Stellungnahme zum Referentenentwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor Digitaler Gewalt

Executive Summary

Der Bundesverband Digitale Wirtschaft (BVDW) begrüßt den Referentenentwurf zum Schutz vor digitaler Gewalt und unterstützt das Ziel, digitale Räume sicherer zu gestalten. Der Entwurf verbindet strafrechtliche Ergänzungen mit einer verbesserten zivilrechtlichen Rechtsdurchsetzung und folgt damit einem grundsätzlich sachgerechten Ansatz. Der BVDW bedankt sich für die Möglichkeit, eine Stellungnahme zu dem Referentenentwurf abgeben zu können.

Auf strafrechtlicher Ebene begrüßt der BVDW insbesondere die Erweiterung des § 184k StGB zur Erfassung bildbasierter sexualisierter Gewalt sowie den neuen § 201b StGB zum Schutz vor täuschenden Inhalten. Zugleich betont der Verband, dass die neuen Tatbestände eng auf konkrete Persönlichkeitsrechtsverletzungen begrenzt bleiben müssen, um grundrechtlich geschützte Bereiche wie Meinungsfreiheit, Kunst und Satire nicht unverhältnismäßig zu beeinträchtigen. Zudem sollte die Begriffssystematik stärker an die europäische KI-Verordnung (KI-VO) angenähert werden, um Rechtsunsicherheiten beim Umgang mit Deepfakes zu vermeiden.

Im zivilrechtlichen Teil bewertet der BVDW den richterlich kontrollierten Auskunftsanspruch sowie die Möglichkeit präventiver Kontosperren als grundsätzlich geeignete Instrumente. Kritisch ist jedoch der sehr weite Anwendungsbereich, der neben klassischen Plattformen auch Hosting- und Infrastrukturdienstleister erfasst und damit insbesondere für kleinere Anbieter erhebliche praktische und organisatorische Belastungen erzeugt. Die im Entwurf unterstellte weitgehende Automatisierbarkeit bildet diese Realität nicht angemessen ab. Zugleich muss die Ausgestaltung sicherstellen, dass Datenschutzgrundsätze gewahrt und der Schutz des anonymen Diskurses nicht durch unverhältnismäßige Identifizierungs- oder Überwachungseffekte geschwächt wird.

Der BVDW hält daher fest: Nicht neue Pflichten als solche sind das Kernproblem, sondern eine Ausgestaltung, die technisch realisierbar, rechtssicher und grundrechtssensibel sein muss. Effektiver Opferschutz gelingt nur, wenn gesetzliche Anforderungen an digitale Dienste die praktischen Umsetzungsbedingungen, datenschutzrechtlichen Grenzen und die Bedeutung anonymer Kommunikation von Anfang an mitberücksichtigen.

Stellungnahme

1) Einleitung

Soziale Netzwerke, Foren und digitale Plattformen sind wichtige Orte des öffentlichen Diskurses. Gerade deshalb darf die digitale Öffentlichkeit kein Raum sein, in dem Einschüchterung, Entwürdigung oder gezielte Rechtsverletzungen unwidersprochen bleiben. Digitale Gewalt ist kein abstraktes Phänomen. Beleidigende Beiträge, Drohnachrichten oder die unerwünschte Verbreitung persönlicher und manipulierter intimer Inhalte treffen konkrete Menschen, deren Rechte und Würde verletzt werden – häufig mit langfristigen Belastungen für die Betroffenen. Besonders gravierend sind Fälle, in denen technische Möglichkeiten gezielt missbraucht werden, um andere bloßzustellen. Dass solche Übergriffe nicht hingenommen werden dürfen, muss Konsens sein. Vor diesem Hintergrund begrüßt der Bundesverband Digitale Wirtschaft (BVDW) e. V. ausdrücklich, dass der Gesetzgeber das Thema digitale Gewalt aktiv aufgreift. Der vorliegende Gesetzentwurf setzt ein wichtiges Signal: Rechtsstaatlichkeit und gesellschaftliche Verantwortung gelten auch im digitalen Raum. Als Vertreter einer vielfältigen digitalen Wirtschaft unterstützen wir das Ziel, digitale Räume sicherer und verlässlicher zu gestalten, und sehen uns als konstruktiven Mitgestalter beim Gelingen dieses Prozesses.

Der vorliegende Entwurf folgt einem zweistufigen Ansatz, der auf strafrechtliche Ergänzungen sowie eine verbesserte zivilrechtliche Rechtsdurchsetzung setzt. Diese Systematik bildet entsprechend den inhaltlichen Rahmen der vorliegenden Stellungnahme. Im Folgenden soll auf die einzelnen Regelungsbereiche eingegangen werden, die aus Sicht der Digitalwirtschaft einzuordnen sind.

2) Strafrechtliche Säule: Schutzwirkung, Rechtssicherheit und europäische Kohärenz

2.1) Zielsetzung des Entwurfs und strafrechtliche Schließung zentraler Schutzlücken

Digitale Gewalt von Hassrede über Doxing bis hin zu bildbasierter sexualisierter Gewalt kann erhebliche Persönlichkeitsrechtsverletzungen verursachen. Insbesondere der Bereich der sexualisierten Deepfakes zeigt, dass die bestehenden strafrechtlichen Regelungen digitale Gewalt und Deepfakes nur begrenzt erfassen und Betroffene bisher nicht in allen Konstellationen hinreichend geschützt sind. Diese Gemengelage hatte bereits eine Analyse des BVDW vom Gesetzesantrag des Freistaat Bayern im Bundesrat zum Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes (BR-Drs. 222/24) im Jahr 2024 festgestellt (Analyse hier abrufbar). Vor diesem Hintergrund ist das Ziel des Entwurfs, bestehende Schutzlücken zu schließen und digitale Gewalt effektiver zu erfassen, grundsätzlich nachvollziehbar und zu begrüßen.

Der strafrechtliche Teil des Entwurfes adressiert insbesondere solche Konstellationen, in denen Deepfakes gezielt zur Demütigung, Bloßstellung oder Verletzung der Intim- und Privatsphäre eingesetzt werden. Die geplante Erweiterung des § 184k StGB zur Erfassung bildbasierter sexualisierter Gewalt setzt an einer zentralen Unrechtskonstellation an und reagiert auf Fälle pornographischer Deepfakes, die bislang nur unzureichend oder mit erheblichen Abgrenzungsproblemen strafrechtlich erfasst werden konnten. Insoweit sind die Klarstellung und die ausdrückliche Einbeziehung solcher Inhalte geeignet, den Schutz der Betroffenen spürbar zu stärken und ein wichtiges Signal für das Ziel eines effektiveren Vorgehens gegen solche Taten.

Die Einführung eines neuen Straftatbestandes zum Schutz von Persönlichkeitsrechten vor täuschenden Inhalten in § 201b StGB stellt darüber hinaus einen eigenständigen und systematisch relevanten Schritt dar. Der Entwurf erkennt damit an, dass nicht sexualisierte, aber täuschend echt wirkende Inhalte ebenfalls erhebliche Persönlichkeitsrechtsverletzungen verursachen können und räumt konsequenterweise auch gegen die Verwendung solcher Inhalte ein mögliches Vorgehen ein. Positiv ist hierbei, dass nicht die zugrunde liegende Technologie pauschal kriminalisiert wird, sondern an die konkrete Verletzung von Rechtsgütern durch täuschende Inhalte angeknüpft wird.

Ebenso ist zu begrüßen, dass im Vergleich zum vorherigen Bundesratsentwurf (BR-Drs. 222/24) zentrale Kritikpunkte an der Formulierung von § 201b StGB aufgegriffen wurden und der Tatbestand deutlich gestrafft ist. Insbesondere wurde die Verwendung unklarer oder weit gefasster Begriffe eingeschränkt, was die Systematik schärft und die Anwendbarkeit der Norm grundsätzlich erleichtern kann.

Zugleich bedarf dieser Tatbestand aber einer besonders präzisen Auslegung, da er ein weites Spektrum möglicher Anwendungsfälle adressiert und damit berührungsanfällig für grundrechtlich geschützte Kontexte wie Meinungsäußerung, Kunst oder Satire ist. Entsprechende Ausnahmen, insbesondere für die Wahrnehmung berechtigter Interessen, sind daher von großer Bedeutung. Entscheidend wird daher sein, diese möglichst klar zu formulieren und dass die strafrechtliche Relevanz klar an die Täuschungswirkung und die konkrete Persönlichkeitsrechtsverletzung gekoppelt bleibt.

Flankierend ergänzt der Entwurf die strafrechtlichen Regularien durch einen neuen Tatbestand zur unbefugten Überwachung mittels Informations- oder Kommunikationstechnik. Auch dieser Ansatz ist grundsätzlich folgerichtig, da digitale Überwachung und Nachstellung zunehmend mit technischen Mitteln erfolgen und bestehende Normen diese Erscheinungsformen nicht immer eindeutig abdecken.

Insgesamt ist festzuhalten, dass der Entwurf mit den vorgesehenen neuen und erweiterten Straftatbeständen reale Schutzlücken adressiert und deutlich macht, dass digitale Gewalt nicht als bloßes Randphänomen, sondern als ernstzunehmende Rechtsgutsverletzung verstanden wird.

2.2) Präzision, Grundrechtswahrung und Kohärenz mit dem europäischen Rechtsrahmen

Gleichzeitig ist aus Sicht der digitalen Wirtschaft entscheidend, dass strafrechtliche Regelungen präzise, verhältnismäßig und systematisch eingebettet sind.

Der Referentenentwurf verwendet den Begriff Deepfake zwar ausdrücklich in der Gesetzesbegründung, verzichtet jedoch auf eine Legaldefinition und knüpft nicht erkennbar an die im europäischen Recht bereits etablierte Begriffsbestimmung an. Verwendet werden in den neuen Straftatbeständen unterschiedliche Begriffe, wie veränderte Bildaufnahmen oder veränderte Inhalte, die einen bestimmten Anschein erwecken.

Die KI-VO definiert Deepfakes technologieneutral als durch KI erzeugte oder manipulierte Bild-, Ton- oder Videoinhalte, die realen Personen oder Ereignissen ähneln und als echt erscheinen können. Diese Definition bildet den Referenzrahmen für Transparenz- und Kennzeichnungspflichten auf EU-Ebene und unterscheidet bewusst nicht nach der intendierten Nutzung oder dem Schadenseintritt.

Diese begriffliche Divergenz birgt das Risiko einer inkonsistenten Abgrenzung zwischen strafbaren Inhalten und solchen, die zwar kennzeichnungspflichtig, aber grundsätzlich zulässig sind. Zwar scheint es gut nachvollziehbar, dass jedenfalls im Rahmen des neuen § 184k StGB (Verletzung der Intimsphäre durch Bildaufnahmen) nur bestimmte intime Bildaufnahmen (und wohl auch Videoaufnahmen) erfasst werden sollten und daher nicht die Deepfake-Definition der KI-VO genutzt wurde. Für § 201b StGB (Verletzung von Persönlichkeitsrechten durch täuschende Inhalte), der den Schutz des Persönlichkeitsrechts durch alle schädlichen Inhalte zum Gegenstand hat, hätte dennoch eine Angleichung an die KI-VO-Definition erwogen werden können.

Aus Sicht des BVDW wäre es daher sachgerecht, den strafrechtlichen Ansatz stärker an die Begriffslogik des KI VO anzulehnen und damit Kohärenz zwischen europäischem KI-Recht und nationalem Strafrecht herzustellen.

Darüber hinaus werden auch hier in den vorgeschlagenen Straftatbeständen Begrifflichkeiten genutzt, die ihrerseits einer Erklärung bedürfen und nicht in allen Fällen aus sich heraus klar abgrenzbar sind. So wird es beispielsweise bei der aktuellen Formulierung des § 184k StGB in der Praxis erheblichen Abgrenzungsbedarf geben, wann etwas „in sexuell bestimmter Weise“

abgebildet wurde oder ab wann der „Anschein erweckt“ wurde, dass etwas abgebildet wurde. Im Rahmen des § 201b StGB wird beispielsweise zu klären sein, wann der Anschein eines „tatsächlichen Geschehens“ besteht.

Unabhängig von der dogmatischen Ausgestaltung gilt, dass die Wirksamkeit eines Gesetzes nicht allein an der Existenz neuer Strafnormen gemessen werden kann. Neben Strafnormen bleibt die praktische Durchsetzung zentral. Erst damit entfaltet ein Gesetz seine Wirkung. Damit dies geschehen kann, müssen die Anforderungen technisch umsetzbar und sowohl für die Betroffenen als auch für die Unternehmen praktikabel ausgestaltet sein.

Kernaspekte im strafrechtlichen Teil:

- **Lückenschluss:** Der BVDW begrüßt die konsequente strafrechtliche Erfassung digitaler Gewalt, insbesondere bei sexualisierten Deepfakes (§ 184k StGB).
- **Rechtsgutschutz:** Der neue § 201b StGB muss den Fokus strikt auf die Persönlichkeitsrechtsverletzung legen.
- **Grundrechtssicherung:** Eine präzise Tatbestandsauslegung ist zwingend erforderlich, um Meinungsfreiheit, Kunst und Satire wirksam zu schützen.
- **EU-Harmonisierung:** Die Verwendung des Begriffs „Deepfakes“ muss so weit wie möglich an die Begriffslogik der europäischen KI-VO angeglichen werden.
- **Rechtssicherheit:** Eine klare Abgrenzung zwischen strafbaren Inhalten und lediglich kennzeichnungspflichtigen Inhalten ist zur Vermeidung von Divergenzen essenziell.

3) Zivilrechtliche Rechtsdurchsetzung: Zwischen Schutzwirkung und technischer Realität

3.1) Anwendungsbereich und Erfüllungsaufwand

Der zivilrechtliche Teil des Entwurfs verfolgt einen zweistufigen Ansatz: die erleichterte Täteridentifizierung durch richterlich kontrollierte Auskunfts- und Beweissicherungsansprüche (§§ 2, 3 GgdG-E) sowie die präventive Sperrung von Nutzerkonten bei schwerwiegenden Rechtsverletzungen (§ 4 GgdG-E).

Der BVDW unterstützt ausdrücklich das Ziel, die Rechtsdurchsetzung für Betroffene praktikabler zu gestalten. Eine wehrhafte digitale Öffentlichkeit erfordert effektive Mechanismen, um Persönlichkeitsrechte im Netz zu schützen. Damit die vorgesehenen Instrumente ihre beabsichtigte Wirkung in der Praxis entfalten können, bedarf der Entwurf jedoch an mehreren Stellen einer präziseren prozessual technischen Ausgestaltung. Nur so lassen sich technisch und wirtschaftlich unerfüllbare Belastungen für die Digitale Wirtschaft vermeiden, verfassungsrechtliche Schutzstandards wahren und Zielkonflikte reduzieren.

Aus Sicht der digitalen Wirtschaft ist dabei zunächst hervorzuheben, dass der Anwendungsbereich sehr weit gefasst ist. Der Entwurf adressiert nicht nur Online-Plattformen, sondern greift die Definition des Art. 3 lit. g Ziff. iii DSA auf. Damit sind neben Online-Plattformen auch Web-Hosting-Dienste und Cloud-Hosting-Dienste inbegriffen. Der Entwurf erfasst somit eine Vielzahl sehr unterschiedlicher Dienste- und Geschäftsmodelle – einschließlich solcher Anbieter, die keine klassischen „Plattform-Moderationsstrukturen“ vorhalten, sondern primär Infrastruktur- oder Hosting-Leistungen erbringen.

Damit werden – je nach Ausgestaltung des jeweiligen Dienstes – auch solche Anbieter erfasst, die nicht über die etablierten Strukturen großer Plattformen verfügen, sondern häufig technisch und organisatorisch deutlich schlanker aufgestellt sind. Gerade für kleine und mittlere Unternehmen sowie spezialisierte Hosting-Anbieter bedeutet dies in der Praxis einen erheblichen Aufbau von Compliance-Prozessen: gerichtsfeste Prüfung, sichere Datenhaltung, fristgerechte Kommunikation mit Gerichten und die Umsetzung von Sicherungsanordnungen. Vor diesem Hintergrund erscheint der im Entwurf ausgewiesene Erfüllungsaufwand nicht realistisch. Die Annahme eines „hohen Grades an Automatisierung“ verkennt, dass es sich auch um rechtlich und organisatorisch anspruchsvolle Verfahren handelt, die eine sorgfältige Einzelfallprüfung erfordern, um Haftungsrisiken und Fehlidentifikationen zu vermeiden.

3.2) Auskunftsanspruch und Beweissicherung

Der Ansatz, den Opferschutz durch effektivere Rechtsdurchsetzung zu stärken, ist ausdrücklich zu begrüßen. Eine wehrhafte digitale Öffentlichkeit erfordert Mechanismen, um Betroffene vor Gewalt zu schützen. Der Entwurf verankert den Auskunftsanspruch ausdrücklich als richterlich kontrolliertes Verfahren.

Der dabei vorgesehene strikte Richtervorbehalt ist zentral: Eine Datenherausgabe darf nur nach sorgfältiger Prüfung erfolgen, ob tatsächlich eine strafbare Rechtsverletzung vorliegt. In der praktischen Umsetzung ist allerdings sicherzustellen, dass strukturelle Engpässe vermieden und zeitnahe Entscheidungen gewährleistet werden. Die Aufdeckung von Nutzeridentitäten berührt die Meinungsfreiheit (Art. 5 Abs. 1 GG) sowie das Fernmeldegeheimnis (Art. 10 Abs. 1 GG). Ein hoher Prüfungsmaßstab ist essenziell, um den Schutz des anonymen Diskurses zu wahren und missbräuchliche Inanspruchnahmen (z. B. SLAPP-Klagen zur Unterbindung legitimer Kritik) wirksam zu verhindern. Zugleich muss das Auskunftsverfahren so gestaltet sein, dass rechtmäßige Kritik nicht durch eine zu niedrige Schwelle bei der Identitätsfeststellung unterbunden wird und missbräuchliche Inanspruchnahmen (etwa über strategische Klageinstrumente) wirksam eingehegt werden. Bei der Ausgestaltung der Regelungen zur Beweissicherung und Datenübermittlung ist darauf zu achten, dass bestehende datenschutzrechtliche Grundsätze, insbesondere die Datenminimierung und Zweckbindung, konsistent berücksichtigt werden. Zusätzliche spezialgesetzliche Vorgaben sollten klar auf diese bestehenden Rahmenbedingungen abgestimmt sein, um widersprüchliche Pflichten und Rechtsunsicherheiten in der praktischen Umsetzung zu vermeiden.

3.3) Kontosperren

Der BVDW unterstützt das Ziel, Betroffene in besonders gravierenden Konstellationen auch präventiv vor weiteren Rechtsverletzungen zu schützen. Die in § 4 GgdG-E vorgesehene richterlich angeordnete Kontosperre ist hierfür grundsätzlich ein nachvollziehbares Instrument, weil sie – anders als eine reine Inhaltsentfernung – die Wiederholungsgefahr adressiert und damit über den Einzelfall hinauswirken soll.

Der im Entwurf angelegte „Read only"-Ansatz trägt dem Anliegen Rechnung, präventive Kontosperren nicht als vollständigen Ausschluss von der digitalen Teilhabe auszugestalten. Nach § 4 Abs. 2 GgdG-E bleibt die passive Nutzung eines Dienstes grundsätzlich möglich, während das Veröffentlichen, Kommentieren und Teilen untersagt wird.

Zugleich geht eine solche differenzierte Nutzungsbeschränkung mit erheblichen technischen und organisatorischen Herausforderungen einher. Die Umsetzung erfordert tiefgreifende Eingriffe in bestehende Systemarchitekturen und ist je nach Dienst, Struktur und Größenklasse unterschiedlich komplex. Der Read-only-Ansatz kann daher nur dort Wirksamkeit entfalten, wo er technisch realisierbar und wirtschaftlich zumutbar ist; andernfalls besteht die Gefahr, dass die Maßnahme in der Praxis entweder ins Leere läuft oder faktisch auf weitergehende Sperrmodelle hinausläuft. Daher ist eine Orientierung an der individuellen Plattformlogik notwendig.

Zentral ist außerdem die Formulierung, dass Diensteanbieter Umgehungsversuche – insbesondere die Eröffnung neuer Konten während des Sperrzeitraums – nur „soweit technisch und wirtschaftlich möglich und zumutbar" unterbinden müssen. Diese Zumutbarkeitsschwelle ist aus Sicht der Digitalwirtschaft ein notwendiges Korrektiv, weil sie anerkennt, dass „Umgehungsverhinderung" nicht grenzenlos erwartet werden kann und die Umsetzung je nach Dienst, Architektur und Größenklasse erheblich variiert. Dennoch wäre es hilfreich, einige der Begriffe in diesem Paragrafen klarer zu definieren. Die Verpflichtung zur Sperrung von Accounts besteht für einen „angemessenen Zeitraum" (§ 4 Abs. 2 Satz 3 GgdG-E). Eine konkrete Zeitspanne wäre hilfreich, um Rechtssicherheit bei der Umsetzung zu schaffen. Ebenso besteht die Verpflichtung zur Verhinderung von Umgehungen (§ 4 Abs. 2 Satz 3 GgdG-E) nur, soweit dies „technisch und wirtschaftlich möglich und zumutbar" ist. Hier wäre es hilfreich zu wissen, wo die Grenzen der Zumutbarkeit in diesem Kontext liegen.

Gleichzeitig zeigt sich hier ein Wirkungs- und Abwägungskonflikt: Je konsequenter eine Umgehung verhindert werden soll, desto stärker entsteht in der Praxis der Bedarf, Konten verlässlich derselben Person zuzuordnen. Das kann – je nach gewählter Lösung – den Anreiz erhöhen, zusätzliche Identifikations- oder Verknüpfungsdaten zu erheben oder länger vorzuhalten. Damit steigt das Risiko einer Kollision mit dem datenschutzrechtlichen Grundsatz der Datenminimierung, wonach personenbezogene Daten auf das für den Zweck notwendige Maß zu beschränken sind.

Wo Nutzer*innen dem Gericht nicht bekannt sind, können Diensteanbieter dazu verpflichtet werden, diese über eingeleitete Verfahren zu unterrichten. Ebenso müssen Diensteanbieter die Einreichung der Stellungnahme von Nutzer*innen anonym oder unter einem Pseudonym ermöglichen (§ 6 Abs. 2 S. 2 GgdG-E). Dies betrifft insbesondere die vorgesehene Pflicht zur Anfertigung von Screenshots der angegriffenen Inhalte (§ 6 Abs. 2 Nr. 3 GgdG-E). Es sei darauf hingewiesen, dass die technische Umsetzung durchaus komplex ist.

Kernaspekte im zivilrechtlichen Teil:

- **Realistische Aufwandsschätzung:** Korrektur der Kostenannahmen, Anerkennung des hohen manuellen Prüfungsaufwands statt fiktiver Vollautomatisierung.
- **Richtervorbehalt und Grundrechtsschutz:** Der richterlich kontrollierte Auskunftsanspruch ist richtig, muss aber so ausgestaltet sein, dass anonymer Diskurs, Meinungsfreiheit und Schutz vor missbräuchlicher Inanspruchnahme gewahrt bleiben.
- **Rechtssicherheit bei Umgehungsschutz:** Beibehaltung und Präzisierung der Zumutbarkeitsschwelle zur Vermeidung übermäßiger Überwachungspflichten.
- **Praktikable Ausgestaltung der Kontosperren**: Präventive Kontosperren können in schwerwiegenden Fällen sinnvoll sein, müssen aber technisch realisierbar und an der jeweiligen Plattformlogik ausgerichtet sein.
- **Umgehungsschutz:** Anforderungen zu Kontosperren und dem Umgehungsschutz müssen technisch praktikabel, zumutbar und mit Datenschutzgrundsätzen vereinbar sein.

4) Fazit

Der Referentenentwurf setzt ein wichtiges politisches Signal: Digitale Gewalt wird nicht länger als Randerscheinung behandelt, sondern als ernstzunehmende Verletzung von Persönlichkeitsrechten im digitalen Raum. Der gewählte Ansatz, strafrechtliche Ergänzungen mit Instrumenten der zivilrechtlichen Rechtsdurchsetzung zu verbinden, ist dabei grundsätzlich geeignet, bestehende Schutzlücken zu adressieren.

Ob das Gesetz seine Schutzwirkung tatsächlich entfalten kann, entscheidet sich jedoch weniger an der Schaffung neuer Instrumente als an deren konkreter Ausgestaltung. Der Erfolg des Entwurfs hängt maßgeblich davon ab, ob die Regelungen präzise und mit den technischen Realitäten digitaler Dienste kompatibel umgesetzt werden (können).

Ob das Gesetz seine Schutzwirkung tatsächlich entfalten kann, entscheidet sich jedoch weniger an der Schaffung neuer Instrumente als an deren konkreter Ausgestaltung. Der Erfolg des Entwurfs hängt maßgeblich davon ab, ob die Regelungen präzise formuliert, grundrechtssensibel angewendet und mit den technischen Realitäten digitaler Dienste kompatibel ausgestaltet werden. Eine wirksame Umsetzung erfordert daher zweierlei: Zum einen müssen die neuen Straftatbestände hinreichend bestimmt bleiben und sich kohärent in den europäischen Rechtsrahmen einfügen. Zum anderen müssen Auskunftsansprüche, Beweissicherung und Kontosperren so ausgestaltet sein, dass sie unterschiedlichen Dienste- und Geschäftsmodellen gerecht werden, praktikabel umsetzbar bleiben und datenschutzrechtliche sowie grundrechtliche Anforderungen wahren. Nur wenn technologische Grenzen, Datenschutz und die Bedeutung des anonymen Diskurses konsequent mitgedacht werden, lässt sich effektiver Opferschutz erreichen, ohne unverhältnismäßige Folgewirkungen für digitale Dienste und die digitale Öffentlichkeit zu erzeugen.

Bundesverband Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e. V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Mit seinen Mitgliedern aus der gesamten Digitalen Wirtschaft gestaltet der BVDW bereits heute die Zukunft – durch kreative Lösungen und modernste Technologien. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle setzt der Verband auf faire und klare Regeln und tritt für innovationsfreundliche Rahmenbedingungen ein. Dabei hat der BVDW immer Wirtschaft, Gesellschaft und Umwelt im Blick. Neben der DMEXCO, der führenden Fachmesse für Digitales Marketing und Technologien, und dem Deutschen Digital Award richtet der BVDW auch den CDR-Award, die erste Preisverleihung im DACH-Raum für Digitale Nachhaltigkeit und Verantwortung sowie eine Vielzahl von Fachveranstaltungen aus.

Autoren:

Fabian Miller, Junior Public Affairs Manager – Data Society, miller@bvdw.org
Janek Kuberzig, Public Affairs Manager – (Future) Data & Tech, kuberzig@bvdw.org

www.bvdw.org

Impressum

Erscheinungsort und -datum	Berlin, Mai 2026
Herausgeber	Bundesverband Digitale Wirtschaft (BVDW) e.V. Obentrautstraße 55, 10963 Berlin, +49 30 2062186 - 0, info@bvdw.org, www.bvdw.org Vorstand gem. § 26 BGB Carsten Rasner
Präsident	Dirk Freytag
Vizepräsident*innen	Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr. Moritz Holzgraefe, Julian Simons, Eva Werle
Kontakt	politik@bvdw.org Vereinsregisternummer Amtsgericht Charlottenburg VR 42449 B
Rechtshinweise	Alle in dieser Veröffentlichung enthaltenen Angaben und Informationen wurden vom Bundesverband Digitale Wirtschaft (BVDW) e.V. sorgfältig recherchiert und geprüft. Diese Informationen sind ein Service des Verbandes. Für Richtigkeit, Vollständigkeit und Aktualität können weder der Bundesverband Digitale Wirtschaft (BVDW) e.V. noch die an der Erstellung und Veröffentlichung dieses Werkes beteiligten Unternehmen die Haftung übernehmen. Die Inhalte dieser Veröffentlichung und / oder Verweise auf Inhalte Dritter sind urheberrechtlich geschützt. Jegliche Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen, Bildmaterial oder sonstigen Inhalten, bedarf der vorherigen Zustimmung durch den Bundesverband Digitale Wirtschaft (BVDW) e.V. bzw. die Rechteinhaber (Dritte).

EU-Transparenzregister-Nummer: 479540331468-69 Deutsches Lobbyregister: R000257