Stellungnahme zum Eckpunktepapier zum Gesetz gegen digitale Gewalt

Eckpunktepapier des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt

Mai 2023

selbstregulierung informationswirtschaft e.V.

Herausgeber

Selbstregulierung Informationswirtschaft e.V.
Großbeerenstraße 88
10963 Berlin
https://sriw.de

+49 (0)30 30878099-0
info@sriw.de

Amtsgericht Berlin Charlottenburg
Registernummer: VR 30983 B
USt-Nummer: DE301407624
Deutsche Bank AG
IBAN: DE33 1007 0000 0550 0590 00

Vorstandsvorsitz
Dr. Claus-Dieter Ulmer

Geschäftsführer
Frank Ingenrieth

Inhalt

1 Executive Summary

- Es erscheint fraglich, inwieweit neben den bereits umfassenden anwendbaren regulatorischen Rahmenbedingungen überhaupt eine gesetzliche Regelungslücke vorliegt.

- Dem Gesetzesentwurf ist bisher kein klares Schutzgut zu entnehmen.
- Das naheliegendste Schutzgut erscheint die Integrität der Verbraucher:innen.

- Eine mögliche gesetzliche Maßnahme sollte eine umfassendere Problem- und Bedarfsanalyse voranstellen, und die vorgesehenen Maßnahmen deutlicher auf das Schutzgut einzahlen.
- Derzeit vorgesehene Maßnahmen erscheinen wenig bis gar nicht geeignet, eine Verbesserung für das Schutzgut herbeizuführen.

- Das Gesetz scheint einen in der Praxis komplexen Sachverhalt, etwa aufgrund der internationalen Dimension, der Vielzahl involvierter Stakeholder in Form eines Mehrpersonenverhältnisses, aber auch der hohen Entwicklungsdynamiken, unnötig zu simplifizieren.
- Die Simplifizierung löst im Ergebnis Bedenken dahingehend aus, ob die erforderlichen Aufwände zur Umsetzung des Gesetzes nicht unnötig Ressourcen binden, die ansonsten in die Umsetzung bereits bestehender Pflichten genutzt würden.
- Die Simplifizierung betrifft auch technisch-organisatorische sowie rechtliche Grundsätze. Die vereinfachten Maßnahmen erscheinen in der konkreten Form schlicht ungeeignet einen praktischen Mehrwert zu liefern.

- Neben bzw. in Teilen anstelle der gesetzlichen Regelung, sollten Alternativen, etwa koregulatorische Ansätze, geprüft und möglicherweise bevorzugt werden.
- Auch Alternativen sollten jedoch nur verfolgt werden, soweit die Problem- und Bedarfsanalyse eine Notwendigkeit ergeben.
- Koregulatorische Ansätze sollten die relevanten Stakeholder sowie sachdienliche Experten beteiligen. Hierdurch kann materielle Effektivität der Vorgaben sichergestellt und lediglich auf dem Papier sinnvoll wirkende, in der Praxis aber ggf. sogar kontraproduktive Maßnahmen vermieden werden.
- Koregulatorische Ansätze sollten bestehende Good Pracises weiter effektuieren und stärken, und neue Parallelstrukturen vermeiden.
- Der Gesetzgeber sollte analysieren, ob es bestehende Rechtsunsicherheiten der beteiligten Stakeholder gibt, effektivere Maßnahmen in Anwendung zu bringen, und ggf. Klarstellungen veranlassen.

2 Über den SRIW

Der SRIW e.V. (Selbstregulierung Informationswirtschaft) wurde 2011 als unabhängige, private Aufsichtsstelle branchenspezifischer Verhaltensregeln gegründet. Oberste Prämisse seit Gründung war und ist es, die notwendigen, unabhängigen Strukturen bereitzustellen, um branchenspezifische Verhaltensregeln zu etablieren und zu verwalten sowie deren glaubwürdige und wirksame Überwachung, inklusive eines Beschwerdemanagements, zu gewährleisten. Seither ist der SRIW erfolgreich an der Entwicklung von Verhaltensregeln, unter anderem im Bereich Datenschutz, beteiligt und engagiert sich auch in anderen Formen rund um das Thema *modern-regulation*[1]. Nicht zuletzt durch die Datenschutzgrundverordnung verstärkte der SRIW seine Aktivitäten insbesondere auf europäischer Ebene durch die in Brüssel sitzende Tochtergesellschaft SCOPE Europe spr[2] („SCOPE Europe“).

Der SRIW ist folglich täglich mit den besonderen Fragestellungen im Bereich der Verhaltensregeln und deren glaubwürdiger und unabhängiger Überwachung konfrontiert. Der SRIW konnte insbesondere wertvolle praktische Erfahrungen sammeln, inwieweit unterschiedliche Lösungen und Prozesse überhaupt einer wirtschaftlichen Umsetzung zugänglich sind und inwieweit umsetzbare Lösungen und Prozesse seitens der überwachten Stellen akzeptiert werden. Auf Basis dieser langjährigen Erfahrung wurde die folgende Stellungnahme verfasst.

3 Intention/Hintergrund der Stellungnahme

Mit dem vom Bundesministerium für Justiz (BMJ) geplanten Gesetz gegen digitale Gewalt[3] sollen Betroffene in die Lage versetzt werden gegen „Gewalt im digitalen Raum“ vorgehen zu können. Im dem zum Gesetz vorliegenden Eckpunktepapier wird „Gewalt im digitalen Raum“ nicht klar definiert, aus dem Kontext lässt sich ableiten, dass strafrechtlich relevante, aber auch andere im Internet begangene Rechtsverletzungen gemeint sind. Das Gesetz schlägt Maßnahmen vor, die den Geschädigten die Durchsetzung ihrer Rechte erleichtern und die Vorbeugung vor weiteren Rechtsverletzungen verbessern sollen. Auf eine allgemeine Kritik im Hinblick auf grundlegende verfassungsrechtliche Fragestellungen im Rahmen des Gesetzesvorhabens wird vonseiten des SRIW aufgrund zu erwartender umfänglicher Stellungnahmen durch andere Verbände, Expert:innen und Interessenvertreter:innen diesbezüglich bewusst verzichtet. Stattdessen wird in dieser Stellungnahme im Sinne des durch den SRIW angestrebten Verbraucher:innenschutzes zur Effektivität der Überlegungen des Gesetzgebers Stellung bezogen. Zu diesem Zweck wird in der folgenden Stellungnahme zunächst das mit dem

[1] Eine Übersicht aktueller Projekte und Tätigkeiten des SRIW ist zu finden unter: https://sriw.de/projekte-kodizes.html
[2] Mehr Informationen zu SCOPE Europe spr sind zu finden unter: https://scope-europe.eu/en/home/
[3] Zum Eckpunktepapier für ein Gesetz gegen digitale Gewalt: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Digitale_Gewalt.html

Gesetz adressierte Schutzgut und das verfolgte Schutzziel hergeleitet sowie die Ursachen des mit dem Gesetz zu lösen bestrebte Problem analysiert. Die Ergebnisse beider Abschnitte ermöglichen im Anschluss eine Analyse der Notwendigkeit und Geeignetheit des Gesetzes und der darin vorgesehenen Maßnahmen in Hinblick auf die Erreichung des Schutzziels. Im Kontext einer effektiven Strategie zur Verhinderung und Reduktion von Rechtsverletzungen im digitalen Raum werden abschließend ergänzende, außergesetzliche Lösungsmöglichkeiten, beispielsweise Ko-Regulierung, abgeleitet und deren mögliche Ausgestaltung dargestellt. Mit dieser Stellungnahme knüpft der SRIW an seine Stellungnahme zum NetzDG[4] aus dem Jahr 2017[5] an.

4 Stellungnahme

4.1 Schutzgut und Schutzziel

Eine Effektivitätsanalyse und -evaluierung der durch das Gesetz gegen digitale Gewalt vorgesehenen Maßnahmen ist in Hinblick auf das mit dem Gesetz adressierte Schutzgut durchzuführen. In dem entsprechenden Eckpunktepapier wird das Schutzgut nicht eindeutig benannt. Da das Gesetz jedoch den Schutz von Betroffenen von Rechtsverletzungen im digitalen Raum anstrebt, wird wohl konsequenterweise die Integrität von Verbraucher:innen in den Blick genommen. Diese wird mithin als Schutzgut indiziert. Im Kontext des digitalen Raums wird das mit dem Gesetz verfolgte Ziel für diese Stellungnahme dahingehend verstanden, dass Integrität von Verbraucher:innen vor Verletzungen im Internet effektiv geschützt werden soll.

4.2 Problemursachenanalyse

Um diesen Integritätsschutz zu erreichen und sicherzustellen bedarf es zunächst der Ergründung der Ursache der thematisierten Rechtsverletzungen. Diese haben ihren Ursprung bei dem/der Rechtsverletzenden, dessen/deren Verletzungshandlung unterschiedliche Umstände zugrunde liegen können. Im Wesentlichen können die drei folgenden Szenarien beschrieben werden:

1) Die rechtsverletzende Person ist aufgrund der durch die genutzten Plattformen überwiegend ermöglichten Anonymität wenig bis gar keiner unmittelbaren sozialen Kontrolle ausgesetzt. Dies kann einen Enthemmungseffekt nach sich ziehen. Dieser Enthemmungseffekt kann darin resultieren, unter Anderem Ärger und Hass unreflektiert zu äußern. Sofern mit entsprechenden Äußerungen die Rechte Dritter verletzt werden, kann eine rechtswidrige Verletzungshandlung vorliegen. In diesem Szenario kann weiter zwischen zwei Personengruppen

[4] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz)
[5] https://sriw.de/detail/stellungnahme-des-selbstregulierung-informationswirtschaft-zum-gesetz-zur-verbesserung-der-rechtsdur

differenziert werden. Einerseits gibt es rechtsverletzende Personen, bei denen der Enthemmungseffekt erst vor kurzem eingesetzt hat. Diese sind abzugrenzen von solchen Personen, die bereits seit längerem unmittelbarer sozialer Kontrolle entzogen sind oder sich durch Gleichgesinnte im Internet in ihren Handlungen sogar bestärkt sehen. Bei dieser Personengruppe haben sich rechtsverletzende Verhaltensweisen vermutlich derart manifestiert, dass eine ergebnisoffene, kritische Reflektion ohne weiteres nicht mehr erwartet werden kann.

2) Die rechtsverletzende Person wird für eine Verletzungshandlung bezahlt. Dies kann auf zwei Wegen geschehen: Entweder wird die Person, beispielsweise im Rahmen einer (professionellen) Hetzkampagne, dafür bezahlt, die Verletzungshandlung selbst manuell vorzunehmen. Ziel einer solchen Kampagne ist es in der Regel die Bevölkerung gegen eine bestimmte Person oder eine Personengruppe aufzuwiegeln, ggf. durch die Lancierung unrichtiger Informationen. Oder die Person wird damit beauftragt Bots zu programmieren, die wiederum die Verletzungshandlung begehen. In dieser Variante ermöglicht die Person erst das besondere Ausmaß der Verletzungshandlung. Eine derartige Automatisierung der rechtsverletzenden Handlung bietet sich besonders im Kontext genannter professionalisierter Kampagnen an, ist aber auch – auf Grund der teilweise geringen erforderlichen technischen Kenntnisse – Einzelpersonen oder kleineren nicht professionalisierten Personengruppierungen möglich.

In dem letztgenannten Szenario sind die Möglichkeiten zur Verhinderung, jedenfalls aber einer signifikanten Reduktion von Rechtsverletzungen begrenzt. Dies ist dem Umstand geschuldet, dass die Motivation der betreffenden rechtsverletzenden Personen für das Begehen bzw. Ermöglichen der Verletzungshandlung in diesen Fällen überwiegend extrinsisch ist. Zur Erreichung eines effektiven Schutzes der Integrität von Verbraucher:innen müssten in diesem Fall diejenigen in den Fokus genommen werden, die die finanziellen oder organisatorischen Mittel zur Durchführung und Koordination der Hetzkampagnen bereitstellen. Da es sich um Rechtsverletzungen im Internet handelt, erfolgt dies nicht zwingend aus Deutschland heraus. Dies erschwert insbesondere das Ausfindigmachen der betreffenden Einzelpersonen oder Gruppierungen.

Beim ersten Szenario, in dem durch den/die einzelne/n, durch Anonymität vermeintlich geschützte/n Nutzer:in gezielt Hass verbreitet wird, könnte zur Erreichung des Schutzziels hingegen auf niederschwellige, unmittelbare Mechanismen zurückgegriffen werden. Derartige Mechanismen ermöglichen es, den Rechtsgutverletzenden die Unangemessenheit ihres Handelns unmittelbar aufzuzeigen, und somit eine direkte Reflektion des Handelns anzustreben. Hierdurch könnten Strukturen von Echoblasen pro-aktiv durchbrochen werden. Auch Personen dieser Gruppe befinden sich sowohl im In- als auch im Ausland, sodass die transnationale Anwendbarkeit etwaiger Mechanismen zur Vorbeugung von weiteren Rechtsverletzungen Berücksichtigung zu finden hat.

4.3 Zum Gesetz gegen digitale Gewalt

Das Gesetz gegen digitale Gewalt wird im Folgenden sowohl in Hinblick auf seine Notwendigkeit als auch seine Geeignetheit zur Erreichung des Schutzziels evaluiert. Abschließend wird auf die praktische Umsetzung des Gesetzes Bezug genommen.

4.3.1 Notwendigkeit des Gesetzes zur Erreichung des Schutzziels

Bevor auf die Geeignetheit des geplanten Gesetzes zur Erreichung des unter Abschnitt 4.1 hergeleiteten Schutzziels einzugehen ist, ist zunächst die grundsätzliche Notwendigkeit des Gesetzes zu hinterfragen. Für das Schutzziel/das Schutzgut existieren bereits eine Vielzahl rechtlicher Regelungen: Auf gesetzlicher Ebene sind hier insbesondere das NetzDG sowie einschlägige Normen des Strafrechts (z.B. § 185 StGB[6]) zu nennen. Darüber hinaus adressieren auch Verhaltenskodizes, wie bspw. der Strengthened Code of Practice on Desinformation 2022[7], das gleiche Schutzgut. Vor diesem Hintergrund verbleibt unklar, welche konkrete bisher bestehende, relevante Regelungslücke das Gesetz zu schließen beabsichtigt.

4.3.2 Geeignetheit des Gesetzes zur Erreichung des Schutzziels

4.3.2.1 Mehrpersonenverhältnisse

An der Verfolgung von Rechtsverletzungen im digitalen Raum sind eine Vielzahl von Akteuren beteiligt: Der/die Betroffene, der/die Rechtsverletzende, der Diensteanbieter, der Internet Service Provider sowie ggf. Gerichte, Staatsanwaltschaft und die Polizei. Im internationalen Kontext sind zudem die weiteren Beteiligten im Rahmen der Rechtshilfeersuchen zu berücksichtigen.

Diese Parteien haben grundsätzlich unterschiedliche Funktionen und entsprechend verschieden weitreichende Befugnisse. Sie müssen jedoch zusammenarbeiten, um die Integrität von Verbraucher:innen vor Rechtsverletzungen im digitalen Raum wirksam schützen zu können. Hierfür bedarf es Prozesse, die auf die Bedürfnisse und Möglichkeiten der unterschiedlichen Akteure eingehen und flexibel an neue Gegebenheiten, die sich im digitalen Bereich ergeben können, anpassbar sind. Ein Gesetz, das schon aufgrund seiner Natur eine Vielzahl von Szenarien langfristig erfassen soll, kann diesem Umstand bei einem Mehr-Personen-Konstrukt nur schwerlich gerecht werden. Hierzu müsste das Gesetz einen sehr hohen Detailgrad aufweisen, dessen Gültigkeit stark befristet ist. Alternativ müsste das Gesetz so abstrakt bleiben, dass eine unmittelbare Auswirkung nicht zu erwarten ist.

---

[6] Strafgesetzbuch
[7] Mehr Informationen zum Verhaltenskodex sowie der Kodex selbst sind zu finden unter: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

Eine derartige Ausgangslage ist ein starker Indikator um untergesetzliche Regelungsinstrumente unter Beteiligung der relevanten Stakeholder zu bevorzugen.

4.3.2.2 Territorialer Anwendungsbereich

Ein nationales Gesetz gegen digitale Gewalt wäre auf das deutsche Territorium begrenzt. Wie jedoch bereits in der Problemursachenanalyse in Abschnitt 4.2 dargestellt, können rechtsverletzende Handlungen nicht nur aus Deutschland heraus, sondern auch aus dem (Außer-)Europäischen Ausland begangen werden. Mithin ist ein nationales Gesetz nur begrenzt dazu geeignet, Rechtsverletzungen im digitalen Raum entgegenzuwirken.

4.3.2.3 Geplante Erweiterung des Auskunftsverfahrens nach TTDSG[8]

Mit dem geplanten Gesetz gegen digitale Gewalt soll zunächst das in §§ 22 und 24 TTDSG vorgesehene Auskunftsverfahren, durch das unter anderem Betroffene von Betreibern von sozialen Netzwerken Auskunft über die Identität von Verfassern rechtsverletzender Äußerungen verlangen können, erweitert werden.

Bei dem Auskunftsverfahren nach §§ 22, 24 TTDSG handelt es sich auch nach den durch das Eckpunktepapier vorgeschlagenen Gesetzesänderungen um ein gerichtliches Verfahren. Dieser Umstand alleine rechtfertigt unter Berücksichtigung der derzeitig bestehenden Auslastung der Gerichte bereits die Annahme, dass ein solches Verfahren nicht hinreichend schnell abgeschlossen wäre. Hinreichend schnell ist unter Würdigung von Abschnitt 4.2 in dem Sinne zu verstehen, dass den/die Rechtsverletzende:n rechtliche Konsequenzen früh genug erreichen, um diese/n tatsächlich zur angemessenen Reflektion seiner/ihrer Verhaltensweisen zu anzuleiten: Je größer der zeitliche Abstand zwischen Verletzungshandlung und Konsequenz, desto weniger werden beide Ereignisse in Verbindung gebracht. Die Annahme, dass es zu zeitlichen Verzögerungen zulasten der Betroffenen kommen könnte wird auch durch einen Vergleich mit dem Ablauf des strafrechtlichen Verfahrens in diesem Kontext gestützt. Betroffene von strafrechtlich einschlägigen Rechtsverletzungen haben bereits jetzt die Möglichkeit ein strafrechtliches Verfahren anzustreben – diese bleibt von dem aktuellen Gesetzesvorhaben auch unbenommen. In diesem Verfahren scheitert die Strafverfolgung oftmals an dem zu späten Tätigwerden der zuständigen Gerichte/Behörden, sodass der/die Täter:in nicht ermittelt werden kann. Fraglich ist, warum ein Zivilgericht schneller agieren können sollte.

Negative Auswirkungen auf die zeitliche Komponente des Verfahrens hat auch der Umstand, dass das Eckpunktepapier Verletzungen jeglicher absoluter Rechte zu erfassen vorsieht. Hierzu zählt unter anderem das Recht am eingerichteten und ausgeübten Gewerbebetrieb, sodass auch negative

[8] Telekommunikation-Telemedien-Datenschutz-Gesetz

Restaurantkritiken ein Auskunftsverfahren rechtfertigen könnten. Zwar sollten Gewerbeeigentümer:innen durchaus vor Falschaussagen zu ihrem Betrieb geschützt werden, jedoch ist ein Gesetz gegen digitale Gewalt, das auf den Schutz der Integrität von Verbraucher:innen angelegt ist, nicht das einschlägige Instrument dafür. Auch die Verletzung von Urheberrechten könnte zum jetzigen Zeitpunkt ein Auskunftsverfahren rechtfertigen. Eine Erweiterung der Auskunftsverfahren etwa zur Durchsetzung von Ansprüchen bei der Verletzung geistigen Eigentums erscheint jedoch nicht zielführend, da dies bereits in § 101 UrhG festgeschrieben ist und dort ausreichend Rechnung trägt. Das Gesetzesvorhaben lässt mithin eine ausdifferenzierte Analyse des Schutzguts und darauf abgestimmter, notwendiger Regelungen vermissen. Bleibt der Anwendungsbereich des Gesetzes derart weit, so hätte dies zur Folge, dass die Anzahl der Verfahren über Gebühr steigt und Verfahren somit verlangsamt würden.

Davon abgesehen übersieht der Gesetzgeber in seinem Eckpunktepapier, dass eine Identifizierung des/der Rechtsverletzenden nur in den wenigsten Fällen eindeutig möglich sein dürfte. Zwar sieht das Eckpunktepapier eine Erweiterung des Auskunftsrechts auf die IP-Adresse vor, allerdings ist diese nicht dazu geeignet, ein/e Nutzer:in eindeutig zu identifizieren. Dies gilt beispielsweise in den Fällen, in denen sich mehrere Personen einen Haushalt teilen und Geräte von unterschiedlichen Nutzer:innen in Gebrauch genommen werden oder Nutzer:innen sich über das mobile Netz einwählen und somit eine Vielzahl von Nutzer:innen sich eine IP-Adresse teilen. Insofern wäre das gerichtliche Verfahren nicht geeignet, den/die Rechtsverletzende direkt zu adressieren. Sofern der/die Nutzer:in allerdings zumindest davon erfährt, dass ein Verfahren eingeleitet wurde, bspw. indem sein/ihr Haushalt kontaktiert wurde, kann dies unter Umständen dennoch einen positiven Effekt auf den/die Nutzer:in haben. Dass überhaupt eine rechtsrelevante Reaktion auf sein/ihr Verhalten erfolgt, kann den Gedanken vollkommener Anonymität als Schutz vor Konsequenzen ins Wanken bringen und den/die Nutzer:in in Zukunft von Verletzungshandlungen absehen lassen. Dies setzt jedoch voraus, dass es sich um Nutzer:innen handelt, die edukativen Maßnahmen noch zugänglich sind.

4.3.2.4 Geplante richterlich angeordnete Accountsperre

Als weitere Maßnahme zur Bekämpfung von Rechtsverletzungen im digitalen Raum sieht das geplante Gesetz einen Anspruch Betroffener auf eine richterlich angeordnete Sperre des Accounts des/der Rechtsverletzenden vor, sofern eine schwerwiegende Persönlichkeitsverletzung vorliegt und weitere, enge Voraussetzungen erfüllt sind. In der Konsequenz ordnet das Gericht dann gegenüber dem Diensteanbieter die zeitlich befristete Sperrung des Accounts an.

Eine solche Accountsperre ist zumindest ein Signal an den/die Nutzer:in des Accounts, dass sein/ihr Verhalten nicht geduldet wird. Sie alleine ist jedoch nicht dazu geeignet, einen Lerneffekt bei dem/der

rechtsverletzenden Nutzer:in zu erzielen, da die Hürde für den/die Rechtsverletzende:n nach Accountsperrung sich unverzüglich oder in Zukunft einen neuen Account anzulegen nicht hoch ist. Die Accountsperre könnte durch die rechtsverletzende Person negativ aufgenommen werden, und deren - der Handlung möglicherweise zugrunde liegende - Sichtweise bestärken, dass die Plattform, die Gesellschaft oder das Ziel der rechtsverletzenden Handlung sich systematisch gegen die rechtsverletzende Person stellt. In diesem Falle könnte eine bloße Accountsperre im Ergebnis kontraproduktiv wirken.

Darüber hinaus ist zu berücksichtigen, dass nach dem vorliegenden Gesetzesvorschlag die Accountsperre gerichtlich angeordnet werden müsste. Entsprechend ist auch in diesem Verfahren zunächst mit zeitlichen Verzögerungen einer Umsetzung der Accountsperre zu rechnen. Dies gilt insbesondere deshalb, da das Eckpunktepapier als Bedingung für die Anordnung der Accountsperre vorsieht, dass zuvor ein Hinweis durch den Diensteanbieter an den/die Accountinhaber:in mit Gelegenheit zur Stellungnahme zu erfolgen hat. Welche praktischen Anforderungen an die betroffenen Diensteanbieter für das Benachrichtigen der Accountinhaber über die Kommunikationskanäle der Plattform gestellt werden, sollte zudem genau definiert werden, um eine korrekte Umsetzung gewährleisten zu können. Darüber hinaus ist formaljuristisch anzumerken, dass, indem Diensteanbieter zur Gewährung von Gehör verpflichtet werden, Grundfeste des gerichtlichen Verfahrens an den Diensteanbieter ausgelagert würden. Eine derartige Vermischung erscheint aus Effizienzgründen zweifelhaft, und auch verfahrensrechtlich mindestens kritikfähig. Überdies verdeutlicht es, dass eine Vielzahl von Akteuren involviert werden müssen, um die vom Gesetz intendierten Ziele zu erreichen. Die Rechtsbeziehungen und Aufgaben zwischen all diese Akteuren sollten daher Bestandteil der Überlegungen des Gesetzgebers im Entwicklungsprozess sein. Nur so wird es möglich, die notwendigen Maßnahmen an der richtigen Stelle zu implementieren.

4.3.3 Praktische Folgen einer Gesetzesumsetzung

Unabhängig von der Effektivität der mit dem Eckpunktepapier avisierten Maßnahmen sind deren praktischen Folgen im Fall einer Umsetzung des Gesetzes von Anfang an mitzudenken. Diesbezüglich ist wünschenswert, dass der Gesetzgeber die Konsequenzen, die bei der zivilgerichtlichen Auflösung im Urheberrecht (siehe Abschnitt 4.3.2.3) beobachtet werden konnten, bei der Erarbeitung einer ähnlichen Lösung im hier besprochen Kontext angemessen berücksichtigt.

4.4 Ko-Regulierung als (ergänzende) Lösungsmöglichkeit

Wie oben bereits beschrieben ist die Effektivität der im Eckpunktepapier avisierten Maßnahmen zur Erreichung des Schutzziels (partiell) zu bezweifeln, da das geplante Gesetz primär auf Einzelfälle abzielt und erst dann ansetzt, wenn die Rechtsverletzung bereits begangen wurde. Sofern der aktuelle

Ansatz nicht zur Erreichung des Schutzziels führt, kommen neben der vorgeschlagenen gesetzlichen Lösung im Eckpunktepapier auch andere Instrumente in Betracht, die die Erreichung des Schutzziels mit der Umsetzbarkeit von etwaigen Maßnahmen durch Stakeholder bestmöglich in Einklang bringen können. Dem Schutzziel könnte sich auch durch präventive Maßnahmen, die die Gesellschaft edukativ und damit auch die Nutzer:innen erreichen, genähert werden, sodass Rechtsverletzungen gar nicht erst entstehen können bzw. verringert werden. Dies würde in der Konsequenz langfristig den Justizapparat entlasten und die Sensibilität der Gesamtbevölkerung im Umgang mit und der Perzeption von Medien weiter erhöhen. Um dies zu erreichen, kann mit unterschiedlichen Instrumenten, neben oder anstatt eines Gesetzes, gearbeitet werden.

4.4.1 Bedarfsanalyse als zwingende Voraussetzung

Die Entwicklung und Einführung von neuen regulatorischen Rahmenwerken setzen jedoch zwingend eine sorgfältige Analyse dahingehend voraus, ob tatsächlich ein Bedarf für solche besteht. Wie bereits in Abschnitt 4.3.1 ausgeführt, ist auf komplementäre Regelwerke – ob gesetzlich oder auf anderem Wege – nur dann zurückzugreifen, sofern eine Regelungslücke besteht, deren Schließung zur Erreichung des verfolgten Schutzziels unbedingt erforderlich ist. Grund dafür ist, dass bedarfslose Regulierung das Risiko birgt, konträre Regelungen hervorzubringen, wodurch ihre praktische Umsetzung erschwert und ihre Wirksamkeit erheblich gemindert wird. Vor diesem Hintergrund ist der im Folgenden aufgezeigte regulatorische Ansatz nur unter der Prämisse zu verfolgen, dass eine entsprechende Bedarfsanalyse positiv ausfällt. Aufgrund der in Abschnitt 4.3.1 benannten Vielzahl an bestehenden rechtlichen Bestimmungen ist diese Voraussetzung jedoch vermutlich nicht erfüllt.

4.4.2 Ko-Regulierung als Möglichkeit effektiven Rechtsschutzes

Um effektiv Rechtsverletzungen im digitalen Raum zum Schutze der Integrität von Verbraucher:innen zu reduzieren, bietet sich als alternatives Instrument eine Ko-Regulierung der beteiligten Stakeholder, an. Dieses Instrument ist dazu geeignet, dynamischer auf die Perspektive und Beweggründe derjenigen Nutzer:innen einzugehen, die Rechtsverletzungen im digitalen Raum begehen. Auch können koregulatorische Maßnahmen effizienter die bestehenden Mehrpersonenverhältnisse adressieren.

Ko-regulatorische Maßnahmen können dabei effizienter wirken als gesetzliche Maßnahmen, da sich diese mit den direkten Rechtsbeziehungen der Vielzahl der unterschiedlichen Stakeholder auseinandersetzen. Hierzu zählen insbesondere neben den Nutzer:innen, die die Rechtsverletzungen begehen, auch die Betroffenen, die unterschiedlichen Plattformbetreiber und Internetzugangsanbieter sowie der Justizapparat. Als Konsequenz wären höhere und nachhaltigere Effekte im Rahmen der präventiven Vermeidung und reaktiven Entfernung digitaler Gewalt zu erwarten.

4.4.3 Ziel und Vorteile einer Ko-Regulierung durch einen Verhaltenskodex

Ziel eines solchen Verhaltenskodex als Instrument der Selbst- oder Ko-Regulierung ist zumeist eine Vereinheitlichung in einem speziellen Bereich oder einer konkreten Branche zu schaffen. Ein Verhaltenskodex ermöglicht es individuell auf praktische Bedürfnisse der Beteiligten einzugehen, sodass im Kodex niedergelegte Regelungen mit bestehenden Prozessen bestmöglich kompatibel sind und deshalb in der Praxis effektiv funktionieren können. Dabei ist in diesem Fall aufgrund des engen Bezugs zur und der gesellschaftlichen Bedeutung des Grundrechts auf Meinungsfreiheit eine Ko-Regulierung gegenüber einer Selbstregulierung vorzuziehen.

4.4.3.1 Bedeutung des zeitlichen Aspektes

Bei der Entwicklung von Mechanismen und Instrumenten zur Verbesserung des Schutzes von Verbraucher:innen vor Rechtsverletzungen im digitalen Raum ist Folgendes zu berücksichtigen: Zum einen ist, wie unter Abschnitt 4.3.2.3 gezeigt, der zeitliche Aspekt von großer Bedeutung. Nutzer:innen, die Rechtsverletzungen im digitalen Raum begehen, soll möglichst unmittelbar das Signal vermittelt werden, dass ihre Rechtsverletzung gesellschaftlich nicht toleriert wird. Sofern gerichtliche Anordnungen nicht aus anderen rechtsdogmatischen und grundrechtlichen Erwägungen zwingend sind, ließen sich durch eine Ko-Regulierung die zeitlichen Handlungsspannen insoweit verkürzen, dass ein Signal an den/die Nutzer:in hinreichend zeitnah für eine psychologische Verknüpfung der rechtswidrigen Verletzungshandlung und der Reaktion darauf ergehen kann. In diesem Falle könnten die betroffenen Stakeholder, etwa Diensteanbieter, ihre Handlungen auf eine vertragliche Basis stützen. Durch die deutlich schnellere Reaktionszeit würde sich der gewünschte Effekt bei den Rechtsverletzenden wahrscheinlicher einstellen. In diesem Kontext ist aber hervorzuheben, dass dennoch eine eingehende Prüfung der Inhalte im Vordergrund stehen muss und nicht durch verkürzte Handlungsspannen eine ordentliche inhaltliche Prüfung auf Zulässigkeit des Verhaltens ausgehebelt werden darf. Insofern kann und sollte auf starre Fristen verzichtet werden. Starre Fristen sind eher geeignet, eine ordentliche Inhaltliche Prüfung zu konterkarieren; zugleich sind auch ohne derartige Fristen für den psychologischen Effekt und Schutz der Verbraucher:innen hinreichend zeitnahe Reaktionen zu erwarten. In diesem Kontext ist der relevante Vergleichshorizont die Reaktionszeit unter Einbeziehung der Gerichte, welche – wie zuvor in den Abschnitten 4.3.2.3 und 4.3.2.4 dargestellt – nicht als besonders zügig zu erwarten ist. Bereits heute haben die meisten Diensteanbieter umfangreiche interne Richtlinien zur Entfernung rechtwidriger Inhalte auf ihren Plattformen und setzen diese auch erfolgreich um.

4.4.3.2 Accountunabhängiger Ansatz

Um ein tatsächliches Umdenken von rechtsverletzenden Nutzer:innen zu erzielen, ist im jedem Falle nicht nur das bloße Unterbinden von dessen/deren Äußerungen erforderlich. Wie in Abschnitt 4.3.2.4 dargestellt, können sich Nutzer:innen ohne viel Aufwand einen anderen Account auf derselben oder

einer anderen Plattform erstellen, der anstelle des bisherigen Accounts für rechtsverletzende Äußerungen genutzt werden kann. Es gilt mithin, den/die Nutzer:in so zu erreichen, dass diese/r von rechtsverletzenden Äußerungen - accountunabhängig – absieht. Bereits durch niederschwellige, aber pointierte Maßnahmen könnten sich positive Effekte erzielen lassen, bspw. im Sinne eine Auseinandersetzung mit den jeweiligen Nutzer:innen sodass diese bestmöglich zur Einsicht ihrer Handlungen gelangen und rechtsverletzende Äußerungen zukünftig unterlassen. Die Zusammenarbeit mit den Stakeholdern, um die Implementierung edukativer Ansätze zu ermöglichen, könnte dabei zuträglich sein. Sowohl der Aspekt der Verkürzung der Handlungsspannen als auch die Verfolgung eines edukativen Ansatzes gegenüber Nutzer:innen, die rechtsverletzende Äußerungen veröffentlichen, können mit einem Verhaltenskodex adressiert werden, an welchen sich die beteiligten Stakeholder binden.

4.4.3.3 Internationale Anwendbarkeit

Um eine Anwendbarkeit der Maßnahmen zu gewährleisten, erscheint eine reine Beschränkung auf den deutschen Raum nicht sinnvoll, da das zugrunde liegende Problem im Sinne einer „Verrohung der Kommunikation“ nicht nur auf den deutschen Raum beschränkt ist, sondern ebenso international festzustellen ist. Des Weiteren sind der überwiegende Anteil der Plattformen in mehreren Staaten aktiv, sodass im Sinne der Effizienz eine Harmonisierung der Regelungsanforderungen effektiver erscheint, da somit der Fokus und die Ressourcen in die Zielerreichung investiert werden können. Dies gilt selbst gemäß dem Fall, dass Stakeholder nicht ausdrücklich in mehreren Staaten und/oder internationalen Märkten aktiv sind, da deren Nutzer:innen dennoch international sein können bzw. der Zugang aus dem Ausland schwerlich auszuschließen ist. Gerade bei grenzüberschreitenden Sachverhalten ist die Anwendbarkeit von Maßnahmen durch einen Verhaltenskodex einfacher abzubilden.

Der Vorteil eines potenziellen Verhaltenskodex für Rechtsverletzungen im digitalen Raum gegenüber einem nationalen Gesetz liegt unter anderem in dem internationalen Anwendungsbereich eines solchen Kodex und einem Aufheben der territorialen Bindung, den ein nationales Gesetz mit sich bringt. Durch breite territoriale Anwendbarkeit böte ein solcher Kodex das Potenzial international agierende Plattformen im Verhältnis zu deren internationalen Nutzer:innen tätig werden zu lassen. Damit könnten auch Nutzer:innen erreicht werden, die aus dem Ausland tätig werden und nach nationaler Gesetzgebung schwer oder gar nicht belangt werden können. Insofern hätte der Verhaltenskodex im Vergleich zu einem nationalen Gesetz einen größeren Schutzbereich und bereits bestehende Strukturen bei den Diensteanbietern könnten sinnvoll, effizient und innovationsfreundlich erweitert werden.

Die Eckpunkte eines solchen Verhaltenskodex und welche Anforderungen an ihn gestellt werden müssten, werden im Folgenden beispielhaft dargestellt.

4.4.4 Eckpunkte eines potenziellen Verhaltenskodex

Eine verpflichtende Kontaktaufnahme der beteiligten Stakeholder mit Autor:innen rechtsverletzender Postings mit aufklärenden und auf Gewaltprävention abzielenden Hinweisen könnte dazu beitragen, eine Accountsperre obsolet zu machen bzw. diese erst als Ultima Ratio (erst temporär, dann endgültig) zu nutzen. Eine solche Accountsperre könnte ohne gerichtliche Beteiligung zeitlich flexibler erfolgen.

Grundsätzlich ist aber auch hier darauf hinzuweisen, dass derartige Eckpunkte nur insoweit in Betracht kommen, wie ein konkreter Bedarf für die Erreichung des Schutzziels in einer entsprechenden Analyse gemäß Abschnitt 4.4.1 festgestellt wird.

4.4.4.1 Beispiel des Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet

Am Beispiel des Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet[9] ist zu sehen, dass ein solcher transnationaler Kodex ein effektives Mittel sein kann, im Einklang mit der Meinungsfreiheit illegale Hassrede und damit Rechtsverletzungen im digitalen Raum zu bekämpfen. Das aktuelle Fact Sheet zur siebten Evaluation des Verhaltenskodex von November 2022 zeigt dabei, dass in knapp 65% der Fälle notifizierter Content an die Plattform innerhalb von weniger als 24 Stunden bearbeitet wird und dieser in knapp 64% der Fälle dann auch von der Plattform entfernt wird.[10]

4.4.4.2 Effektuieren und Stärken der Good Practices der Plattformen

Das Beispiel in 4.4.4.1 zeigt, dass für die Zielerreichung bereits Mechanismen im Markt implementiert sind, entweder in Folge gesetzlicher Pflichten oder in Folge durch die Stakeholder bereits erkannter, ungewollter Entwicklungen. Ein guter Anknüpfungspunkt für die weitere Optimierung des Status Quo im Kontext digitaler Gewalt sollten die Good Practices der Plattformen sein, die aus diversen Gründen sehr versiert im Umgang mit renitenten Rechtsverletzer:innen sind. Aus Effizienzgründen sollte vermieden werden, neue Parallelstrukturen aufzubauen.

4.4.4.3 Förderung der Zusammenarbeit der betroffenen Stakeholder

Ein zu entwickelnder Verhaltenskodex mit größerem Anwendungsbereich sollte die Zusammenarbeit der betroffenen Stakeholder fördern. Insbesondere im Hinblick auf die in 4.3.2.1 dargestellten Mehrpersonenverhältnisse könnte die Förderung Spannungsverhältnisse auflösen und Klarheiten

[9] Mehr Informationen zum Verhaltenskodex sowie der Kodex selbst sind zu finden unter: https://ec.europa.eu/commission/presscorner/detail/de/QANDA_20_1135

[10] https://commission.europa.eu/system/files/2022-12/Factsheet%20-%207th%20monitoring%20round%20of%20the%20Code%20of%20Conduct.pdf

schaffen. Im Sinne des Schutzziels sollte eine Hinzuziehung von Expert:innen aus dem Bereich Gewaltprävention in Betracht gezogen werden.

4.4.4.4 Feinjustierung bereits bestehender Maßnahmen

Die bestehenden Maßnahmen der Diensteanbieter als Ausfluss des bereits beschriebenen europäischen Verhaltenskodex und auch des NetzDG sind dabei grundsätzlich schon effektiv. Unmittelbare Konsequenzen, etwa edukativ, oder auch gestaffelte Accountsperren, könnten allenfalls im Bedarfsfall feinjustiert werden. Auch komplexe Fragen des „Overblockings“, die bereits aus anderen Rechtsgebieten bekannt sind, können und müssten hierbei Berücksichtigung finden. Aufgrund der Tatsache, dass bestimmte Accounts inzwischen eine zentrale Bedeutung im täglichen Leben der Betroffenen haben und diese Accounts innerhalb einer Plattform für mehrere Dienste genutzt werden aber auch im Sinne eines Single-Sign-On über Plattformen hinweg als Zugänge genutzt werden, erscheint es zudem sinnvoll, zwischen einer dienstgebundenen und dienstübergreifenden Accountsperre zu unterscheiden.

4.4.4.5 Hohe Komplexität erfordert Expertise und kontinuierliche Überarbeitung

Die Mannigfaltigkeit der betroffenen Interessen, ebenso wie unterschiedliche Grundrechtspositionen bedeuten daher eine hohe Komplexität, die mit Hilfe von Expert:innen kontinuierlich und mit nötiger, aber für die Entwicklung und Innovation hinreichender Generalität adressiert werden sollte. Durch die Zusammenarbeit von Stakeholdern mit (staatlichen), gewaltpräventionsfördernden Stellen könnte ein effektiver Verbraucher:innenschutz gefördert werden.

4.4.4.6 Überwindung von Informationsstaus durch erhöhte Kooperation der beteiligten Stakeholder

Elemente der möglicherweise nicht hinreichend effektiven Rechtsdurchsetzung sind bestehende Inkonsistenzen, Rechtsunsicherheiten und Barrieren im Informationsfluss zwischen den beteiligten Stakeholdern. Es erscheint daher zielführend, anstatt weitere individuelle Pflichten für einzelne Stakeholder zu definieren, dieser eher organisatorischen Fragestellung mehr Aufmerksamkeit zu schenken. Hierbei könnte – im Sinne eines ko-regulatorischen Ansatzes – der Gesetzgeber klarstellen, dass bestimmte Informationsflüsse zulässig, oder gar gewünscht sind, währenddessen die Operationalisierung derartigen Informationsaustauschs den Stakeholdern überlassen wird.

5 Zusammenfassung

Abschließend lässt sich festhalten, dass die Intention und die Bemühungen des Gesetzgebers Betroffenen von Rechtsverletzungen im digitalen Raum einfacher Abhilfe zu verschaffen, indem bereits bestehende Verfahren erweitert werden sollen, eine grundsätzlich sachdienliche und gesellschaftlich positive Initiative darstellt. Im Detail scheinen die vorgeschlagenen Maßnahmen jedoch nicht

vollständig ausgereift und nicht zur Erreichung des zu recht angestrebten Schutzziels geeignet. Eine klarere Definition des Schutzziels sowie die Ausrichtung der Maßnahmen an eben diesem Schutzziel wäre wünschenswert.

Daneben sollten auch Instrumente der Selbst- und Ko-Regulierung in Betracht gezogen werden. Ein Beispiel dafür, dass Ko-Regulierung auf transnationaler Ebene auch in hochkomplexen Sachverhalten erfolgreich sein kann, ist etwa der EU Cloud Code of Conduct[11]. Dieser durch SCOPE Europe verwaltete Verhaltenskodex verhilft den Anbietern von Cloud-Diensten die datenschutzrechtlichen Anforderungen der DSGVO einzuhalten. Als erster von der belgischen Datenschutzbehörde im Mai 2021 nach positiver Stellungnahme vom Europäischen Datenschutzausschuss[12] genehmigter[13] Kodex gem. Art. 40 DSGVO[14] in diesem Bereich profitieren Betroffene als auch Unternehmen von einheitlichen und umsetzbaren Verhaltenspflichten, sodass der Kodex in der Konsequenz einen positiven Beitrag zum Datenschutz leistet.

Ein Verhaltenskodex für Rechtsverletzungen im digitalen Raum kann in Form einer Ko-Regulierung ein Instrument neben einer gesetzlichen Verpflichtung sein. Jedoch sollte ein solcher Ansatz ebenfalls nur verfolgt werden, soweit ein konkreter Bedarf festgestellt wird. Zur Förderung der Entwicklung eines effektiven Verhaltenskodex sollte daher sichergestellt werden, dass nicht nur die relevanten Stakeholder an dessen Entwicklung partizipieren. Vielmehr sollte eine klare Problemanalyse, eine klare gesetzliche Zielvorgabe sowie ein bestmöglicher Rückgriff auf bestehende (internationale) Good Practices ermöglicht werden. Im Spannungsfeld unterschiedlicher Rechtsrahmen sollte eine etwaige gesetzliche Regelung Klarheit über das Verhältnis der Rechtsrahmen schaffen, und somit rechtliche Unsicherheiten bei der Entwicklung und Implementierung von effektiven Maßnahmen vermeiden.

[11] Mehr Informationen zum EU Cloud Code of Conduct sind zu finden unter: https://eucoc.cloud/en/about/about-eu-cloud-coc
[12] Stellungnahme abrufbar unter: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf
[13] Anerkennungsbeschluss abrufbar unter: https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[14] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Die Intention und die Bemühungen des Gesetzgebers Betroffenen von Rechtsverletzungen im digitalen Raum einfacher Abhilfe zu verschaffen, in dem bereits bestehende Verfahren erweitert werden sollen, eine grundsätzliche sachdienliche und gesellschaftlich positive Initiative darstellt. Im Detail scheinen die vorgeschlagenen Maßnahmen jedoch nicht vollständig ausgereift und nicht zur Erreichung des zu recht angestrebten Schutzziels geeignet. Eine klarere Definition des Schutzziels sowie die Ausrichtung der Maßnahmen an eben diesem Schutzziel wäre wünschenswert.

Daneben sollten auch Instrumente der Selbst- und Ko-Regulierung in Betracht gezogen werden. Ein Beispiel dafür, dass Ko-Regulierung auf transnationaler Ebene auch in hochkomplexen Sachverhalten erfolgreich sein kann, ist etwa der EU Cloud Code of Conduct.

Ein Verhaltenskodex für Rechtsverletzungen im digitalen Raum kann in Form einer Ko-Regulierung ein Instrument neben einer gesetzlichen Verpflichtung sein. Jedoch sollte ein solcher Ansatz ebenfalls nur verfolgt werden, soweit ein konkreter Bedarf festgestellt wird. Instrument neben einer gesetzlichen Verpflichtung sein. Zur Förderung der Entwicklung eines effektiven Verhaltenskodex sollte daher sichergestellt werden, dass nicht nur die relevanten Stakeholder an dessen Entwicklung partizipieren. Vielmehr sollte eine klare Problemanalyse, eine klare gesetzliche Zielvorgabe sowie ein bestmöglicher Rückgriff auf bestehende (internationale) Good Practices ermöglicht werden. Im Spannungsfeld unterschiedlicher Rechtsrahmen sollte eine etwaige gesetzliche Regelung Klarheit über das Verhältnis der Rechtsrahmen schaffen, und somit rechtliche Unsicherheiten bei der Entwicklung und Implementierung von effektiven Maßnahmen vermeiden.

Über den SRIW

Der SRIW e.V. wurde 2011 als unabhängige, private Aufsichtsstelle branchenspezifischer Verhaltensregeln gegründet. Oberste Prämisse seit Gründung war und ist es, die notwendigen, unabhängigen Strukturen bereitzustellen, um branchenspezifische Verhaltensregeln zu etablieren und zu verwalten sowie deren glaubwürdige und wirksame Überwachung, inklusive eines Beschwerdemanagements, zu gewährleisten. Seither ist der SRIW erfolgreich an der Entwicklung von Verhaltensregeln, unter anderem im Bereich Datenschutz, beteiligt und engagiert sich auch in anderen Formen rund um das Thema *modern-regulation*.

selbstregulierung
informationswirtschaft e.V.