Stellungnahme zum Eckpunktepapier zum Gesetz gegen digitale Gewalt

Eckpunktepapier des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt

Februar 2025

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. Oliver Draf

Geschäftsführer
Frank Ingenrieth

Inhalt

1 Executive Summary

- Es erscheint nach wie vor fraglich, inwieweit neben den bereits umfassenden anwendbaren regulatorischen Rahmenbedingungen überhaupt eine gesetzliche Regelungslücke vorliegt.
- Der Gesetzesentwurf erhält einige Konkretisierungen im Gegensatz zum Eckpunktepapier. Diese sind jedoch nicht ausreichend, um eine Verbesserung der Situation „Gewalt im digitalen Raum“ herbeizuführen.
- Eine mögliche gesetzliche Maßnahme sollte eine umfassendere Problem- und Bedarfsanalyse voranstellen, und die vorgesehenen Maßnahmen deutlicher auf das Schutzgut einzahlen.
- Derzeit vorgesehene Maßnahmen erscheinen nach wie vor wenig bis gar nicht geeignet, eine Verbesserung für das Schutzgut herbeizuführen.
- Der Begriff „Gewalt im digitalen Raum“ ist nicht ausreichend präzisiert worden.
- 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 Practises 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 srl[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. In dem veröffentlichten Diskussionsentwurf wird „Gewalt im digitalen Raum" nun klarer definiert, als es noch im Eckpunktepapier der Fall war. 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. Insgesamt ist auf die umfangreiche Stellungnahme des SRIW zum Eckpunktepapier[4] zu verweisen. In der vorliegenden Stellungnahme zum Diskussionsentwurf sollen lediglich Themen

[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
[4] Stellungnahme zum Eckpunktepapier zum Gesetz gegen digitale Gewalt

adressiert werden, die Neuerungen oder Änderungen enthalten oder zu denen der SRIW seine Position besonders betonen möchte.

Dabei schenkt der SRIW auch in diesem Fall erneut dem mit dem Gesetz adressierte Schutzgut und des verfolgte Schutzziels besondere Aufmerksamkeit, sowie den Ursachen des mit dem Gesetz zu lösen bestrebte Problem. Auch auf die bereits in der letzten Stellungnahme ergänzenden, außergerichtlichen Lösungen, wie beispielsweise eine Ko-Regulierung wird noch einmal eingegangen.

4 Stellungnahme

4.1 Schutzgut und Schutzziel

Im Gegensatz zum Eckpunktepapier wird im Diskussionsentwurf nun ein konkretes Schutzziel genannt: die individuelle Rechtsdurchsetzung. Eine Effektivitätsanalyse und -evaluierung der durch das Gesetz gegen digitale Gewalt vorgesehenen Maßnahmen ist in Hinblick auf das mit dem Gesetz adressierte Schutzgut durchzuführen.

4.2 Zum Gesetz gegen digitale Gewalt

Das Gesetz gegen digitale Gewalt wird im Folgenden in Hinblick auf seine Geeignetheit zur Erreichung des Schutzziels evaluiert. Im Übrigen wird auf die Stellungnahme zum Eckpunktepapier verwiesen.

4.2.1 Geeignetheit des Gesetzes zur Erreichung des Schutzziels

4.2.1.1 Präzisierung des Begriffs „Gewalt im digitalen Raum“

Eine genaue Definition des Begriffs „Gewalt im digitalen Raum“ ist bedauerlicherweise nicht zu finden. Zwar wird der Begriff in der Beschreibung des Gesetzestextes näher präzisiert, eine Legaldefinition im vorgeschlagenen Gesetz findet sich jedoch nicht.

Möglicherweise kann der Begriff jedoch aufgrund anderer Definitionen hergeleitet werden.

Positiv hervorgehoben werden soll, dass soziale Netzwerke in § 1 Absatz 4 des Gesetzes legaldefiniert werden. Diese Definition unterscheidet sich insofern von der Definition in § 1 Absatz 1 NetzDG, in dem es in diesem Falle nicht mehr auf die Gewinnerzielungsabsicht ankommt. Dadurch ließe sich das Gesetz auch auf nicht-kommerzielle Plattformen anwenden, was den Anwendungsbereich erweitert.

Darüber hinaus findet sich in § 1 Absatz 1 des vorliegenden Textes auch eine Definition der Rechtsverletzung.

Aus den genannten Definitionen lässt sich nur mittelbar erschließen, was „Gewalt im digitalen Raum“ gemäß des Gesetzes bedeutet. Es entsteht der Eindruck, dass der Gesetzgeber sich der genauen Definition des Gesetzes nicht annehmen möchte. Eine Legaldefinition wäre zur genaueren Einordnung des Schutzziels wünschenswert.

4.3 Ko-Regulierung als (ergänzende) Lösungsmöglichkeit

Wie bereits in der Stellungnahme zum Eckpunktepapier erläutert, kommen neben der vorgeschlagenen gesetzlichen Lösung 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.

4.3.1 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. Auf komplementäre Regelwerke – ob gesetzlich oder auf anderem Wege – ist 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 Vielzahl an bestehenden rechtlichen Bestimmungen ist diese Voraussetzung jedoch vermutlich nicht erfüllt.

4.3.2 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.

4.3.3 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.

4.3.3.1 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 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 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.

4.3.3.2 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. Nutzer:innen können sich 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.

4.3.3.3 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.

4.3.4 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 4.3.1 festgestellt wird.

4.3.4.1 Beispiel des Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet

Am Beispiel des Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet[5] 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.[6]

4.3.4.2 Effektuieren und Stärken der Good Practices der Plattformen

Das Beispiel in 4.3.4.1 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.

---

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

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

4.3.4.3 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 der Stellungnahme zum Eckpunktepapier dargestellten Mehrpersonenverhältnisse könnte die Förderung Spannungsverhältnisse auflösen und Klarheiten schaffen. Im Sinne des Schutzziels sollte eine Hinzuziehung von Expert:innen aus dem Bereich Gewaltprävention in Betracht gezogen werden.

4.3.4.4 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.

4.3.4.5 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.

4.3.4.6 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 konkrete Ausgestaltung des Gesetzes einige positiv hervorzuhebenden Aspekte enthält, die im Eckpunktepapier noch nicht enthalten waren. Die Intention und die Bemühungen des Gesetzgebers Betroffenen von Rechtsverletzungen im digitalen Raum einfacher Abhilfe zu verschaffen, indem bereits bestehende Verfahren erweitert werden sollen, stellt eine grundsätzlich sachdienliche und gesellschaftlich positive Initiative dar. Die vom Gesetzgeber geplanten Maßnahmen zahlen aus den oben genannten Gründen jedoch nicht vollständig auf die Erreichung des angestrebten Schutzziels ein.

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[7]. 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[8] genehmigter[9] Kodex gem. Art. 40 DSGVO[10] 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.

Wiederholt möchte der SRIW betonen, dass ein Verhaltenskodex für Rechtsverletzungen im digitalen Raum in Form einer Ko-Regulierung ein Instrument neben einer gesetzlichen Verpflichtung sein kann. Auch aktuell im Diskussionsentwurf fehlende Definitionen könnten in einem Verhaltenskodex adressiert werden und so für mehr Klarheit sorgen. 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.

---

[7] Mehr Informationen zum EU Cloud Code of Conduct sind zu finden unter: https://eucoc.cloud/en/about/about-eu-cloud-coc
[8] Stellungnahme abrufbar unter: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf
[9] Anerkennungsbeschluss abrufbar unter: https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[10] 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 nach wie vor nicht vollständig ausgereift und nicht zur Erreichung des zu recht angestrebten Schutzziels geeignet. Eine klarere Definition des Begriffs „Gewalt im digitalen Raum“ 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.