# Stellungnahme von D64 – Zentrum für Digitalen Fortschritt zum Eckpunktepapier des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt

## Übersicht

Executive Summary....2
1. Einleitung....3
2. Vereinfachtes Auskunftsverfahren....3
Zur Anwendbarkeit auf alle Fälle der Verletzung absoluter Rechte....4
Die Bedeutung der Anonymität für die Meinungsfreiheit....4
Chilling Effects....6
Maßnahmen bei Rechtsverletzungen durch anonyme Nutzer:innen....6
Zur Ausweitung auf Messenger- und Internetzugangsdiensten....6
Zur effektiveren Ausgestaltung des Auskunftsverfahren....7
Beweissicherungsanordnung....7
Video-Verhandlung und Amtsermittlungsgrundsatz....7
3. Accountsperren....7
4. Zustellungsbevollmächtigte in Deutschland....8
5. Was im Eckpunktepapier fehlt....8
Anonymität/Impressumspflicht....8
Verbesserung des Beratungsangebots....9
Strafverfolgung als staatliche Aufgabe....9

Das Eckpunktepapier des Bundesjustizministeriums kann hier abgerufen werden: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Digitale_Gewalt.html

D64 e.V.
Gipsstraße 3
10119 Berlin

030 577 142 56
info@d-64.org
www.d-64.org

GLS Bank
DE13 4306 0967 1134 4765 00
GENODEM1GLS

Vereinsregister
AG Charlottenburg VR 31163 B
Lobbyregister: R000251

## Executive Summary

**D64 – Zentrum für Digitalen Fortschritt begrüßt die Initiative des Bundesjustizministeriums, sich dem Thema Hass im Netz anzunehmen.** Bedauerlicherweise scheint jedoch als zentrales Problem für den Diskurs im digitalen Raum Anonymität identifiziert worden zu sein. So sollen mit der Ausweitung des Anwendungsbereichs der Auskunftsansprüche zukünftig Unternehmenskritik wie Todesdrohungen gleichermaßen zur Aufhebung der Anonymität eines:r Nutzers:in berechtigen. **Die Bedeutung, die der Schutz der Anonymität insbesondere für vulnerable Gruppen hat, wird grundlegend verkannt.** Es besteht die erhebliche Gefahr des Missbrauchs der angedachten Regelungen zum Zwecke der Identifizierung von Journalist:innen und politischen Aktivist:innen, deren Adressen sodann in einschlägigen politischen Kreisen geteilt werden können. **D64 lehnt die Ausweitung des Anwendungsbereichs der Auskunftsansprüche auf die Verletzung sämtlicher absoluter Rechte daher ab und fordert eine Beschränkung auf Straftaten.**

**Die Einführung der Möglichkeit richterlich angeordneter und damit rechtsstaatlich abgesicherter Accountsperren begrüßt D64.** Hier ist jedoch die Möglichkeit der kollektiven Rechtsverteidigung durch entsprechende Verbandsklagerechte bei der Begehung von Straftaten ohne individuelles Opfer, wie Volksverhetzung, zu ermöglichen. Positiv hervorzuheben ist die Möglichkeit der Gewährung rechtlichen Gehörs für die Nutzer:innen von Accounts, gegen die vorgegangen wird, bei gleichzeitiger Wahrung der Anonymität.

**In einigen zentralen Punkten enthält das Eckpunktepapier leider noch keine Vorschläge.** So wird nicht dargelegt, wie das **Beratungsangebot für Betroffene** von Hass im Netz verbessert werden soll, obwohl dies im Koalitionsvertrag explizit angekündigt wurde. D64 setzt sich dafür ein, dass über **Beratungsschnittstellen** auf den Plattformen Betroffene zukünftig unmittelbar an dem digitalen Ort, an dem sie sich befinden, digitale Beratungsangebote zur Verfügung gestellt bekommen sollten. D64 fordert ferner der Schutz vor Bedrohungen und Übergriffen zu verbessern, in dem die **Impressumspflicht** überarbeitet sowie der **Schutz der persönlichen Daten von Opfern und Zeug:innen im Strafverfahren** verbessert wird.

**Schließlich bleibt die Verfolgung von Straftaten – im analogen wie im digitalen Raum – eine originär staatliche Aufgabe.** Die Verteidigung der eigenen Rechte gegen strafbare Angriffe darf keine Frage der (finanziellen) Leistungsfähigkeit einer Person sein, indem sie von aufwändiger und teurer privaten Rechtsdurchsetzung abhängig gemacht wird. Zur Verbesserung der Strafverfolgung im Internet ist vielmehr eine umfangreiche Verbesserung der Digitalkompetenz der Strafverfolgungsbehörden anzustreben, in deren Rahmen Prozesse standardisiert und über Schnittstellen abgebildet werden. Keinesfalls bedarf es neuer Strafgesetze oder Datenspeicherungen, sondern vielmehr eines gezielten Vorgehens nach rechtsstaatlich bestätigtem Anfangsverdacht. Dass dabei auch anonyme Nutzerkonten ein lösbares Problem darstellen, zeigen wir mit unserem **Konzept der „Login-Falle“**.

D64 e.V.
Gipsstraße 3
10119 Berlin

030 577 142 56
info@d-64.org
www.d-64.org

GLS Bank
DE13 4306 0967 1134 4765 00
GENODEM1GLS

Vereinsregister
AG Charlottenburg VR 31163 B
Lobbyregister: R000251

## 1. Einleitung

Wir begrüßen es sehr, dass die Bundesregierung das Thema Hass im Netz ernst nimmt und nun mit dem Eckpunktepapier für ein Digitales Gewaltschutzgesetz mit der Umsetzung eines zentralen Versprechens des Koalitionsvertrags in diesem Bereich beginnt. An dieser Stelle sei auch ein besonderer Dank für den guten Prozess der Verbandsbeteiligung ausgesprochen, insbesondere die Form eines Eckpunktepapiers sowie die vergleichsweise lange Frist für die Abgabe einer Stellungnahme.

Die Bedeutung von Hasskriminalität im Netz geht weit über die individuelle Tat hinaus. Ein verrohter Diskus im digitalen Raum führt dazu, dass Personengruppen, die besonders von Beleidigungen und Bedrohungen, sei es individuell oder als Teil eines Kollektivs, betroffen sind, sich aus digitalen Diskussion zurückzuziehen. Diesen *silencing effects* gilt es entgegenzuwirken. Demokratie lebt von dem vielfältigen, kontroversen Austausch von Meinungen, in dem nicht eine Seite die andere niederbrüllen und zum Schweigen bringen darf.

Ziel eines jeden Gesetzgebungsvorschlags in diesem Bereich muss es deshalb sein, Maßnahmen zu ergreifen, die besonders vulnerable Gruppen im Internet schützen, um ihre aktive Partizipation an der digitalen Debatte zu ermöglichen und zu fördern. Eine besondere Bedeutung hat dabei der Schutz der Anonymität. Für viele ist Anonymität die Voraussetzung für Freiheit. Nicht weil Schutz vor dem staatlichen Sanktionssystem gesucht wird, sondern weil Anonymität Schutz vor Rechtsextremen vor der eigenen Haustür bietet, und vor Kampagnen gegen den Arbeitgeber. Sie führt dazu, dass das eigene Verhalten Angehörige nicht gefährdet. Diese grundsätzliche Bedeutung der Anonymität verkennt das Eckpunktepapier, nur an einer Stelle heißt es lapidar, dass die „die grundsätzliche Freiheit zur anonymen Meinungsäußerung […] gewahrt [bleibt]".

Einen anderer Weg wird durch die – im Eckpunktepapier etwas an den Rand gedrängten – richterlich angeordneten Accountsperren gewählt. Diese ermöglichen ein Vorgehen gegen anonyme Konten, berücksichtigen damit die Spezifika der Verbreitung von Hass und Hetze im digitalen Raum, die im ganz besonderen Maße auf Verbreitung durch Follower:innen angewiesen ist.

Die Stärkung der Rechte Betroffener von Hass und Hetze ist ein wichtiges Signal. Dringend notwendig ist deshalb eine Verbesserung des Beratungsangebots, auch in dem das bestehende Angebot einfacher zugänglich gemacht wird. Betroffene müssen in den digitalen Räumen, in denen sie sich aufhalten, unmittelbar Hilfe anfordern können. Betroffene dürfen jedoch nicht allein gelassen werden. Es ist eine öffentliche, staatliche Aufgabe, Strafverfolgung im Internet effektiv durchzuführen.

## 2. Vereinfachtes Auskunftsverfahren

Das Eckpunktepapier des Justizministeriums betont dagegen vor allen Dingen die Bedeutung der effektiven privaten Rechtsdurchsetzung. Nach der bisherigen Rechtslage können Betroffene von sozialen Netzwerken Auskunft über die Identität von Verfasser:innen von rechtsverletzenden Äußerungen verlangen. Der Auskunftsanspruch ist begrenzt auf Bestandsdaten (also bspw. Name und Anschrift der nutzenden Person) und auf solche Fälle, in denen eine Katalogstraftat des § 1 Abs. 3 NetzDG vorliegt (also bspw. eine Beleidigung, Verleumdung oder Bedrohung).

Zur Verbesserung der bisherigen Rechtslage schlägt das Eckpunktepapier vor, das Auskunftsverfahren deutlich zu erweitern. So sollen zukünftig alle Fälle der Verletzung absoluter Rechte zu einem Auskunftsanspruch führen, der auch Messenger- und Internetzugangsdienste erfasst, sowie die Herausgabe von Nutzungsdaten (wie IP-Adressen) verlangt werden kann.

Insbesondere der Erweiterung des Anwendungsbereichs begegnen wir mit großer Skepsis. Sie stellt eine erhebliche Gefahr für die anonyme Nutzung des Internets dar und ist derart missbrauchsanfällig, dass eine Viel-

zahl von Fällen erfasst werden, bei denen — von den Ersteller:innen des Eckpunktepapiers wohl nicht intendiert — es sich dem Grunde nach um wünschenswertes zivilgesellschaftliches Engagement handelt.

## Zur Anwendbarkeit auf alle Fälle der Verletzung absoluter Rechte

Absolute Rechte sind sämtliche Rechte, die gegenüber „jedermann" bestehen. Während man also beispielsweise bei einem Kaufvertrag nur einen Anspruch darauf hat, dass eine bestimmte Person eine Sache übereignet (subjektives Recht), darf niemand eine andere Person beleidigen oder verleumden (Verletzungen des Allgemeinen Persönlichkeitsrechts). Neben dem allgemeinen Persönlichkeitsrecht sind andere absolute Rechte beispielsweise dingliche Rechte (also Abwehransprüche, die sich aus dem Eigentum an einer Sache ergeben), Immaterialgüterrechte (also Urheber-, Marken- oder Patentrechte, sog. „Recht am geistigen Eigentum") und das Recht am eingerichteten und ausgeübten Gewerbebetrieb (alles, was in seiner Gesamtheit den wirtschaftlichen Wert eines Betriebes ausmacht, als bspw. Bestand, Erscheinungsform, Tätigkeitskreis und Kundenstamm).

Nach der aktuellen Rechtslage sind Rechte am geistigen Eigentum gegenüber anderen absolut geschützten Rechten privilegiert, weil eine Verletzung dieser Rechte auch ohne das Vorliegen einer Straftat zur Auskunft von Bestandsdaten berechtigt (§ 21 Abs. 1 TTDSG).

Nichtsdestotrotz handelt es sich bei der geplanten Gleichstellung aller absoluten Rechte nicht um das Schließen einer Schutzlücke zugunsten der Persönlichkeitsrechte gegenüber den bisher privilegierten Rechten am geistigen Eigentum, sondern vielmehr um die Erweiterung und Vertiefung eines Fehlers. Das Leben und das Recht sind kompliziert. Aus diesem Grund unterscheidet unser Rechtssystem zwischen der einfachen Verletzung privater Rechte, gegen die Individuen sich nur selbst wehren können, und solchen Verletzungen von Rechtsgütern, die einen besonderen Unrechtsgehalt mit sich bringen und deshalb strafrechtlich verfolgt werden. Das ist – so defizitär die Umsetzung in der Praxis der Strafverfolgung in diesen Bereichen auch sein mag – beispielsweise bei jeder Beleidigung der Fall (§ 185 StGB). Strafbar sind auch Bedrohungen gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert (§ 241 StGB), die üble Nachrede (§ 186 StGB), Verleumdungen (§ 187 StGB) etc. Die Auskunftsverfahren – und damit die Deanonymisierung/Identifizierung von Nutzenden – sollten auf diese Fälle beschränkt werden, in denen ein solcher besonderer Unrechtsgehalt vorliegt.

## *Die Bedeutung der Anonymität für die Meinungsfreiheit*

Der Grund hierfür ist die Bedeutung der Anonymität für die Meinungsfreiheit und damit für das Funktionieren unserer liberalen Demokratie. Meinungsfreiheit lebt davon, dass Menschen ohne Angst vor Repressalien ihre persönlichen Überzeugungen äußern können. Die Form der Repressalien können dabei vielfältig sein, auch staatliche Zwangsmaßnahmen gehören dazu, vor allen Dingen können es aber auch sanktionierende Maßnahmen durch den:die Arbeitgeber:in sein, Bedrohungen und Angriffe auf die persönliche Sicherheit durch andere Privatpersonen, Ächtung im unmittelbaren sozialen Umfeld und vieles mehr. Es sind insbesondere vulnerable Gruppen, die auf den Schutz der Anonymität angewiesen sind. Je privilegierter die gesellschaftliche Position einer Person ist, desto wahrscheinlicher ist es, dass sie sich der Angriffe zu erwehren weiß und auf Anonymität nicht angewiesen ist. Je verletzlicher ihre Position ist, desto unwahrscheinlicher ist es. Dass Geheimheit ein Schutz für Freiheit ist, ist von unserer Rechtsordnung erkannt. Das verfassungsrechtlich garantierte Wahlgeheimnis beruht beispielsweise auf der Annahme, dass nur eine geheime Wahl wirklich frei sein kann.

Selbstverständlich gilt die Meinungsfreiheit nicht unbeschränkt, sondern findet ihre Grenzen in den allgemeinen Gesetzen, die ihrerseits im Lichte der Meinungsfreiheit auszulegen sind. Der Schutz der Anonymität ist aber binär: Sobald er einmal aufgehoben ist, besteht er – für dieses Nutzerkonto – nie wieder. Das gilt insbesondere für solche Fälle, in denen beispielsweise der politische Gegner die Identität einer anonym agierenden Person erfährt. Zwar erfährt die gegnerische Partei nur den Namen und die Adresse einer Person zur Durchsetzung von Rechten in einem konkreten Verfahren, als logische Konsequenz erfährt sie somit aber auch den

Namen und die Adresse der Person, die vielleicht über Jahre hinweg politische Äußerungen getätigt hat, die ihr zwar ein Dorn im Auge, von der Meinungsfreiheit aber gedeckt waren. Die sanktionierende Wirkung tritt in diesen Fällen nicht durch die mögliche Verurteilung zu einem Schmerzensgeld ein, sondern durch die dauerhafte Identifizierbarkeit der Person. Die tatsächlichen Auswirkungen dürften dabei vergleichbar sein mit Fällen der rechtswidrigen Veröffentlichung personenbezogener Daten im Internet (sog. „Doxxing"). Betroffene von Doxxing werden in ihrer Lebensqualität erheblich eingeschränkt. Nicht selten müssen sie und ihre Angehörigen physische Übergriffe durch Gewalttäter fürchten, werden gestalkt, mit Bedrohungen und Hass überzogen und ihre Arbeitgeber kontaktiert. In der Folge müssen sie oft umziehen und sich eine neue Identität aufbauen. Zwar ist das „gefährdende Verbreiten personenbezogener Daten" seinerseits strafbar (§ 126a StGB), der individuelle Tatnachweis aber schwer zu führen und das Abschreckungspotential der Vorschrift überschaubar.

Auf zwei Personengruppen möchten wir an dieser Stelle eingehen, die besonders von den vorgesehenen Änderungen betroffen wären:

**Whistleblower**

Das Eckpunktepapier selbst nennt die Restaurantkritik, also die Schädigung durch wahrheitswidrige Nutzerkommentare, als Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb als Beispiel. Schon hier stellt sich sehr ernsthaft die Frage, ob der Streit über die verbrannte Pizza tatsächlich dazu führen sollten, dass die nutzende Person hinter einem Konto identifiziert werden soll. Dies gilt insbesondere vor dem Hintergrund, dass das entsprechende Konto regelmäßig nicht nur für Unternehmensbewertungen benutzt wird, sondern oft auch auch mit Social Media-Konten verknüpft ist, die zur Teilhabe am politischen Diskurs dienen.

Die Gefahr erhöht sich aber noch deutlich, wenn man sich Fälle vor Augen führt, in denen Whistleblower aus einem Unternehmen heraus über schädliche und sogar rechtswidrige Handlungen des Unternehmens berichten. Regelmäßig streiten die Unternehmen diese Vorwürfe (zunächst) ab; die Sach- und Beweislage ist unklar. Ähnliches gilt für Portale, in denen Arbeitnehmer:innen anonym ihre Arbeitgeber:innen bewerten. Der Gesetzesentwurf birgt ernsthafte Gefahren, dass wirtschaftsstarke Unternehmen zukünftig mit dem Vorwurf der wahrheitswidrigen Kritik die Identität der Personen erfahren können, die über ihre Praktiken berichten. Hier stehen auf der einen Seite gut bezahlte und hervorragend ausgestattete Anwaltskanzleien, während sich Whistleblower:innen, die unter dem Schutz der Anonymität agieren, im gerichtlichen Verfahren zum Zwecke ihrer Identifizierung nicht einmal äußern können. Denn sie sind keine Partei des Verfahrens, es handelt sich um einen Anspruch des Unternehmens gegen die Plattform, die eigentlich betroffene Person ist nicht beteiligt.

**(Foto-)Journalist:innen mit Extremismus-Schwerpunkt**

Journalist:innen mit entsprechenden Schwerpunkten berichten regelmäßig von Demonstrationen extremistischer Gruppen. Dazu gehört beispielsweise auch die Dokumentation der Vernetzung rechtsextremer Gruppen aus ganz Deutschland (oder sogar Europa) anlässlich einzelner Veranstaltungen. Es handelt sich um wichtige Dokumentations- und Aufklärungsarbeit, die notwendig ist, um in der Öffentlichkeit die Tätigkeiten extremistischer, demokratiegefährdender Gruppen im Blick zu behalten. Die Foto-Journalist:innen agieren insbesondere in den sozialen Netzwerken oft unter dem Schutz der Anonymität, weil sie sonst der persönlichen Verfolgung durch die Angehörigen extremistischer Gruppierungen ausgesetzt wären. Diese Dokumentationsarbeit geht regelmäßig mit Fotos der Personen und ihren Namen einher. Im Einzelnen kann es dabei rechtlich äußerst umstritten sein, ab wann eine Person als Person des öffentlichen Lebens einzustufen ist, so dass ihr Name und ihr Foto veröffentlicht werden darf, und welche Art von Fotos von öffentlichen Veranstaltungen, insbesondere Demonstrationen, zulässig sind. Eindeutige, allgemeine Antworten sind nahezu unmöglich. Ein einziges Foto einer Bildreportage, welches zu sehr auf eine Einzelperson konzentriert ist (und damit eine Verletzung des Rechts am eigenen Bild darstellt), könnte somit einen Auskunftsanspruch bezüglich des Namens und der Adresse des:r Journalist:in hinter dem Nutzerkonto auslösen. Die ständige Gefahr der Identifizierung würde die Arbeit der Journalist:innen aufgrund ihrer persönlichen Gefährdung faktisch unmöglich machen.

D64 e.V.
Gipsstraße 3
10119 Berlin

030 577 142 56
info@d-64.org
www.d-64.org

GLS Bank
DE13 4306 0967 1134 4765 00
GENODEM1GLS

Vereinsregister
AG Charlottenburg VR 31163 B
Lobbyregister: R000251

### *Chilling Effects*

Wichtig ist hierbei, dass es für den einschüchternden Effekt auf Meinungs- und Pressefreiheit („*chilling effects*“) nicht auf die tatsächliche Rechtmäßigkeit oder Rechtswidrigkeit des Verhaltens ankommt. Vielmehr reicht die (vermeintliche) Gefahr der möglichen Identifizierung, um eine abschreckende Wirkung für die Grundrechtsausübung zu entfalten. Rechtsunsicherheiten gehen also erheblich zu Lasten der Grundrechtsträger:innen. Auch hier ist die Wirkung stärker, je eher eine betroffene Person einer vulnerablen Gruppe angehört und damit von einer Aufhebung der Anonymität besonders betroffen wäre. Während die Notwendigkeit der Verfolgung von Straftaten im Internet und auch damit verbundene Identifizierungsmaßnahmen wohl unmittelbar den meisten im Internet Aktiven einleuchten, dürfte eine Identifizierung nach einer Restaurantkritik (deren Richtigkeit selbst nach einer Beweisaufnahme nur schwer festzustellen sein dürfte) überraschen. Diese Überraschung führt zu einer erheblichen Unsicherheit bei den Nutzer:innen von sozialen Plattformen, bei welchen Äußerungen mit der Aufhebung der Anonymität zu rechnen ist. Im Endeffekt wird insbesondere der kritische, für eine Demokratie charakteristische, Austausch von Meinungen nur noch zurückhaltend geführt werden. Nicht weil dieser klassischerweise von den Verletzungen absoluter Rechte geprägt ist, sondern weil bei einem Großteil der Internetnutzer:innen schlicht keine Kenntnis besteht, was absolute Rechte sind und in welchen Fällen die Meinungsfreiheit einen Eingriff in solche Rechte auch rechtfertigen kann. Fragen, über die auch Jurist:innen mit Jahrzehnten der Berufserfahrung in Randbereichen trefflich streiten können. Ein Jura-Studium darf jedoch nicht zur Voraussetzung für die Meinungsfreiheit werden. Vielmehr ist es essentiell, dass Bürger:innen erkennen können, welche Rechtsfolgen sich aus ihrem Verhalten ergeben. Die Anknüpfung an Straftatbestände und damit den strafrechtlichen Bestimmtheitsgrundsatz stellt dies sicher.

### *Maßnahmen bei Rechtsverletzungen durch anonyme Nutzer:innen*

An dieser Stelle sei darauf hingewiesen, dass Betroffene von rechtswidrigen, aber nicht strafbaren Äußerungen keinesfalls schutzlos gestellt sind. Vielmehr gehört es zu den allgemeinen Grundsätzen der europäischen Plattformregulierung, dass Plattformen zur Löschung rechtswidriger Inhalte verpflichtet sind, sobald sie von Ihnen Kenntnis erhalten. Dies ist auch für den Bereich der Verletzung absoluter Rechte etabliert, Bewertungsportale sind beispielsweise regelmäßig mit entsprechenden Löschanfragen konfrontiert. Für den Bereich der Persönlichkeitsrechtsverletzungen wurde sogar - wenn auch noch nicht rechtskräftig - eine Überwachungspflicht der Plattformen bezüglich der erneuten Veröffentlichung kerngleicher Rechtsverletzungen bejaht, die solche Inhalte unmittelbar zu löschen, beziehungsweise ihre Veröffentlichung zu verhindern haben.

Darüber hinaus würde auch das Instrument der richterlich angeordneten Accountsperren (dazu unten) ein rechtsstaatliches Verfahren gegen anonyme Nutzer:innen ermöglichen. Durch den Verlust des entsprechenden Nutzerkontos und der damit verbundenen Follower:innen träten neben die beabsichtigte Gefahrenabwehr — die Verhinderung gleichgelagerter Posts durch dasselbe Konto — auch faktisch sanktionierende Effekte, die individual- und generalpräventiv wirken dürften.

Sobald — aber auch erst wenn — die Äußerungen die Grenze zur Strafbarkeit übertreten, ist es Aufgabe des Staates, die Rechtsordnung durchzusetzen und staatlichen Strafanspruch geltend zu machen. Eine Identifizierung der Nutzer:innen kann in diesen Fällen beispielsweise mit Hilfe der von D64 konzipierten Login-Falle erfolgen (siehe unten).

## Zur Ausweitung auf Messenger- und Internetzugangsdiensten

Die geplante Ausweitung der Auskunftsansprüche auf Messenger- und Internetzugangsdienste hat zumindest für erhebliche Irritationen gesorgt. So haben sich beispielsweise die privatsphäreorientierten Messengerdienste Threema und Signal ablehnend gezeigt und betont, dass sie keine entsprechenden Daten speichern und diese damit auch nicht herausgegeben werden können. Es muss gesetzgeberisch eindeutig klargestellt werden, dass eine etwaige Ausweitung der Auskunftspflichten keine neuen Speicherpflichten mit sich bringt. Ver-

fügt ein Dienst also nicht über die entsprechenden Daten, weil sie nicht erfasst werden, besteht dementsprechend auch keine Auskunftsverpflichtung.

### Zur effektiveren Ausgestaltung des Auskunftsverfahren

#### *Beweissicherungsanordnung*

Zukünftig sollen sämtliche Dienste nach Einleitung des Auskunftsverfahrens verpflichtet werden, die Bestands- und Nutzungsdaten der:s Verfassers:in der mutmaßlich rechtsverletzenden Äußerung, sowie die Äußerung selbst, bis zum Abschluss des Auskunftsverfahrens gezielt zu sichern. Damit soll eine Löschung der Daten verhindert werden, die vermeintlich dazu führen würde, dass ein entsprechender Auskunftsanspruch ins Leere läuft.

Diese Regelung begegnet erheblichen Bedenken unsererseits. Zum einen sind die Anforderungen für die Anordnung der Beweissicherung klar. Reicht tatsächlich die bloße Einleitung des Auskunftsverfahrens, so handelt es sich um eine „Vorratsdatenspeicherung light". Diese beträfe zwar nicht die gesamte Bevölkerung oder alle Nutzer:innen einer Plattform, stellt allerdings trotzdem eine Speicherung „auf Vorrat" ohne die Prüfung des Anfangsverdachts einer Straftat beziehungsweise der Plausibilität der Rechtsverletzung dar. Es bedarf also nach derzeitiger Ausgestaltung gerade nicht der Bejahung des Verdachts einer (Persönlichkeits-)Rechtsverletzung, damit eine Speicherung angeordnet werden kann, sondern nur der Einleitung eines Verfahrens, welches in der Sache auch völlig unbegründet sein könnte.

Würde ein Anfangsverdacht als Voraussetzung für den Erlass der Beweissicherungsanordnung eingeführt, würde es sich der Sache nach um das anlassbezogene „Einfrieren" von Daten, also eine „Quick Freeze"-Anordnung handeln. Diese Regelung wirkt jedoch inkonsistent. Während im offiziellen Quick Freeze-Entwurf des BMJ aus dem vergangenen Jahr die Speicherung von Daten nur bei Straftaten „von erheblicher Bedeutung" möglich ist, genügt hier jede behauptete Verletzung absoluter Rechte.

Darüber hinaus ist der mit der präventiven Speicherung der Daten verbundene Eingriff auch nicht erforderlich, weil mildere, gleich geeignete Mittel zur Verfügung stehen. In aller Regel werden nutzerkontenbasierte (Persönlichkeits-)Rechtsverletzungen nicht von Wegwerfkonten begangen, sondern leben von der Reichweite und Öffentlichkeit, die mit einem über längere Zeit betriebenem Konto einhergehen. Das führt dazu, dass immer wieder neue Zugriffe auf das Nutzerkonto durch die hinter dem Konto stehende Person erfolgen („Logins"). Es genügt daher, wenn ein entsprechendes Auskunftsrecht nach Abschluss des gerichtlichen Verfahrens für den nächsten Login angeordnet wird, so dass dann der:die Anschlussinhaber:in hinter der IP-Adresse ermittelt werden könnte. Hierbei handelt es sich der Sache nach um die Anwendung der für das strafrechtliche Verfahren entwickelten Login-Falle, die besonders grundrechtsschonend ist (siehe unten).

#### *Video-Verhandlung und Amtsermittlungsgrundsatz*

Wir begrüßen die angedachte Möglichkeit der Videoverhandlung. Dies dürfte den mit den Verfahren verbundenen Aufwand regelmäßig senken, den Zugang zum Recht somit erleichtern und die Verfahren selbst beschleunigen. Auch die Anwendung des Amtsermittlungsgrundsatzes für diese Verfahren ist sinnvoll, da so das Verfahren insbesondere für nicht anwaltlich vertretene Betroffene deutlich erleichtert wird.

## 3. Accountsperren

Wir begrüßen die Einführung richterlich angeordneter Accountsperren. Im Vergleich zu den Auskunftsverfahren, die in der nicht mehr rückgängig zu machenden Identifizierung der natürlichen Personen hinter einem Konto münden und mit den oben beschriebenen dauerhaften erheblichen negativen Folgen verbunden sind, dürfte es sich bei den Accountsperren regelmäßig um mildere Maßnahmen handeln. Diese sind somit auch unter dem Aspekt der Verhältnismäßigkeit geboten.

Es handelt sich bei den richterlich angeordneten Accountsperren um ein Verfahren mit rechtsstaatlichen Garantien, welches die Bedeutung der Anonymität im Internet achtet und sinnbildlich digitalen Baseballträger:innen ihr Tatwerkzeug entzieht. Accountsperren berücksichtigen insbesondere die spezifische Logik von Hass und Hetze im Internet, in der sich die Intensität der Beeinträchtigung nicht nur aus der Äußerung als solcher ergibt, sondern zu einem erheblichen Anteil auch aus der Öffentlichkeit, die ein Nutzerkonto aufgrund seiner Follower:innen hat. Die Sperre des Kontos schränkt damit den Handlungsspielraum der hinter dem Konto stehenden Person erheblich ein, insbesondere was die Wiederholung von Angriffen mit gleicher Intensität angeht. Es geht dabei nicht darum, den hinter den Konten stehenden Personen die Möglichkeit zur Meinungsäußerung zu nehmen, sondern um die Einschränkung der Nutzung eines bestimmten Mediums für Straftaten.

Nichtsdestotrotz handelt es sich um eingriffsintensive Maßnahmen. Positiv hervorzuheben ist daher die starke Betonung des Verhältnismäßigkeitsgrundsatzes, die Betonung der zeitlichen Befristung der Sperrung und die Möglichkeit der Gewähr (faktischen) rechtlichen Gehörs in anonymer Art und Weise über die Plattform. Ein - soweit wir es überblicken - innovatives Novum im deutschen Prozessrecht.

Während der Anwendungsbereich des vereinfachten Auskunftsrechts jedoch deutlich zu weit gezogen ist, verkennt der Fokus auf Individualrechte bei Accountsperren die systemische Bedeutung von Hass im Netz. Wie auch bei den Auskunftsverfahren sollte ein Anspruch auf Accountsperren nur geltend gemacht werden können, wenn das Vorliegen einer Straftat angenommen wird. Angelehnt an den von der Gesellschaft für Freiheitsrechte (GFF) veröffentlichten Entwurf für ein Digitales Gewaltschutzgesetz (https://freiheitsrechte.org/uploads/documents/Demokratie/Marie-Munk-Initiative/2023-05-22-DigGewSchG_GFF.pdf) ist die Durchsetzung von Accountsperren auch in anderen Fällen, wie Volksverhetzung, der Verbreitung von Abbildungen von Kindesmissbrauch und der öffentlichen Androhung von Straftaten, zu ermöglichen. Da eine individuelle Betroffenheit hier oft nicht ohne Weiteres festzustellen ist, könnten klageberechtigte Verbände die Accountsperren gerichtlich einfordern (Verbandsklagerecht). Die Bedrohung des öffentlichen Diskurses durch die Begehung solcher Straftaten erfordert - neben der staatlichen Verfolgung - die Möglichkeit kollektiver, gesellschaftlich organisierter Antworten.

## 4. Zustellungsbevollmächtigte in Deutschland

Die Beibehaltung der Pflicht der großen sozialen Plattformen zur Benennung eines:r inländischen Zustellungsbevollmächtigten aus § 5 NetzDG, verbunden mit der Ausweitung auch auf außergerichtliche Schreiben, begrüßen wir. Sie erleichtert die rechtssichere Kommunikation mit den Plattformen und damit die effektive Rechtsdurchsetzung durch die Betroffenen. Neben der Rechtsverletzung durch Inhalte auf den Plattformen sollten aber auch rechtswidrige Sperren oder Löschungen von Inhalten und Nutzerkonten auf diesem Wege geltend gemacht werden.

## 5. Was im Eckpunktepapier fehlt

Darüber hinaus möchten wir die Gelegenheit nutzen, Ergänzungen anzuregen, die Betroffene von Hass und Hetze im Internet unterstützen, schützen und die Verteidigung ihrer Rechte verbessern würden.

### Anonymität/Impressumspflicht

Während das Eckpunktepapier Anonymität im Internet vor allen Dingen als Gefahr für Betroffene von Hass im Netz versteht, handelt es sich vielmehr für viele Angehörige vulnerabler Gruppen um die notwendige Voraussetzung, um sich frei äußern zu können. Die Bundesregierung sollte sich deshalb dafür einsetzen, ein Recht auf Anonymität überall dort zu verankern, wo es nicht zwingend auf die Identität einer Person ankommt. Das betrifft insbesondere die Nutzung sozialer Medien. Privaten Identifizierungspflichten ist entgegenzuwirken. Sehr erfreulich ist insofern die – wenn auch noch auf der alten Rechtslage basierende – Entscheidung des Bundesgerichtshof aus dem Januar 2022 (siehe hierzu https://d-64.org/d64-bgh-klarnamenpflicht/).

Aus diesem Grunde ist auch die in § 5 TMG verankerte Impressumspflicht für politisch aktive Personen, die beispielsweise einen eigenen Blog betreiben, ein erhebliches Problem. Mangels „ladungsfähiger" Büroanschrift sind diese, selbst wenn sie unter ihrem bürgerlichen Namen auftreten, regelmäßig verpflichtet, ihre private Anschrift zu veröffentlichen. Die Impressumspflicht ist deshalb zu reformieren. Denkbar wäre beispielsweise eine gesetzliche Regelung, die nur bei bestimmten Rechtsformen, erst ab einer gewissen Größe greift oder die auf die tatsächliche Erreichbarkeit abstellt. Letztere könnte auch über Kontaktpersonen wie Rechtsanwält:innen oder „Briefkasten-as-a-Service"-Dienstleistungen sichergestellt werden, die unabhängig von der persönlichen Anschrift sind.

Darüber hinaus muss der Schutz von Betroffenen und Zeug:innen im Straf- und Zivilverfahren verbessert werden. Es gibt keinen sachlichen Grund, warum die gegnerische Seite beziehungsweise der:die Angeklagte regelmäßig die persönlichen Daten eines:r Betroffenen erfährt, insbesondere die Wohnanschrift. Es gibt über die gerichtliche Zustellung der entsprechenden Dokumente im gerichtlichen Verfahren kein objektives Interesse an dieser Information. Schon die Gefahr der Bekanntgabe der Anschrift an eben die Person, vor deren Hass, Stalking und Gewaltandrohungen man sich wehrt, führt dazu, dass Opfer davon absehen, Fälle zur Anzeige zu bringen oder sich zivilrechtlich zu wehren.

## Verbesserung des Beratungsangebots

Mit großem Bedauern mussten wir feststellen, dass die Verbesserung der Situation der Betroffenen durch einen Ausbau und eine stärkere Förderung von Beratungsangeboten im Eckpunktepapier nicht berücksichtigt wurde. Dies ist nicht zuletzt deshalb enttäuschend, weil der Koalitionsvertrag dies noch explizit als Maßnahme vorgesehen hat. So heißt es dort: „Mit einem Gesetz gegen digitale Gewalt werden wir rechtliche Hürden für Betroffene, wie Lücken bei Auskunftsrechten, abbauen und umfassende Beratungsangebote aufsetzen."

Neben einem Ausbau der Beratungsstellen sollte auch die einfache Erreichbarkeit und Auffindbarkeit der verschiedenen Angebote verbessert werden. Hierbei ist insbesondere an „digitale Streetworker" zu denken, die über Schnittstellen auf den Plattformen von Betroffenen unmittelbar kontaktiert und um Rat gebeten werden können. Die Beratungsangebote müssen jedoch von den Plattformen unabhängig bleiben, um Interessenskonflikte zu vermeiden und die notwendige Qualität zu sichern. Solche Hilfs- und Beratungsangebote können insbesondere nicht nur als Ansprechpartner:innen in Fällen von Hass im Netz fungieren, sondern auch ein niedrigschwelliges Angebot für Kinder und Jugendliche darstellen, die von Grooming, also der sexuell motivierten Annäherung durch einen Erwachsenen, betroffen sind. Konzeptionell ließe sich eine solche „Beratungsschnittstelle" ähnlich wie die „Justizschnittstelle" der Login-Falle (siehe unten) umsetzen. Zentral ist der Anspruch, dass Hilfe für Opfer so niedrigschwellig wie möglich sein muss. Es muss unmittelbar an den Orten auf sie zurückgegriffen werden können, wo es im digitalen Raum zu Übergriffen kommt.

## Strafverfolgung als staatliche Aufgabe

Wir sehen es als primäre Aufgabe des Staates an, Rechtsverletzungen im Internet wie in der analogen Welt zu verfolgen und zu sanktionieren. Dies ist nicht zuletzt auch eine Frage der Gerechtigkeit: Private Rechtsverfolgung muss man sich leisten können, es muss daher der Anspruch eines sozialen Staates sein, den Schutz der Rechte aller Bürger:innen durchzusetzen. Bemühungen der Bundesregierung, die Strafverfolgung im Netz faktisch zu verbessern, sind leider bisher kaum erkennbar. Dafür bedarf es insbesondere keiner neuen Strafgesetze oder Überwachungsmaßnahmen, sondern einer Verbesserung der Ermittlungsfähigkeiten der Strafverfolgungsbehörden im digitalen Raum. Hierzu gehört auch eine digitale Transformation der alltäglichen Arbeit, in dem Routineaufgaben und Prozesse standardisiert und als Ende-zu-Ende-Digitalisierung abgebildet werden.

Ein erster Ansatzpunkt ist dabei die Abschaffung des Schriftformerfordernisses für Strafanträge. Bis heute ist es so, dass Betroffene von Beleidigungen im Netz einen schriftlichen, also handschriftlich unterschriebenen, Strafantrag stellen müssen. Laut dem Koalitionsvertrag hat die Bundesregierung sich vorgenommen, „die

rechtlichen Rahmenbedingungen für elektronische Verfahren zur Anzeigenerstattung [zu schaffen]". In der Hoffnung, dass es hierbei nicht nur um die Anzeigenerstattung, sondern auch um die Antragserstattung geht, würden wir Maßnahmen in diesem Bereich sehr begrüßen.

Damit Polizeiarbeit im 21. Jahrhundert funktionieren kann, braucht es standardisierte Schnittstellen. Hierauf basiert auch unser Konzept der Login-Falle zur Identifikation von Tatverdächtigen im Internet ohne Massenüberwachung (siehe https://d-64.org/login-falle). Es braucht im Bereich der nutzerkontenbasierten Kriminalität keine präventive Speicherung von Daten, sondern es genügt, dass nach der Bejahung des Anfangsverdachts einer Straftat auf richterlichen Beschluss die IP-Adresse des nächsten Logins zu dem:r dahinterstehenden Anschlussinhaber:in aufgelöst wird. Der Aufwand für solche Maßnahmen ließe sich durch Standardisierung substantiell reduzieren und sogar in den Bereichen, in denen keine Wertentscheidungen oder Abwägungen erfolgen, automatisieren.

Neben der Möglichkeit der verbesserten Identifikation könnten auch im Sinne einer „Justizschnittstelle" Anzeigemöglichkeiten aus den Apps heraus für Betroffene geschaffen werden (siehe https://d-64.org/justizschnittstelle). Schon jetzt bieten viele Messenger – auch solche von Ende-zu-Ende-verschlüsselter Kommunikation – Meldemechanismen an, mit denen ein spezifischer Inhalt ausgeleitet werden kann. Es gibt keinen vernünftigen Grund, warum man nicht über die gleiche Funktion auch eine Anzeige bei staatlichen Behörden erstatten können sollte.

Damit das möglich ist, braucht es einen einheitlichen offenen Standard für die Kommunikation zwischen den jeweiligen Apps und den Strafverfolgungsbehörden. So können alle relevanten Beweise gesichert werden, gegebenenfalls erforderliche persönliche Daten der anzeigeerstattenden Person müssen nicht immer wieder aufs Neue angelegt werden und es wird keine Zeit durch unnötige Formalitäten verwendet. Die Zuständigkeit der Strafverfolgungsbehörde kann sich hierbei nach dem Bundesland der anzeigeerstattenden Person richten, die die jeweilige Äußerung wahrgenommen hat. So wird der Föderalismus, der als Bollwerk gegen Machtmissbrauch und zentrale Datensammlungen dient, weiterhin ernst genommen. Ein möglichst offener Standardisierungsprozess mit allen relevanten Stakeholdern würde zudem zu einer breiten Akzeptanz der Schnittstelle führen, die dann auch international die Bekämpfung von Internetkriminalität erleichtern würde.

Zur Einrichtung solcher Schnittstellen für Beratung, Anzeige und Identifizierung der Personen bedürfte es keiner neuen Grundrechtseingriffe. Sämtliche Ermächtigungsgrundlagen bestehen bereits. Für den Fall, dass Plattformen und/oder Telekommunikationsunternehmen eine Übermittlung auf diesem Wege verweigern, sind hier gesetzliche Maßnahmen zur Standardisierung des Kommunikationsprozesses zu ergreifen.

D64 e.V.
Gipsstraße 3
10119 Berlin

030 577 142 56
info@d-64.org
www.d-64.org

GLS Bank
DE13 4306 0967 1134 4765 00
GENODEM1GLS

Vereinsregister
AG Charlottenburg VR 31163 B
Lobbyregister: R000251