevor ein rechtskräftiges Urteil ergangen ist.

Das vorliegende Eckpunktepapier trifft hier keine Abwägung. Angemessenheit und Geeignetheit der Maßnahmen sind – je nach Einzelfall – stark zweifelhaft. Viele Nutzer haben gute Gründe für das Verschleiern ihrer Identität in öffentlicher Online-Kommunikation. Ein Zwang zur Offenlegung von Identitäten, um einen Widerspruch gegen ein Verfahren wegen „digitaler Gewalt“ durchzuführen, ist daher nicht akzeptabel. Hier müssen Regelungen gefunden werden, die eine anonyme Durchführung der Wahrnehmung der Rechte von Betroffenen ermöglichen.

Die Einführung von Regelungen zu Accountsperren wird absehbar zu einer Überlastung der Justiz führen, da eine zunehmende Anzahl von Fällen behandelt werden muss. Dies wird zu längeren Verfahrenszeiten und einer Beeinträchtigung des Zugangs zur Justiz führen.

Die vorgeschlagenen Maßnahmen zu privaten Auskunftsverfahren sowie Accountsperren werfen gewichtige Fragen zur Verhältnismäßigkeit auf. Das Missbrauchspotential durch ungerechtfertigte Accountsperren und Auskunftsverfahren ist erheblich. Durch die Anlehnung der Auskunftsverfahren an bestehende Regelungen des Urheberrechts erlangen Kläger frühzeitig Zugang zu den Identitäten bisher anonymer oder pseudonymer Nutzer. Es besteht somit ein hohes Risiko einer unkontrollierten Offenlegung der Identität und realer, schwer wieder gutzumachender Schäden für Personen, die vom jeweiligen politischen Gegner ins Visier genommen werden.

Lernen aus den Fehlern des NetzDG

Das NetzDG hat aufgezeigt, welche negativen Auswirkungen ein unausgereiftes Gesetz zur Regulierung des digitalen Raums haben kann. Es kam zu zahlreichen Fehlentscheidungen und Überblockierungen von Inhalten, die keine rechtswidrigen Inhalte darstellten. Dies führte zu einer

Einschränkung der Meinungsfreiheit und der Zensur legitimer Meinungsäußerungen. Ein Bericht von Justitia Initiatives for International Standards[3] zeigt, wie das deutsche Modell der Online-Zensur weltweit Nachahmer findet und als Vorlage für ähnliche Gesetze auch in undemokratischen Ländern dient. Dies verdeutlicht, dass die Auswirkungen des NetzDG über die nationalen Grenzen hinausreichen.

Der Kommentar des UN-Sonderberichterstatters zum Schutz der Meinungsfreiheit kritisiert die Auswirkungen des NetzDG auf die Meinungsfreiheit und den Schutz der Privatsphäre.[4] Selbst die Evaluation im Auftrag des BMJV hat auf rechtliche Bedenken hinsichtlich des NetzDG hingewiesen.[5] Sie weist darauf hin, dass schon dieses Gesetz nicht ausreichend klar definierte Begriffe und rechtliche Standards enthält, was zu Unsicherheiten und willkürlichen Entscheidungen führen kann.

Trotz der negativen Erfahrungen und Kritikpunkte scheint eine kritische Evaluation im Hinblick auf die Ausarbeitung des Eckpunktepapiers nicht stattgefunden zu haben. Die fehlende Evaluierung und die mangelnde Berücksichtigung der negativen Erfahrungen und Kritikpunkte des NetzDG sind bedenklich. Nötig ist eine umfassende Bewertung des Gesetzes und eine kritische Überprüfung der Auswirkungen auf die Meinungsfreiheit und den Schutz der Privatsphäre.

Es ist von entscheidender Bedeutung, aus den Fehlern des NetzDG zu lernen und regulatorische Ansätze zu entwickeln, die sowohl den Schutz vor Hassrede und „digitaler Gewalt“ als auch die Grundrechte gewährleisten. Nur so kann ein ausgewogenes und effektives Regelwerk für den digitalen Raum geschaffen werden.

Mangelndes Fachwissen bei Behörden und Anlaufstellen

Aus Gründen der Zuständigkeit geht das Eckpunktepapier des BMJ nicht auf die nötigen strukturellen Maßnahmen zur effektiven Bekämpfung des Problems ein. Eine fachlich übergreifende Lösung ist jedoch unerlässlich für eine nachhaltige Lösung des Problems. Daraus ergeben sich die folgenden Forderungen.

Das Fehlen von Fachwissen bei den ausführenden Strafverfolgungsbehörden stellt ein erhebliches Hindernis bei der Bekämpfung „digitaler Gewalt“ dar. Die Komplexität der technischen Aspekte, die mit solchen Fällen verbunden sind, erfordert spezialisiertes Wissen, um angemessene Ermittlungen durchzuführen und Betroffene zu schützen.

---

[3] Jacob Mchangama: How the German Prototype for Online Censorship went Global, https://justitia-int.org/en/the-digital-berlin-wall-act-2-how-the-german-prototype-for-online-censorship-went-global-2020-edition/ vom 1. Oktober 2020.

[4] Vgl. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf vom 1. Juni 2017.

[5] Evaluation des NetzDG im Auftrag des BMJV, https://www.bmj.de/SharedDocs/Downloads/DE/News/PM/090920_Juristisches_Gutachten_Netz.pdf, 20. September 2020.

Um eine effektive Bekämpfung „digitaler Gewalt“ zu gewährleisten, sehen wir die folgenden Maßnahmen als unerlässlich:

Personelle Stärkung und bessere Ausbildung der Ermittlungsbehörden

Es ist von entscheidender Bedeutung, dass die Strafverfolgungsbehörden ausreichend Personalressourcen und finanzielle Mittel erhalten, um Fachkräfte einzustellen und sie entsprechend auszubilden. Die Behörden sollten eng mit Experten und fachlich kompetenten Organisationen zusammenarbeiten, die über das erforderliche Know-how in Bezug auf „digitale Gewalt“ verfügen, um ein umfassendes Verständnis der Herausforderungen und Lösungsansätze zu erlangen.

Durchführung von Studien

Um die Gründe für die nicht ausreichend genutzten vorhandenen Ermittlungsansätze zu herauszufinden, sind umfassende Studien erforderlich. Es ist wichtig zu verstehen, welche Faktoren dazu führen, dass Ermittlungen in Fällen „digitaler Gewalt“ nicht ausreichend vorangetrieben werden. Nur durch eine fundierte Analyse dieser Problematik können geeignete Maßnahmen zur Verbesserung ergriffen werden.

Ursachenforschung

Eine intensive Forschung ist notwendig, um die Ursachen des Fachwissendefizits bei den ausführenden Behörden zu identifizieren. Es müssen die Barrieren und Hindernisse untersucht werden, die dazu führen, dass Fachwissen und technisches Know-how nicht angemessen in den Behörden etabliert werden.

Der Kampf gegen „digitale Gewalt“ erfordert einen umfassenden Ansatz, der auch Frauenhäuser und vergleichbare Organisationen mit technischem Fachwissen und ausreichenden Ressourcen ausstattet.

Eine zentrale Herausforderung besteht in unzureichenden finanziellen Ressourcen. Häufig verfügen diese Organisationen über begrenzte Budgets, die nicht ausreichen, um angemessene Schulungen für ihre Mitarbeiterinnen anzubieten oder qualifizierte technische Experten einzustellen. Auch hier liegt ein erheblicher Mangel an technischem Fachwissen vor.

Um Betroffene von „digitaler Gewalt“ effektiv unterstützen zu können, ist fundiertes Wissen über digitale Sicherheit, Datenschutz und technologische Risiken von entscheidender Bedeutung. Dazu gehören Kenntnisse über den Einsatz von Verschlüsselungstechnologien, den verantwortungsvollen Umgang mit Social-Media-Plattformen und die sichere Nutzung von Kommunikationsgeräten. Ohne dieses Wissen sind Frauenhäuser und vergleichbare Organisationen nur eingeschränkt in der Lage, adäquate Unterstützung anzubieten.