VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt

Köln/Berlin, 19. Mai 2026

Ein immer größerer Teil des sozialen Miteinanders spielt sich im digitalen Raum ab. Menschen können grenzenlos insbesondere mittels Sozialer Medien miteinander in Kontakt treten und Informationen teilen, Meinungen austauschen und Diskussionen anstoßen. Damit einhergehend kommt es aber auch zu Rechtsgutsverletzungen im digitalen Raum und neuen Formen der Gewalt (sog. “digitale Gewalt”), Persönlichkeitsrechtsverletzungen nehmen hier eine besondere Rolle ein.

Dem soll mit dem Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) vom 16. April 2026 für ein Gesetz zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt entgegengetreten werden. Das Konzept beruht auf zwei Säulen: Für einen effektiven Schutz der Betroffenen soll einerseits die zivilrechtliche Rechtsdurchsetzung wesentlich erleichtert und andererseits das Strafrecht an neue Phänomene des digitalen Zeitalters angepasst werden.

Zivilrechtlich soll das neue Gesetz gegen digitale Gewalt (GgdG) dazu beitragen, den Rechtsweg für die Opfer digitaler Gewalt effizienter zu gestalten, und so die Rechtsdurchsetzung neben strafrechtlicher Verfolgung stärken: Das GgdG soll es Betroffenen von digitaler Gewalt ermöglichen, Informationen über rechtswidrig handelnde Nutzer zu bekommen, um zivilrechtliche Ansprüche verfolgen zu können. Dazu sieht der Entwurf des GgdG richterliche Sicherungsanordnungen gegen Anbieter digitaler Dienste vor, sofern die Tatbestands-Voraussetzungen für bestimmte Rechtsverletzungen erfüllt sind. Zusätzlich eröffnet das geplante Gesetz die Möglichkeit der temporären Accountsperre bei wiederholten Rechtsverletzungen. Weiterhin wird insbesondere für Anbieter ohne Sitz in einem EU-Land die Benennung eines Zustellungsbevollmächtigten geregelt.

Zur Effektivierung des Strafrechts sollen bestehende Lücken geschlossen werden: Die Herstellung und Verbreitung von sexualisierten Deepfakes soll künftig strafrechtlich ebenso erfasst werden wie die Verbreitung von sonstigen (nicht sexualbezogenen) Deepfakes, die die Persönlichkeitsrechte einer anderen Person verletzen.

eco – Verband der Internetwirtschaft e.V. (eco) nimmt gerne die Gelegenheit wahr, zu diesem Referentenentwurf Stellung zu nehmen. Dabei fokussieren sich die nachfolgenden Anmerkungen auf die für die Internetwirtschaft relevanten Punkte des Gesetzentwurfs:

Zum zivilrechtlichen Auskunftsanspruch

Mit dem geplanten Auskunftsanspruch sollen Betroffene von digitaler Gewalt in einem gerichtlichen Verfahren die Herausgabe von Daten über den verletzenden Nutzer verlangen können, wenn sie nachweisen können, dass eine Rechtsverletzung vorliegt und sie den verletzenden Nutzer nicht identifizieren können.

- **Materiell-rechtlicher Anwendungsbereich (§ 1 GgdG-E)**

§ 1 GgdG-E regelt neben den Definitionen der betroffenen Anbieter auch die nach diesem Gesetz zur Auskunft berechtigenden Rechtsverstöße. eco hebt positiv hervor, dass der materiell-rechtliche Anwendungsbereich, also die zur Auskunft berechtigenden Rechtsverstöße, auf strafbewehrte Äußerungen bzw. Handlungen beschränkt ist. Dies bietet den Anbietern der betroffenen Dienste Klarheit und Rechtssicherheit.

- **Auskunft über Daten, Sicherungsanordnungen und Richtervorbehalt (§§ 2 und 3 GgdG-E)**

Der mit dem GgdG-E gewählte Ansatz zur Datenherausgabe und Datensicherung erscheint aus Sicht von eco grundsätzlich geeignet, Rechtssicherheit für alle am Verfahren Beteiligten zu gewährleisten.

§ 2 GgdG-E formuliert zum einen die essenziell wichtige, richterliche Anordnung als Voraussetzung und benennt zum anderen die herauszugebenden Daten. Darunterfallen nicht nur Daten über den zur Begehung der rechtswidrigen Handlung genutzten Internetanschluss, sondern auch persönliche Daten wie Name, Geburtsdatum sowie Kontaktdaten wie Anschrift und Telefonnummer und eine Kopie des angegriffenen Inhalts. Die Herausgabe dieser Daten stellt einen starken Eingriff in die Rechte der Nutzer dar. Daher ist der angedachte Richtervorbehalt ausdrücklich zu begrüßen. Es ist ausgesprochen wichtig, dass mit derart sensiblen Daten entsprechend sensibel umgegangen wird. Die Notwendigkeit eines richterlichen Beschlusses stellt sicher, dass bereits vorher ausführlich geprüft wurde, ob ein zur Auskunft verpflichtender Rechtsverstoß vorliegt. Dies gibt den betroffenen Anbietern die notwendige Sicherheit, da so das für sie bestehende Risiko von rechtlichen Konsequenzen aufgrund von Datenschutzverletzungen minimiert wird.

§ 3 GgdG-E stellt die rechtliche Grundlage für die Sicherungs- und Herausgabeanordnung durch ein Gericht dar. Positiv hervorzuheben ist, dass die beim Dienstanbieter vorliegenden Daten im ersten Schritt explizit nur gegenüber dem Gericht, nicht jedoch dem Antragsteller zu übermitteln sind. So wird ein möglichst kleiner Adressatenkreis gewährleistet, um den Eingriff in die Rechte der von der Anordnung betroffenen Person möglichst gering zu halten. Aus Sicht der Internetwirtschaft begrüßenswert ist zudem, dass § 3 Absatz 4 GgdG-E den Anbietern explizit die Datenverarbeitung zum Zwecke der Sicherung und

Herausgabe durch eine Anordnung erlaubt. Dadurch sind Anbieter rechtlich abgesichert vor jeglichen Konsequenzen wegen vermeintlicher Datenschutzverletzungen.

Die geplanten Regelungen stehen dabei neben den Plänen für eine IP-Adressspeicherung für staatliche Verfahren, insbesondere zur Verfolgung von bestimmten Straftaten. Wichtig ist für den weiteren Gesetzgebungsprozess, dass die geplanten, nebeneinander bestehenden Regelungen weiterhin kongruent ausgestaltet bleiben und insbesondere im Rahmen des GgdG weder eine Ausweitung der Parallelregelung erfolgt noch widersprüchliche Vorgaben geschaffen werden.

Zur Sperrung der Nutzerkonten, § 4 GgdG-E

Neben der Sicherung und Herausgabe von Daten sieht der Entwurf zusätzlich die Möglichkeit vor, ein Nutzerkonto zeitweise sperren zu lassen. Auch hierfür ist eine richterliche Anordnung notwendig, die nur in bestimmten, in Absatz 3 aufgeführten, Fällen erfolgen darf. So muss der von der Anordnung betroffene Nutzer eine Unterlassungserklärung verweigern, gegen eine bestehende Unterlassungserklärung verstoßen, oder anderweitig den Verdacht erwecken, weitere Rechtsverletzungen zu begehen.

eco möchte insoweit auf zwei Aspekte hinweisen:
Zum einen stellt die Sperrung eines Nutzerkontos in den geregelten Fällen einen schweren Eingriff in die Rechte des Nutzers dar. Ein entsprechender zivilrechtlicher Anspruch eines betroffenen Nutzers sollte zurecht nur als letztes Mittel eingesetzt werden. Positiv hervorzuheben ist, dass das Gericht bei der Entscheidung mögliche mildere Maßnahmen berücksichtigen muss, die der Anbieter ergreifen kann, um weitere Rechtsverletzungen zu verhindern. Ein Richtervorbehalt ist dabei unerlässlich und wird von eco daher positiv bewertet. Auch die ausdrückliche Beschränkung auf die Konten des Nutzers, über die die Rechtsverletzung begangen wurde, solange auf anderen Konten im festgelegten Zeitraum keine weitere Rechtsverletzung zu erwarten ist, ist eindeutig positiv zu bewerten. Entsprechendes gilt für die Einschränkung der Überprüfung anderer Konten auf ein zumutbares Maß. Hierdurch wird das Risiko von Overblocking verringert und die zusätzliche Belastung und Verantwortung der Diensteanbieter auf ein vertretbares Maß beschränkt.

Zum anderen erscheint der wesentliche Inhalt der Regelung beinahe deckungsgleich mit Art. 23 des Digital Services Act (DSA). Anders als im DSA soll hier jedoch durch den Betroffenen der Rechtsverletzung die Sperrung eines Nutzerkontos verlangt werden können. eco regt an, die Notwendigkeit einer Regelung auf nationaler Ebene nochmals zu überdenken. Der DSA ist eine vergleichsweise neue Regelung, die auch ohne weitere Umsetzung auf nationaler Ebene Anwendung findet. Bevor ergänzende nationale Regelungen implementiert werden, sollte zunächst die Umsetzung bestehender unionsrechtlicher Regelungen

in der Praxis bewertet werden. Bei Beibehaltung einer ergänzenden nationalen Regelung sieht eco zudem einen potenziellen Konflikt mit dem DSA, der als unionsrechtliche Regelung Vorrang genießt.

Zur Möglichkeit einer anonymen Stellungnahme des rechtsverletzenden Nutzers

Falls eine Identifizierung des betroffenen Nutzers durch das Gericht nicht möglich ist, soll der Anbieter nach § 6 GgdG-E dazu verpflichtet werden, den Nutzer unverzüglich über das Verfahren nach den §§ 2 bis 4 GgdG-E zu informieren. Ferner soll der Anbieter dem Nutzer die Möglichkeit zu einer anonymen Stellungnahme geben und diese an das Gericht weiterleiten.

Grundsätzlich ist es vernünftig, dem betroffenen Nutzer die Möglichkeit zur Äußerung zu geben, zumal die rechtliche Bewertung einer Äußerung bzw. eines Online-Postings von der Einlassung des entsprechenden Nutzers abhängen kann. Das angedachte Prozedere zeigt auch, dass die Entscheidung darüber, ob eine tatsächliche Rechtsverletzung vorliegt oder nicht, vor der Frage nach der Identität steht. Daher erscheint es sinnvoll, dass betroffene Nutzer eine Stellungnahme abgeben können, ohne ihre Identität preiszugeben, wenn diese wesentlicher Streitgegenstand ist.
Kritisch bewertet eco den vorgeschriebenen Detailgrad der durch die Diensteanbieter vorzunehmenden Information. Auf den ersten Blick vermag die Regelung durch den vorgeschriebenen Detailgrad für die Diensteanbieter eine hohe Rechtssicherheit zu bieten. Auf den zweiten Blick erscheint dies jedoch (auch) eine Verlagerung der gerichtlichen Amtsermittlungsverantwortung auf die Diensteanbieter und eine hohe Bürde für die betroffenen Unternehmen zu sein. Die nötige Rechtssicherheit ohne Verlagerung von Amtsermittlungsverantwortung auf die Diensteanbieter ließe sich beispielsweise auch dadurch erreichen, dass das zuständige Gericht eine Stellungnahmeaufforderung oder Verfügung übermittelt, die dann lediglich vom Diensteanbieter an den betroffenen Nutzer weitergeleitet wird.
Mit Blick auf die geforderte Unverzüglichkeit seitens der Diensteanbieter gilt es, den maßgeblichen Zeitrahmen wohlwollend auszulegen. Denn entsprechende Unterstützungshandlungen in Bezug auf die Amtsermittlungspflicht der zuständigen Gerichte ist keine primäre Aufgabe der Unternehmen und muss sich ggfs. anderen dringenden Tätigkeiten des Tagesgeschäfts unterordnen.
Insgesamt ist zu berücksichtigen, dass die Möglichkeit einer anonymen Stellungnahme für den involvierten Anbieter einen zusätzlichen organisatorischen und administrativen Aufwand bedeutet. Dieser Mehraufwand sollte bei der Bemessung einer angemessenen Entschädigung entsprechend berücksichtigt werden. Vor diesem Hintergrund erscheint es sachgerecht, einen Entschädigungsanspruch in entsprechender Anwendung des § 23 JVEG festzusetzen.

Zur Verkürzung der Rechtsmittelfrist auf zwei Wochen

eco kritisiert die Verkürzung der Frist zur Einlegung von Rechtsmitteln gegen die erstinstanzlichen Entscheidungen auf zwei Wochen nach § 5 Abs. 5 GgdG-E. Den Entscheidungen werden regelmäßig komplexe Sachverhalte zugrunde liegen. Auch in diesen Fällen muss eine angemessene Zeit eingeräumt werden, in der entschieden werden kann, ob Rechtsmittel eingelegt werden sollen bzw. erfolgreich sein können. Eine Frist von zwei Wochen zur Überprüfung der erstinstanzlichen Entscheidungen erscheint nicht angemessen und kann insbesondere die verpflichteten Diensteanbieter benachteiligen.

Ausweitung des strafrechtlichen Schutzes

Artikel 2 – Änderung des Strafgesetzbuches

Allgemeine Bewertung

eco unterstützt das Ziel des Referentenentwurfs, Betroffene wirksam vor digitaler Gewalt zu schützen. Insbesondere die Bekämpfung bildbasierter sexualisierter Gewalt sowie der missbräuchlichen Nutzung von Deepfakes ist angesichts technologischer Entwicklungen und der zunehmenden Verbreitung entsprechender Inhalte ein berechtigtes und notwendiges Anliegen.

Gleichwohl wirft der Entwurf aus Sicht der Diensteanbieter erhebliche rechtliche und praktische Fragen auf. Dies betrifft insbesondere die Ausgestaltung der neuen Straftatbestände, ihre Abgrenzung zum bestehenden Recht sowie die Auswirkungen auf die Umsetzung durch Plattformen und andere digitale Dienste. In der vorliegenden Form besteht die Gefahr, dass Rechtsunsicherheiten entstehen, die sowohl die effektive Rechtsdurchsetzung als auch die praktische Handhabbarkeit für Anbieter erschweren.

Zu den vorgeschlagenen Änderungen im Strafrecht

Mit der Neufassung des § 184k StGB wird der strafrechtliche Schutz der Intimsphäre deutlich ausgeweitet. Hervorzuheben ist insbesondere, dass künftig bereits die Herstellung entsprechender Bildaufnahmen strafbar sein soll und nicht mehr allein deren Verbreitung. Auch die Einbeziehung von Aufnahmen aus öffentlich zugänglichen Räumen stellt eine erhebliche Erweiterung dar. Diese Zielrichtung ist aus Opferschutzgesichtspunkten nachvollziehbar, führt jedoch zu einer deutlichen Vorverlagerung der Strafbarkeit, die mit Blick auf die Funktion des Strafrechts als „ultima ratio“ staatlichen Eingreifens kritisch zu bewerten ist. Hinzu kommt, dass zentrale Tatbestandsmerkmale wie „sexuell bestimmte Weise“ auslegungsbedürftig

sind und damit Rechtsunsicherheiten schaffen, die sich in der Praxis insbesondere bei der Bewertung digitaler Inhalte und ihrer rechtlichen Einordnung auswirken.

Auch der neu eingeführte § 201b StGB zur Erfassung täuschender Inhalte adressiert ein relevantes Phänomen, da die zunehmende Verbreitung von Deepfakes erhebliche Auswirkungen auf Persönlichkeitsrechte haben kann. Gleichwohl ist zu berücksichtigen, dass bereits nach geltendem Recht verschiedene straf- und zivilrechtliche Instrumente zur Verfügung stehen, wie etwa §§ 185 ff. StGB, 184b ff. StGB, § 201a StGB, § 33 KUG sowie §§ 823 Abs. 1, 1004 BGB, um gegen entsprechende Inhalte vorzugehen. Die Einführung eines weiteren eigenständigen Straftatbestands birgt daher die Gefahr einer zusätzlichen Fragmentierung des Strafrechts und kann zu systematischen Unübersichtlichkeiten sowie Abgrenzungsproblemen zwischen den einzelnen Normen führen.

Unabhängig davon wirft die konkrete Ausgestaltung des § 201b StGB eigenständige dogmatische Bedenken auf. Insbesondere zentrale Tatbestandsmerkmale wie der „Anschein eines tatsächlichen Geschehens“ oder die „Eignung zur erheblichen Ansehensschädigung“ eröffnen erhebliche Auslegungsspielräume. In einem digitalen Umfeld, in dem Inhalte kontextabhängig sind und unterschiedliche Bedeutungen annehmen können, führt dies zu zusätzlichen Abgrenzungsschwierigkeiten und kann die Rechtsanwendung erheblich erschweren.

Der neu vorgesehene § 202e StGB zur unbefugten Überwachung mittels Informations- und Kommunikationstechnik dient der Umsetzung der Richtlinie (EU) 2024/1385 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt. Auch wenn damit ein legitimes Ziel verfolgt wird, ist festzustellen, dass vergleichbare Sachverhalte bereits durch bestehende Vorschriften, wie etwa § 201a StGB, §§ 202a ff. StGB, erfasst werden können. Es stellt sich somit die Frage, ob ein weiterer Tatbestand tatsächlich zur Rechtsklarheit beiträgt oder vielmehr zusätzliche Komplexität schafft.

Übergreifend ist festzustellen, dass mehrere der vorgesehenen Regelungen zentrale Begriffe verwenden, die einer präzisen juristischen Konturierung bedürfen.

Auswirkungen auf Diensteanbieter und Anbieter von Internetzugangsdiensten

Für Diensteanbieter sowie Anbieter von Internetzugangsdiensten ergeben sich aus den vorgeschlagenen Regelungen erhebliche praktische Herausforderungen. Dabei sind die Rollen und Pflichten der beiden Gruppen unterschiedlich ausgestaltet, führen jedoch jeweils zu relevanten praktischen Belastungen.

Für Diensteanbieter (insbesondere Plattformen und Hoster) sind bereits heute nach dem Digital Services Act (DSA) Mechanismen zur Entfernung illegaler Inhalte vorgesehen. Diese Verpflichtung setzt jedoch voraus, dass eine rechtssichere Einordnung der Inhalte möglich ist. Unklare oder auslegungsbedürftige strafrechtliche Tatbestände erschweren diese Einordnung erheblich.

Hinzu kommt, dass zentrale Voraussetzungen strafrechtlicher Normen für Diensteanbieter regelmäßig nicht überprüfbar sind. Insbesondere bei antragsabhängigen Delikten ist häufig nicht erkennbar, ob ein Strafantrag vorliegt oder ob die meldende Person tatsächlich die betroffene Person ist. Gleichzeitig steigen die Anforderungen an die Prüfung und Bewertung gemeldeter Inhalte, was zu einem erheblichen zusätzlichen Compliance-Aufwand führt.

Dies wird durch die Rechtsprechung zu den Prüfpflichten von Host-Providern zusätzlich verstärkt. Danach ist der Anbieter bei hinreichend konkreten Beanstandungen verpflichtet, den betroffenen Inhalt nicht lediglich summarisch zu bewerten, sondern ein abgestuftes Prüfverfahren durchzuführen. Hierzu gehört insbesondere, die Beanstandung an den verantwortlichen Nutzer weiterzuleiten und ihm Gelegenheit zur Stellungnahme zu geben (vgl. BGH, Urt. v. 25.10.2011 – VI ZR 93/10). Bestreitet dieser die Rechtsverletzung, hat der Anbieter wiederum den Beschwerdeführer zur weiteren Substantiierung und gegebenenfalls zur Vorlage von Nachweisen aufzufordern (vgl. OLG Düsseldorf, Urt. v. 08.08.2014 – I-16 U 30/14).

Dies gilt insbesondere vor dem Hintergrund, dass Plattformen und andere Hoster regelmäßig weder über vollständige Kontextinformationen noch über gesicherte Erkenntnisse zur Einwilligung betroffener Personen verfügen. Gerade dieses „Ping-Pong“-Verfahren verdeutlicht, dass Diensteanbieter letztlich auf die Mitwirkung der Beteiligten angewiesen sind und keine eigenständige, abschließende Tatsachenaufklärung leisten können.

In der Praxis entsteht hieraus ein erheblicher Druck, Inhalte im Zweifel eher zu entfernen, um rechtliche Risiken zu vermeiden. Denn verbleiben nach Durchführung des Prüfverfahrens Unsicherheiten, trägt der Anbieter das Risiko einer fehlerhaften Entscheidung und sieht sich potenziellen Haftungsansprüchen ausgesetzt.

Ein solcher Effekt des sogenannten Overblockings kann dazu führen, dass auch rechtmäßige Inhalte gelöscht werden, etwa aus den Bereichen Kunst, Satire oder journalistische Berichterstattung. Dies wiederum zieht vertragliche Haftungsrisiken für Diensteanbieter nach sich. Die im Entwurf vorgesehenen Ausnahmen für berechtigte Interessen sind zwar grundsätzlich zu begrüßen, bieten jedoch nur

eingeschränkte Rechtssicherheit, da auch sie einer wertenden Einzelfallprüfung unterliegen.

Für Anbieter von Internetzugangsdiensten ergeben sich demgegenüber vor allem mittelbare Belastungen. Zwar sind sie in der Regel nicht in die inhaltliche Prüfung oder Moderation von Inhalten eingebunden, können jedoch im Rahmen von Sperrungs- oder Durchleitungsmaßnahmen faktisch betroffen sein. Auch hier besteht die Gefahr, dass unklare rechtliche Vorgaben zu Unsicherheiten bei der Umsetzung führen und im Ergebnis ebenfalls zu Overblocking-Effekten beitragen können.

Prävention und Medienkompetenz

Der Entwurf setzt in seiner derzeitigen Ausgestaltung primär auf strafrechtliche Instrumente. Dabei ist zu berücksichtigen, dass das Strafrecht regelmäßig erst bei bereits eingetretenen Rechtsgutverletzungen greift und nur begrenzt präventiv wirkt. Eine nachhaltige und effektive Bekämpfung digitaler Gewalt erfordert daher ergänzende präventive Ansätze.

Neben technischen Schutzmechanismen und klaren Melde- und Löschverfahren kommt hierbei insbesondere der Stärkung der Medienkompetenz eine zentrale Bedeutung zu. Nutzer:innen müssen in die Lage versetzt werden, digitale Inhalte kritisch zu bewerten, Manipulationen zu erkennen und digitale Technologien – insbesondere im Bereich der künstlichen Intelligenz – verantwortungsvoll zu nutzen. Gerade im Umgang mit Deepfakes ist es entscheidend, ein grundlegendes Verständnis für Funktionsweisen, Risiken und Missbrauchspotenziale zu vermitteln.

Die Stärkung von Medienkompetenz sollte daher als wesentlicher Bestandteil einer umfassenden Strategie zur Bekämpfung digitaler Gewalt verstanden werden. Dies umfasst sowohl den schulischen Bereich als auch außerschulische Bildungsangebote und Maßnahmen der allgemeinen Aufklärung. Eine entsprechend breite gesellschaftliche Sensibilisierung kann dazu beitragen, die Verbreitung schädlicher Inhalte bereits im Vorfeld einzudämmen.

Sonstiges

Der Entwurf geht von einem finanziellen Aufwand für die Wirtschaft von rund 53.000 EUR aus. Dieser berechnet sich nach einem zeitlichen Aufwand pro Fall von 10 Minuten, bei geschätzten 6.400 Fällen pro Jahr und durchschnittlichen Personalkosten von 49,30 EUR pro Stunde. Allerdings wird bereits im Entwurf

darauf hingewiesen, dass die Zahl der zu erwartenden Fälle nicht genau ermittelt werden kann.

Die Zahlen entsprechen den Zahlen aus dem Diskussionsentwurf von 2024, jedoch enthält der vorliegende Referentenentwurf weitere Pflichten für den Diensteanbieter, wie die Anfertigung einer Kopie des Inhalts oder die unverzügliche Information des betroffenen Nutzers, die bei der bisherigen Kalkulation nicht berücksichtigt wurden. Allein dies lässt eine Überprüfung und mögliche Anpassung der Zahlen notwendig erscheinen. Es wird daher angeregt, im weiteren Gesetzgebungsverfahren die Kalkulation des Aufwands und entsprechend auch die Kalkulation der Kosten zu überprüfen, und bei Bedarf anzupassen. Ferner sollte beachtet werden, dass in solchen Fällen Möglichkeiten für eine angemessene Kompensation bestehen.

Vor dem Hintergrund der in den letzten Jahren deutlich gestiegenen Anzahl von Datenabfragen sowie der wiederholten Erweiterung gesetzlicher Grundlagen sollte sichergestellt werden, dass die praktischen Abläufe für Diensteanbieter und Anbieter von Internetzugangsdiensten möglichst effizient und standardisiert ausgestaltet werden. Hierzu können insbesondere einheitliche Anfrageformate sowie technische Schnittstellen zur strukturierten Übermittlung von Auskunftsersuchen beitragen. Soweit technisch und rechtlich möglich, sollten zudem digitale und automatisierte Prozesse genutzt werden, um die Bearbeitung entsprechender Anfragen ressourcenschonend zu unterstützen.

Zusammenfassende Bewertung und Fazit

Grundsätzlich ist es begrüßenswert, Opfern von digitaler Gewalt die Möglichkeit zu geben, rechtliche Ansprüche konsequent durchzusetzen. Dazu ist in manchen Fällen die Herausgabe von Daten zur Identifikation unvermeidlich. Es ist jedoch sehr wichtig, dass diese Fälle genau reguliert und geprüft werden. Aus Sicht des eco liefert der vorliegende Entwurf hier einige sinnvolle Ansätze, gerade die Voraussetzung des richterlichen Vorbehalts ist hier hervorzuheben. Dennoch gibt es einige Punkte, die im weiteren Gesetzgebungsprozess genauer beleuchtet werden sollten.

Das Verhältnis zu bestehenden und parallel geplanten Regelungen zur Vorratsdatenspeicherung sollte dabei ebenso berücksichtigt werden wie die Gefahr widersprüchlicher Vorgaben im Zusammenspiel verschiedener Rechtsrahmen.

Zudem sollte eine Möglichkeit zur anonymen Stellungnahme der betroffenen Nutzer so ausgestaltet werden, dass sie praktikabel für Diensteanbieter bleibt und keine zusätzliche Verlagerung staatlicher Ermittlungsaufgaben auf private Unternehmen erfolgt.

Auch die vorgesehene Verkürzung der Rechtsmittelfrist auf zwei Wochen erscheint kritisch und sollte im Hinblick auf die praktische Umsetzbarkeit sowie die angemessene Wahrung der Verfahrensrechte der Beteiligten nochmals überprüft

werden.

Besonders der Aufwand für die Wirtschaft sollte überprüft werden, da hier bisher nur mit ungefähren Zahlen gearbeitet wurde. An anderen Stellen, wie der Anordnung der Sperrung eines Nutzerkontos, muss sichergestellt werden, dass die hier geplanten Regelungen erforderlich sind sowie nicht im Widerspruch mit anderen, auch internationalen Regelungen stehen. Andernfalls ist zu befürchten, dass Anbieter in rechtliche Zwickmühlen geraten, wenn unterschiedliche Regelungen aufeinandertreffen.

Darüber hinaus ist sicherzustellen, dass der Prozess der Datenherausgabe für Diensteanbieter und Anbieter von Internetzugangsdiensten möglichst standardisiert und automatisiert ausgestaltet wird. Die entsprechenden Datenabfragen sollten auf Basis eines vorgegebenen Formblatts erfolgen und – soweit technisch möglich – über standardisierte Schnittstellen, etwa ETSI-basierte Schnittstellen, übermittelt werden, um den administrativen Aufwand zu reduzieren und eine effiziente Umsetzung zu gewährleisten.

Zudem ist der den Anbietern entstehende Aufwand angemessen zu berücksichtigen und entsprechend zu entschädigen. Vor dem Hintergrund der erheblichen Unsicherheiten hinsichtlich der künftig zu erwartenden Fallzahlen sowie der zusätzlich im Referentenentwurf vorgesehenen Pflichten erscheint es sachgerecht, eine ausdrückliche Kostenerstattung im Einzelfall vorzusehen. Eine entsprechende Regelung in Anlehnung an § 23 JVEG würde hierbei einen geeigneten und rechtssicheren Rahmen bieten.

Der Referentenentwurf greift im strafrechtlichen Teil ein zentrales gesellschaftliches Problem auf, schafft in seiner aktuellen Ausgestaltung jedoch rechtliche Unsicherheiten und praktische Umsetzungsprobleme für Diensteanbieter. Eine Überarbeitung mit Blick auf klarere Tatbestände, eine bessere systematische Einordnung sowie eine stärkere Berücksichtigung präventiver Ansätze erscheint daher angezeigt.

Nur durch ein ausgewogenes Zusammenspiel von klaren rechtlichen Rahmenbedingungen, praktikablen Vorgaben für Diensteanbieter und einer gestärkten Medienkompetenz in der Bevölkerung kann das Ziel eines wirksamen Schutzes vor digitaler Gewalt nachhaltig erreicht werden.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.