Mai 2026

Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt

Stellungnahme zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 16. April 2026

Rechtsanwalt Frank Ingenrieth, LL.M.

Executive Summary

Einordnung, Prämissen und die veränderte Realität digitaler Gewalt

Der vorliegende **Referentenentwurf (Ref-E)** reagiert folgerichtig auf fundamentale gesellschaftliche Transformationen im virtuellen Raum, die durch veränderte technische Möglichkeiten und Verhaltensweisen geprägt sind. Die Entstehung dieses virtuellen Raums hat neuartige, spezifische Formen der Delinquenz – die sogenannte „**digitale Gewalt**“ – hervorgebracht. Diese unterscheidet sich in ihrer Phänomenologie grundlegend von analoger Gewalt, da digitale Inhalte durch ihre **Ubiquität** (Allgegenwärtigkeit) und **Dauerhaftigkeit** eine erhebliche Intensivierung von Rechtsgutsverletzungen bewirken. Übergriffe im Netz verbleiben nicht isoliert im virtuellen Raum, sondern sind eng mit der analogen Lebenswelt verknüpft und führen zu realen psychischen, sozialen sowie körperlichen Folgen für die Betroffenen.

Gleichzeitig bewegt sich jede staatliche Regulierung in diesem Bereich in einem komplexen verfassungsrechtlichen Spannungsfeld: Der Staat hat zwar die Pflicht, die grundrechtlichen Werte einfachgesetzlich zwischen Privaten zu effektuieren, bleibt jedoch im Rahmen dieses staatlichen Eingreifens selbst streng an den **Verhältnismäßigkeitsgrundsatz** gebunden. Nicht jeder individuell unliebsame Sachverhalt ist automatisch abstrakt-generell regelungspflichtig oder regelungsberechtigt. Vor diesem Hintergrund widmet sich diese Stellungnahme einer methodischen Analyse und der Aufdeckung potenzieller struktureller Regelungslücken.

Die Stellungnahme geht nicht im Detail auf etwaige Besonderheiten der **gesetzgeberischen Kompetenzen** ein. Bei der Regulierung von „Diensten der Informationsgesellschaft“ und „Telekommunikationsdiensten“ ist die Kompetenz des nationalen Gesetzgebers durch das vorrangige Recht des europäischen Binnenmarktes stark limitiert. Gleichzeitig liegt die Zuständigkeit für die Medienregulierung in Deutschland originär bei den Bundesländern und nicht beim Bund. Ein echter ganzheitlicher Ansatz hätte diese abweichenden Kompetenzen transparent ausweisen und eine koordinierte Zusammenarbeit oder ergänzende Beschlussfassungen in den Ländern und europäischen Organen initiieren können.

Der Mangel dieser vorangestellten Gesamtanalyse führt zur methodischen Kritik der Stellungnahme dahingehend, dass sich ungeachtet der Kompetenzen kein Gesamtbild erkennen lässt. Die der Stellungnahme zu entnehmenden **Lösungsvorschläge sind indessen erfolgsorientiert** und klammern insoweit zunächst die Kompetenzen aus. Es obläge dem Gesetzgeber, die für die jeweiligen Maßnahmen kompetente Ebene künftig zu identifizieren.

Defizite in der methodischen Fundierung und Zielbestimmung

Die systematische Untersuchung offenbart, dass der Ref-E trotz seines explizit proklamierten „ganzheitlichen Anspruchs“ diesem Anspruch wohl nicht gerecht wird. Der Gesetzgeber listet zwar einen breiten Katalog an Phänomenen auf – wie Hate Speech, Doxing, Cyberflashing, Cybergrooming, bildbasierte sexualisierte Gewalt, Cyberstalking und Cybermobbing –, versäumt es jedoch, eine strukturierte Analyse darüber vorzulegen, wo tatsächlich **materielle Schutzlücken** im Recht existieren und wo lediglich reine **Durchsetzungsdefizite** vorliegen. Eine solche Analyse ist dem Entwurf allenfalls mittelbar zu entnehmen, da er im Ergebnis nur sehr begrenzt neue strafrechtliche Normen schafft und sich im Wesentlichen auf redaktionelle Konsolidierungen bestehender Schutznormen beschränkt.

Zudem fehlt eine klare Definition und dogmatische Priorisierung der primären gesetzgeberischen Schutzziele. Es wird nicht sauber unterschieden, ob das vorrangige Ziel die **präventive Vermeidung** künftiger Delikte, die **schnelle Beseitigung** (Löschung, Sperrung) von Inhalten oder die **nachträgliche Sanktionierung** der Täter*innen ist. Da je nach Primärziel gänzlich unterschiedliche regulatorische Instrumente zielführend sind, führt dieses methodische Versäumnis zu weitgehenden Fehllenkungen und im Ergebnis geringen Effekten der vorgeschlagenen Regelungen.

Grundlegende Kritik bzgl. des präventiven Ansatz

Aus kriminalpsychologischer und regulatorischer Sicht greift der präventive Ansatz des Ref-E zu kurz. Die Annahme, dass eine bloße Schärfung oder Ergänzung materiell-rechtlicher Sanktionsnormen eine spürbare abstrakte Prävention bewirkt, ist durchaus umstritten. Eine präventive Wirkung entfalten Sanktionen wohl vor allem dann, wenn sie unmittelbar und zeitnah auf die Tat folgen. Für ein effektives, auf Effizienz ausgerichtetes Konzept ist es entscheidend, dass möglichst jedes Einzeldelikt eine schnelle, spürbare Konsequenz nach sich zieht („**zügiger Abschluss des Erstverfahrens**“), anstelle wenige schwere Delikte mit drakonischen, aber in der Praxis kaum durchsetzbaren Strafen zu belegen. Die Schärfe der Erstsanktion ist dabei sekundär; entscheidend ist das gesellschaftliche Bewusstsein, dass digitale Handlungen konsequent verfolgt werden.

Darüber hinaus klammert der Entwurf die **tieferliegenden strukturellen und psychosozialen Ursachen** digitaler Gewalt vollständig aus. Phänomene wie die mangelnde Unrechtsbewusstheit bei Kindern und Jugendlichen, persönliche Perspektivlosigkeit, die Nutzung digitaler Räume als Frustrationsventil sowie individuelle Traumata oder destruktive Fehlvorbilder werden im Rahmen des „ganzheitlichen“ Konzepts nicht durch flankierende Maßnahmen der Jugend- und Sozialarbeit adressiert.

Strukturelle Mängel des GGDG-E und verfahrenstechnische Hürden

Der zivilrechtliche Teil des Entwurfs (GGDG-E) offenbart erhebliche praxisferne Einschränkungen, die zu signifikanten Durchsetzungslücken führen.

- **Einschränkung des Geltungsbereichs**: Die Beschränkung von folgenschweren Maßnahmen wie Account-Sperren auf „**Soziale Netzwerke**“ greift zu kurz. Digitale Gewalt findet in erheblichem Maße auch auf **Plattformen im beruflichen und professionellen Kontext** sowie auf **Gaming-Plattformen** statt, die von den vorgeschlagenen §§ 1 und 4 GGDG-E unberücksichtigt bleiben. Da das Nutzerkonto auf jeder modernen Online-Plattform von Relevanz ist, sollte das Gesetz gänzlich auf diese einschränkenden Definitionen verzichten.

- **Mängel der Beweissicherung**: Das Gesetz sieht für die Verwaltung der gesicherten Informationen durch die Gerichte lediglich die „**Textform**“ vor, was sich für moderne **forensische Untersuchungen** als vollkommen ungeeignetes Datenformat erweist. Es fehlen verbindliche Vorgaben für strukturierte, manipulationssichere und maschinenlesbare Datenbereitstellungen.

- **Beweiswürdigungsprobleme bei nachträglicher Manipulation**: Löschen oder verändern Täter*innen ihre Inhalte oder Personalien im Nachgang einer Tat, führt die starre Orientierung an einem bloßen „Live-Inhalt“ zum Zeitpunkt der behördlichen Abfrage zu unauflösbaren Widersprüchen zwischen den Beweisen der Betroffenen und den Auskünften des Anbieters. Dies führt im Rahmen der gerichtlichen Beweiswürdigung zu erheblichen **Nachteilen zu Lasten der Opfer** digitaler Gewalt, obwohl die Modifikation direkt auf die Manipulation der Täter*innen zurückzuführen ist. Ein effektiver Auskunftsanspruch muss daher zwingend auch verfahrensrelevante Nebeninformationen und Historisierungsdaten (z. B. Reichweitenkonfigurationen, Interaktionsdaten, Änderungshistorien) umfassen.

Ignoranz technischer Realitäten bei der Identitätsfeststellung (§ 2 Abs. 2 GGDG-E)

Die vorgeschlagenen Auskunftsmechanismen basieren auf der praxisfremden Prämisse einer fehlerfreien und eindeutigen Zuordbarkeit digitaler Identitäten. Die Stellungnahme identifiziert zahlreiche Faktoren, die zu einer gravierenden Unzulänglichkeit der Informationen nach § 2 Abs. 2 GGDG-E führen können:

- **Dritt- und Verwandtennutzung**: Die Nutzung eines Internetanschlusses durch unbekannte Dritte, Familienmitglieder oder Verwandte erschwert die Täter*innen-Identifikation.

- **Account-Hacking**: Das unbefugte Kapern oder Hacken von legitimen Nutzerkonten wird prozessual nicht adäquat abgefangen.
- **Fehlerhafte Zeitstempel und IP-Übertragungsfehler**: Die automatisierte Abfrage von IP-Adressen kann unter asynchronen Aktualisierungsverzögerungen in den Zuweisungsdatenbanken der Internetzugangsanbieter sowie unter fehlerhaften Zeitstempeln bei den Diensteanbietern leiden. Schon minimale Abweichungen führen zur Zuordnung völlig unbeteiligter Personen.
- **Identitätsdiebstahl und Fake-Accounts**: Das gezielte Agieren unter falschem Namen oder mittels gefälschter Profile hebelt die einfache Abfrage gespeicherter Personalien aus.

Um diesen Mängeln zu begegnen, bedarf es engmaschigerer Verfahren. Die gerichtliche Sicherung und Identitätsfeststellung sollte innerhalb eines straffen, maximal 48 Stunden umfassenden Gesamtverfahrens direkt über die Gerichte abgewickelt werden, anstatt Anbieter zu „Schutzpatronen der Rechtsstaatlichkeit“ zu stilisieren und mit unnötigen Rechtsmitteln auszustatten.

Kritik an eingeschränkten strafrechtlichen Tatbeständen am Beispiel des § 202e StGB-E

Die im Ref-E vorgesehenen strafrechtlichen Verschärfungen erweisen sich bei näherer Betrachtung als lückenhaft und inkonsequent. Am Beispiel des neuen Tatbestands der **unbefugten digitalen Überwachung** (§ 202e StGB-E), der den Einsatz von Stalking-Software und Spionage-Apps sanktionieren soll, zeigt sich eine fundamentale Schutzlücke. Die Norm enthält restriktive Tatbestandsmerkmale, wie das Erfordernis einer **„ständigen“ Überwachung**, was zu erheblichen Auslegungszweifeln im Hinblick auf das Bestimmtheitsgebot führt und massives Umgehungspotenzial eröffnet. Wer eine Person engmaschig, aber mit bewussten Unterbrechungen überwacht, bliebe straffrei, obwohl der psychische Überwachungsdruck und die Einschränkung der freien Lebensführung der Betroffenen identisch sind.

Die Stellungnahme legt daher einen **modifizierten Formulierungsvorschlag** vor: Die Strafbarkeit sollte primär an die Unbefugtheit der Überwachungshandlung und den gezielten Einsatz von Informations- oder Kommunikationstechnik anknüpfen. Zudem wird eine gesetzliche Vermutungswirkungen und Regelbeispiele vorgeschlagen.

Differenzierter Umgang mit Anonymität, KI-Bots und innovative Sanktionsinstrumente

Ein zukunftsfähiges Gesetz gegen digitale Gewalt darf die zunehmende Automatisierung durch KI-Bots und anonyme Netzwerke nicht ignorieren. Da klassische, nachträgliche Sanktionsmechanismen bei vollständig anonymen Profilen oder automatisierten Bots in der Regel ins Leere laufen, schlägt die Stellungnahme ein Konzept vor, das die zur Verfügung stehenden Maßnahmen anhand der **Anonymität des Nutzerkontos** abstuft.

Je höher der Grad der Anonymität eines Profils ist, desto niedriger müssen die Hürden für **Unmittelbarkeitsautomatismen** (Inhalts- und Account-Sperren) angesetzt werden.

Der Kanon der rechtlichen Anordnungen muss dafür um strukturell wirksame Maßnahmen erweitert werden:

- **Sperrung von Geldflüssen**: Konten, die rechtswidrige Inhalte verbreiten und monetarisieren, müssen durch die Sperrung der damit verknüpften Finanzströme ausgetrocknet werden.
- **Rücksetzung digitaler Netzwerke**: Da die Breitenwirkung digitaler Gewalt zwingend auf der Existenz eines Multiplikationsnetzwerks beruht, sollte gerichtlich die Löschung von Accounts und die vollständige Rücksetzung des Netzwerks (Follower*innen, Kontakte, Freunde) angeordnet werden können. Dies bricht die Verbreitungsmacht künftiger rechtswidriger Inhalte und korrigiert die auf Online-Plattformen erfolgte Gewichtung im Rahmen der Feed-Algorithmen.
- **Untersagung algorithmischer Empfehlungen**: Plattformbetreibern muss gerichtlich untersagt werden können, die betroffenen Inhalte über ihre internen Empfehlungsalgorithmen weiterzuverbreiten. Dies erhöht den Aufwand für den Betrieb von Bot-Netzwerken signifikant.

Verlagerung der Tatorte und Tatformen

Infolge der unnötigen definitorischen Einschränkungen, Unklarheiten und der mangelnden methodischen Verknüpfung zwischen analoger und digitaler Welt erweist sich der Ref-E an vielen Stellen selbst als **„Geburtshelfer“ für neue Delinquenzphänomene**. Ein zukunftsfähiger und ganzheitlicher Ansatz müsste den logischen Grundsatz etablieren, dass eine strafbewehrte Handlung unabhängig vom gewählten Medium identisch bewertet wird und regulatorische Anpassungen sich primär an den spezifischen Besonderheiten digitaler Kommunikation – wie der Verbreitungsgeschwindigkeit, Reichweite und verringerten Reversibilität – ausrichten. Da der Ref-E diese systematische Harmonisierung versäumt und bestehende Erkenntnisdefizite

sowie verfahrenstechnische Verzögerungen ungelöst lässt, steht zu befürchten, dass die vorgeschlagenen Regelungen zu keiner nachhaltigen Eindämmung, sondern lediglich zu einer inhaltlichen und räumlichen Verlagerung digitaler Gewalt führen:

- **Inhaltliche Verlagerung (Anpassung des modus operandi)**: Da die im Entwurf vorgesehenen Effizienz- und Effektivitätsgewinne des GGDG-E starr an eng umgrenzte Katalogtaten gekoppelt sind, wird für potenzielle Täter*innen ein erheblicher Anreiz geschaffen, ihre Verhaltensmuster gezielt anzupassen. Durch das bewusste Ausnutzen verbleibender Regelungs- und Durchsetzungslücken können Schutzmechanismen systematisch umgangen werden, wodurch der beabsichtigte Opferschutz im Ergebnis ins Leere läuft.

- **Räumliche Verlagerung (Ausweichen auf alternative Plattformen und Infrastrukturen)**: Durch die sachlich nicht gerechtfertigte Beschränkung folgenschwerer zivilrechtlicher Maßnahmen (wie Account-Sperren) auf klassische „Soziale Netzwerke“ verlagert sich das Tatgeschehen absehbar auf professionelle Plattformen, Messenger-Dienste oder Gaming-Netzwerke, die vom Schutzbereich der §§ 1 und 4 GGDG-E unberücksichtigt bleiben. Zudem nutzen professionell agierende Täter*innen zunehmend **Proxy- oder VPN-Dienste**, um ihre Nachverfolgbarkeit einzuschränken und ein Profiling zu vermeiden. Da der Entwurf es versäumt, derartige Intermediäre und Dienstketten konsequent als Adressaten gerichtlicher Auskunftsanordnungen einzubeziehen, droht eine vollständige Verschiebung der Tathandlungen in nach dem GGDG-E regulatorisch unzugängliche Räume.

In beiden Dimensionen dieser Ausweichbewegungen steht zu befürchten, dass der Schutzeffekt für die Betroffenen vollständig ausbleibt oder sich zumindest drastisch verringert. Mithin wird sich die dem ganzheitlichen Ansatz des Ref-E innewohnende Hoffnung, die fortschreitende „Verrohungstendenz“ virtueller Räume wirksam auszubremsen oder gar umzukehren, ohne eine fundamentale Überarbeitung dieser strukturellen Lücken nicht zeitnah erfüllen.

Defizite im Opferschutz: Prozessuale Beschleunigung, finanzielle Risikominimierung und innovative Sanktionsinstrumente

Um das proklamierte Ziel eines effektiven Präventivkonzepts zu erreichen, greift der Referentenentwurf prozessual und sanktionsrechtlich zu kurz. Aus kriminalpsychologischer Sicht erfordert Abschreckung vor allem **Schnelligkeit und Konsequenz**. Daher fordert die Stellungnahme die Verpflichtung von Plattformanbietern zu **vollautomatisierten Verfahren** zur Beweissicherung und Identitätsextraktion. Dieses Erstverfahren ist durch **engmaschige Fristen zu beschleunigen**: Eine Informationsweiterleitung an Nutzer*innen muss binnen 24 Stunden erfolgen, die Rückmeldefrist zur Inhaltsverteidigung ist auf 72 Stunden zu begrenzen, und das gerichtliche Identitätsfeststellungsverfahren darf insgesamt maximal 48 Stunden umfassen.

Um echte **strukturelle Wirkkraft** zu entfalten, muss zudem der bloße Fokus auf Account-Sperren durch eine massive Erweiterung des gerichtlichen Anordnungskanons durchbrochen werden:

- Dies betrifft etwa die gezielte **Unterbindung von Finanzströmen** zur Austrocknung der Täter-Monetarisierung, die **Rücksetzung digitaler Netzwerke** oder die **algorithmische Verbreitungsmacht** künftiger Inhalte zu reduzieren.
- Im Bereich der **Strafvollstreckung** regt die Stellungnahme an, das präventive Potenzial, dass bereits von Bewährungsweisungen gemäß § 56c StGB bekannt ist, konsequent auszuschöpfen, festzuschreiben und weiterzuentwickeln. (Wiederholungs-)Tätern kann die **Nutzung bestimmter Plattformkategorien oder ein unbeaufsichtigter Internetzugang** untersagt werden.

Im Rahmen finanzieller Wirkkraft, wird eine Optimierung der **Verfahrenskosten** aneregt. Angesichts der Ubiquität und Dauerhaftigkeit digitaler Gewalt verlangt die Stellungnahme zudem eine klarstellende Norm zum **Ersatz von Folgeschäden**: Täter*innen sollte verpflichtet werden, die Kosten für professionelle Monitoring-Services zu erstatten. Nur so kann eine Sekundärverbreitung (auch im Darknet) wirksam unterbunden werden, ohne Betroffene im Wege der Eigenrecherche einer permanenten **Retraumatisierung** auszusetzen.

Strukturell sollte diese Rechtsdurchsetzung durch **spezialisierte Ermittlungseinheiten und Schwerpunktstaatsanwaltschaften** flankiert sowie die unzureichende ‚Textform' durch forensisch verwertbare, maschinenlesbare Datenstandards ersetzt werden

Fazit und Kernempfehlungen

Der vorliegende Referentenentwurf bedarf einer fundamentalen materiell-rechtlichen und prozessualen Überarbeitung. Um digitale Gewalt wirksam und nachhaltig zu bekämpfen, muss der Gesetzgeber von rein symbolischen Strafverschärfungen Abstand nehmen. Stattdessen müssen die **prozessuale Schnelligkeit, forensisch verwertbare Datenstandards, plattformübergreifende Geltungsbereiche** sowie **reichweitenbezogene Sanktionsinstrumente** (Netzwerkrücksetzungen und Monetarisierungsverbote) in den Mittelpunkt gestellt werden. Ohne diese Präzisierungen droht das Gesetz zu einem stumpfen Schwert im Kampf gegen die dynamischen Phänomene digitaler Gewalt zu werden.

Über den Autor

Frank Ingenrieth, LL.M. ist Führungskraft und niedergelassener Anwalt mit über 15 Jahren interdisziplinärer, internationaler Erfahrung im Bereich Steuerung von Datenschutz- und Regulierungsstrategien für nachhaltige, innovationsorientierte Lösungen. Sein Schwerpunkt liegt im Medien-, Internet- und Datenschutzrecht, sowie verbundenen Rechtsgebieten, z.B. Mietrecht, oder wechselwirkende Rechtsgebiete, etwa dem Wettbewerbs- und Kartellrecht, sowie im Bereich der Fragen der Good Governance.[1]

Seine Erfahrung sammelte Frank Ingenrieth während seines beruflichen Werdegangs, inklusive seiner Ausbildung, in internationalen Großkanzleien, datenschutzrechtlicher Aufsichtsbehörden, internationaler Konzerne, gemeinnütziger Organisationen. Er veröffentlicht regelmäßig, entweder im Rahmen von juristischer Fachliteratur, Fachkommentare, sowie in Form von Diskussionsrunden und Panels[2].

Diese Stellungnahme wurde unabhängig und ohne Auftrag durch etwaige Mandant*innen erstellt. Die Stellungnahme und die Anmerkungen basieren auf der langjährigen praktischen Erfahrung des Autors in der Entwicklung und Durchsetzung von Konformitätsbewertungsprogrammen, inklusive solcher Prüfprogramme, die aufgrund ihrer rechtlichen Vermutungswirkungen behördlicher Anerkennung bedürfen.

Pflicht- und Kontaktinformationen des Autors

Richard-Sorge-Straße 69a
10249 BERLIN

Fon +49 30 985 387 95
Fax +49 30 521 036 88
E-Mail office@ingenrieth-online.de

Steuer-Nummer 14/358/01684,
FA Friedrichshain-Kreuzberg.

Ich optiere gem. **§ 19 UstG** als Kleinunternehmer.

IBAN DE22 5002 4024 7497 0388 01

Zuständige Kammer
Rechtsanwaltskammer Berlin, Littenstraße 9, 10179 Berlin

In Deutschland verliehene **Berufsbezeichnung**
Rechtsanwalt

wesentliche **berufsrechtliche Regelungen**

- Bundesrechtsanwaltsordnung
- Berufsordnung
- Rechtsanwaltsvergütungsgesetz.

Diese und weitere können auf der Webseite der Rechtsanwaltskammer Berlin abgerufen werden.

1 Näheres über den Autor kann auf der Webseite der Kanzlei abgerufen werden: https://ingenrieth-online.de/de/ueber.

2 Eine Übersicht der Veröffentlichungen kann auf der Webseite der Kanzlei abgerufen werden: https://ingenrieth-online.de/de/publikationen.

Inhaltsverzeichnis

Executive Summary....2

Einordnung, Prämissen und die veränderte Realität digitaler Gewalt....2
Defizite in der methodischen Fundierung und Zielbestimmung....3
Grundlegende Kritik bzgl. des präventiven Ansatz....3
Strukturelle Mängel des GGDG-E und verfahrenstechnische Hürden....4
Ignoranz technischer Realitäten bei der Identitätsfeststellung (§ 2 Abs. 2 GGDG-E)....4
Kritik an eingeschränkten strafrechtlichen Tatbeständen am Beispiel des § 202e StGB-E....5
Differenzierter Umgang mit Anonymität, KI-Bots und innovative Sanktionsinstrumente....6
Verlagerung der Tatorte und Tatformen....6
Defizite im Opferschutz: Prozessuale Beschleunigung, finanzielle Risikominimierung und innovative Sanktionsinstrumente....7
Fazit und Kernempfehlungen....8

Über den Autor....9

Inhaltsverzeichnis....10

1 Einordnung, Prämissen....13

1.1 Prämissen und thematischer Fokus....14
1.2 Im Ref-E angesprochene Phänomene, Begriffsbestimmung....15
1.3 Gesetzgebungskompetenzen, Ganzheitlichkeit....17

2 Analyse der Ganzheitlichkeit....18

2.1 Präventivmaßnahmen....19
2.2 Schnelle Beseitigung digitaler Gewalt....21

2.2.1 Konkretisierungspotential der Rechtsmittel durch Anbieter....23
2.2.2 Konkretisierungs- und Effektuierungspotential durch engmaschige Fristen....24

2.2.2.1 Fristen für Nutzer*innen zur Verteidigung eigener Rechte....24
2.2.2.2 Fristen und Verfahren zur Sicherung der für die Aufdeckung der Identität erforderlichen Informationen....25

2.2.3 Kostenerleichterungn für das Auskunftsverfahren; Regelbeispiele des Umfangs der Beseitigungsansprüche....26

2.3 Sanktionierung digitaler Gewalt....28

290 2.3.1 Beschränkung der Anwendbarkeit, Regelkatalog § 1 GGDG-E....30
291 2.3.2 Beschränkung der Anwendbarkeit, Anbieter §§ 1, 4 GGDG-E....31
2.3.2.1 Plattformen mit besonderen Schutzbedarfen der Nutzer*innen....32
2.3.2.1.1 Plattformen im beruflichen, professionellen Kontext....32
2.3.2.1.2 Gaming-Plattformen....33
2.3.2.2 Weitere Plattformen....33
2.3.2.3 Fazit....34
292 2.3.3 Beweissicherung und Verwertbarkeit im Strafverfahren....35
2.3.3.1 Anbieter als Regelungsadressat....35
2.3.3.2 Gericht als Regelungsadressat....35
2.3.3.3 Betroffene als Regelungsadressat....35
2.3.3.4 Generelle Zielsetzung der Norm – Datenschutz oder Sicherung der Beweisverwertung....36
293 2.4 Unzulänglichkeit der Informationen nach § 2 Abs. 2 GGDG-E....37
294 2.4.1 Nutzung des Anschlusses durch (unbekannte) Dritte oder Verwandte....38
295 2.4.2 Hack des Nutzerkontos....40
296 2.4.3 Übertragungsfehler der IP-Adressen; fehlerhafte Zeitstempel....41
2.4.3.1 (voll)-automatisierung der Abfragen....41
2.4.3.2 falscher Zeitstempel bei Diensteanbieter....41
2.4.3.3 falscher Zeitstempel bei Internetzugangsanbieter....42
2.4.3.4 (asynchrone) „Aktualisierungsverzögerungen“ der Zuweisungsdatenbank bei Internetzugangsanbietern bzw. der gespeicherten Logfiles der Diensteanbieter....43
297 2.4.4 Fake-Account, Identitätsdiebstahl....44
2.4.4.1 Abfrage von Bestandsdaten, Verhältnis zur IP-Adressen....44
2.4.4.2 weitere sinnvolle Informationen und Anbieter....45
298 2.4.5 Nachträgliche Änderungen der Inhalte und Personalien durch Täter*in....46
2.4.5.1 Redundanz und Wirkungslosigkeit der §§2 und 3 GGDG-E....46
2.4.5.1.1 Verwaltung der gesicherten Informationen durch das Gericht....46
2.4.5.1.2 Beweiswert der durch das Gericht verwalteten Informationen....46
2.4.5.1.3 Für forensische Untersuchungen ungeeignetes Datenformat....48
2.4.5.1.4 Unzureichender Sicherungszeitraum....49
2.4.5.1.5 Unzureichender Sicherungsumfang....50
2.4.5.2 Unzureichender Informationsanspruch....51
2.4.5.2.1 nachträglich geänderte oder gelöschte Personalien....51
2.4.5.2.2 nachträglich geänderte oder gelöschte Inhalte....52
299 2.4.6 Mangelnde Informationen als Durchsetzungsdefizit sind mögliches Defizit der
300 Rechtsstaatlichkeit....53
301 2.5 Beispielhafte Ausführungen zu § 202e StGB-E....54

302 2.5.1 Zweifel am Bestimmtheitsgebot; Aufhebung des eigenen Schutzziels durch zu weitreichende Tatbestandseinschränkung....55
304 2.5.2 Modifizierter Vorschlag....56

305 **3 Strukturelle Perpetuierung einer unnötigen definitorischen Komplexität....58**

306 **4 Annahme eines Rechts auf anonyme Meinungsäußerung....63**

307 **5 Verlagerung der Tatbegehung und Tathandlung....67**

308 5.1 Verlagerung hinsichtlich des modus operandi....69
309 5.2 Verlagerung hinsichtlich der räumlichen Tatbegehung....72

1 Einordnung, Prämissen

Der Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt in der Fassung vom 16. April 2026 (im Weiteren **Ref-E**)[3], stellt fest, dass sich Veränderungen im gesellschaftlichen Zusammenleben und im respektvollen und rechtskonformen Umgang der Individuen untereinander ergeben haben.[4]

Die Ursache dieser Entwicklung wird im Wesentlichen in Veränderungen im Rahmen der (technischen) Möglichkeiten und Gepflogenheiten gesehen.[5] Zusammenfassend betrachtet der Ref-E dies als eine „digitale Transformation".[6]

Konkret heißt es:

> ***Zugleich hat die digitale Transformation einen neuen, virtuellen Raum zur Begehung von Rechtsgutsverletzungen mit digitalen Mitteln eröffnet und damit neue Formen der Gewalt – die „digitale Gewalt" – ermöglicht.***[7]

Der Ref-E beabsichtigt nun, dieses erkannte Phänomen ganzheitlich zu adressieren.[8] Diese Ganzheitlichkeit ergibt sich daraus, dass sich das Ref-E dem Phänomen rechtsübergreifend widmet. So heißt es:

> ***Dieser Entwurf zielt darauf ab, den Schutz vor digitaler Gewalt rechtsgebietsübergreifend zu verbessern.***[9]

Sowie

> ***Die Bekämpfung digitaler Gewalt erfordert ein ganzheitliches Vorgehen.***[10]

Insoweit wäre zu erwarten, dass der Ref-E sowohl in seiner Analyse als auch in seinen Konsequenzen eine umfassende Betrachtung erkennen ließe. Eine solche umfassende Betrachtung erscheint als *conditio sine qua non* für gesetzte Ziel, nämlich einer „*effektiven Durchsetzung zivilrechtlicher Ansprüche*"[11] sowie einer „*Effektivierung des Strafrechts*"[12].

3 Abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_GgdG.pdf

4 Abschnitt A Ref-E, S. 1.

5 Abschnitt A Ref-E, S. 1.

6 Abschnitt A Ref-E, S. 1.

7 Abschnitt A Ref-E, S. 1.

8 Abschnitt A Ref-E, S. 1, Ref-E Begründung, Abschnitt A I, S. 19.

9 Abschnitt A Ref-E, S. 1.

10 Ref-E Begründung, Abschnitt A I, S. 20.

11 Abschnitt A Ref-E, S. 1.

12 Abschnitt A Ref-E, S. 1.

1.1 Prämissen und thematischer Fokus

Diese Generalität des Ref-E verlangt eine Einordnung der Stellungnahme vor dem Hintergrund der vom Ref-E adressierten Sachverhalte. Eine Umfänglichkeit hinsichtlich jedweder Thematik ist im Hinblick auf die erforderlichen Ressourcen nicht zu leisten. Entsprechend bedarf diese Stellungnahme einer inhaltlichen Einschränkung sowie transparent kommunizierter Prämissen.

Die inhaltlichen Einschränkungen betreffen die juristischen Einzelfalltiefe. Diese Stellungnahme widmet sich vordergründig der **methodischen Analyse** und der **potentiellen strukturellen Regelungslücken**.

Methodische Aspekte betreffen die Fragestellung, ob und inwieweit der Ref-E die für die Erreichung der selbst definierten Ziele hinreichende systematische Aufarbeitung erkennen lässt. Hierbei gilt es zu betrachten, ob und inwieweit sich der Ref-E ausreichend damit auseinandergesetzt hat, auf welcher Ebene etwaige Schutzlücken für Betroffene existieren. Diese können auf Ebene des materiellen Rechts oder der effektiven Rechtsdurchsetzung belegen sein.

Strukturelle Regelungslücken betreffen entweder Aspekte, die bereits jetzt existieren aber möglicherweise bewusst oder unbewusst im Ref-E nicht adressiert werden. Zugleich betreffen strukturelle Regelungslücken solche Aspekte, die zwar derzeit im Ref-E adressiert werden, die konkrete Regelung aber künftige Verlagerungseffekte vermuten lässt, sodass der erwünschte Effekt des Ref-E binnen kurzer Zeit ausbleiben wird.

Ungeachtet des Vorgenannten wird die Stellungnahme soweit möglich **tatsächliche Effektivitäten in den Fokus** stellen. Dies wird als Unterfall der methodischen Analyse betrachtet. Hierbei wird zur Kenntnis genommen, dass einer ganzheitliche Betrachtung der Phänomene „digitaler Gewalt“ auch eine Vielzahl unterschiedlicher Sachverhalte zugrunde liegen wird. Die Vielzahl der zugrundeliegenden Sachverhalte wird höchstwahrscheinlich auch unterschiedliche regulatorische Themengebiete betreffen, aus denen sich letztlich auch **abweichende gesetzgeberische Kompetenzen** ergeben. Eine detaillierte Auseinandersetzung mit den jeweils zutreffenden oder erforderlichen Gesetzgebungskompetenzen wird in dieser Stellungnahme zugunsten einer methodischen Erfolgsanalyse vermieden. Vielmehr sollte für die Ermittlung und Verabschiedung effektiver und erforderlicher Rechtsinstrumente zunächst unerheblich sein, wer für deren Beschluss letztlich zuständig ist. Soweit die Gesetzgebungskompetenzen für einzelne Regelungen oder Regelungsbereiche bei anderen Beschlussorganen liegen, als denjenigen, die für den Ref-E zuständig sind, so könnte dies in einer ganzheitlichen Betrachtung durchaus Berücksichtigung finden; etwa dahingehend, dass die abweichende Kompetenz ausgewiesen wird, eine Zusammenarbeit mit den abweichenden Organen angestrebt wird, oder so weit möglich sogar die ergänzende Beschlussfassung in den weiteren Organen eingeleitet wird.

1.2 Im Ref-E angesprochene Phänomene, Begriffsbestimmung

Das Ref-E spricht selbst einen weitreichenden Katalog an Phänomenen an, die als „digitale Gewalt“ verstanden werden. Dies umfasst beispielsweise[13]

- „**Hate Speech**“ (abwertende, bedrohliche, gewaltverherrlichende oder zu Straftaten aufrufende Beiträge in sozialen Netz werken, Blogs oder Foren),
- „**Doxing**“ (das unerlaubte Veröffentlichen personenbezogener Daten wie Adresse oder Telefonnummer),
- „**Cyberflashing**“ (das unerwünschte Zusenden von Bildmaterial, das Gewalttätigkeiten und/oder Pornographie („Dick Pics“) enthält),
- „**Cybergrooming**“ (das gezielte Ansprechen und Manipulieren Minderjähriger im Internet, um sexuelle Kontakte anzubahnen oder sexuelle Handlungen zu fördern),
- **bildbasierte sexualisierte Gewalt**,
- „**Cyberstalking**“ (das Verfolgen, Belästigen und/oder Überwachen einer Person mit digitalen Technologien),
- „**Cybermobbing**“ (das Beleidigen, Bedrohen, Bloßstellen oder Belästigen über digitale Kommunikationsmedien) und der Identitätsmissbrauch (das Kommunizieren unter einem Fake-Profil zum Nachteil einer real existierenden Person).

Hierbei stellt der Ref-E fest, dass es keine gesetzlich abschließende Definition des Begriffs „digitale Gewalt“ gibt.[14] Der Ref-E stellt zudem wiederholt auf die Besonderheiten einer digitalen Tatbegehung im Vergleich zu einer analogen Tatbegehung ab, vgl. nachstehende Zitate:

> ***Digitale Gewalt unterscheidet sich in ihrer Wirkung und ihrer Wirkweite grundlegend von analoger Gewalt.[15]***

> ***Durch die Ubiquität und Dauerhaftigkeit digitaler Inhalte erfahren Eingriffe in rechtlich geschützte Güter oft eine Intensivierung, die über analoge Beleidigungen oder Belästigungen hinausgeht.[16]***

Zugleich werden auch Gemeinsamkeiten und Interdependenzen erwähnt:

> ***Zudem sind digitale und analoge Lebenswelten eng miteinander verknüpft, sodass Übergriffe im Netz reale psychische, soziale und körperliche Folgen haben können.[17]***

13 Abschnitt A Ref-E, S. 1.

14 Ref-E Begründung, Abschnitt A I, S. 19.

15 Ref-E Begründung, Abschnitt A I, S. 20.

16 Ref-E Begründung, Abschnitt A I 1, S. 21.

17 Ref-E Begründung, Abschnitt A I, S. 20.

> ***Zusätzlich muss für die Rechtsverletzung der Dienst eines Diensteanbieters genutzt werden, um den kausalen Beitrag des Diensteanbieters zur Rechtsverletzung sicherzustellen und zugleich die Taten, die ausschließlich in der analogen Welt begangen werden, auszuschließen.***[18]

Insoweit ist festzuhalten, dass der Ref-E nach eigenen Ansprüchen einen ganzheitlichen Anspruch definiert. Er erkennt an, dass der Begriff der „digitalen Gewalt“ der jeweiligen Dynamik der konkreten Tathandlungen unterworfen ist.

Hieraus ergeben sich sowohl **materielle Regelungsbedarfe** als auch solche, die sich der Rechtsdurchsetzung widmen. **Elemente der effektiven Rechtsdurchsetzung** können durch prozessrechtliche Aspekte adressiert werden, soweit denn ein „Prozess“ im Sinne der Rechtsordnung vorliegt. Es ist auch vorstellbar, dass eine effektive Rechtsdurchsetzung auch ohne einen förmlichen Prozess erreicht werden kann, wenn und soweit sonstige, eher tatsächliche Regelungen und Maßnahmen effektuiert würden.

Zugleich ergeben sich aus dem ganzheitlichen Anspruch des Ref-E auch Fragestellungen im Rahmen der **Konsistenz und der Begrenzung staatlichen Eingreifens**. Denn nicht jeder individuell unliebsame Sachverhalt begründet einen gesellschaftlich unliebsamen Sachverhalt, der staatlicher Regulierung verlangt. Grundrechtsverpflichtet ist zunächst nur der Staat. Es gehört aber zu den vornehmen Pflichten eines Staats, die in den Grundrechten zum Ausdruck kommenden Werte in seine allgemeinen Gesetze zu überführen und somit Wirkung grundrechtlicher Werte auch zwischen Privaten zu begründen.[19] Zugleich ist der Staat im Rahmen seiner vornehmen Pflicht, die grundrechtlichen Werte einfachgesetzlich zu effektuieren, wiederum selbst an die Grundrechte, und mithin den **Verhältnismäßigkeitsgrundsatz**, gebunden.

- Nicht jeder Sachverhalt, der abstrakt-generell regelungsfähig ist, ist automatisch regelungspflichtig.
- Nicht jeder Sachverhalt, der abstrakt-generell regelungsfähig ist, ist automatisch regelungsberechtigt.

Vor diesem Hintergrund gilt es den Ref-E systematisch und methodisch zu analysieren.

18 Ref-E Begründung, Abschnitt B, zu Artikel 1, zu § 1, zu Absatz 1, S. 43.

19 So auch der Ref-E, vgl. Ref-E Begründung, Abschnitt B zu Artikel 1 zu § 2, zu Absatz 1, S. 46.

1.3 Gesetzgebungskompetenzen, Ganzheitlichkeit

„Digitale Gewalt“ betrifft eine **dynamisches Phänomen**, welches in dessen zugrundeliegenden Sachverhalten ebenso dynamische Erscheinungsformen aufweist.

Insofern ist es nachvollziehbar, dass diese unterschiedlichen Sachverhalte ebenso eine Vielzahl von Themenfeldern und Rechtsgebieten betreffen. Insoweit ist zu erwarten, dass sich effektive Maßnahmen aus einem **Konglomerat aus Regelungen** in unterschiedlichsten Themenfeldern und Rechtsgebieten zusammenstellen. Eine solche Diversität der betroffenen Rechtsgebiete legt nahe, dass auch die Gesetzgebungskompetenz über mehrere zuständige Organe verteilt liegt.

Insbesondere im Rahmen der Regulierung der „Dienste der Informationsgesellschaft“ sowie der „Telekommunikationsdienste“ ist aufgrund des Europäischen Binnenmarktes davon auszugehen, dass die Kompetenz **des nationalen Gesetzgeber** erheblich durch absolute oder konkurrierende Gesetzgebungskompetenzen der **Europäischen Union** limitiert sein dürfte. Zugleich ist davon auszugehen, dass im Rahmen der Medienregulierung zumindest in Deutschland die Gesetzgebungskompetenz ganz oder teilweise nicht dem **Bund**, sondern den **Ländern** zugewiesen ist.

Im Rahmen der Stellungnahme wird nicht im Detail darauf eingegangen werden, ob das den Ref-E bzw. dessen finalen Gesetzesbeschluss zu verantwortende Organ die tatsächliche Gesetzgebungskompetenz besitzt. Es wird auch nicht darauf eingegangen werden, ob für etwaige Alternativvorschläge die Gesetzgebungskompetenz vorläge. Vielmehr wird methodisch und systematisch untersucht, ob der Ref-E den avisierten ganzheitlichen Anspruch erfüllt. Die Frage der Gesetzgebungskompetenz stellt sich erst im Anschluss, nachdem eine sachdienliche Analyse der derzeitigen Sachlage stattgefunden hat. Nachdem der Ref-E selbst auch bereits auf weitere Gesetzgebungsvorhaben verweist, welche das Gesamtkonzept vervollständigen sollen[20], wäre eine solche Darstellung und Ganzheitlichkeit auch methodisch vorstellbar gewesen im Falle abweichender Gesetzgebungskompetenzen.

Ein solcher **systematischer Überblick** hätte es auch ermöglicht, das **Zusammenspiel der unterschiedlichen Ansprüche sicherzustellen**. Insbesondere, dass beweiserhebliche Tatsachen durch Diensteanbieter nicht gelöscht werden, wenn diese auf anderem Wege, als einer Anordnung der Strafverfolgungsbehörden oder des Gerichts gem. GGDG-E von den rechtswidrigen Inhalten erfahren haben, und den Zugriff auf diese rechtswidrigen Inhalte beschränken müssten, etwa auf Basis des Digital Services Act. Es wäre mindestens unglücklich, wenn sich Betroffenen entscheiden müssen, ob ihnen eine Rechtsverfolgung der Täter*innen oder eine Beseitigung der Inhalte wichtiger ist.

20 Ref-E Begründung, Abschnitt B, zu Artikel 1, zu § 2, S. 45

2 Analyse der Ganzheitlichkeit

Der Ref-E behauptet das Phänomen der „digitalen Gewalt“ ganzheitlich zu adressieren. Letztlich beschränkt sich der Ref-E jedoch auch zwei wesentliche Regelungsbereiche, nämlich das **Strafrecht** und das **Zivilrecht**.

Der Ref-E nennt eine Vielzahl von konkreten Phänomenen der „digitalen Gewalt“ Zugleich lässt der Ref-E eine strukturierte Analyse dahingehend vermissen, für welche dieser Phänomene tatsächlich eine regulatorische Lücke existiert. Eine solche Analyse ist dem Ref-E allenfalls mittelbar zu entnehmen. Etwa immer dann, wenn der Ref-E zu den Phänomenen bereits existierende Schutznormen anführt und keine eigenen, neuen Schutznormen etabliert. Im Ergebnis sieht der Ref-E nur begrenzt neue strafrechtliche Normen vor, § 201b StGB-E[21] und § 202e StGB-E werden ergänzt, § 184k StGB-E wird ersetzt.[22]

Die „Ersetzung“ von $ 184k StGB-E ist eher eine editorielle Erleichterung. Bereits der aktuelle § 184k StGB hat die „Verletzung des Intimbereichs durch Bildaufnahmen“ zum Regelungsgegenstand. Die Gesetzesbegründung führt aus, dass § 184k StGB-E eine Konsolidierung der Straftatbestände verfolge und bestehende Schutzlücken schließe.[23]

Neu eingeführt wird zudem das GGDG-E, welches die zivilrechtliche Durchsetzung der Ansprüche erleichtern soll.

Dabei stellen sich indessen mehrere Fragen:

Ist Ziel die **Vermeidung** von künftigen digitalen Gewaltdelikten?

Ist Ziel die **schnelle Beseitigung** (Löschung, Sperrung oder sonstige Verhinderung der Verbreitung) von digitalen Gewaltinhalten?

Ist Ziel die **nachträgliche Sanktionierung** der digitalen Gewaltdelikte?

Je nach Primärziel sind andere Maßnahmen zielführend.

Da der Ref-E eine solche methodische Unterscheidung erst gar nicht aufweist, ist zu vermuten dass bei der Ausarbeitung des Ref-E die nötigen Vorüberlegungen nicht stattgefunden haben. Dies könnte auch die im Ergebnis geringen Effekte der neuen Regelungen erklären.

21 Vorgeschlagene Änderungen sind in Artikel 2 des Ref-E geregelt; die modifizierte Fassung des StGB wird im Folgenden als StGB-E referenziert.

22 Vergleiche Artikel 2, Ziffer 5 und Ziffer 7 Ref-E.

23 Ref-E Begründung, Abschnitt B, zu Artikel 2, zu Nummer 5, S. 64.

2.1 Präventivmaßnahmen

Digitale Gewalt ist, wie der Ref-E feststellt, ein Resultat gesellschaftlicher Entwicklungen. Gesellschaftliche Entwicklungen hinsichtlich des respektvollen Umgangs sind nicht notwendigerweise eine Frage regulatorischer Rahmenbedingungen.

Der abstrakte **Präventiveffekt von Sanktionsregelungen** ist durchaus umstritten. Eine höhere Signifikanz wird in den Fällen angenommen, in denen die Sanktion zumindest zeitnah auf die Tat erfolgt. Insoweit ist fraglich, inwieweit die Maßnahmen aus dieser Perspektive überhaupt präventive Wirkung entfalten können.

Einerseits ist zu begrüßen, dass der Entwurf klarstellt, was ohnehin klar sein sollte: das Verhalten im Digitalen Raum unterliegt ebenfalls den rechtlichen Normen, wie das Verhalten im Analogen Raum. Sollte diese Grundregel der Gesellschaft noch nicht bekannt gewesen sein, kann der Ref-E hier möglicherweise Klarheit schaffen.

Fraglich wäre aber, warum eine solche Grundregel in der Gesellschaft bisher nicht bekannt sein sollte bzw. nicht anerkannt würde.

Ein Gesichtspunkt könnte eine mangelnde Ausprägung zentraler Werte und Normen im Rahmen der **persönlichen Entwicklung** sein. Eine ähnliche Zielrichtung hätte die Frage, ob allen Täter*innen[24], gerade im Bereich der Kinder und Jugendlichen, der Unrechtsgehalt ihrer Handlungen bewusst ist. Ob etwaige Präventionsmaßnahmen im Bereich der Kinder- und Jugendarbeit zielführend(er) wären, obliegt den Stellungnahmen der diesbezüglichen Fachverbände. Ein weiterer Gesichtspunkt könnte eine wachsende **Perspektivlosigkeit** der Täter*innen sein, die digitale Gewalt als **Frustrationsventil** nutzen. Inwieweit hier begleitende Präventionsmaßnahmen im Rahmen der persönlichen Perspektivplanung besser geeignet wären, obliegt den Stellungnahmen der diesbezüglichen Fachverbände. Ebenfalls vorstellbar ist, dass die Ausübung Digitaler Gewalt eine Folge individueller **Traumata** und individueller **Fehlvorbilder** ist. Inwieweit hier begleitende Präventionsmaßnahmen zur Bewältigung erlittener Traumata und Erkenntnis der eigenen Fehlvorbilder zielführender sein könnten, obliegt den Stellungnahmen der diesbezüglichen Fachverbände. Für einen Ref-E, der einen ganzheitlichen Anspruch proklamiert, fällt jedoch auf, dass diese Dimension unbeachtet bleibt.

Soweit der abstrakte Präventionscharakter von Sanktionsnormen in Anrechnung gebracht wird, und aus diesen Gründen sowohl die strafrechtliche als auch zivilrechtliche Durchsetzung von gestärkt werden soll, ist zu erkennen, dass sich die Vorschläge im Wesentlichen auf das materielle Recht beziehen. Insoweit ist die abstrakte Prävention aber höchst umstritten. Für einen

24 Hinweis: Soweit die Stellungnahme den Begriff Täter*in verwendet, und sich nicht aus dem Kontext etwas anderes ergibt, ist zur einfacheren Lesbarkeit generisch jeglicher formelle Zustand im Lauf des zivil- oder strafrechtlichen Verfahrens gemeint, namentlich Verdächtige*r, Beschuldigte*r, Angeklagter*r, Beklagter*r, etc.

ganzheitlichen Ansatz des Ref-E fällt zudem auf, dass eine zielgerichtete Analyse der Hürden im **Durchsetzungsprozess** nicht aus **Sicht der Effizienz** erfolgte, sondern allenfalls aus **Sicht der Effektivität**. Eine auf die Effizienz ausgerichtete Regulierung würde den Fokus insbesondere darauf richten, dass etwaige Sanktionen möglichst schnell nach Tatbegehung durchgesetzt werden.

Aus psychologischer Sicht erscheint der zügige Abschluss des „Erstverfahrens“ besonders wichtig. Hierzu genügt bereits die Erkenntnis, das „digitale Handlungen“ verfolgt werden können. Die konkrete Schärfe der „**Erstsanktion**“ erscheint weniger ausschlaggebend. Soweit etwaige Rechtsmittel längere Zeit in Anspruch nehmen, erscheint dies für den psychologischen Effekt jedenfalls nachrangig, wenn die Rechtsmittel nicht mit signifikanter Wahrscheinlichkeit eine gänzliche Aufhebung der Sanktionen begründet. Aus einem Präventivgedanken erscheint es wichtiger, dass möglichst jedes Einzeldelikt schnell zu einer (wenn auch geringeren) Sanktion führt, anstelle weniger schwere Delikte zu schweren Sanktionen.

Denn eine Erkenntnis über die Schwerpunktsetzung der Sanktionsverfahren ließe gerade im „Bagatellbereich“ die Präventivwirkung entfallen, in der Erwartung, dass eine Sanktionierung, etwa mangels Ressourcen, nicht erfolgen wird. Es ist auffällig, dass der Ref-E auch bei der Aufwandsberechnung zu erkennen gibt, dass die empirische und methodische Entscheidungsgrundlage wenig belastbar ist. Um es in ein Verhältnis zu setzen:

- Der Ref-E gibt an, die Gesamtheit der Tathandlungen bzgl. „Tatmittel Internet“ als Grundlage heranzuziehen, das sind nach eigenen Angaben aus den Jahren 2022/2023 97.000.[25]
- Von den Tathandlungen wurden lauf Ref-E bereits 83.000 Fälle aufgeklärt auf Grundlage der bisherigen Rechtslage – bzw. der Rechtslage in den Jahren 2022/2023, das entspricht einer Aufklärungsquote von 85,57%.
- Durch den Ref-E wird eine Steigerung der Aufklärungsquote von 10% der bisher nicht aufgeklärten Fälle (14.000) erwartet, also einer Aufklärung von weiteren 1.400 Fällen. Das entspricht ca. 1,5% aller Tathandlungen, und würde zu einer Gesamtaufklärungsquote von 87,01% führen.

Jede aufgeklärte Tathandlung ist ein Fortschritt, und es sollte eine Verbesserung nicht deswegen aufgegeben werden, weil die angestrebte Regelung nicht perfekt ist: „Das Bessere ist der Feind des Guten“. Es ist auffällig, dass der ganzheitliche Anspruch des Ref-E in Widerspruch zu dem doch minimalen Mehrwerten steht. Es ist jedenfalls nicht ersichtlich, wie sich aus einer relativen Steigerung der Aufklärungsquote von 1.5% eine hinreichende Steigerung des **Sanktionsdrucks** ergeben sollte, die tatsächlich präventive Auswirkungen haben könnte.

25 Ref-E Begründung, Abschnitt A VII. 4., S. 38.

2.2 Schnelle Beseitigung digitaler Gewalt

Es ist nicht erkennbar, inwieweit der Ref-E im Ergebnis zu einer schnelleren oder effizienteren Beseitigung der die Tathandlung begründenden Umstände führt.

Die Tathandlung begründende Umstände sind je Tatbestand anderweitige digitale Aspekte. Dies können Inhalte sein, die auf Plattformen veröffentlicht werden, dies kann die Installation von Hard- und Software sein, um die Betroffenen zu überwachen, das kann der bloße Besitz von Inhalten sein, die als Hilfsmittel zur Aufrechterhaltung einer (psychischen) Bedrohungslage dienen.

Der Ref-E scheint sich einer **Effektuierung der Beseitigung** nicht zu widmen. Entweder, weil der Ref-E diese Dimension bereits durch andere Rechtsakte als hinreichend erfüllt sieht, oder weil der Ref-E diese Dimension schlicht ausgeklammert hat. Die mangelnde methodische Transparenz erschwert diesbezügliche Schlussfolgerungen.

Vielmehr scheint der Ref-E Auffassungen zur „Erforderlichkeit der Anonymität im Internet“ zu perpetuieren, die im Ergebnis so nicht zwingend sind, siehe hierzu vertiefend 4.

Ebenso scheint die **Limitierung** der in den **Anwendungsbereich** des GGDG-E fallenden Dienste eine Einladung zur Verlagerung der Tathandlungen auf weitere Dienste in der Zukunft, siehe vertiefend 2.3.2 sowie 5.

An keiner Stelle sieht der Ref-E **Vermutungswirkungen** im Sinne der Betroffenen vor, die zumindest eine vorläufige, schnelle Beseitigung der digitalen Gewalt begründenden Umstände zur Folge hat. Im Gegenteil, selbst die nun vorgesehenen Regelungen zur Account-Sperre (§ 4 GGDG-E) führen im Ergebnis zu einer erheblichen **Verzögerung des Verfahrens**.

- Die Informationsabfrage gem. § 2 GGDG-E muss erfolgt sein; diese ist erst erfolgt, wenn die Entscheidung rechtskräftig ist, d.h., auch etwaige Rechtsmittel final beschieden wurden.[26]
- Ist die Informationsabfrage erfolgreich, muss die erhaltene Information im Falle einer IP-Adresse beim Diensteanbieter in ein Klardatum übersetzt werden – je nach Verfahrenszeit der ersten Stufe, ist dies möglicherweise nicht mehr möglich. Dieses Risiko ist virulent, da jeweils nur eine „Unverzüglichkeit“ vorgesehen ist, jedoch keine klaren Fristen.
- Bei Anordnung der Informationserteilung verbleibt der die Tat begründende Inhalt weiterhin erreichbar.

26 Vgl. Ref-E Begründung, Abschnitt B, zu Artikel 1, zu § 5, zu Absatz 4, S. 57.

- Betroffene müssen im Rahmen der einstweiligen Anordnung bzw. im Rahmen außergerichtlicher Verfahren eine Unterlassungserklärung herbeiführen; welches eine Verzögerung von weiteren zwei Wochen oder mehr nach sich ziehen kann. Inwieweit der Auffangtatbestand „anderen Umstände“ zeitliche Effizienzgewinne begründet, erscheint fraglich.

- Erst mit Anordnung einer Account-Sperre verfügt das Gericht eine Entfernung des die Tat begründenden Inhalts.

Insoweit ist davon auszugehen, dass die die Tat begründenden Inhalte voraussichtlich mindestens einen weiteren Monat unangetastet die Rechtsgutsverletzung fortführen. Ergänzend ist darauf hinzuweisen, dass die Kombination der Löschanordnung zusammen mit der Account-Sperre weitere – nicht nachvollziehbare – Einschränkungen begründet. Denn die Account-Sperre ist nur auf Soziale Netzwerke anwendbar. Insoweit scheint eine Löschanordnung für Inhalte auf anderen Online-Plattformen bisher durch das Gesetz nicht vorgesehen.

Die Diensteanbieter sowie die Internetzugangsanbieter (gemeinsam **Anbieter**) sind vorliegend nicht selbst mit der Prüfung der potentiellen Rechtswidrigkeit der Handlung betraut, im Gegensatz zu anderen gestzlichen Regelungen, etwa denen des Digital Services Act. Im Gegenteil: der im GGDG-E vorgesehene Richtervorbehalt für die Informationsabfrage stellt sich, dass die Plausibilität der Rechtswidrigkeit durch ein Gericht zuvor geprüft und bestätigt wurde.

Insoweit ist nicht erkennbar, inwieweit sowohl Anbieter 1) eine weitere Prüfung der Anordnung zustehen sollte und 2) die Rückmeldefristen nicht konkretisierbar sind.

2.2.1 Konkretisierungspotential der Rechtsmittel durch Anbieter

Der **Grundrechtsschutz** der vermeintlichen Täter*innen ist durch den **Richtervorbehalt** gewährt. Die dem Gesetz innewohnende Skepsis gegenüber der Rechtmäßigkeit der richterlichen Anordnung ist bedenkenswert. Es ist zwar dem Rechtsstaat immanent, dass gerichtliche Entscheidungen einer Überprüfung zugänglich sind. Jedoch verlangt dies eine Betroffenheit. Die Anbieter werden durch das GGDG-E zu Vertretern der Nutzer*innen und somit als Private Wirtschaftsakteure zum Schutzpatron der Rechtsstaatlichkeit stilisiert.

Dies wäre möglicherweise nachvollziehbar, wenn und soweit die Rechte der Anbieter durch die Anordnung selbst betroffen wären. Es ist nicht ersichtlich, wie im Einzelfall eine gerichtliche Anordnung zur Informationserteilung die Rechte der Anbieter unrechtmäßig verletzt, wenn und soweit das GGDG-E dem Grunde nach als rechtmäßig angesehen wird. Allenfalls wäre vorstellbar, dass das Gericht die Anordnung gegenüber den falschen Anbietern ausspricht. Es sollte hierzu klargestellt werden, dass die **Rechtsmittel der Anbieter** auf derartiger Fälle reduziert ist, und die Anbieter nicht in Vertretung der Nutzer*innen deren Rechte schützen sollen.

Ein **Vertretung der Nutzer*innen** durch die Anbieter wäre insoweit zumindest methodisch vorstellbar, in denen die Nutzer*innen dem Gericht unbekannt sind, und somit nicht selbst im Verfahren ihre eigenen Rechte schützen können. Allerdings sieht das GGDG-E hierzu bereits einen Mechanismus vor, vgl. § 6 GGDG-E. Anbieter haben eigene direkte Möglichkeiten, mit den Nutzer*innen in Kontakt zu treten. Insoweit ist sichergestellt, dass auch für das Gericht zunächst anonyme Nutzer*innen über das Verfahren informiert werden.

Nicht nachvollziehbar ist, warum das GGDG-E für die **Verteidigung der eigenen Rechte** vorsieht, dass Nutzer*innen in diesem Falle **weiterhin anonym oder pseudonym** bleiben können, indem sie etwaige Stellungnahmen über die Anbieter als Proxy einreichen. Sollte der angegriffene Inhalt aus Sicht der Nutzer*innen nicht rechtswidrig sein, und diese sich in der Sache verteidigen wollen, so steht ihnen dieses Recht zu. Es besteht aber **kein Recht auf anonyme Beteiligung an einem Gerichtsprozess**.

Soweit der Gesetzgeber befürchtet, dass der **Informationsanspruch** des GGDG-E **missbraucht** wird, und nach Offenlegung der Identität einzelne Nutzer*innen erhebliche Nachteile zu befürchten hätten, so können **Schutzmaßnahmen** im Rahmen der **Aktenführung** der Gerichte sichergestellt werden. Umgekehrt ist nicht nachvollziehbar, warum ein Gesetz, welches ausdrücklich die **Anonymität** im Internet als **tatbegünstigen Faktor** eliminieren möchte, die Anonymität im gerichtlichen Verfahren perpetuiert.

2.2.2 Konkretisierungs- und Effektuierungspotential durch engmaschige Fristen

Soweit nicht der **Ausnahmefall** vorliegt, dass anonyme Nutzer*innen unrechtmäßig Gegenstand eines Informationsanspruchs werden und trotz eines Richtervorbehalts diesem unzulässigen Informationsbegehren auch stattgegeben wurde, ist davon auszugehen, dass tatsächlich eine rechtswidrige Handlung vorliegt. In diesem Fall ist nicht nachvollziehbar, warum das GGDG-E keine strafferen Verfahrensfristen vorsieht.

2.2.2.1 Fristen für Nutzer*innen zur Verteidigung eigener Rechte

Anbieter, die möglicher Adressat des GGDG-E sind, können sich technisch und organisatorisch darauf vorbereiten. Es ist sogar eine **Automatisierung** ohnehin – auch im Rahmen der Reduktion von Fehlerquellen – **vorauszusetzen**, nämlich dahingehend, dass die Informationen auf Basis einen vollautomatisierten Verfahrens gesichert und extrahiert werden. Gerade für große Plattformen kann hier auch gesetzlich eine entsprechende Schnittstelle für die Gerichte vorgesehen werden. So erscheint die Sicherung der relevanten Daten binnen weniger Stunden möglich.

Die Weiterleitung von Informationen an Nutzer*innen hat **sofort** zu erfolgen, jedenfalls nicht später als **24 Std.** nach Erhalt durch die Anbieter.

Die **Rückmeldefrist** durch die Nutzer*innen im Sinne einer Anzeige, ob Nutzer*innen sich gegen den Vorwurf verteidigen wollen oder nicht, kann optimiert werden. Konkret erscheinen unterschiedliche Anzeigen vorstellbar:

- eine Anzeige, ob die **Inhalte** während des laufenden Verfahrens in der angegriffenen Form **verfügbar bleiben** sollen
- eine Anzeige, ob eine **Verteidigung gegen die Offenlegung** der Identität angestrebt wird.

Eine Anzeige dahingehend, dass der angegriffene Inhalt weiterhin zugänglich bleiben muss, sollte binnen **72 Std.** für Nutzer*innen möglich sein. Eine Anzeige dahingehend, dass Rechtsmittel gegen die Aufdeckung der Identität eingelegt werden, kann hiervon unabhängig die üblichen Rechtsmittelfristen vorsehen.

Eine solche Unterscheidung würde es Betroffenen digitaler Gewalt ermöglichen, die **Auswirkungen der Tathandlung** jedenfalls nach 72 Std. effektiv **unterbinden** zu können, und somit auch weitere **Streu-Effekte** der **Tathandlung** zu **begrenzen**.

2.2.2.2 Fristen und Verfahren zur Sicherung der für die Aufdeckung der Identität erforderlichen Informationen

Es ist nicht ersichtlich, warum die Sicherung der Informationen, die für eine Identitätsaufdeckung erforderlich sind, nicht unmittelbar an das Gericht übermittelt werden. Ein etwaiger Missbrauch dieser Informationen ist durch geeignete (digitale) Aktenführung sicherzustellen. Ein möglicherweise dem Ref-E innewohnende Skepsis über die adäquate Datensicherungsfähigkeiten der Gerichte, erschiene bedenkenswert.

Soweit der Diensteanbieter eigene Klardaten zur Identität der Nutzer*innen vorhält, erscheint zunächst eine weitere **Identifikation der Nutzer*innen anhand der IP-Adresse** nicht erforderlich. Der Ref-E erkennt an, dass es durchaus eine neue Gefährdungslage des Identitätsmissbrauchs durch „Fake-Accounts“ gibt. Insoweit erscheint es in allen Fällen zwingend, auch die Identitätsdaten mit Hilfe der IP-Adresse zumindest zu plausibilisieren.

Es sollte daher vorgesehen werden, dass die Diensteanbieter die gesicherten IP-Adressen (inkl. Port) in einem klar definierten **Zeitfenster weniger Stunden** an das Gericht übermitteln, sodass das Gericht auf dieser Basis sofort die Anordnung gegenüber den Internetzugangsanbietern zur Sicherung der dort gespeicherten Informationen erlassen kann.

Das **Gesamtverfahren** hinsichtlich der Sicherung der auf Basis der IP-Adressen relevanten Informationen sollte **48 Std.** nicht übersteigen. Verteidigt sich eine Nutzer*in im Anschluss erfolgreich gegen die Identitätsaufdeckung ist sicherzustellen, dass alle die Identitätsaufdeckung ermöglichenden Informationen bei den Anbietern sowie in der Gerichtsakte irreversibel gelöscht werden.

2.2.3 Kostenerleichterungn für das Auskunftsverfahren; Regelbeispiele des Umfangs der Beseitigungsansprüche

Soweit die Gesetzesbegründung ausführt, dass auf einen **Gebührentatbestand** für das Auskunfsverfahren verzichtet werden, sind die dortigen Gründe nur teilweise nachvollziehbar.

Einerseits ist zwar zu begrüßen, dass Betroffene, die aufgrund der Erfahrung durch digitale Gewalt bereits Nachteie erfahren, von unnötigen Kosten zur Durchsetzung der eigenen Ansprüche befreit sein sollten. Soweit es sich hierbei also um einen psychologischen Effekt handeln sollte, endet dieser bereits bei den **Folgeverfahren**. Etwaige Unterlassungs- oder Schadenersatzansprüche unterlägen den auch sonst geltenden Regeln des Zivilprozesses. Je nach Höhe des erlittenen Schadens, ist das damit einhergehende Kostenrisiko, und die zu leistenden Kostenvorschüsse, signifikant.

Im Vergleich scheint das **Kostenrisiko** für das Auskunftsverfahren relativ gering, zumal der Gesetzgeber das Risiko konkretisieren, d.h. z.B. einen fiktiven Streitwert festlegen könnte.

Nutznießer dieser Kostenregelung sind letztlich **Täter*innen**. Soweit diese identifiziert werden können, wären auch die mit dem Auskunftsanspruch angefallenen Kosten als notwendige Rechtsverfolgungskosten schadenersatzpflichtig. Diese Kosten verblieben nur dann bei den Betroffenen, wenn der Auskunftsanspruch fruchtlos bliiebe, also keine Täter*in identifiziert werden konnte, das Folgeverfahren keine rechtswidrige Handlung feststellen konnte, oder die Täter*in mangels Solvenz keinen Schadenersatz leisten kann, und zwar für die gesamte Dauer der Vollstreckbarkeit des Titels.

Diese Risiken könnten durch zielgerichtetere Regelungen mitigiert werden.

- Verbleibt der Auskunftsanspruch **fruchtlos**, da **keine hinreichenden Informationen** ermittelt werden konnten, so könnte das Gesetz vorsehen, dass in diesen Fällen die Kosten des Verfahrens durch den Staat zu tragen sind.
- Verbleibt der Auskunftsanspruch **fruchtlos**, da dieser **nicht hinreichend glaubhaft** gemacht wurde, so ist durchaus vorstellbar, dass die Betroffenen (einen Teil der/) die Kosten zu tragen haben; schließlich liegt die Ursache der Fruchtlosigkeit in ihrer eigenen Einflusssphäre.
- Ist ein Auskunftsanspruch erfolgreich, aber die Betroffenen **verzichten auf einen zivilrechtlichen Folgeprozess**, so ist durchaus vorstellbar, dass die Betroffenen (einen Teil der/) die Kosten zu tragen haben;
- Wird im **Folgeverfahren** festgestellt, dass die **angegriffenen Inhalte nicht rechtswidrig** waren, so ist durchaus vorstellbar, dass die Betroffenen keine oder allenfalls einen Teil der Kosten zu tragen haben; schließlich hat das Gericht im Auskunftsverfahren ebenfalls die Ansprüche für überwiegend wahrscheinlich (glaubhaft) eingeschätzt.

- Wird im **Folgeverfahren** die Rechtswidrigkeit festgestellt, könnte der **Kostenanspruch auf den Staat** übergehen, und durch diesen durchgesetzt werden; auf den ansonsten möglichen Rückgriff auf die Klägerpartei bei Zahlungsausfall der Beklagtenpartei könnte explizit verzichtet werden.

Fraglich ist, ob auch etwaige **Kostenrisiken** im **Verhältnis Betroffene** und **Anbieter** entstehen. Aufgrund der zivilrechtlichen Ausgestaltung, sind die Anbieter Verfahrensgeger der Betroffenen. Soweit diese also erfolgreich **Rechtsmittel** einlegen, so wären alle damit verbundenen Aufwände für die Betroffenen erstattungspflichtig. Insoweit ist das Kostenrisiko nicht auf die Gebühren des Gesichts beschränkt. Insoweit sollte klargestellt werden, dass die durch die erfolgreichen Rechtsmittel der Anbieter anfalenden Kosten des Verfahrens durchd den Staat getragen werden. Ob eine Kostentragung auch geboten ist für die Fälle, in denen Anbieter erfolglos Rechtsmittel einlegen, wird hier bewusst offen gelassen.

Aus ähnlichen Überlegungen lässt das GGDG-E bzw. der gesamte Ref-E **Potentiale verpuffen**, die einen **nachhaltigen Schutz** der **Betroffenen** vor den **Konsequenzen der rechtswidrigen Inhalte** etabliert. Es ist bisher keine etablierte Rechtsfolge, dass im Falle einer rechtswidrigen Verurteilung der Täter*innen, die Täter*innen auch verpflichtet wären, etwaige **Folgeschäden** zu kompensieren, d.h., auch die Verbreitung der eigenen Inhalte durch Dritte zu unterbinden und den Betroffenen nötigenfalls – jedenfalls zeitweise – die Kosten für etwaige **Monitoring-Services** zu erstatten.

Dabei sind es neben der eigentlichen Tathandlung gerade die **Langzeitfolgen**, die auch der Ref-E als besonders schwerwiegend und die Betroffenen belastend darstellt. Zugleich kann es nicht von den Betroffenen verlangt werden, sich selbst ständig mit der „historischen Tat“ auseinanderzusetzen, in diese selbst aktiv das Internet – und mögicherweise Darknet – auf entsprechende Vervielfältigungen der Inhalte durchforsten.

Insoweit wird angeregt, die **gesetzlichen** Regelungen um eine **klarstellende Norm** zu erweitern, dahingehend, dass Täter*innen auch etwaige **Folgeschäden zu ersetzen** haben, und zu den üblicherweise erforderlichen Maßnahmen der Betroffenen auch die Beauftragung von Monitoringdiensten gehört. Vorstellbar sind zwei separate oder kombinierbare Ansätze:

- eine **Allgemeinklausel**, die die konkrete angemessen Auftragsdauer in das Ermessen des Gerichts stellt
- **Regelbeispiele**, bei welchen Tathandlungen eine Angemessenheit der Auftragsdauer vermutet wird.

Eine Regelung zu den **angemessenen Vergütungssätzen** der Dienste erscheint nicht erforderlich, da dies druch die Täter*innen im Rahmen eines eigenen Gerichtsverfahrens festgestellt werden kann.

2.3 Sanktionierung digitaler Gewalt

Soweit der Ref-E eine effektive **Sanktionierung** in den Fokus nimmt, ergeben sich auch Fragen. Einerseits lässt die Gesetzesbegründung im Rahmen der zu erwartenden Erfüllungsaufwände erkennen, dass lediglich eine Verbesserung der Aufklärungsquote im strafrechtlichen Bereich von 1.5% erwartet wird.[27]

Hier sei dem Gesetzgeber zu Gute gehalten, dass die Vorausschau der tatsächlichen Effekte natürlich schwierig ist. In Summe wird ohnehin von nur ca. 6.400 neuen Verfahren ausgegangen, was wohl auch die Verfahren inkludiert, die aufgrund der neuen und angepassten Tatbestände erst möglich werden. Sollte diese Annahme zutreffen, so würde der Ref-E lediglich ein **Wachstum von 6,5%** der Verfahren im Bereich der für den Ref-E relevanten Internetkriminalität begründen. Ob und inwieweit das in Einklang mit der möglichen Dunkelziffer und der laut Ref-E signifikant ansteigenden Verrohung und somit Ausbreitung des Phänomens „digitale Gewalt“ steht, ist zumindest fraglich.

Auffällig ist andererseits, dass sich im Gesetz keine Maßnahmen dahingehend finden, die eine **effizientere Bearbeitung der Verfahren** begründen könnte, etwa im Sinne von **spezialisierten Ermittlungseinheiten**, **Schwerpunktstaatsanwaltschaften** oder **Schwerpunktgerichten**. Eine solche Konzentration ist aus anderen Rechtsgebieten bekannt und hat dort durchaus zu einer effizienteren und konsistenteren Rechtsanwendung geführt.

Ebenfalls auffällig ist, dass der Ref-E an vielen Stellen **unnötige Beschränkungen** seiner eigenen **Reichweite** vorsieht und schon fast eine Anleitung für angepasste Tathandlungen mitliefert, um eine Anwendbarkeit des Ref-E zu umgehen und somit die künftige Durchsetzung der materiell-rechtlichen Aktualisierungen zu Nichte machen könnte.

Hinzukommt, dass der Ref-E nur einen sehr **kleinen Ausschnitt möglicher Maßnahmen** adressiert, dabei bestünden durchaus weitreichende Optionen, die **Erstellung und Verbreitung digitaler Gewaltinhalte**, die **Nutzbarkeit und den Bestand der** die Inhalte verbreitenden **Nutzerkonten**, oder die **wiederholte Rechtsverletzung** durch konkreten Täter*innen effektiver zu **unterbinden**. Insoweit wird auf die Optionen unter 4 verwiesen. Ergänzend können zudem nachstehende Überlegungen angestellt werden:

- Untersagung eines freien und / oder unbeaufsichtigten Internetzugangs für Täter*innen
- Untersagung der Nutzung bestimmten (Kategorien) von Online-Plattformen

27 Ref-E Begründung, Abschnitt A VII. 4., S. 38.

Beide Aspekte sind der deutschen Rechtsordnung nicht fremd.

- Die **Untersagung des Internetanschlusses** ist nach Auffassung der Rechtsprechung als Bewährungsauflage, konkret in Form der Bewährungsweisung § 56c StGB, zulässig.[28]

- Eine gezielte **Untersagung der Nutzung von Sozialen Netzwerken** wurde in der Vergangenheit durch die Strafverfolgungsbehörden auch angestrebt.

  Dies hat die Rechtsprechung aber teils als unzulässig betrachtet, wobei die dafür angeführten Gründe erwähnenswert sind, nämlich (1) vermeintlich leichte Umgehungsmöglichkeit, (2) Mehrpersonenhaushalt und damit einhergehende Unsicherheiten, wer den Anschluss und das in Rede stehende Endgerät benutzt haben könnte, und – das war wohl der primäre Grund – (3) eine mangelnde Definition, was denn ein Soziales Netzwerk und was eine „Nutzung“ dessen sei.[29] Alle genannten Gründe können durch entsprechende gesetzliche Ausgestaltung ausgeräumt werden.

Eine solche gesetzliche Ausgestaltung könnte inzwischen auch geboten sein. Die etwa vom LG Nürnberg-Fürth geäußerte These, dass verurteilte Straftäter*innen spätestens durch die Verurteilung über das Unrecht der begangenen Tathandlung Bescheid wüssten, und daher eine Wiederholung unterlassen würden, ist so nicht tragfähig.

Zwar ist es nicht Aufgabe des Staates, dessen Bürger*innen zu erziehen, wie es sich zwischen den Zeilen des Urteils liest, aber es ist Aufgabe der Staates, potentielle künftige Opfer hinreichend zu schützen.

Insoweit erscheint – jedenfalls für nachweisliche Wiederholungstäter*innen – ein **Schutzpflicht des Staates** dahingehend vertretbar, dass er diesen Täter*innen in angemessener Weise die **Mittel für eine weitere Tatwiederholung entzieht**. Dies gilt umso mehr, soweit für diese Täter*innen psychiatrische Erkrankungen – etwa Suchtkrankheiten oder Zwangsstörungen – eine ansonsten mögliche Selbstdisziplin erschweren oder verunmöglichen.

28 Vgl. OLG Hamm, Beschluss v. 10.11.2015, Az. 1 Ws 507/15 und 508/15.

29 Vgl. LG Nürnberg-Fürth, Beschluss v. 16.02.2015, Az. 17 Qs 7/15.

2.3.1 Beschränkung der Anwendbarkeit, Regelkatalog § 1 GGDG-E

Es ist nachvollziehbar, dass Betroffene nicht in allen Fällen eine **strafrechtliche Sanktion** der Täter*innen anstreben, etwa je persönlichem (**Nähe**-)**Verhältnis** zwischen Täter*innen und Betroffenen oder in Anbetracht des **Alters der Täter*innen**, bei denen Betroffene und deren gesetzliche Vertreter erkennen können, dass die Täter*innen die Auswirkung des eigenen Handelns nicht haben umfänglich absehen können und die real eingetretenen Konsequenzen ehrlich und nachhaltig bereuen. Eine strafrechtliche Verfolgung, die möglicherweise negative Auswirkungen auf den weiteren persönlichen und beruflichen Werdegang der Person hat, ist nicht für alle Betroffene das Ziel. Diese Gedankengänge sind auch den Wertungen des StGB zu entnehmen, da viele der Tatbestände als absolute oder relative Antragsdelikte ausgestaltet sind.

Das GGDG-E vermeidet nun strafrechtliche Verfahren, lediglich um die **Identität der Täter*innen zu ermitteln**. Insoweit führt die Gesetzesbegründung aus, dass ausdrücklich nur die Absicht einer zivilrechtlichen Durchsetzung verlangt wird, und nicht bereits die Einleitung eines zivilrechtlichen Gerichtsverfahrens, um den Betroffenen je nach Identität der Täter*innen noch eine **Entscheidungsoption** zu ermöglichen, etwa im Falle einer Verwandtschaftsbeziehung.[30] Zugleich stellt das GGDG-E auch fest, dass die ermittelten Identitäten und die gesicherten Informationen auch in einem späteren Strafverfahren verwendet werden dürfen, § 3 Abs. 4 S. 2 GGDG-E.

Dem GGDG-E kann insoweit die Zielsetzung entnommen werden, den **Durchsetzungsdruck** auf Täter*innen niederschwellig zu erhöhen. Und zwar auch in den Fällen, in denen eine strafrechtliche Relevanz vielleicht nicht gegeben ist, oder die Betroffenen eine strafrechtliche Durchsetzung für zu weitreichend halten. Vor dem Hintergrund ist nicht verständlich, warum das GGDG-E nur in den **ausdrücklich normierten Fällen** Anwendung finden soll. Gerade mit Hinblick der dem Ref-E zugrundeliegenden „**Verrohungstendenz**“ erschiene es sachdienlich, eine Möglichkeit zu schaffen, grundsätzlich **jegliche Rechtsverletzungen** effektiver verfolgen zu können. Insoweit sollte der Regelkatalog gänzlich aufgegeben werden, und im Sinne eines ganzheitlichen Ansatzes das Verfahren nach GGDG-E umfassend Anwendung finden, wenn Betroffene eine Rechtsgutsverletzung glaubhaft machen können. Als **vermittelnder Ansatz** wäre vorstellbar, dass dieser weite Anspruch insoweit in das Ermessen des Gerichts gestellt wird, also der Richtervorbehalt nicht nur prüft, ob eine Rechtsgutsverletzung hinreichend glaubhaft gemacht wurde, sondern auch ob eine Identitätsfeststellung in Verhältnis für die in Rede stehende Tat steht. Dieses **Ermessen** könnte insoweit durch den bestehenden **Regelkatalog** gebunden werden. So könnte etwa vorgesehen werden, dass jedenfalls in den Fällen der im Regelkatalog aufgeführten oder vergleichbarer Tatbestände die Identitätsfeststellung in jedem Fall im Verhältnis zur glaubhaft gemachten Tat stehe. Aktuell scheint ein **Wertungswiderspruch** zum vergleichsweise breiten Anspruch nach **§ 101 UrhG**.

30 Ref-E Begründung, Abschnitt B, zu Artikel 1, zu § 1, zu Abs. 3, zu Nummer 2, S. 49.

2.3.2 Beschränkung der Anwendbarkeit, Anbieter §§ 1, 4 GGDG-E

Insoweit das GGDG-E in dessen Begriffsbestimmungen **einzelne Formen der Anbieter** gesondert regelt, ist der Gesetzesbegründung zu entnehmen, dass hierdurch die Anwendbarkeit bewusst eingeschränkt werden sollte. Einerseits aufgrund vermuteter Umstände, dass bestimmte Dienste technisch für eine Tatbegehung nicht in Betracht kommen. Andererseits um bestimmte Dienste auszuschließen, bei denen die Tatbegehung derzeit allenfalls als Randphänomen wahrgenommen wird.[31]

Diese Unterscheidung erschien dem Gesetzgeber notwendig, um im Rahmen der **Account-Sperre** gesonderte Regelungen zu treffen. Denn diese Account-Sperre findet lediglich für Nutzerkonten in **Sozialen Netzwerken** statt.

Die Begründung sowie die Begrenzung der Account-Sperre auf Nutzerkonten in Sozialen Netzwerken erscheint inkonsistent. Die Gesetzesbegründung erweckt einerseits den Anschein, dass das GGDG-E im Gegensatz zum NetzDG einen umfassenderen Anspruch erhebt, mithin ausdrücklich keine besonderen Plattformen aufgrund ihrer primären vermeintlich Tat-aversen inhaltlich-fachlichen Ausrichtung ausschließen möchte, Stichwort Berufs- und Gaming-Plattformen. Denn die Vergangenheit habe gezeigt, dass sich Täter*innen entweder nicht von der offiziellen Intention einer Plattform einschränken lassen, oder der (befürchtete) Durchsetzungsdruck auf den weiteren Plattformen **Ausweich- und Fluchtbewegungen** zur Folge hatte. Jedenfalls konnten relevante (und steigende) Tatzahlen auch auf den Berufs- und Gaming-Plattformen festgestellt werden.

Hierbei **limitiert** der Gesetzgeber die **Durchsetzbarkeit** der GGDG-E bewusst und ohne Not. Einerseits verbleibt eine Unsicherheit, ob die durch den Gesetzgeber selbst erkannten Ausweichplattformen, d.h. Berufs- und Gaming-Plattformen, in Gänze von der Definition des Sozialen Netzwerks umfasst sind. Die Gesetzesbegründung lässt erkennen, dass es sehr wohl auf eine Schwerpunktsetzung der jeweiligen Plattformen ankommen soll, da dies ja aus Sicht der Begründung die Abgrenzung etwa zu Online-Marktplätzen erforderlich gemacht habe. Entsprechend lautet auch die Definition von Sozialen Netzwerken:

> ***Soziale Netzwerke im Sinne dieses Gesetzes sind Online-Plattformen im Sinne des Artikels 3 Buchstabe i der Verordnung (EU) 2022/2065, deren Hauptzweck oder wesentliche Funktion darin besteht, dass ihre Nutzer miteinander kommunizieren und interagieren, indem sie Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen.***

31 Ref-E Begründung, Abschnitt B, zu Artikel 1, zu § 1, zu Abs. 2 ff., insb. zu Abs. 4, S. 44; dort wird ausgeführt, dass Online-Marktplätze bewusst von Sozialen Netzwerken abzugrenzen waren. Wohl mit dem Effekt, Online-Marktplätze aus dem Anwendungsbereich auszunehmen da der „Hauptzweck“ eben nicht die Interaktion der Nutzer*innen sei.

Läge das GGDG-E wert auf eine effektive, uneingeschränkte Durchsetzbarkeit, so würde auf eine solche Limitierung verzichtet, einerseits um bereits alle bekannten Phänomene abbilden zu können, andererseits, um Verlagerungseffekte auf künftige Phänomene zu vermeiden oder jedenfalls zu reduzieren.

Derartige zukunftsgerichtete Überlegungen sind dem Ref-E auch nicht fremd. So heißt es in der Gesetzesbegründung[32]:

> ***Eine Sperrung des Nutzerkontos kann nur als Ultima Ratio vom Plattformbetreiber eingefordert werden. Sie muss daher erforderlich sein, um künftige Rechtsverletzungen zu verhindern. Aufgrund der gefestigten Rechtsprechung ist eine Aufnahme von Regelbeispielen in den Tatbestand nicht erforderlich. Eine solche liefe vielmehr Gefahr, die erforderliche Flexibilität der Rechtspraxis, gegebenenfalls auch kurzfristig auf neue Ausprägungen von Persönlichkeitsrechtsverletzungen im sich dynamisch entwickelnden digitalen Raum reagieren und Nachjustierungen hinsichtlich der Anforderungen vornehmen zu können, zu sehr einzuschränken.***

Vor diesem Hintergrund erscheint es an dieser Stelle jedenfalls fraglich, ob der Ref-E dem eigenen, „ganzheitlichen“ Anspruch im Rahmen der Durchsetzung gerecht wird.

2.3.2.1 Plattformen mit besonderen Schutzbedarfen der Nutzer*innen

Die **einschränkende Definition** der der von einer Account-Sperre betroffenen Anbieter hat möglicherweise zur Folge, dass gerade jene Plattformen, auf denen sich **besonders vulnerable Nutzergruppen** befinden, oder sich die Nutzer*innen in einem **besonders vulnerablen Umfeld befinden, ungeschützt** bleiben.

Dies sei bereits an den beiden – nach hiesiger Auffassung weiterhin nicht von der Definition des Sozialen Netzwerks umfassten – Plattform-Typen erläutert.

2.3.2.1.1 Plattformen im beruflichen, professionellen Kontext

Während **professionelle Berufsnetzwerke** einem Sozialen Netzwerk ähneln, muss deren Hauptzweck und Schwerpunkt nicht notwendigerweise in der individuellen Kommunikation und der Verbreitung von Inhalten liegen.

Es ist vorstellbar, dass sich Plattformen im beruflich-professionellen Umfeld entwickeln. Insoweit auch bereits auf dem Markt etabliert sind etwa Plattformen, die lediglich einen **Austausch der Nutzer*innen im Rahmen von Veranstaltungen** ermöglichen.

Hierbei ist der Primärzweck der Plattform, dass die Veranstalter die eigene Veranstaltung bewerben, und deren Operationalisierung erleichtern, etwa durch digitale Anmelde- und Registrierungsprozesse, durch zentrale digitalen Agenden. Die wesentlichen Inhalte – Existenz der Veranstaltung, sowie Untereinheiten – etwa konkrete Ereignisse entlang des Veranstaltungsablaufs – werden nicht von allen Nutzer*innen frei angelegt, sondern durch den Veranstalter. Nutzer*innen haben sodann etwa die Möglichkeit, generell zur Veranstaltung, oder zu den einzelnen Ereignissen zu kommentieren.

32 Ref-E Begründung, Abschnitt B, zu Artikel 1, zu § 4, zu Absatz 1 und zu Absatz 2, S. 54.

Ebenfalls etabliert sich, dass den Teilnehmer*innen neben diesem Primärzweck die Möglichkeit eingeräumt wird, niederschwellig mit weiteren Teilnehmer*innen der Veranstaltung in **private, bilaterale Kommunikation** einzutreten, etwa um bilaterale Gespräche zur Geschäftsanbahnung zu vereinbaren.

Einerseits ist nicht auszuschließen, dass die Kommentarfunktion auf derartigen Plattformen für öffentliche Straftaten gegen einzelne Teilnehmer*innen genutzt wird. Andererseits eröffnet die private Kommunikationsfunktion ein **Dunkelfeld** für etwaige Straftaten. Da sich die Betroffenen in diesem Falle in ihrem beruflichen und professionellen Umfeld befinden, bestärkt dies die **Vulnerabilität**.

Etwaigen Vorgesetzten oder wichtigen Geschäftspartnern entgegenzutreten, kann die eigene persönliche berufliche und professionelle Entwicklung der Betroffenen erheblich beeinflussen. Auch hier muss es möglich sein, dass Betroffene einer wiederholte Tatbegehung durch Account-Sperren entgegenwirken können.

2.3.2.1.2 Gaming-Plattformen

Hinsichtlich Gaming-Plattformen gilt entsprechendes. In diesem Fall ist zu beachten, dass die **besonders vulnerable Gruppe** höchstwahrscheinlich Kinder und Jugendliche sind, und die diese Gruppen gegenüber begangenen **Straftaten möglicherweise besonders schwerwiegend** sind.

Der Schwerpunkt und Hauptzweck einer Gaming-Plattform ist – auch bei Ermöglichung intensiver Kommunikationsmöglichkeiten – in der Regel gerade nicht die Kommunikation zwischen den Nutzer*innen. Diese Kommunikation ist lediglich ein Nebenzweck für das Spielerlebnis. Insoweit ist davon auszugehen, dass Gaming-Plattformen nicht unter die Definition des Sozialen Netzwerks fallen.

2.3.2.2 Weitere Plattformen

Die Ausführungen zu den zuvor benannten Plattform-Typen zeigen, dass die Definition von Sozialen Netzwerken im GGDG-E sehr limitierend ist. Die Gesetzesbegründung weist darauf hin, dass eine solche einschränkende Definition nur deshalb erforderlich war, um die Account-Sperre zu spezifizieren.

Es ist nicht ersichtlich, inwieweit Account-Sperren lediglich auf Soziale Netzwerk beschränkt sein müssen. Die Gesetzesbegründung weist daraufhin, dass eine Account-Sperre lediglich die Ultima Ratio der Handlungsoptionen sein soll. Zudem weist die Gesetzesbegründung daraufhin, dass die grundrechtliche Abwägung stets durch das Gericht im jeweiligen Einzelfall zu prüfen sei. Mithin geht selbst die derzeitige Regelung nicht davon aus, dass in allen Fällen per se eine Account-Sperre für Soziale Netzwerke verhältnismäßig wäre.

Soweit aber ohnehin eine **Einzelfallprüfung** anzustrengen ist, ist nicht erkennbar, warum diese für Soziale Netzwerke durch das Gericht durchgeführt werden kann, für andere Plattformen dem Gericht die nötige Kompetenz fehlen sollte.

Zudem ist zu beachten, dass eine Account-Sperre nur dann überhaupt in Betracht kommt, wenn durch die Täter*in **schwerwiegendste Straftaten** (im Einzelfall) oder ansonsten in nahezu **penetranter Wiederholung sonstige Rechtsgutsverletzungen** begangen wurden, und somit für die Zukunft eine weitere Wiederholungsgefahr besteht.

Vor diesem Hintergrund liegt also ein erheblicher Anteil der **Sanktionsfähigkeit der Täter*innen** in dem **eigenen, rechtswidrigen Verhalten**. Insoweit verringert sich deren grundrechtlicher Schutzbedarf gegenüber dem Schutzbedarf der Betroffenen. Hierbei ist es auch den Täter*innen überlassen, ob diese ihr rechtswidriges Verhalten auf für die Täter*innen privat oder beruflich besonders gewichtigen Plattformen begehen, oder ob sich die Täter*innen auf eher für sie selbst unwichtigen Plattformen rechtswidrig verhalten.

Bisher ist die Account-Sperre nur auf diejenigen Plattformen beschränkt, auf denen sich Täter*innen bereits rechtswidrig verhalten haben, sodass die obige Eigenverantwortung der Täter*innen auch entsprechend stark ins Gewicht fallen sollte. Siehe insoweit auch etwaige Ausführungen im Kontext des § 56c StGB unter 2.3.

2.3.2.3 Fazit

Das Gesetz sollte auf die **einschränkenden Definitionen** verzichten. Ein Nutzerkonto ist für jede Plattform von Relevanz, nicht nur für Soziale Netzwerke. Dies ergibt sich auch bereits aus § 2 GGDG-E.

Informationspflichtig sind die zu den Nutzer*innen gespeicherten Personalien, § 2 Abs. 2 Nr. 1 lit. a) GGDG-E, neben den sonstigen Informationen, z.B. die IP-Adresse, § 2 Abs. 2 Nr. 1 lit. b) GGDG-E. § 2 GGDG-E findet auf jegliche Online-Plattformen Anwendung, unabhängig ob es sich um ein soziales Netzwerk handelt. Die **Personalien** sind voraussichtlich gerade dann durch eine solche Plattform gespeichert, wenn die Täter*innen für die **Online-Plattform ein Nutzerkonto** unterhalten.

Eine solche Referenz zum Nutzerkonto erfolgt auch in § 2 Abs. 2 Nr. 1 lit. c) GGDG-E.

> ***die gespeicherte Internetprotokoll-Adresse einschließlich der Portnummer, die vor der Zustellung der gerichtlichen Anordnung bei Nutzung des betreffenden Nutzerkontos zuletzt verwendet wurde, und den Zeitpunkt des letzten Zugriffs unter Angabe der zugrunde liegenden Zeitzone,***

Somit stellt sich die Frage, ob diese Referenz dort bewusst eine Einschränkung der Anwendbarkeit auf Soziale Netzwerke beabsichtigt, oder ob dies ein der unnötigen begrifflichen Einschränkung geschuldeter Redaktionsfehler ist.

Die derzeitige Ausgestaltung lässt jedenfalls **signifikante Durchsetzungslücken** befürchten.

2.3.3 Beweissicherung und Verwertbarkeit im Strafverfahren

§ 3 Abs. 4 S. 2 GGDG-E ist insoweit unklar, durch wen die Informationen an die Strafverfolgungsbehörden weitergeleitet werden dürfen.

2.3.3.1 Anbieter als Regelungsadressat

Systematisch dürfte das Gesetz die **Anbieter** im Blick haben. Dies erscheint unlogisch, da die Anbieter selbst nicht über die Existenz eines Strafverfahrens bestimmen. Soweit ein Strafverfahren eingeleitet würde, würden die Strafverfolgungsbehörden möglicherweise selbst eine Identitätsfeststellung in die Wege leiten.

Wenn die **Strafverfolgungsbehörden** im Rahmen dieser Feststellung nicht auf eine bereits durchgeführte oder laufende Identitätsfeststellung auf Basis des GGDG-E hinweisen, ist nicht ersichtlich, wie Anbieter rechtmäßig auf die bereits bestehenden Informationen zurückgreifen können sollten.

Denn die nachvollziehbare strenge **Zweckbindung** der Datenverarbeitung im Rahmen der Identitätsfeststellung nach GGDG-E dürfte im Ergebnis eine getrennte Datenhaltung begründen und ein **Rechte- und Rollenkonzept** verlangen, auf dessen Basis bereits die weiteren Daten nur den konkret mit dem Fall betrauten Mitarbeitenden der Anbieter zugänglich sind. Für alle anderen Mitarbeitenden dürften überhaupt keine Zugriffsrechte – nicht einmal insoweit, dass die Existenz der Daten angezeigt würde – bestehen.

2.3.3.2 Gericht als Regelungsadressat

Wenn die **Strafverfolgungsbehörden** von dem bereits durchgeführten oder laufenden Identitätsfeststellung gem. GGDG-E wissen, ist es wesentlich naheliegender, dass sich die Strafverfolgungsbehörden die **Akten vom zuständigen Zivilgericht** übermitteln lassen. In diesem Fall würde sich § 3 Abs. 4 S. 2 GGDG-E nicht auf die Anbieter, sondern auf das Gericht beziehen.

2.3.3.3 Betroffene als Regelungsadressat

Ebenfalls vorstellbar ist, dass die Übermittlung durch die **Betroffenen** gemeint ist. Eine solche Übermittlung wäre für die Betroffenen aber ohnehin bereits zulässig. Eine Übermittlung der „Kopie des angegriffenen Inhalts“, § 2 Abs. 2 Nr. 3 GGDG-E, an die Strafverfolgungsbehörden durch Betroffene würde aber dem **gesetzlichen Zweck der Norm widersprechen**.

Laut Gesetzesbegründung soll eine Sicherung des angegriffenen Inhalts durch den Dienstanbieter erfolgen und an das Zivilgericht übermittelt werden, um die Betroffenen von etwaigen Vorwürfen der Manipulation der angegriffenen Inhalte freizumachen.[33] Dieser Vorwurf würde

33 Ref-E Begründung, Abschnitt B, zu Artikel 1, zu § 2, zu Abs. 2, zu Nummer 3, S. 48.

im – rechtlich deutlich schwerwiegenderen – Strafverfahren wieder aufkommen, wenn die Inhalte vom Zivilgericht zunächst an die Betroffenen ginge, um von dort wieder an die Strafverfolgungsbehörden weitergeleitet würde.

2.3.3.4 Generelle Zielsetzung der Norm – Datenschutz oder Sicherung der Beweisverwertung

Irritierend ist die Wortwahl der „Übermittlung“ und welches Ziel hiermit verfolgt wird. Die Wortwahl lässt darauf schließen, dass eine datenschutzrechtliche Erlaubnisnorm geschaffen werden sollte. Hierbei bliebe auch unklar, wer sich letztlich auf diese Erlaubnisnorm berufen dürfte – ungeachtet der Frage, ob es dieser Norm überhaupt bedurft hätte.

Vor diesem Hintergrund der Uneindeutigkeit des Regelungsziels, scheint zudem vorstellbar, dass der Gesetzgeber mit dieser Vorschrift sicherstellen wollte, dass die im Rahmen des **zivilrechtlichen Verfahrens** erhobenen und **gesicherten Beweise** tatsächlich in einem **nachgelagerten Strafverfahren verwendet** werden dürfen, wenn zum Zeitpunkt des Strafverfahren eine neuerliche Beweissicherung nicht mehr möglich wäre, vgl. auch die Effekte und die Zielsetzung aus § 3 Abs. 5 GGDG-E.

Insoweit ist anzumerken, dass im Strafrecht gem. § 250 StPO der **Unmittelbarkeitsgrundsatz** statuiert wird. Hiernach sind jegliche Beweise – soweit möglich – unmittelbar im Hauptsacheverfahren zu erheben. Sollte der **Gesetzgeber Risiken** hinsichtlich der Vereinbarkeit der nach GGDG-E erhobenen Beweise mit dem strafrechtlichen Unmittelbarkeitsgrundsatz erkannt haben, so sollte § 3 Abs. 4 S. 2 GGDG-E **dringend diesbezüglich nachgeschärft** werden.

2.4 Unzulänglichkeit der Informationen nach § 2 Abs. 2 GGDG-E

Das GGDG-E stellt in § 2 fest, welche Informationen durch Anbieter bereitgestellt werden müssen. Hierbei wird, in Ansehung des ganzheitlichen Charakters, davon ausgegangen, dass dies auch die Entsprechung der im Übrigen durch die Strafverfolgungsbehörden unmittelbar als für die Erhebung zulässig betrachteter Informationen betrifft.

Zumindest ist in Anrechnung zu bringen, dass das GGDG-E den Zweck verfolgt, die **Informationserhebung** und **Beweissicherung** zu **beschleunigen**, und etwa Verzögerungen aufgrund der hohen Belastung Strafverfolgungsbehörden sowie der Prüfanforderungen im Rahmen der Strafverfahren zu vermeiden. Zumindest erklärt sich vor diesem Hintergrund die Regelung des § 3 Abs. 4 S. 2 GGDG-E, auch wenn hier Klarstellungen erforderlich sein dürften.[34]

In Ansehung von § 3 Abs. 4 S. 2 GGDG-E erscheint eine solche Beschleunigung auch effektiv, da die Informationserhebung und die Beweissicherung höchst effizient erfolgen könnte. Hierzu sollten aber die **Fristen** und die **Effekte der Rechtsmittel** noch einmal sachdienlich überprüft und angepasst werden, vgl. 2.2.1 und 2.2.2.

Und dennoch bestehen **Bedenken**, ob das konkrete Verfahren hinsichtlich der betroffenen Informationen ausreicht. Während zivilrechtlich der Grundsatz „in dubio pro reo“ nicht gilt, verhindern im Strafrecht etwaige Zweifel an der Täterschaft eine etwaige Verurteilung. Insoweit sollte das GGDG-E etwaige Schutzbehauptungen antizipieren, um in den anschließenden oder parallelen Strafverfahren eine Verurteilung zu ermöglichen.

- § 2 Abs. 2 Nr. 1 GGDG-E ist sieht vor, dass die Personalien, soweit gespeichert, die IP-Adresse verbunden mit dem angegriffenen Inhalt und die IP-Adresse des letzten Login bereitzustellen sind, inklusive der Zeitstempel und der für die Zeitstempel gültigen Zeitzone.
- § 2 Abs. 2 Nr. 2 GGDG-E sieht vor, dass die Personalien bereitzustellen sind, die der Nutzer*in der IP-Adresse zum genannten Zeitpunkt zugewiesen war.

  Hierbei ist positiv hervorzuheben, dass in § 2 Abs. 2 Nr. 1 und Nr. 2 GGDG-E neben der reinen IP-Adresse auch die Port-Nummer erwähnt wird. Gerade im Falle von IPv4-Adressen ist diese notwendig, wenn sich mehrere Nutzerzugänge eine IP-Adresse[35] teilen. Dies ist insbesondere im Falle von mobilen Zugängen der Fall, einer immer wichtigeren Zugangsform.
- § 2 Abs. 2 Nr. 3 GGDG-E eine Kopie des angegriffenen Inhalts.

Dennoch bleiben Möglichkeiten zumindest **theoretischer Schutzbehauptungen**, die nachträglich aufgrund des Zeitablaufs und voraussichtlich unwiderruflich gelöschter Informationen bei den Anbietern nicht mehr widerlegt werden können, auf die im Einzelnen eingegangen wird.

34 Vgl. 2.3.3, insb. 2.3.3.4.

35 IP-Adresse meint im Folgenden, wenn nicht anders erwähnt, stets IP+Port+Zeitstempel und Zeitzone.

2.4.1 Nutzung des Anschlusses durch (unbekannte) Dritte oder Verwandte

In diesen Fällen ist **trotz Kenntnis der IP-Adresse** nicht final geklärt, welche natürliche Person die Tathandlung begangen hat. Diese Zuweisung auf eine **konkrete Person** ist allerdings für eine strafrechtliche Verurteilung notwendig.

Eine Widerlegung dieser Schutzbehauptung ist allenfalls möglich, soweit die **Endgeräte** der Verdächtigen **beschlagnahmt** und **forensisch ausgewertet** werden. Je nach in Rede stehender Tat könnte dies als unverhältnismäßig eingestuft werden.

Einerseits könnte rechtlich die Schwelle der **Verhältnismäßigkeit** überschritten sein, andererseits könnten die Strafverfolgungsbehörden im Rahmen des **Opportunitätsprinzips** die ohnehin knappen Ressourcen auf andere – schwerwiegendere – Straftaten verwenden wollen.

Fällt die strafrechtliche Ermittlung – und eine damit einhergehende Möglichkeit der Beschlagnahmung und / forensischen Auswertung – zeitlich auseinander zur zivilrechtlichen Anfrage, ist zudem davon auszugehen, dass etwaige Beweise auf den Endgeräten – mit mehr oder weniger Erfolg – in der **Zwischenzeit vernichtet** werden. Insofern bestehen erhebliche Bedenken, ob die bloße Kenntnis über den vermeintlichen Anschluss im Falle von **Mehrpersonenhaushalten** und / oder anderweitig von mehreren Personen genutzten Internetzugängen ausreicht.

Zwar ist zu erwarten, dass ein aktives Nutzerkonto etwa in Sozialen Medien weitere Informationen – etwa Bilder – der Täter*in beinhalten. Dies ist aber mit Nichten zwingend. Einerseits sind auch in Sozialen Netzwerken inzwischen viele Nutzer*innen sehr **bewusst** unter **Pseudonym ohne Bild** aktiv. Zudem ist nicht ausgeschlossen, dass für die Ausübung digitaler Gewalt dedizierte „**Hetz-Accounts**“ angelegt wurden, und diese Accounts in Ansehung der Identifikationsrisiken möglichst auf die Identifikation ermöglichende Informationen verzichten.

Spätestens wenn aber **Online-Plattformen** betroffenen sind, **die nicht Soziale Netzwerke sind**, ist die Ausgestaltung der im Nutzerkonto hinterlegten weiteren Informationen höchst variabel. Insoweit vorauszusetzen, dass im Falle der Schutzbehauptung aus den im Nutzerkonto (öffentlich) zugänglichen Informationen auf auf die Täter*in geschlossen werden kann, erscheint fahrlässig und naiv.

An dieser Stelle sei auf den – wohl ungewollten – begrifflichen **Zirkelschluss des Gesetzes** hingewiesen. Durch die Verwendung des Begriffs Nutzerkonto in § 2 Abs. 2 Nr. 1 GGDG-E findet dieser aufgrund des Wortlauts von § 1 Abs. 7 GGDG-E nur auf Soziale Netzwerke Anwendung. Ein Einschränkung, die als **Redaktionsversehen** betrachtet wird, da ausweislich der Gesetzesbegründung die Klarstellungen zu Sozialen Netzwerken aufgrund der Regelungen zur Account-Sperre aufgenommen wurden, nicht jedoch um etwaige Einschränkungen der Auskunftspflichten zu begründen.

Es wird daher empfohlen, neben der IP-Adresse auch **andere bei den Anbieter vorhandene Informationen zum Gegenstand der Auskunft** zu machen, soweit diese geeignet sind, die konkreten Nutzer*innen zu identifizieren.

Zu diesen Informationen gehören möglicherweise etwaige

- **Mac-Adressen** der genutzten Endgeräte,
- **sonstige Informationen**, die etwa im Rahmen des Fingerprintings erstellt wurden, oder
- etwaige **Geräte-Ids oder Session-Ids**, die dem Nutzerkonto und der Tathandlung zugeschrieben sind.

Insbesondere die langfristige Zuweisung von **Geräte- und Session-Ids** sind inzwischen eine Gute Praxis im Rahmen der IT-Sicherheitsmaßnahmen der Online-Plattformen. Nutzer*innen können die „aktiv eingeloggten“ Geräte bzw. Login-Sessions im Nutzerkonto einsehen, teilweise sogar mit einer weit zurückreichenden Historie.

Diese weiteren Merkmale sind ein relevanter Baustein, um einer Schutzbehauptung es gäbe „weitere Nutzer*innen des Internetanschlusses“ entgegenzutreten.

Auch diese Informationen sind keine Garantie, um diese Schutzbehauptung gänzlich erfolglos zu machen, insbesondere, wenn und soweit die Täter*innen etwaige nachgelagerte Ermittlungsmaßnahmen **antizipieren** und **Gegenmaßnahmen** bereits bei Begehung der Tat treffen bzw. wenn das zivilrechtliche Verfahren und etwaige Sicherungsmaßnahmen bei den Täter*innen zeitlich auseinanderfallen.

In diesen Fällen tritt neben der **geringfügigen kriminellen Energie** einer möglicherweise begangenen **Spontan-Tat** eine koordinierte und **hohe kriminelle Energie**, mit vorsätzlichen **Planungsbewusstsein** und **nachträglicher Verdeckungsabsicht**. Dies lässt erwarten, dass Straftaten von erheblicher Schwere im Raum stehen, und es sich um kein (relatives) Antragsdelikt mehr handelt. In diesen Fällen erfolgt die Informationsabfrage hoffentlich ohnehin primär durch die Strafverfolgungsbehörden, sodass jedenfalls die Risiken nachträglicher Verdeckungshandlungen, wie etwa einer Beweisvernichtung, deutlich reduziert sind.

2.4.2 Hack des Nutzerkontos

Soweit die Schutzbehauptung eines „Hacks der Nutzerkontos“ vorgetragen wird, gelten zunächst die Ausführung in 2.4.1 entsprechend. Insbesondere die Kenntnis der Geräte- und Login-Session könnten hinreichende Anhaltspunkte bieten, diese Schutzbehauptung zu erschüttern.

Ergänzend müssten sich im Falle eines Hacks weitere **Unregelmäßigkeiten** in den **Internetzugängen** finden, die für die Verwendung des Nutzerkontos genutzt wurden, soweit der Hack einen „Fernzugriff“ auf das Nutzerkonto zur Folge hatte.

Sind keine **Unregelmäßigkeiten** im Rahmen der **IP-Adressen** noch der **Geräte- und Session-Ids** erkennbar, käme allenfalls ein Hack durch auf dem Endgerät installierte Malware in Betracht, die einen validen Login der vermeintlichen Täter*innen aufgreift, und somit die Tathandlung remote über den validen Login der vermeintlichen Täter*innen und deren Endgeräte begangen wird. In diesen Fällen sollte aber eine **forensische Untersuchung** der in Verdacht stehenden Endgeräte eben solche **Malware** nachweisen können.

Dies führt zu weiteren Überlegungen. Der **Auskunftsanspruch** ist derzeit **nicht geeignet**, eine **Plausibilisierung der Informationen** durchzuführen, oder Erkenntnislücken aus den nahezu zufällig gewählten Zeitpunkten der IP-Adressen zu schließen.

Die Gesetzesbegründung stellt selbst fest, dass es vorstellbar ist, dass – gerade im Falle der Verwendung von mobilen Endgeräten – Täter*innen zum Zeitpunkt der Tathandlung und/oder des letzten Logins in einem **öffentlichen Netzwerk** eingeloggt waren. In diesem Fall würde eine Identifizierung ohne weitere Informationen, vgl. in 2.4.1, vermutlich sofort ins Leere laufen.

Insoweit wird empfohlen, die Auskunftspflicht um **weitere Zeitpunkte zu erweitern**. Sowohl in die **Vergangenheit**, als auch in die **Zukunft**. Soweit der Gesetzgeber die konkreten Werte nicht festlegen möchte, kann dies auch in das Ermessen des mit der Entscheidung befassten Gerichts gestellt werden.

Vorstellbar scheint:

n-IP-Adressen unmittelbar vor und nach der in Rede stehenden **Tathandlung**; wobei ein maximaler Wert von n=5 sehr zielführend erscheint

- IP-Adressen der n **letzten Zugriffe / Aktivitäten des Nutzerkontos**; wobei ein maximaler Wert von n=5 sehr zielführend erscheint; wobei in Abweichung zum aktuellen Wortlaut von § 2 Abs. 2 Nr. 1 lit. c) GGDG-E klargestellt werden sollte, dass es sich um eine unmittelbare (menschliche) Nutzung handeln muss; soweit Online-Plattformen Interaktions-API bereitstellen, könnte die „letzte“ IP-Adresse ansonsten die IP-Adresse eines API-Proxies sein.

2.4.3 Übertragungsfehler der IP-Adressen; fehlerhafte Zeitstempel

Eine bereits aus den urheberrechtlichen Streitigkeiten bekannte Schutzbehauptung betrifft etwaige „**Übertragungsfehler**“.

Diese Übertragungsfehler seien entweder eine Folge menschlichen Versagens – falsch kopiert, falsch abgeschrieben, in der Zeile verrutscht. Oder eine Folge technischer Fehler, wie etwa einem fehlerhaften Zeitstempel. Dieser fehlerhafte Zeitstempel hätte dazu geführt, dass aufgrund der dynamischen IP-Adresse der falsche Internetanschluss identifiziert wurde.

Diese Schutzbehauptung lässt sich insoweit entkräften, wenn wenige, aber in Summe hocheffiziente Maßnahmen getroffen werden.

2.4.3.1 (voll)-automatisierung der Abfragen

Jedenfalls die Behauptung menschlichen Versagens aufgrund von Übertragungsfehlern kann durch eine weitreichende **Automatisierung** entkräftet werden.

Fehler könnten bei einer Automatisierung am Anfang entstehen, weil etwa die falsche „Nutzeraktivität“ als Referenzpunkt gesetzt wird. Dies würde aber aufgrund der bereitgestellten Informationen (Kopie) gem. § 2 Abs. 2 Nr. 3 GGDG-E erkennbar sein.

Fehler könnten im Übrigen aufgrund eines grundsätzlichen Fehlers in der Automatisierungslogik entstehen. Derartige behauptete Fehler können leicht durch eine Prüfung der implementierten Logiken entweder verifiziert oder falsifiziert werden.

2.4.3.2 falscher Zeitstempel bei Diensteanbieter

Vorstellbar erscheint die Behauptung, dass der durch den Diensteanbieter bereitgestellte Zeitstempel fehlerhaft sei.

Der **Zeitstempel** folgt in der Regel der **Server-Zeit**. Diese kann, wie jede andere Uhr, falsch eingestellt sein. Dies wird heutzutage eigentlich durch regelmäßige **Synchronisation** mit Zeitservern vermieden. Es ist aber nicht ausgeschlossen, dass derartige Synchronisationsvorgänge fehlerbehaftet sind, oder sich die Serverzeit zwischen den jeweiligen Synchronisationsvorgängen verstellt hat.

Gerade in komplexen Systemstrukturen haben die Plattformbetreiber ein hohes **Eigeninteresse**, dass die Server-Zeit auf allen (eigenen) Servern identisch ist und diese auch synchron mit weiteren (externen) Servern ist, da deren eigene Funktionalität in höchstem Maße von korrekten Zeitstempeln abhängig ist.

Trotzdessen ist nicht ausgeschlossen, dass einer derartige Schutzbehauptung vorgetragen wird. Möglicherweise verfängt dieser Vortrag, da die zur Auskunft verpflichtete Online-Plattform relativ klein ist, und kein besonderes Eigeninteresse an einer korrekten Server-Zeit hat.

In diesen Fällen wäre es dennoch ziemlich einfach dieser Schutzbehauptung entgegen zutreten, nämlich indem neben dem Zeitstempel (und Zeitzone) zwei **weitere Informationen** bereitgestellt werden:

- **implementierte Maßnahmen** zur Synchronisation der Server-Zeit, inklusive Bestätigung / relevanter Teilauszug aus den erfolgreichen **Synchronsisations-Protokollen**
- ein **aktueller Zeitstempel** zum Zeitpunkt der Informationsermittlung nebst einem **zeitgleich** von einem **offiziellen Zeitserver abgerufenen Zeitstempel**. .

Die erste Information lässt erkennen, ob grundsätzlich die Validität der Zeitstempel vorausgesetzt werden kann.

Die zweite Informationen sichert diese Vermutung der ersten Information ergänzend ab. Sollte wider Erwarten eine Abweichung auftreten können (oder sollten keine Prozesse zur Sicherung der Validität des Zeitstempels implementiert sein), ließen die aktuellen Zeitstempel Rückschlüsse über das einschlägige Zeitfenster zu, um welches der Zeitstempel des Logeintrags „fehlerhaft“ sein könnte. Diese Information einer **Eventualabweichung** könnte für eine **erweiterte Sicherung** bei den Internetzugangsanbietern genutzt werden.

2.4.3.3 falscher Zeitstempel bei Internetzugangsanbieter

Auch **Internetzugangsanbieter** können dem Vorwurf ausgesetzt sein, dass deren Zeitstempel fehlerhaft seien. Insoweit gelten zunächst die Ausführungen zu 2.4.3.2 entsprechend.

Ergänzend können auch hier **vorsorgliche Sicherungsmechanismen** etabliert werden. So könnten die Internetzugangsanbieter stets verpflichtet werden, neben den Zuordnungen für den konkreten Zeitstempel alle weiteren Zuordnungen zu der IP-Adresse in einem Zeitraum n ebenfalls in den eigenen System zu sichern. Der konkrete Zeitraum n gälte es auf Basis der vorstellbaren Abweichungen zu ermitteln; eine Zeitspanne von mehr als 5min erscheint aber besonders rechtfertigungsbedürftig, bringt man in Ansatz, dass Telekommunikationsanbieter, von denen Internetzugangsanbieter eine Untergruppe sind, besondere Sorgfaltspflichten in diesem Bereich treffen.

Unabhängig der „**Regelabweichung**“ sind etwaige **Streubreiten** aufgrund der in 2.4.3.2 erkannten möglicherweise fehlerhaften Zeitstempel ergänzend zu berücksichtigen.

Es ist hervorzuheben, dass auch im Sinne der **grundrechtlichen** Überlegungen der **Fehlidentifikation Sicherungsmechanismen** im Verfahren vorgesehen werden sollten.

- Internetzugangsanbieter sollten zwar verpflichtet sein, die **weiteren Zuordnungen** zu **sichern**; die übermittelten **Personalien** sollten aber in der Regel nur **einen konkreten**, vom Gericht bei der Anfrage **identifizierten Zeitstempel betreffen**.

- Soweit das **Gericht** in den von den Diensteanbietern erhaltenen Informationen relevante **Unschärfen erkennt**, die eine Begrenzung auf einen konkreten Zeitstempel verunmöglicht, soll das Gericht den Umfang der erstmalig zu übermittelnden Daten **verhältnismäßig erweitern** können, soweit diese bereits Gegenstand der erweiterten Sicherung der Informationen durch die Internetzugangsanbieter sind;

- Es ist sicherzustellen, dass im Falle von bereits durch das Gericht **erkannte Unschärfen**, die **Plausibilitätsprüfung** der zutreffenden Identität **durch** das **Gericht** erfolgt, und etwaige Personalien **unbeteiligter Dritter** zunächst nicht Gegenstand der Akte(nteile) werden, auf die die weiteren Verfahrensbeteiligten Zugriff haben.

- Das **Gericht** hat darauf **hinzuweisen**, wenn die Identifikation aufgrund der IP-Adresse nicht ein-eindeutig war, sondern aufgrund der **Korrelation mehrerer Personalien** und **Zeitstempel** abgeleitet bzw. plausibilisiert wurde. Für diesen Fall soll es den vermeintlichen **Täter*innen** ermöglicht werden, diese abgeleitete **Identifikation** unter Wahrung der Rechte unbeteiligter Dritter angemessen in Zweifel zu ziehen und zum **Gegenstand einer Überprüfung** machen zu können.

2.4.3.4 (asynchrone) „Aktualisierungsverzögerungen“ der Zuweisungsdatenbank bei Internetzugangsanbietern bzw. der gespeicherten Logfiles der Diensteanbieter

Es ist eine Schutzbehauptung vorstellbar, in dem Täter*innen behaupten, dass die Zuweisung der Personalien deswegen fehlerhaft sei, weil die Zuweisungsdatenbank der Internetzugangsanbieter einen minimalen zeitlichen Verzug aufweise, oder weil die Speicherung des Logeintrags bei den Diensteanbietern einen minimalen Verzug aufweise.

Hierbei ist zu berücksichtigen, dass gerade im Bereich des mobilen Internets eine neue Zuweisung bereits durch Wechsel der Funkzelle erfolgen kann und dass Zeitstempel bis auf die Millisekunde exakt sind. Zumindest in der Theorie ist möglich, dass die Abweichung von nur einer Millisekunde zu einer Abweichung in den ausgelesenen Personalien führen könnte.

Dieser **theoretischen Schutzbehauptung** könnte mit entsprechender Ergänzung der zu sichernden Informationen entgegen getreten werden. Insoweit wird auf 2.4.3.2 und 2.4.3.3 verwiesen. Im **Zusammenspiel des Vorgesagten** wäre auch diese – sicherlich höchst theoretische – Schutzbehauptung in den meisten Fällen entkräftet.

2.4.4 Fake-Account, Identitätsdiebstahl

Der Ref-E erkannt an, dass es durchaus eine neue **Gefährdungslage** des **Identitätsmissbrauchs** durch „**Fake-Accounts**“ gibt.

2.4.4.1 Abfrage von Bestandsdaten, Verhältnis zur IP-Adressen

Die Gesetzesbegründung lässt hierbei erkennen, dass der Gesetzgeber sich bei der Abfrage der Bestandsdaten bei Internetzugangsanbietern im Wesentlichen auf die **ladungsfähige Anschrift** fokussiert hat, aber wohl nicht die Risiken eines Identitätsdiebstahls berücksichtigt.[36]

So heißt es dort:

> ***In einem zweiten Schritt sind regelmäßig die bei dem Anbieter von Internetzugangsdiensten hinterlegten Bestandsdaten erforderlich, wenn die bei dem Diensteanbieter hinterlegten Daten nicht zur Identifizierung des Nutzers, dem die Rechtsverletzung vorgeworfen wird, ausreichen. Nutzerkonten bei Diensteanbietern werden häufig unter Pseudonymen ohne Angabe einer ladungsfähigen Anschrift erstellt; in der Regel genügt die Angabe eines (fiktiven) Namens und einer E-Mail-Adresse. Folglich reicht die Mitteilung der bei dem Diensteanbieter vorhandenen Daten zur Identifizierung in der Regel nicht aus. Um eine effektive Rechtsverfolgung und den grundrechtlich gebotenen Rechtsschutz zu ermöglichen, ist daher die Zuordnung der beim Diensteanbieter protokollierten dynamischen IP-Adresse durch den jeweiligen Internetzugangsanbieter unter Berücksichtigung des exakten Zeitstempels zwingend erforderlich, da eine Identifizierung auf anderem Wege regelmäßig ausscheidet.***

Dabei ist der Gesetzgeber selbst **inkonsistent**. Einerseits schränkt er die Erforderlichkeit auf die Fälle ein, in denen die Personalien der Diensteanbieter nicht genügen. Insoweit scheint der Gesetzgeber hier eine gedankliche Bedingung für die Zulässigkeit der Abfrage bei Internetdiensteanbietern zu etablieren: „Nur wenn die Personalien nicht genügen, dann darf auch die IP-Adresse herangezogen werden.“ Zugleich erwähnt die Gesetzesbegründung, dass diese ergänzenden Informationen für eine grundrechtlich gebotene Rechtsverfolgung zwingend seien. Entweder ist etwas zwingend (in allen Fällen), oder eine im Einzelfall erforderliche Information je nach Faktenlage.

Der **Richtervorbehalt** für jede einzelne Anordnung verlangt, dass das Gericht somit nach der Anordnung gegenüber den Diensteanbietern eine weitere Anordnung gegenüber den Internetzugangsanbietern erlassen muss. Aufgrund des „**Erforderlichkeitsgebots**“ in § 2 Abs. 1 GGDG-E, das für diese zweite Anordnung erneut zu prüfen sei, ergibt sich aus der Gesetzesbegründung, dass Gerichte eine Anordnung nach § 2 Abs. 2 Nr. 2 GGDG-E dann ablehnen können oder gar sollten, wenn die Diensteanbieter bereits einen umfassenden (aber **nicht verifizierten) Datensatz** übermittelt haben.

Die Erkenntnis eines **Identitätsmissbrauchs** würde zwar sodann eine nachgelagerte Abfrage ermöglichen. Zu diesem Zeitpunkt ist aber davon auszugehen, dass zur **Tathandlung keine notwendigen Informationen mehr vorliegen**. Hinsichtlich einer zeitlichen Beschleunigung des Verfahrens wird zudem auf 2.2.2 verwiesen.

36 Ref-E Begründung, Abschnitt B zu Artikel 1 zu § 2, zu Absatz 2, zu Nummer 2, S. 48.

Im Übrigen sollte inhaltlich klargestellt werden, dass es in **allen Fällen zwingend** ist, auch die **Identitätsdaten mit Hilfe der IP-Adresse** zumindest **zu plausibilisieren**. Insoweit wird auch auf die Ausführungen unter 2.4.1, 2.4.2, 2.4.3.2, 2.4.3.3, sowie 2.4.3.4 verwiesen, woraus sich ergänzende Informationen als erforderlich erweisen.

Insoweit wird auch ausdrücklich empfohlen, die **Beweissicherung** nach § 3 GGDG-E **nicht einzuschränken**, sondern auf alle Informationen nach § 2 Abs. 2 GGDG-E zu erstrecken, inklusive der für die Ermittlung der Informationen möglicherweise anfallenden **Zwischeninformationen**.

Soweit der Gesetzgeber ledilgich die **Zustellung erleichtern** wollte, läge es im Ermessen und in den Möglichkeiten des Gesetzgebers, die förmliche Zustellung, soweit erforderlich, anzupassen und eine Zustellung etwa an die hinterlegte E-Mailadresse genügen zu lassen. Ein solcher Ansatz ist § 5 und § 6 GGDG-E auch zu entnehmen, wobei sich § 5 Abs. 3 GGDG-E nur auf formlose Dokumente bezieht. § 6 Abs. 2 GGDG-E kann aber als eine Modifikation der förmlichen Zugangsregeln verstanden werden. Anstelle die Täter*innen unmittelbar über die Eröffnung des Verfahrens zu informieren, etabliert § 6 Abs. 2 GGDG-E ein Auffangverfahren. Hierbei werden die Diensteanbieter zu Ersatzzustellbevollmächtigten und Ersatzempfangsberechtigten, ähnlich eines Rechtsbeistands. Über die Sinnhaftigkeit, Diensteanbieter derart intensiv in das Verfahren einzubinden, lässt sich streiten, und es wird auf 2.2.1 verwiesen.

Insoweit sollte einerseits das Verfahren dahingehend präzisiert werden, sodass sich etwaige Kunstgriffe des derzeitigen Ref-E erübrigen.

2.4.4.2 weitere sinnvolle Informationen und Anbieter

Es ist je nach Diensteanbieter vorstellbar, dass entweder die Nutzer*innen selbst diese Online-Plattform zur **Monetarisierung** nutzen, oder aber auf der Online-Plattform etwaige **kostenpflichtige Premium-Dienste** in Anspruch nehmen, oder aber die Online-Plattform selbst **Zahlungsdienste** bereitstellt.

Insofern ist davon auszugehen, dass Nutzer*innen auch etwaige **Zahlungsinformationen** mit dem Nutzungskonto verknüpft haben oder Zahlungsinformationen (**Kreditkartendaten** oder **Kontodaten**) hinterlegt haben.

Insoweit sollte überlegt werden, den **Informationsanspruch** auf derartige Informationen **auszudehnen** und auch entsprechend **weitere Anbieter** für eine Informationsbereitstellung zu verpflichten. Soweit „**Gutschein- oder Zahlungskarten**“ für etwaige Zahlungen an den Diensteanbieter genutzt werden, sind auch diese teilweise rückverfolgbar; jedenfalls, soweit diese nicht lokal durch Bargeld erworben wurden.[37] Auch im Digitalen gilt: folgt man dem Geldfluss, findet man die Quelle. Siehe zudem auch 5.2.

37 Allerdings verbietet sich eine unwiderlegliche Vermutung, da diese Gutscheinkarten, wie der Name schon sagt, nicht personengebunden sind, und durchaus verschenkt, weiterverkauft oder anderweitig die Besitzer*innen wechseln können.

2.4.5 Nachträgliche Änderungen der Inhalte und Personalien durch Täter*in

§ 2 Abs. 2 Nr. 3 GGDG-E schreibt vor, dass der angegriffene Inhalt durch die Diensteanbieter in **Kopie** an Betroffene zu übermitteln sei; insoweit besteht auch eine teilweise Redundanz zu den Regelungen des § 3 Abs. 1 GGDG-E.

Die Gesetzesbegründung gibt zu verstehen, dass diese Norm insbesondere notwendig erscheint, um etwaigen Behauptungen der Täter*innen entgegen zu treten, dass die **Betroffenen** die Inhalte nachträglich selbst **manipuliert** hätten.[38]

2.4.5.1 Redundanz und Wirkungslosigkeit der §§2 und 3 GGDG-E

Zunächst ist festzuhalten, dass die **Redundanzen** der §§ 2 und 3 GGDG-E unnötig sind. Der durch § 2 GGDG-E intendierte Zweck einer Vermeidung der Manipulationsvorwürfe ist in dem Moment obsolet, in dem die Kopie der Inhalte wieder in den alleinigen Verfügungsbereich der Betroffenen übergeht.

2.4.5.1.1 Verwaltung der gesicherten Informationen durch das Gericht

Insoweit ist die Regelung des § 3 GGDG-E durchaus zu begrüßen, dass eine **Kopie der angegriffenen Inhalte** zu erstellen ist. Die Regelung lässt zunächst offen, was mit der Kopie der Informationen erfolgen soll; ob diese etwa unmittelbar an das Gericht zu übermitteln sind, oder ob die Informationen bis auf Weiteres im Verfügungsbereich der Diensteanbieter verbleiben sollen, oder ggf. sogar beides erwartet wird.

§ 3 Abs. 2 GGDG-E schafft insoweit Klarheit, da Diensteanbieter angeordnet werden, die Informationen dem Gericht „**in Textform**“ zu übermitteln. Positiv ist, dass hierdurch die Informationen ab diesem Zeitpunkt (auch) dem Gericht vorliegen und durch das Gericht verwaltet werden. Etwaige Manipulationen durch an dem Verfahren Beteiligte sind somit wohl grundsätzlich auszuschließen.

2.4.5.1.2 Beweiswert der durch das Gericht verwalteten Informationen

Insoweit ist aber die Gesetzesbegründung **inkonsistent**: Gegenstand des erhöhten **Beweiswertes** sollten und können eigentlich nur die bei Gericht eingegangenen und durch das Gericht verwalteten Informationen haben. So heißt es konkret:

> ***Zwar werden Betroffene in aller Regel ihrem Antrag einen Screenshot beifügen, der die behauptete Rechtsverletzung beweisen soll. Allerdings kann es vorkommen, dass der rechtsverletzende Inhalt bis zur Entscheidung des Gerichts gelöscht wird. In einem solchen Fall ist der Beweisführer regelmäßig dem Vorwurf ausgesetzt, den Screenshot gefälscht oder manipuliert zu haben. Diesem Einwand kann mit der vom Diensteanbieter erstellten Kopie entgegengetreten werden, sodass ein Gericht dem Screenshot einen höheren Beweiswert zu sprechen kann.***

38 Ref-E Begründung, Abschnitt B zu Artikel 1 zu § 2, zu Absatz 2, zu Nummer 3 S. 48.

Warum die durch die Diensteanbieter erstellte Kopie dem durch die Betroffenen erstellten Screenshot einen erhöhten Beweiswert ermöglichen soll, ist nicht nachvollziehbar. Zumal die Gesetzesbegründung offenlässt, was in den Fällen passiert, in denen ein Widerspruch zwischen Screenshot der Betroffenen und durch den Diensteanbieter gesicherten Informationen festgestellt wird.

Im Falle eines Widerspruchs ist – nach jetziger Formulierung des Gesetzes – eigentlich davon auszugehen, dass den durch den **Diensteanbieter gesicherten** und an das Gericht **übermittelten** Informationen der **höhere Beweiswert** im Rahmen einer Beweiswürdigung zukommen würde.

Denn einerseits sind die bei der Sicherung beteiligten Parteien nicht Beteiligte des Verfahrens, somit sollten diese also – in der Regel – keine **Interessenkonflikte** haben, die eine eigenständige Manipulation der Informationen erwarten ließe.[39] Im Anschluss werden die Informationen durch das Gericht verwaltet. Die **Rechtsstaatlichkeitsprinzipien** verlangen an dieser Stelle bereits, dass die Informationen nicht durch das Gericht manipuliert werden. Betroffene müssten also vermutlich erhebliche Umstände vortragen, die den durch das Gericht gesicherten Beweiswert erschüttern könnten; realistisch kann davon ausgegangen werden, dass Betroffene diese Hürde nicht überwinden können.

Denn man muss diese Überlegung auch von der anderen Seite her anstellen: Wenn die Informationen des Diensteanbieters und der Screenshot sich nicht widersprechen, muss auch die **Möglichkeit** für Täter*innen bestehen, sich **effektiv zu verteidigen**. Insoweit müssten auch die Täter*innen den Beweiswert der gesicherten Informationen anzweifeln können.

Wenn also Betroffene den **Beweiswert** im Falle von Widersprüchen aus Sicht des Gesetzgebers leicht **erschüttern** könnten, so könnten Täter*innen den Beweiswert vermutlich ebenso leicht im Falle konsistenter Informationen erschüttern.

Das würde im Ergebnis aber bedeuten, dass die **Beweissicherung** derzeit an **mindestens** einer Stelle einen **erheblichen Konstruktionsfehler** aufweisen müsste, und die gesetzliche **Regelung** derzeit also den **intendierten Zweck nicht erreichen kann**. Einige Schwachstellen im Rahmen der Beweissicherung sollen im Folgenden dargestellt werden, deren Auflösung durch den Gesetzgeber vermutlich ohne besondere Aufwände möglich wäre.

39 Es wird zwar durchaus stellenweise vorgetragen, dass Diensteanbieter aufgrund ihres Finanzierungsmodells von Aufmerksamkeit-heischenden und rechtswidrigen Inhalten profitieren, da dies die Zahl der „aktiven“ Nutzer*innen vergrößere. Hierbei scheinen aber unterschiedliche Ebenen betroffenen, nämlich einerseits das allgemeine Geschäftsmodell, und andererseits die bilaterale Geschäftsbeziehung; eine unmittelbare Interessenkollision im Einzelfall scheint aus diesem Grund nicht ohne Weiteres überzeugend, sollte aber natürlich im Rahmen einer künftigen Evaluation der rechtlichen Rahmenbedingungen in untersucht werden.

2.4.5.1.3 Für forensische Untersuchungen ungeeignetes Datenformat

Das Gesetz schreibt vor, dass die Informationen an das Gericht „**in Textform**“ übermittelt werden sollen, § 3 Abs. 2 GGDG-E. Hierbei lässt weder das Gesetz, noch die Gesetzesbegründung erkennen, wie „Textform“ in diesem Kontext zu verstehen ist. Textform ist per definitionem in Abgrenzung zur Schriftform zu verstehen. D.h., es kommt nur darauf an, dass der Inhalt lesbar ist und auf einem dauerhaften Datenträger erfolgt, und zwar dergestalt, dass es möglich ist, eine auf dem Datenträger befindliche Erklärung so aufzubewahren oder zu speichern, dass diese während eines für ihren Zweck angemessenen Zeitraums zugänglich ist, und die Erklärung unverändert wiedergegeben werden kann.

Insoweit wird auf etwaige qualifizierende Merkmale der Urheberschaft der Erklärung im Vergleich zur Schriftform verzichtet. Textform ist insoweit also keine weitere Ausgestaltung des Datenformats, oder eine Sicherstellung in der Gestalt, dass eine weitere Analyse der übermittelten Informationen ermöglicht wird.

Nach den obigen Ausführungen, wäre eine **Übermittlung der Informationen im Rohformat**, also als exportierte Zeilen der log-Dateien, als exportierte Datensätze der Datenbank, oder als eine – alle Sourcen inkludierende – HTML-Datei, oder eine sonstige ausführbare Datei **vorstellbar**. Hierbei ist nicht sichergestellt, dass die übermittelten **Dateiformate ohne proprietäre** Software ausgelesen werden können. **Ebenso** würde es aber auch **genügen**, wenn die Informationen durch die Diensteanbieter in Form von **(virtuellen) Screenshots** an das Gericht übermittelt würden.

Bloße (virtuelle) Screenshots verhindern jegliche, künftige **forensische Untersuchung** der Informationen auf etwaige Manipulationen oder sonstige, ggf. verfahrensrelevante Zusammenhänge. Die Übermittlung in Form **proprietärer Formate** würde es den Diensteanbietern ermöglichen, den Anordnungen Folge zu leisten, ohne dass die Gerichte (oder Betroffenen) im Anschluss mit angemessenem Aufwand die Informationen verwenden könnten; es stünde sogar zu befürchten, dass die Diensteanbieter an dieser Stelle ein **profitables Geschäft** wittern dahingehend, dass für die Verwertung der bereitgestellten Informationen durch die Diensteanbieter lizenzierte Dienstleistungen in Anspruch genommen werden müssten.

Insoweit wird empfohlen, das GGDG-E nachzuschärfen, um die für die **rechtsstaatliche** und **effektive Verfahrensführung notwendigen Informationen** jedenfalls bei Gericht vorrätig zu halten.

Zwar ist vorstellbar, dass dem Gericht zunächst nur durch die Diensteanbieter erstellte (virtuelle) Screenshots bereitgestellt werden, und weitere Informationen nur dann durch das Gericht abgerufen werden können, wenn dies im Verlauf des Verfahrens erforderlich wird. Dieser Ansatz birgt aber das **Risiko**, dass die **Informationen** bei **einer privaten Stelle vorgehalten**

werden, und somit diese private Stelle einerseits für diese Sicherung **kompensatoriche Maßnahmen** erwartet oder aber, die private Stelle – absichtlich oder unabsichtlich – die **Informationen verliert** oder **verändert**.

2.4.5.1.4 Unzureichender Sicherungszeitraum

§ 3 Abs. 1 GGDG-E stellt sicher, dass die Informationen bei Anbietern bis zum **Abschluss des Verfahrens** vorgehalten werden müssen. Das GGDG-E enthält insoweit keine weiteren Klarstellungen, auf welches Verfahren sich die Regelung bezieht.

Vorstellbar ist:

- ausschließlich das **zivilrechtliche Auskunftsverfahren** gem. GGDG-E
- einschließlich etwaiger **zivilrechtlicher Verfahren im Anschluss**, wobei es zu klären gälte, was passiert, wenn ein solches zivilrechtliches Verfahren nicht „sofort“, „in definierter angemessener Zeit“, „während der Verjährungsfristen“ durch die Betroffenen angestrengt wird
- einschließlich etwaiger **strafrechtlicher Verfahren im Anschluss**, wobei sich ähnliche Fragestellungen wie für etwaige zivilrechtliche Verfahren stellen.

§ 3 Abs. 5 GGDG-E lässt hier eine eindeutige Wertung erkennen, nämlich dahingehend, dass ausschließlich das **zivilrechtliche Auskunftsverfahren** gem. GGDG-E gemeint sein soll. Hierbei kann § 3 Abs. 5 S. 2 GGDG-E sogar so verstanden werden, dass die Anbieter die eigene Kopie mit Erfüllung der Auskunft sofort irreversibel zu löschen haben, und zwar ungeachtet, ob das Verfahren rechtskräftig abgeschlossen wurde. Letzteres ist insoweit nachvollziehbar, da gem. § 5 Abs. 4 GGDG-E Entscheidungen erst mit Rechtskraft wirksam werden, was aus anderen Gründen möglicherweise und unnötig das Verfahrensziel gefährdet, vgl. 2.2.2.

Aber selbst, wenn man diese **Rechtskraftregelung** für **erforderlich** hält, ist davon auszugehen, dass die Beteiligten erst zu diesem Zeitpunkt **erstmalig** die von den Anbietern bereitgestellten Informationen **erhalten** und einsehen können. Sollten die Beteiligten, hier insbesondere die Betroffenen, **Zweifel** an den übermittelten Informationen anzeigen, könnten diese aufgrund der unmittelbaren **irreversiblen Löschung nicht mehr** im Rahmen des Verfahrens **ausgeräumt werden**.

Insoweit sind dringend **Klarstellungen** angeraten, die sowohl

- eine vollständige **Überführung** der Informationen in einem **Format** an das Gericht sicherstellt, die auch anschließende (**forensische**) **Untersuchungen** der Informationen **ermöglichen**

- insoweit diese Informationen, die nach § 3 GGDG-E nicht mehr lediglich Informationen darstellen, sondern wohl **gerichtlich erhobene Beweise**, diese auch in **Folgeverfahren** im jeweils gebotenen Umfang **zur Verfügung** stehen, vgl. auch **Klarstellungsbedarf für strafrechtliche Verfahren** unter 2.3.3.

2.4.5.1.5 Unzureichender Sicherungsumfang

Die von der Sicherung umfassten Informationen sind **inhaltlich** gegenüber dem Informationsanspruch **beschränkt**, jedenfalls lässt die derzeitige Formulierung Spielraum dahingehend, dass wichtige (**Zwischen-)Informationen** nicht von einer **Sicherungsanordnung** umfasst wären.

Beispielhaft ist hier insbesondere auf § 3 Abs. 3 GGDG-E verwiesen. Hiernach sind die Information aus § 2 Abs. 2 Nr. 1 lit. b) und c) einem **Anschlussinhaber** zuzuordnen, und sodann die anhand der Zuordnung nach § 2 Abs. 2 Nr. 2 GGDG-E **erlangten Daten** zu speichern.

Insofern beschränkt sich die **Speicheranordnung** dem reinen Wortlaut lediglich auf die **Personalien**. Das ergibt sich auch aus der Gesetzesbegründung. Etwaige **Zwischeninformationen** wären allenfalls auf Basis einer noch nicht verabschiedeten, getrennten Aktualisierung des TKG möglich. Wobei auch an dieser Stelle die Gesetzesbegründung offenlässt, ob lediglich die Zwischenspeicherung der Bestandsdaten, oder die Zwischenspeicherung aller zur Ermittlung erforderlichen Umstände gemeint ist. So heißt es in der Gesetzesbegründung:

> ***§ 174 Absatz 1 Satz 3 in Verbindung mit Absatz 5 Nummer 9 TKG-E, der die in § 2 Absatz 1 Satz 1 geregelte Befugnis zur Datenverarbeitung ergänzt, berechtigt den Internetzugangsdienst, hierbei – neben sämtlichen unternehmensinternen Datenquellen – auch die nach § 177 Absatz 1 TKG-E vorsorglich gespeicherten Daten zu verwenden und das Ergebnis der Zuordnung in einem Zwischenschritt der Bestandsdatenauskunft betriebsintern zu speichern.***

An dieser Stelle sollte sichergestellt werden, dass die **Verfahren des GGDG-E** auch ohne Annahme etwaiger **sonstiger Gesetzesvorhaben** effektiv und effizient funktionieren.

Der vom Gesetzgeber angesprochene, weitere Gesetzesentwurf betrifft die mögliche Wiedereinführung einer allgemeinen **Vorratsdatenspeicherung**. Der Erfolg des Gesetzesvorhabens und eine verfassungsrechtliche Bestandskraft kann derzeit jedenfalls als höchst umstritten angesehen werden. Das GGDG-E sollte insoweit dessen Effektivität nicht von diesem weiteren Gesetzesvorhaben abhängig machen.

Die für das GGDG-E **erforderliche Datenverarbeitung** betrifft gerade **nicht** eine etwaige **Vorratsdatenspeicherung**. Vielmehr sind aufgrund eines konkreten Tatvorwurfs angefallene Informationen zu sichern; etwaige darüber hinausgehende Informationen (vgl. die weiteren Ausführungen in diesem Abschnitt 2.4) wären jedenfalls **deutlich geringeren verfassungsrechtlichen Bedenken** ausgesetzt, da ein wesentlich **stärkerer Bezug** zu einer **rechtswidrigen Handlung** bestünde. Es wird insoweit dringend empfohlen, das GGDG-E an dieser Stelle um **eigene Rechtsfertigungsgrundlagen** zu **ergänzen**.

Hierbei sollte auch sichergestellt werden, dass **nicht nur** das **Ergebnis** der Zuordnung Gegenstand der Speicher- und Übermittlungsanordnung ist, **sondern auch** die bei der Zuordnung **angefallenen** bzw. **genutzten Zwischeninformationen**. Diese Zwischeninformationen sind möglicherweise erforderlich, um im Anschluss im Sinne eines rechtsstaatlichen Verfahrens, Bedenken bezüglich etwaiger Zuordnungsfehler auszuräumen.

2.4.5.2 Unzureichender Informationsanspruch

Im Übrigen erscheint auch der **Informationsumfang dem Grunde** nach bereits nicht ausreichend im Falle nachträglicher Änderung der Informationen.

Der Informationsanspruch gem. § 2 Abs. 2 GGDG-E, und somit eine darauf basierende Sicherungsanordnung gem. § 3 GGDG-E, bezieht sich lediglich auf die Informationen, wie diese **zum Zeitpunk des Eingangs der Anordnung** als „**live-Zustand**“ bei den Anbietern vorhanden ist.

Hierdurch bestehen sowohl für die Personalien als auch für die rechtsverletzenden Inhalte Durchsetzungsrisiken.

2.4.5.2.1 nachträglich geänderte oder gelöschte Personalien

Dieses Phänomen betrifft vermutlich stärker Diensteanbieter, und weniger Internetzugangsanbieter, obgleich es theoretisch in beiden Fällen möglich ist.

Soweit Täter*innen zum Zeitpunkt der Tat kein vollständig anonymes Nutzerkonto unterhalten haben, könnten die Reaktionen auf die rechtswidrigen Inhalte Bedenken seitens der Täter*innen über die Rechtmäßigkeit auslösen, die im Ergebnis in der Sorge münden, Gegenstand von zivil- oder strafrechtlichen Verfahren zu werden.

Es ist somit damit zu rechnen, dass Täter*innen in diesem Moment anfangen, etwaige sie **identifizierende Informationen** aus den vergangenen **Nutzeraktivitäten** sowie aus dem im **Nutzerkonto** unmittelbar hinterlegten Daten **zu ändern**, entweder indem diese ersatzlos **entfernt** werden, soweit möglich, oder durch **anonymisierte (Fake)-Informationen ersetzt** werden.

Bliebe der Informationsanspruch auf die zum Zeitpunkt der Anfrage vorgehaltenen Informationen beschränkt, entstünde hierdurch eine die Durchsetzung massiv gefährdende Erkenntnislücke.

Deshalb sollte **klargestellt** werden, dass die Anbieter **auch verpflichtet** sind, auch **historische Informationen** jedenfalls zu **sichern** und an das Gericht zu **übermitteln**. Betroffenen sind – soweit erforderlich – ebenfalls diese historischen Informationen zur Verfügung zu stellen.

2.4.5.2.2 nachträglich geänderte oder gelöschte Inhalte

Aus den gleichen Überlegungen wie zuvor, ist damit zu rechnen, dass Täter*innen r**echtswidrige Inhalte nachträglich editieren, löschen, deren (öffentliche) Zugänglichkeit einschränken, oder in sonstiger Art und Weise im Vergleich zur ursprünglichen Tathandlung verändern**.

Derzeit ist lediglich eine **Kopie der angegriffenen Inhalte** zu übermitteln. Hierbei verbleibt der Ref-E unklar, was eine hinreichende „Kopie“ darstellt. Zielführend scheint es allerdings nur, wenn hiervon auch **alle – potentiell tatbestandlich relevanten – Nebeninformationen** umfasst sind, d.h., der konkrete **Inhalt**, der **Zeitstempel** der Veröffentlichung, die bei der Veröffentlichung ausgewählte **Reichweite**, insbesondere soweit die Reichweite eingeschränkt wurde, zum Zeitpunkt der Veröffentlichung **ermöglichte Interaktionen**, insbesondere soweit diese eingeschränkt wurden, etc.

Neben diesen „**Nebeninformationen**“, ist auch eine **Historie** zu all den Informationen möglicherweise verfahrensrelevant. Denn soweit die rechtswidrigen Inhalte etwa im Nachgang entfernt würden, so würde eine Kopie des „**live-Inhalts**“ zum Zeitpunkt der Informationsbereitstellung den rechtswidrigen Inhalt nicht mehr beinhalten. Dies führt sodann zu **Widersprüchen** in den von den Betroffenen vorgelegten Tatsachen und den durch die Diensteanbieter bereitgestellten Tatsachen, mit möglicherweise **negativen Folgen im Rahmen der Beweiswürdigung**, vgl. 2.4.5.1.2. Dabei läge in diesem Fall **keine Manipulation durch die Betroffenen** vor, sondern eine Manipulation durch Täter*innen. Die **gesetzliche Regelung** würde aber möglicherweise eine **Vermutung der Manipulation durch Betroffene statuieren** und somit das Gegenteil des intendierten Gesetzeszwecks zur Folge haben.

Neben der **Historie der eigentlichen Inhalte** ist auch eine **Historie zu den Nebeninformationen** möglicherweise verfahrensrelevant. Soweit etwa tatbestandlich eine „Veröffentlichung“ voraussetzt ist, und ein Inhalt ursprünglich tatsächlich „jeder Nutzer*in“ der Online-Plattform zugänglich gemacht wurde, hätte zum Zeitpunkt der Tatbegehung eine Veröffentlichung vorgelegen. Wäre die Reichweite nachträglich durch Täter*innen eingeschränkt worden, zwar auf eine handvoll enger Freunde, stünde das Tatbestandsmerkmal „Veröffentlichung“ in Zweifel. Insoweit wäre auch hier eine Information lediglich auf Basis des „live-Zustands“ geeignet, die Durchsetzung zu verunmöglichen.

Ergänzend ist klarzustellen, dass die Information durch Diensteanbieter **auch etwaige als gelöscht oder gesperrt markierte Inhalte** betrifft. Vereinfacht kann formuliert werden: Diensteanbieter sollten verpflichtet sein, alle zu den Inhalten vorhanden Informationen bereitzustellen bzw. jedenfalls zu sichern, soweit diese noch bei den Diensteanbietern vorhanden sind und soweit diese Informationen nicht ansonsten irrelevante Daten zu weiteren Nutzerkonten und/oder deren Interaktionen mit dem Inhalt betrifft.

2.4.6 Mangelnde Informationen als Durchsetzungsdefizit sind mögliches Defizit der Rechtsstaatlichkeit

Einerseits sind die fehlenden Informationen, wie in diesem Abschnitt 2.4 erläutert, ein Risiko für die Durchsetzbarkeit. Informationen und Zustände, die nicht zu Beginn des Verfahrens und möglichst umfassend erhoben und gesichert werden, können im weiteren Verlauf des Verfahrens möglicherweise nicht mehr nachträglich festgestellt werden.

Diese Lücke kann einerseits als **Durchsetzungsdefizit** betrachtet werden, da dies Täter*innen ermöglichen könnte, hinreichende Zweifel zu etablieren.

Andererseits kann man dies auch als ein **potentielles Defizit der Rechtsstaatlichkeit** verstehen. Einerseits können die vorgenannten Aspekte als bloße Schutzbehauptungen abgetan werden. Andererseits können – in den zuvor benannten Situationen oder in ähnlich gelagerten Sachverhalten – sich durchaus Fehler im Verfahren befunden haben.

Auf diese diese Fehler hinzuweisen und diese ggf. auch nachzuweisen zu können, ist Teil des **rechtsstaatlich und grundrechtlich geschützten Rechts auf Verteidigung**. Diese Verteidigung kann sich möglicherweise aber nur darauf beschränken, Umstände in Zweifel zu ziehen oder mit Unwissen zu bestreiten. Während im Strafrecht der Grundsatz des in dubio pro reo gilt, ist dieser in der Intensität im Zivilrecht nicht einschlägig.

Im **Zivilrecht** gilt grundsätzlich, dass diejenige Partei, die sich auf einen Umstand (positiv) berufen möchte, diesen Umstand auch **beweisen** muss. Das Zivilrecht kennt hiervon auch Abweichungen, etwa die die **Substantiierungspflicht** und die sekundäre **Darlegungslast**. Es ist daher nicht ausgeschlossen, dass im Ergebnis die Vermutungswirkungen aus den gem. § 2 Abs. 2 GGDG-E erhobenen Informationen gegen die Täter*innen wirken, und eine hinreichende Verteidigung ins Leere läuft.

Je nachhaltiger und verlässlicher die Darlegung der klagenden Partei ist, umso stichhaltiger muss dieser Vortrag bestritten werden. Ein bloßes Bestreiten mit **Nicht-Wissen** oder Bestreiten „**ins Blaue**“ ist unzulässig. Ein Bestreiten mit Nicht-Wissen ist jedoch dann möglich, wenn die Partei selbst keine Möglichkeiten der weiteren Substantiierung hat. Dies kann man in den hier zu erwartenden Fällen wohl annehmen. Die Täter*innen haben keine Möglichkeiten, selbst die in den Systemen der Anbieter hinterlegten Informationen zu erheben. Die **Pflicht zur Mitwirkung der Anbieter** mag zwar gegeben sein – wobei auch das streitig gestellt werden kann –, der Zeitablauf wird aber in der Regel dafür Sorgen, dass Anbieter einen **Großteil der relevanten Informationen gelöscht** haben werden. Insofern würde zwar ein **unsubstantiiertes Bestreiten** genügen, und die klagende Partei müsste weiteren **substantiierten Vortrag** leisten. Jedoch spricht für die klagende Partei, dass diess den gleichen **Unmöglichkeiten** gegenübersteht, sich aber auf gerichtlich erhobene und gesicherte Informationen berufen kann.

2.5 Beispielhafte Ausführungen zu § 202e StGB-E

§ 202e StGB-E wie im Ref-E vorgesehen, enthält nicht **nachvollziehbare Tatbestandseinschränkungen**, die dem Ziel der Norm höchstwahrscheinlich zuwiderlaufen. Insoweit lässt sich auch nicht erkennen, wie die vorgeschlagene Regelung dem ganzheitlichen Ansatz zuträglich sei. Im Gegenteil, die Norm verliert sich in Einschränkungen, um einen ganzheitlichen Effekt zu vermeiden.

Der Ref-E stellt fest, dass die Auswirkungen „digitaler Gewalt“ sowohl auf psychischer als auch physischer Ebene signifikant sein können.[40] Das Bundesverfassungsgericht hat in seinem „Volkszählungsurteil“[41] das Grundrecht auf „Informationelle Selbstbestimmung“ etabliert, welches feststellt:

> ***Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.*** [42]

Das BVerfG leitet hieraus ab:

> ***Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.*** [43]

Dies mündet in der durch das BVerfG abstrakt-generellen Risikobetrachtung:

> ***Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.*** [44]

Mithin ist somit schon 1983 festgestellt worden, dass sich bereits aus einer **bloßen Unsicherheit**, ob eine Überwachung stattfindet oder nicht, **erhebliche Einschränkungen** für jedes Individuum ergeben können. Der **psychologische Effekt** der rein **potentiellen Nachteile und Risiken**, schlägt über in **reale**, **physische Nachteile**. Dies betrifft sowohl die Selbstbeschränkung eigenen Handelns, als auch möglicherweise die Materialisierung körperlicher, physischer Symptome aufgrund der psychologischen Belastung.

40 Abschnitt A I, S. 19, 20, Abschnitt A I 1, S. 21.

41 BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83 et al.

42 BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83 et al., Rn. 146.

43 BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83 et al., Rn. 146.

44 BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83 et al., Rn. 146.

2.5.1 Zweifel am Bestimmtheitsgebot; Aufhebung des eigenen Schutzziels durch zu weitreichende Tatbestandseinschränkung

Begrifflich umfasst bereits der Begriff „**Überwachung**“ eine **Signifikanz**, die über eine vereinzelte Verarbeitung von Informationen hinausgeht. Eine Überwachung setzt voraus, dass die Informationen **qualitativ** hinreichend erhoben werden, um Rückschlüsse ziehen zu können. Das umfasst sowohl die **zeitliche Perspektive** (Erhebungsfrequenz) und die **qualitative Perspektive** (welche Informationen sind betroffen). Die Aufnahme der dem Begriff „Überwachung“ immanenten Attribute „wiederholt oder ständig“ in den Gesetzestext erschiene nur dann nachvollziehbar, soweit der Gesetzgeber diese beiden Dimensionen im Rahmen von Regelbeispielen näher ausgestaltet hätte. Ohne die Aufnahme von Regelbeispielen wird ein ohnehin unbestimmter Rechtsbegriff „Überwachung“ durch zwei weitere unbestimmte Rechtsbegriffe „wiederholt“ und „ständig“ ergänzt. Dies lässt zumindest Zweifel aufkommen, ob und inwieweit dies letztlich dem Bestimmtheitsgebot strafrechtlicher Normen genügt.

Die sodann ergänzende Beschränkung auf Fälle, in denen ein **schwerer Schaden wahrscheinlich** ist, läuft dem Zweck erst recht zu wider. Wie das BVerfG bereits feststellt, genügt bereits eine bloße Ungewissheit, um nachteilige Effekte im Verhalten der betroffenen Person zu begründen. Das Gesetz etabliert hier erneut **unbestimmte Rechtsbegriffe**, die letztlich die Einhaltung des **Bestimmtheitsgebots zweifelhaft** erscheinen lassen. Weder ist geregelt, auf welcher Basis eine „Wahrscheinlichkeit“ zu ermitteln sei, noch ist definiert, was ein „schwerer Schaden“ im Sinne der Norm sei.

Im Ergebnis lässt sich somit festhalten:

- § 202e StGB-E begründet möglicherweise **keinen ergänzenden Schu**tz, da dessen Anwendbarkeit an den verfassungsrechtlichen Hürden des **Bestimmtheitsgebots** scheitern könnten.
- Selbst wenn § 202e StGB-E die verfassungsrechtlichen Hürden überwände, sind die **einfachgesetzlichen Einschränkung** des Tatbestands derart **weitreichend**, dass eine **strafrechtliche Verfolgung** allenfalls in **Ausnahmefällen** in Betracht kommt. Dies steht im **Widerspruch** zum im Ref-E festgestellten **Handlungsdrucks** aufgrund wachsender Fallzahlen.
- Soweit eine strafrechtliche Verfolgung als **ultima ratio** auf Ausnahmefälle beschränkt wurde, so verbliebe dennoch eine **Schutzlücke**, da den Betroffenen auch zivilrechtlich vor der Herausforderung stünden, dass diese nicht ohne Weiteres herausfinden können, durch wen die unbefugte Überwachung stattfindet.
    - Das GGDG-E umfasst aber weder § 202e StGB-E im Regelkatalog, § 1 Abs. 1 Nr. 2 GGDG-E, noch adressiert es die Anbieter etwaiger Überwachungs-Hard- und Software.

2.5.2 Modifizierter Vorschlag

Vor diesem Hintergrund wird **konzeptionell eine modifizierte Formulierung** vorgeschlagen. Der Ref-E anerkennt, dass eine unbefugte Überwachung des Aufenthaltsorts oder Tätigkeiten einer Person gesellschaftlich zu missbilligen ist. Zugleich anerkennt der Ref-E, dass es einen relevanten Anstieg des Erwerbs und der unbefugten Verwendung von Produkten (Hard- und Software) gibt, die eine solche Überwachung ermöglichen.[45] Hieraus ergäbe sich logisch, dass es einen erheblichen gesetzgeberischen Druck gibt, dieser Dynamik entgegen zu treten. Sowohl im Sinne des Individualrechtsschutzes als auch im Sinne der für eine demokratische Gesellschaft immanente individuelle Freiheit als Voraussetzung einer funktionieren demokratischen Grundordnung.

Insoweit sollte zunächst auf eine **unnötige Einschränkung** des Tatbestandsmerkmals „Überwachung“ **verzichtet** werden (vgl. neuer Abs. (1)). Wie zuvor dargelegt, ist es dem Begriff „Überwachung“ bereits immanent, dass es sich um einen sich wiederholenden Vorgang handelt. „Ständig“ ist aber nur die maximal größte Frequenz einer Wiederholung.

Soweit die Gesetzesbegründung ausführt, dass diese Einschränkung deshalb notwendig sei, damit die Verarbeitung von Informationen aus bzw. das Nachschlagen von Social Media Profilen oder anderweitig berechtigterweise zugänglichen Quellen ausgeschlossen wird, erscheint dies nicht überzeugend. Der Umstand der Überwachung und der sich daraus ergebende psychische Druck auf die Betroffenen hat nur bedingt eine Konnexität mit dem berechtigten Zugang zu den für die Überwachung erforderlichen Informationen. Insoweit kann der **unberechtigte Zugriff** auf Informationen als **Voraussetzung des Tatbestandsmerkmals „unbefugt“** definiert werden (vgl. neuer Abs. (2)).

Wenn überhaupt erscheint der Umkehrschluss zudem naheliegender: wurden für die Überwachung Informationen genutzt, die lediglich unberechtigterweise zugänglich sind, bedürfte es keiner weiteren Wiederholung oder anderer Nachweise der tatsächlichen Überwachung. Um jedoch eine uferlose Strafbarkeit durch lediglich einmaliges, unberechtigtes Abrufen von Informationen zu vermeiden, erscheint hier ein derartiger Automatismus nicht zielführend. Allerdings, wenn für die **Informationsbeschaffung gezielt Soft- oder Hardware** installiert wurde[46], erscheint es vertretbar, **von der Installationshandlung auf den Überwachungszweck zu schließen** (vgl. neuer Abs. (4)).

Doch auch die Verarbeitung von **Informationen, auf die berechtigterweise zugegriffen werden kann**, ist geeignet eine unbefugte Überwachung zu begründen, aus der sich erhebliche Nachteile für die Betroffenen in deren Lebensführung ergeben. Insoweit sollte auch diese Dimension nicht gänzlich der Strafbarkeit entzogen werden, jedenfalls dann, wenn für die

45 Ref-E Begründung, Abschnitt B, zu Artikel 2, zu Nummer 2, S. 64.

46 Etwa Hardware-Tracker, etwa GPS-Tracker, Audio-Visuelle Überwachungstechnik, oder Spyware.

Betroffenen **erhebliche Nachteile** zu befürchten sind. Die Nachteile können die freie, allgemeine **Lebensführung** betreffen, da sich Betroffene aufgrund des **Überwachungsdrucks** einschränken, oder weil zu befürchten steht, dass die Überwachung tatsächlich in physische Übergriffe münden könnte (vgl. neuer Abs. (3)). Soweit einer berechtigten **Aufforderung zur Unterlassung** nicht Folge geleistet wird, erscheint es vertretbar, die erhebliche Beeinträchtigung zu vermuten. Die Ergänzung einer „berechtigten Aufforderung“ erscheint notwendig, um einen Strafbarkeitsreflex für ansonsten durch die Rechtsordnung gebilligtes Verhalten zu vermeiden.

> ***§ 202e StGB-E (modifiziert)***
>
> ***(1) Wer den Aufenthaltsort oder die Tätigkeit einer anderen Person mittels Informations- oder Kommunikationstechnik unbefugt überwacht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.***
>
> ***(2) Eine mangelnde Befugnis setzt neben dem mangelnden Einverständnis durch die andere Person oder mangelnder Befugnisnorm, die Verarbeitung von ansonsten nicht berechtigterweise zugänglicher Informationen voraus.***
>
> ***(3) Die Verarbeitung von ansonsten berechtigterweise zugänglicher Informationen begründet in Abweichung von Abs. 2 eine Strafbarkeit, wenn eine ansonsten unbefugte Überwachung stattfindet und die andere Person hierdurch in ihrer allgemeinen Lebensführung wesentlich beeinträchtigt wird oder die Handlung wahrscheinlich dazu führt, dass dieser Person ein Schaden zugefügt wird. Eine wesentliche Beeinträchtigung ist jedenfalls dann gegeben, wenn die Überwachung nach Satz 1 trotz berechtigter Aufforderung zur Unterlassung fortgesetzt wird.***
>
> ***(4) Ungeachtet der tatsächlichen Verarbeitung hinsichtlich der Häufigkeit, Dauer oder inhaltlichen Qualität, liegt eine Überwachung jedenfalls dann vor, wenn unbefugt Hard- oder Software installiert wurde, die eine Informationsbeschaffung zum Zwecke der Überwachung ermöglicht.***

3 Strukturelle Perpetuierung einer unnötigen definitorischen Komplexität

Für einen ganzheitlichen Ansatz, wie dies der Ref-E laut eigener Aussage verfolgt, wäre zu erwarten, dass die einzelnen Fallgruppen systematisch aufgearbeitet und die jeweiligen Kernelemente der Fallgruppen in die gesetzlichen Regelungen überführt wird.

Hierbei ist es dem gesetzgeberischen Prozess stets immanent, dass Gemeinsamkeiten in **allgemeine Regelungen** vorgezogen werden. Ein Unterfall dieser Methodik sind **zentrale Begriffsbestimmungen**, soweit diese Begriffe wiederholt in den gesetzlichen Bestimmungen auftauchen.

Einerseits erhöht eine Zentralisierung der Begriffsbestimmungen die **Lesbarkeit**, da mehrere Aspekte in einen definierten Begriff zusammengeführt werden können. Andererseits erhöht es auch die **Flexibilität**, **Aktualisierbarkeit** und **Umfänglichkeit** der gesetzlichen Regelungen. Verändern sich die gesellschaftlichen oder rechtlichen Rahmenbedingungen und bedürfen einzelne Definitionen einer Anpassungen, so ist dies nur an einer Stelle erforderlich, und alle weiteren Normen aktualisieren sich automatisch. Sollte im Ausnahmefall eine Aktualisierung für eine konkrete Rechtsnorm nicht erforderlich sein, sondern sogar negativ Effekte nach sich ziehen, kann dies für diese eine Rechtsnorm im Wege eine lex specialis Regelung adressiert werden.

Der Ref-E lässt **Potentiale** durch zentrale Begriffsbestimmungen **ungenutzt**. Im Ergebnis scheint dies sogar zu ungewollten Regelungslücken zu führen.

Beispielhaft werden die Regelungen der §§ 184 ff. , sowie 201b StGB herangezogen.

Etwaige Fallgruppen sind

A)

1. künstlich generierte oder manipulierte Inhalte – ohne und ohne besondere Ehrverletzung
2. künstlich generierte oder manipulierte Inhalte – mit offensichtlichen objektiven sexualisierten Inhalten
3. künstlich generierte oder manipulierte Inhalte – mit aus Sicht bestimmter Erzeuger und Empfängerkreise sexualisierten Inhalten

B)

1. fiktive Inhalte entsprechend A), die aufgrund einzelner Inhalte Rückschlüsse auf konkrete Betroffene zulassen

C)

1. tatsächliche Inhalte entsprechend A), die konkrete Betroffene zum Inhalt haben, während diese auch für informierte Kreise erkennbar sind bzw. bleiben
2. tatsächliche Inhalte entsprechend A), ohne dass diese konkrete Betroffene zum Inhalt haben, und diese auch für informierte Kreise nicht erkennbar sind oder erkennbar werden

In allen Fällen von A) bis C) gilt, dass diese unterschiedliche Qualitäten aufweisen können, etwa aufgrund Inhalte

- allgemeiner Qualität
- besonders verwerflicher Qualität (vgl. 184a StGB)
- besonderes verwerflicher Qualität aufgrund des tatsächlichen Alters der Betroffenen
- besonders verwerflicher Qualität aufgrund der bewusst erzeugten Wirkung über das Alter der Betroffenen

Nun sollte davon ausgegangen werden können, dass das Gesetz jedenfalls hinsichtlich der objektiv **offensichtlich sexualisierten Körperregionen** eine einheitliche Wertung aufweist. Ein Vergleich der Regelungen §§ 184b, 184c, und 184k StGB lässt daran **Zweifel** aufkommen.

So heißt es in § 184b Abs. 1 Nr. 1 lit. c) sowie in § 184c Abs. 1 Nr. 1 lit. c):

> ***die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes***

Im neuen § 184k Abs. 1 Nr. 2 StGB-E heißt es:

> ***die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abbildet***

Eine solche inhaltliche Abweichung gab es in der Form auch schon in der gültigen Fassung des § 184k Abs. 1 Nr. 1 StGB.

Soweit für Erwachsene ergänzende Körperregionen deshalb für erforderlich gehalten werden, um etwaige **Urlaubsfotos** der von §§ 184b oder 184c StGB erfassten Betroffenenkreise nicht unter Strafe zu stellen, erscheint dies nicht überzeugend. Die jeweilige litera der Regelung verlangt ausdrücklich, dass eine „**sexuell aufreizende Wiedergabe**“ erforderlich ist. Insofern ist trifft die Regelung bereits anderweitig Sicherungsmaßnahmen, um ein nicht-verwerfliches Handeln von einer Strafe auszuschließen; zumal es fraglich wäre, warum das nicht-verwerfliche Handeln nur einzelne Körperregionen betreffen können sollte. Vielmehr ist davon auszugehen, dass der Gesetzgeber hier eine **systematisch Vorgehensweise vermissen** lässt, weil die Beschäftigung der Thematik möglicherweise Tabuthemen betrifft oder höchst unterschiedliche

gesellschaftliche moralische Vorstellungen betreffen könnte. Doch eine Diversität der moralischen gesellschaftlichen Vorstellungen sollte nicht dazu führen, dass sich am Ende ein **inkonsistentes Schutzkonzept** ergibt. Hiervon ist den potentiellen Opfern nicht geholfen.

An dieser Stelle sei zudem darauf hingewiesen, dass die Abweichung nicht in der – wohl noch eher – nachvollziehbaren Weise erfolgt, dass ergänzende körperliche Schutzregionen für die **besonders vulnerablen Gruppen** der §§ 184b und 184c StGB geregelt wurden. Im Gegenteil, den besonders vulnerablen Gruppen wird der **geringere Umfang besonders geschützter Körperregionen** gewährt.

Im entsprechenden Abschnitt des StGB existiert bereits eine Norm, die konkrete Begriffsbestimmungen beinhaltet, **§ 184h StGB**. Insoweit ist es auch kein Argument, dass es der bisherigen Systematik des StGB zuwiderliefe, in einem Abschnitt **ergänzende Begriffsbestimmungen** zentral zu regeln.

Begriffsbestimmungen könnten und sollten etwa umfassen:

- „tatsächliches Geschehen“, „wirklichkeitsnahes Geschehen“, „fiktives Geschehen“
- „besonders geschützte Körperregionen“
- „nackt“ bzw. „(un-)bekleidet“
- „sexuell aufreizend“, „in sexuell bestimmter Weise“

Hieraus ergibt sich eine weitere Inkonsistenz der genutzten Begrifflichkeiten, die zu nicht notwendigerweise nachvollziehbaren Wertungsunterschieden führt.

§§ 184b Abs. 1 Nr. 1 lit. c) und 184c Abs. 1 Nr. 1 lit c) verwenden jeweils die Formulierung „**sexuell aufreizende Wiedergabe**“. § 184k Abs. 1 Nr. 3 verwendet „**in sexuell bestimmter Weise**“.

Einerseits zeigt die Gesetzesbegründung, die im Kontext von „in sexuell bestimmter Weise“ auf § 184i StGB verweist, dass eine zentrale Norm für relevante Begriffe sachdienlich sein könnte, da sich die Begrifflichkeiten über mehrere Normen hinweg wiederholen und der Gesetzgeber offenkundig ein sich einheitlich entwickelndes oder entwickeltes Verständnis zu Grunde legen möchte.

Andererseits ist für die beiden zuvor genannten Formulierungen festzuhalten, dass rein dem Wortlaut nach, „**sexuell aufreizend**“ im Vergleich zu „**sexuell bestimmt**“ die wohl höheren Anforderungen stellen müsste. „Sexuell aufreizend“ hat eine **ausschließlich objektive Komponente,** während „sexuell bestimmt“ eine **starke subjektive Komponente** beinhaltet. Auf diese subjektive Komponente kann aus objektiven Kriterien zurückgeschlossen werden, was auch

der Gesetzesbegründung zu entnehmen ist.[47] „Sexuell aufreizende" Inhalte sind aufgrund ihrer objektiven Aspekte immer auch „sexuell bestimmt", während der Umkehrschluss nicht immer zulässig sein dürfte.

Und hieraus resultiert ein **Wertungswiderspruch**, der den Ganzheitlichen Anspruch des Ref-E in Zweifel zieht. Dieser Wertungswiderspruch könnte zudem bei konsistenter Verwendung von definierten Begriffen vermieden werden.

„**Sexuell bestimmt**" findet Verwendung bei der Abbildung **von bekleideten besonders schützenswerten Körperregionen**. „**Sexuell aufreizend**" hingegen, findet **bei unbekleideten (!) besonders schützenswerten Körperregionen** Anwendung. „**Sexuell bestimmt**" findet insoweit für **alle Altersgruppen** Anwendung, „**sexuell aufreizend**" lediglich bei der **besonders vulnerablen Gruppe** der von §§ 184b und 184c Betroffenen.

Unbenommen, ob die Beschränkung der **Tatbestandsvoraussetzungen** in § 201b Abs. 3 StGB gF, bzw. § 184 Abs. 2 StGB-E auf eine **Entgeltlichkeit** sachdienlich ist, ist die durch das Gesetz verwendete Wortwahl inkonsistent. Während §§ 184b Abs. 1 und 184c Abs. 1 StGB sowie § 184 Abs. 1 StGB-E jeweils von bekleidet, unbekleidet sowie „ganz oder teilweise unbekleidet" spricht, verwendet § 184 Abs. 2 StGB-E „**die Nacktheit**" eine anderen Person. Begrifflich entspräche dies, dass diese andere – abgebildete – Person „ganz unbekleidet" wäre. Hierauf kommt es aber wohl nicht an, da davon ausgegangen werden kann, dass der Gesetzgeber in diesem Falle die gleiche Formulierung verwendet hätte. Somit könnte genügen, dass die andere Person „teilweise unbekleidet" abgebildet wird.[48] Auch dies scheint nicht die Intention, denn dann hätte der Gesetzgeber es wohl so formuliert. Denn neben der Abweichung „(un-)bekleidet" tritt die weitere Abweichung „**abbilden**" und „**zum Gegenstand**" haben. Der Gesetzgeber könnte hierdurch eine Intention der Darstellung zum Ausdruck bringen wollen. Es käme dann nicht nur darauf an, dass eine (teilweise) unbekleidete Person abgebildet ist, sondern das Bild muss gerade wegen oder zum Zwecke dieser „Nacktheit" erstellt oder angeboten/verschafft werden. Die (teilweise) unbekleidete Person wird somit **objektifiziert**. Insoweit stellt sich die Frage, wo der Unterschied gegenüber der Formulierung „in sexuell bestimmter Weise" läge, oder ob es nicht gerade doch – aufgrund des Entgeltumstands – auf die bloße Abbildung ankommen solle.

In § 201b StGB-E bleibt offen, ob ein „mittels Computerprogramms erstellter Inhalt, der den **Anschein eines tatsächlichen Geschehens** erweckt" einer Erstellung eines „**wirklichkeitsnahen Geschehens**" entspricht, oder die abweichende Formulierung **materielle Unterschiede** begründen soll.

47 Vgl. Ref-E Begründung, Abschnitt B zu Artikel 2, zu Nummer 5, zu Absatz 1, S. 66.

48 Diese „teilweise unbekleidete" Darstellung scheint zumindest des Gesetzgeber auch abdecken zu wollen, da die Gesetzesbegründung zur Einführung der Norm im Rahmen des § 201a StGB gF, auch von „Personen in Badebekleidung" spricht.

Soweit die Gesetzesbegründung zum Ausdruck bringt, dass konkrete **Regelbeispiele** zu vermeiden seien, da diese die **Rechtssprechung** daran **hindern** würden, auf künftige, neuere Formenen **flexibel zu reagieren**, erscheint diese Auffassung höchst fragwürdig.

Das **Bestimmtheitsgebot** verlanngt, dass das Gesetz aus sich heraus verständnlich ist, um den Unrechtsgehalt des eigenen (künftigen) Verhaltens voraussehen zu können. Hiervon wird **ausnahmsweise** abgewichen, wenn bei **neuen Regelungsbereichen** eine abschließende Regelung nicht sachdienlich möglich ist und damit zu rechnen ist, dass die verbliebenen Unwägbarkeiten der **unbestimmten Rechtsbegriffe alslbald aufgelöst** werden, insbesondere im Wege der Rechtssprechung. Betrifft es einen bereits **bekannten Regelungsbereich**, wird eine Ausnahme des Bestimmtheitsgebots dahingehend akzeptiert, dass die unbestimmten Rechtsbegriffe ja bereits durch die **Rechtssprechung hinreichend Kontur** erhalten hätten.

Zumindest letzteres kann auch kritisch gesehen werden. Soweit die Ausnahme am Anfang aufgrund des neuen Regelungsbereiches geboten scheint, könnte man auch vertreten, dass im Falle einer gefestigten Rechtsprechung, der Gestzgeber im nächst möglichen Zeitpunkt die der Rechtssprechung zu entnehmende Kontuierung in das Gesetz aufnehmen müsste.

Jedenfalls ist es der Rechtssprechung nicht möglich, eine stetige Rechtsprechung ohne Weiteres auf gänzliche unerwartete Fälle zu erweitern oder in ihrer Aussage gänzlich umzukehren. Jedenfalls, kann diese neuerlich Rechsprechung wenn nur Wirkung für dann zukünftige Tathandlungen betreffen. Im Übrigen wird die Rechtssprechung unbestimmte Rechtsbegriffe auch gegenüber ihrer eigenen Rechtsprechung nur in **kleinen Schritten weiterentwickeln** können, um die Anforderungen des **Bestimmtheitsgebots** einzuhalten. Ob die Bindungswirkung nun aber aus gesetzlich normierten Regelbeispielen entsteht, oder aus der bisherigen Rechtssprechung, erscheint im Ergebnis **keinen Unterschied** zu machen; allenfalls ist zu erwarten, dass nicht juristisch ausgebildete Bürger*innen vornehmlich das Gesetz zu rate ziehen würden, und nicht notwendigerweise eine Analyse der bsherigen Rechtssprechung. Vor diesem Hintergrund hätten im Gesetz normierte **Regelbeispiele** und die damit einhergehende **Transparenz** wohl potentiell **höhere Präventiveffekte**, da Bürger*innen leichter und unmittelbarer die Rechtswdrigkeit ihres künftigen Handelns absehen könnten.

4 Annahme eines Rechts auf anonyme Meinungsäußerung

Der Ref-E perpetuiert das Dogma eines Anrechts auf anonyme Meinungsäußerung und anonyme Nutzung von Online-Plattformen. Ein solcher grundrechtlicher Anspruch kann nicht erkannt werden.

Hierbei ist zu unterscheiden zwischen einer **pseudonymen** und einer **anonymen** Nutzung. In der Tat erscheint es geboten, zumindest eine pseudonyme Nutzung erlauben zu müssen. Dies entspricht auch der analogen Welt. Eine echte „Anonymität" ist dort ebenfalls nicht gegeben, sondern allenfalls eine Pseudonymität. Zugleich scheint es aber auch nicht geboten, eine „anonyme Nutzung" per se zu verbieten, soweit die damit einhergehenden Risiken anderweitig mitigiert werden.

Das Dogma des grundrechtlichen Anrechts auf anonyme Meinungsäußerung basiert bereits auf einem **Zirkelschluss**. Dieser Zirkelschluss wird in Zeiten von Künstlicher Intelligenz, KI-Agenten und (Social Media)-Bots umso relevanter.

Anonymität verhindert bereits die Prüfung, ob der persönliche Anwendungsbereich der in Rede stehenden Grundrechte überhaupt betroffen ist. Nicht jedes Grundrecht wird hinsichtlich des persönlichen Anwendungsbereichs uneingeschränkt. Zudem kennt – wenn auch in der Praxis seltenst bis gar nicht relevant – das Grundgesetz auch die sogenannte **Grundrechtsverwirkung**. Ob eine solche einschlägig ist, kann ebenfalls nicht geprüft werden, wenn es einen grundrechtlichen Anspruch auf Anonymität gäbe.

In Zeiten von Künstlicher Intelligenz erscheint zudem der **Rückschluss unzulässig**, dass eine „**Accountaktivität**" zwingend **von** einem **Menschen** ausgeübt werden muss. Zutreffend ist, dass auch eine etwaige **KI-gestützte Aktivität oder ein (Social-Media)-Bot** am Ende der Verantwortungskette eine natürliche Person benötigt, die den automatisierten Prozess in Gang setzt. Fraglich ist aber, ob in diesen Fällen dem „Bot" aufgrund eines mittelbaren Bezugs zu einer natürlichen Person die grundrechtlichen Schutzmechanismen gewährt werden müssen. Insoweit ist auch fraglich, ob die gesetzliche Vermutung, ein anonymer, rechtswidrig agierender Account ist grundsätzlich unmittelbar einem Grundrechtsträger zugeordnet, noch aufrecht erhalten werden kann.

Dies vorangestellt, könnten engmaschige und effizientere **Verfahrensregelungen** den **Schutz der Betroffenen verbessern**. Hierbei ist zu beachten, dass Ziel dieser Regelungen nicht die Versagung der Möglichkeiten auf Anonymität ist. Es ist aber die Frage zu stellen, ob mit den

Vorteilen der Anonymität auf der einen Seite, nicht auch Nachteile auf der anderen Seite hinzunehmen sind. Es gibt ein Recht auf freie Meinungsäußerung, aber nicht notwendigerweise ein Recht auf die effizienteste Form der freien Meinungsäußerung.

Vorstellbar sind daher nachstehende **Regelungsdimensionen**:

- gesetzlich normierter Abstufungen des Schutzbedarfs von Nutzerkonten, je nach Anonymität
- Möglichkeiten drs anonymen Nutzer*innen unter Aufgabe der Anonymität die eigene Rechtsposition effektiv zu verteidigen
- Klare Verfahrensfristen und Vermutungswirkungen (z.T. siehe auch 2.2.2)

Abstufungen des Schutzbedarfs können sich etwa entlang der nachstehenden Varianten bewegen:

- vollständig anonymes Profil, bei dem weder im Nutzerkonto noch in den Aktivitäten Rückschlüsse auf die dahinterstehende Nutzer*in gezogen werden können, und welches – mit Ausnahme der rechtswidrigen Handlungen – keine sonstigen Aktivitäten aufweist; eine Vermutung, dass dieses Nutzerkonto durch KI oder einen Bot gesteuert wird, ist begründet.
- vollständig anonymes Profil, die Aktivitäten sind aber nicht auf rechtswidrige Handlungen beschränkt; die Aktivitäten sind aber ansonsten weiterhin nicht geeignet eine Vermutung zu etablieren, dass die dahinterstehende Nutzer*in ein Mensch ist; die Vermutung, dass dieses Nutzerkonto durch KI oder einen Bot gesteuert wird, bleibt begründet.
- vollständig anonymes Profil, die Aktivitäten sind hinreichend divers und mit Bezug zum realen Leben, dass weder vermutet werden kann, dass das Nutzerkonto durch KI oder einen Bot gesteuert wird, noch vermutet werden kann, dass das Nutzerkonto durch einen Menschen gesteuert werden kann;
- anonymes Profil, bei dem die Aktivitäten starke Bezüge in die reale Welt aufweisen, etwa aufgrund durchgeführter Transaktionen, gepostete Inhalte (Bilder, Videos) von tatsächlichen Umständen, etc.; die Inhalte genügen aber nicht, um mit vertretbarem Aufwand die Aktivitäten zu korrelieren und hieraus die Identität der dahinterstehenden Nutzer*in abzuleiten;
- pseudonymes Profil, bei dem Nutzer*innen nicht unter dem eigenen Klarnamen auftreten, aber entweder im Nutzerkonto ihre (vermeintlichen) Klardaten angegeben haben, oder die gepostеten Inhalte Rückschlüsse auf die reale Person ermöglichen, etwa durch Aktivitäten, die das Gesicht der Nutzer*in beinhaltet, konkrete ggf. auch regelmäßige Aufenthaltsorte zu bestimmten Zeitpunkten, etc.

- Unverifiziertes Klarnamenprofil, bei dem Nutzer*innen selbst unter dem vermeintlichen Klarnamen auftreten, ein Fake-Account aber mangels Verifikation nicht ausgeschlossen ist.
- pseudonymes verifiziertes Profil, bei dem Nutzer*innen nicht unter dem eigenen Klarnamen auftreten, sich aber gegenüber dem Dienstanbieter verifiziert haben, d.h., die im Nutzerkonto hinterlegten Identifikationsdaten (Klarname, Adresse, etc.) nicht nur selbst behaupten, sondern nach einem definierten Prozess gegenüber dem Diensteanbieter bestätigt haben.
- Verifiziertes Klarnamenprofil

Es ist naheliegend, dass der **gewährte Schutz für verifizierte Profile am höchsten** sein sollte; sodann kann der Schutz – teils auch im Interesse der Nutzer*innen – abgeschwächt werden.

Hierbei sollten zwei Elemente in den Fokus genommen werden:

- Schutz vor digitaler Gewalt durch möglichst unmittelbare Entfernung der rechtsverletzenden Inhalte
- Schutz vor digitaler Gewalt durch Sanktionierung der Täter*innen

Bei digitaler Gewalt kann das aus der Liegenschaftspflege bekannte „broken window“ Phänomen übertragen werden. Das „broken window“-Phänomen besagt, dass eine Liegenschaft weiterem Vandalismus umso schneller ausgesetzt ist, sobald die Liegenschaft bereits Schäden (broken window) aufweist; denn in diesem Moment ist ersichtlich, dass die Liegenschaft nicht mehr bewohnt oder gepflegt wird; mithin das Risiko „erwischt zu werden“ augenscheinlich gesunken ist.

Im Falle von digitaler Gewalt bedeutet dies: ist der **„Damm“ erst einmal gebrochen**, dass Betroffene im digitalen Raum etwaigen Schmähungen oder sonstigen Rechtsverletzungen ausgesetzt sind, also „der erste Stein geworfen wurde“, so **senkt dies auch die Hemmschwelle** weiterer Täter*innen, und ein ganze **Welle von Rechtsgutsverletzungen kann sich Bahn brechen** (Shitstorm). Es ist daher von großer Bedeutung, die individuellen rechtsgutsverletzenden Inhalte **möglichst schnell aus der Öffentlichkeit zu entfernen** und somit das Risiko der Nachahmung zu reduzieren.

Eine **Sanktionierung** soll und darf deswegen nicht gänzlich hintangestellt werden. Hierzu sind etwaige Beweis-sichernde Maßnahmen zu treffen. Die **Sanktionierung von anonymen KI-Bots** wird aber ohnehin in den meisten Fällen ins Leere laufen. Deswegen erscheint es im Sinne einer ganzheitlichen Betrachtung zielführend, diese **beiden Dimensionen zu trennen**, und auch anhand der Anonymität der Nutzerkonten abgestuften Schutzbedarfe zu effektuieren.

Im Ergebnis wird **vorgeschlagen**, ein **Konzept zu prüfen** und in einer **Überarbeitung des Gesetzes** aufzunehmen, welches **nachstehende Eckpunkte** berücksichtigt.

- Je höher der Grad der Anonymität, desto höher der Grad an **Unmittelbarkeitsautomatismen** hinsichtlich der zur Verfügung stehenden Maßnahmen, insbesondere hinsichtlich der Inhalts- und Account-Sperren.
- Als mögliche **Erweiterungen des Anordnungskanons** sollte in Betracht gezogen werden
  - etwaige Sperren der über die Nutzerkonten erfolgenden **Geldflüsse**, jedenfalls, soweit die Nutzerkonten auch dazu genutzt werden, die eigenen Inhalte zu monetarisieren.
  - die **Löschung** von Accounts
  - die **Rücksetzung** der durch das Nutzerkonto **aufgebauten „Netzwerke“**, etwa in Form von Follower*innen, „Freunden“, Kontakten, etc.;
    - für die Verbreitung von rechtswidrigen Inhalten, ist ein Netzwerk erforderlich; eine Rücksetzung des Netzwerks würde die Breitenwirkung der (künftigen) rechtswidrigen Inhalte betreffen bzw. die Verbreitung jedenfalls gegenüber den weiteren Nutzer*innen einer Online-Plattform auflösen, die lediglich aus – längst – vergessenen Gründen einen Verbindung zu dem betroffenen Nutzerkonto aufweisen;
    - die „Netzwerkgröße“ ist zudem ein Faktor, sowohl für die „objektive“ öffentliche Wahrnehmung der über einen Account geteilten Inhalte, als auch für die auf Online-Plattformen erfolgte „Gewichtung“ der Inhalte im Rahmen der Feed-Algorithmen
  - **Untersagung der „Empfehlung“** der Inhalte durch die Online-Plattform

Ein Nebeneffekt sowohl der Erweiterung der Maßnahmen als auch einen erhöhten Grad der Automatismen wäre, dass die ebenfalls inzwischen über Automatismen erstellten Nutzerkonten und ganze Nutzerkonten-Netzwerke zur gegenseitigen „Wirkungsbestärkung“ auf lange Sicht ausgetrocknet werden könnten; bzw. deren Betrieb mit deutlichen höheren Aufwänden verbunden wäre.

Derartige Ansätze erscheinen zudem weniger eingriffsintensiv als parallele Diskussionen über eine Vorratsdatenspeicherung oder eine Klarnamenpflicht.

5 Verlagerung der Tatbegehung und Tathandlung

In Folge der unnötigen definitorischen Einschränkungen und Unklarheiten, ist der Ref-E selbst bereits **Geburtshelfer für neue Phänomene**.

Dies liegt im Wesentlichen daran, dass es der Ref-E versäumt, eine klare Linie zu etablieren, die einen Gleichlauf zwischen analoger und digitaler Welt zur Folge hätte.

Im Wesentlichen würden für eine **materielle Betrachtung** als Leitlinie folgende drei Prämissen genügen:

- die Straftatbestände der analogen Welt werden hinreichend geschlossen, etwa im Bereich der Nachstellung, der Bereich des Besitz, Herstellung und Verbreitung besonders verwerflicher tatsächlicher, wirklichkeitsnaher oder fiktiver Inhalte[49], etc.
- die Implementierung des logischen Grundsatzes, dass es für die Strafbarkeit einer strafbewehrten Handlung irrelevant sein muss, über welches Medium diese Tathandlung begangen wird
- erst im dritten Schritt werden etwaige Besonderheiten der digitalen Kommunikation in Ansatz gebracht, nämlich in zwei Dimensionen,
  - eine Verringerung der Strafbarkeitsschwelle oder eine Verschärfung der (Mindest-)Strafrahmen, oder sonstige, die negativen Folgen der Tathandlung mitigierender Maßnahmen, etwa aufgrund größerer Streubreite der Inhalte, erleichterter Tatbegehung, verringerte Reversibilität von Tathandlungen bzw. intensivere Langzeitauswirkungen der Tathandlungen, etc.
  - eine Erhöhung der Strafbarkeitsschwelle oder eine Verringerung der (Mindest-)Strafrahmen, etwa aufgrund Umstände, die bei gleicher objektiver Tathandlung, einen geringeren Unwertgehalt erkennen lassen, die Reversibilität erleichtert ist bzw. die Langzeitwirkungen geringer sind, etc.

49 Der Besitz, die Herstellung und die Verbreitung wirklichkeitsnaher und fiktiver Inhalte ist analog genauso möglich, wie digital. Das Phänomen dieser Inhalte bestand schließlich schon vor der Verbreitung digitaler Kommunikation.

Neben der materiellen Betrachtung sind selbstredend etwaige **Besonderheiten der Durchsetzbarkeit** zu beachten. Auch hier können die Prämissen auf wenige Aspekte kondensiert werden

- Bestehen Erkenntnisdefizite im Rahmen der Ermittlung und/oder Beweissicherung im Vergleich zur analogen Welt?
- Resultieren etwaige Erkenntnisdefizite aus auf Grund für die demokratische Rechtsordnung notwendigen Zugewinnen im Vergleich zur bisher gültigen analogen Welt?
- Können im Einzelfall etwaige Erkenntnisdefizite unter Beibehaltung der Zugewinne für die demokratische Rechtsordnung durch rechtsstaatliche Verfahren behoben werden?
- Sind aufgrund der Flüchtigkeit des Digitalen beschleunigte Verfahren erforderlich?
- Existieren etwaige Nachweisdefizite im Falle von Schutzbehauptungen?

Der Ref-E versäumt es eine in Absehung des Mediums der Tat einheitliche Definition zu etablieren, vgl. auch 3.

Zudem versäumt der Ref-E, die für eine Durchsetzbarkeit bestehenden Erkenntnisdefizite aufgrund effizienter Verfahren hinsichtlich ihres zeitlichen Ablaufes oder ihres inhaltlichen Erkenntnisgewinns zu überwinden, vgl. auch 2.2.2 und 2.4.

Es steht somit zu befürchten, dass sich die Tathandlungen sowohl inhaltlich als auch räumlich lediglich verlagern könnten.

Eine **inhaltliche Verlagerung** bedeutet, dass die Tathandlungen sich hinsichtlich der **modus operandi** anpassen, und neu geschaffene oder beibehaltene Regelungs- oder Durchsetzungslücken ausnutzen.

Eine **räumliche Verlagerung** bedeutet, dass die Tathandlungen sich hinsichtlich der „räumlichen“ Tatumstände verlagern, also im digitalen Raum dahingehend, dass **andere oder ganz neue Formen der Online-Plattformen** in den Fokus rücken, oder **andere (Sekundär)-Funktionalitäten** der Plattformen zur Tatbegehung genutzt werden.

In beiden Fällen der Verlagerung ist zu befürchten, dass der **Schutzeffekt für die Betroffenen ausbleibt**, oder jedenfalls deutlich geringer ausfällt. Mithin steht zu befürchten, dass die dem ganzheitlichen Ansatz des Ref-E innewohnende Hoffnung, die „**Verrohungstendenz**“ digitaler Räume auszubremsen oder im besten Fall umzukehren, sich nicht zeitnah erfüllt.

5.1 Verlagerung hinsichtlich des modus operandi

Einerseits wird auf die möglichen Risiken hinsichtlich des Tatortes hingewiesen, soweit auch dies den modus operandi beeinflusst. Siehe hierzu exemplarisch und entsprechend 2.3.2.

Ebenso ist für den modus operandi relevant, dass derzeit nur bestimmte Katalogtaten von den durch den Ref-E erhofften Effizienz- und Effektivitätsgewinnen durch das GGDG-E profitieren. Auch dies kann den modus operandi dahingehend beeinflussen, dass die **Tathandlungen sich künftig bewusst in den Grauzonen zwischen den Katalogtaten bewegen** werden, vgl. 2.3.1.

Im Übrigen wird nachstehend auf die Normen §§ 184 ff. StGB-E, sowie § 201b StGB-E eingegangen, und warum keine ganzheitliche Überarbeitung, wie diese der Ref-E für sich behauptet, erkannt werden kann. Soweit sachdienlich wird hierzu auch auf die exemplarischen Ausführungen unter 3 verwiesen.

Besonders augenscheinlich sind die **unterschiedlich relevanten Körperregionen**. Es ist daher davon auszugehen, dass (professionelle) Täter*innern die sich verschobenen Grenzlinien gezielt ausnutzen werden.

Insoweit ist – wie bereits unter 3 ausgeführt – nicht nachvollziehbar, warum sich gerade der **Schutz bei besonders vulnerablen Gruppen** geringer darstellt.

Grundsätzlich ist auch nicht nachzuvollziehen, warum die **Strafbarkeit** einer sexuell bestimmten **Objektifizierung** überhaupt von **besonders schützenswerten Körperregionen** abhängig sein sollte. Es mag ein angepasster Strafrahmen geboten sein. Die Annahme eines abweichenden Unwertgehalts, der eine Strafbarkeit gänzlich verneint, erschiene vor dem Hintergrund des Ref-E und dessen Überlegungen in der Gesetzesbegründung inkonsistent.

Dieser **Schutzbedarf** erscheint **unabhängig des Alters der Personen** gegeben, wobei besonders vulnerable Gruppen ggf. einen qualifizierten Strafrahmen rechtfertigen könnten.

Insoweit ist auch die **Entgeltlichkeit** des § 184k Abs. 2 StGB-E **fragwürdig**. Nachvollziehbar erschiene ein **Rückgriff auf die sexuell bestimmte Weise**, und eine gesetzliche Liste von Regelbeispielen, etwa die Verbreitung auf, oder der Bezug über **spezialisierte Online-Plattformen, Chat-Gruppen** oder in Fällen, in denen sich aufgrund des **konkreten Kommunikations-Kontexts** zu den Inhalten, die Intention der Täter*innen eindeutig erkennen lässt.

Im Weiteren erscheint der Rückgriff auf ein **fiktives**, **tatsächliches** und **wirklichkeitsnahes Geschehen inkonsistent**.

Aus § 184b Abs. 1 aE StGB(-E) ergibt sich, dass für die höchst schützenswerte Gruppe der Betroffenen nach § 184b StGB auch fiktive Inhalte strafbar sein sollen. Dort heißt es nämlich

> ***Gibt der [„„] Inhalt in den Fällen von Absatz 1 Satz 1 Nummer 1 und 4 kein tatsächliches oder wirklichkeitsnahes Geschehen wieder, so ist auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu erkennen.***

Eine entsprechende Regelung fehlt aber in § 184c StGB-E, wobei nicht erkennbar ist, woraus sich dieser **Wertungswiderspruch** ergibt. Vorstellbar sind etwaige – internationale – (audiovisuelle) Medien, die zum Teil auch auf eine (weitreichende) Tradition in deren Herkunftskulturen aufbauen. Sollte dies der einzige Grund sein, eine ganze Kategorie der Tathandlungen für die betroffene Gruppe nach § 184c StGB unreguliert zu lassen, scheint eine **zielgerichtetere Ausnahme möglich** und wohl im Sinne des **Opferschutzes** zielführender, wenn nicht gar **geboten**.

§ 201b StGB-E umfasst „einen mittels eines Computerprogramms erstellten oder veränderten Inhalt, der den Anschein erweckt, ein tatsächliches Geschehen in Bezug auf eine andere Person wiederzugeben“.

Also mit anderen Worten die künstliche Generation eines Inhalts mit einem wirklichkeitsnahen Geschehen oder die Manipulation eines Inhaltes mit einem tatsächlichen Geschehen.

Die abweichende Formulierung „**den Anschein erweckt**“ lässt **Zweifel**, ob dieser Gleichlauf zur hier vorgeschlagenen „mit anderen Worten“-Formulierung gewünscht ist. Laut Gesetzesbegründung könnte ein solches **abweichendes Verständnis gewünscht** sein. Es soll laut Gesetzesbegründung nicht nur darauf ankommen, ob wirklichkeitsnahe Inhalte neu oder durch Manipulation erstellt wurden, sondern auch, ob ein objektiver Dritter diese als tatsächliches Geschehen wahrnehmen würde.

Es kommt also auf die **Qualität der Inhalte** an, wiederum gemessen am **objektivierten Erfolg** der tatsächlichen „**Fehlwahrnehmung**“. Mit anderen Worten: eine **Strafbarkeit** der inhaltlich verwerflichsten Inhalte wäre wohl auch dann nach dieser Norm **ausgeschlossen**, wenn Täter*innen in den – etwa bildlichen – Inhalt einen sichtbaren Hinweis „**mit KI erstellt**“ einbinden. Ob dies ausreicht, um den „**erheblichen Schaden**“ von Betroffenen abzuwenden ist fraglich, zumindest, wenn man die parallelen Diskussionen über den erforderlichen Umfang zur transparenten Darstellung von Produktplatzierungen, Werbung, oder ähnlichem berücksichtigt.

Hierbei mag angeführt werden, dass in diesen besonders krassen Fällen wohl etwaige **Spezialnormen** einschlägig wären, die den hohen Unwertgehalt adressieren. Dies ist aber in **Zweifel** zu ziehen, aufgrund der hier bereits **ausgeführten Inkonsistenzen**. Ergänzend ist etwa zu berücksichtigen, dass der **Unwertgehalt von § 184a StGB weiterhin auf tatsächliche Geschehen begrenzt** ist.

Zudem lässt eine solche Betrachtung die **Wirkung auf die Betroffenen** außer Acht. Der **psychologische Effekt** auf Betroffene, dass Dritte den Inhalt wahrgenommen haben (könnten), und das Dritte (im Einzelfall) nicht verstanden haben, dass es sich um künstliche / manipulierte Inhalte handelt, ist nicht zu unterschätzen. Allein dieser psychologische Effekt kann die Betroffenen in ihrer weiteren Lebensführung einschränken, ohne das im Übrigen erhebliche, physische oder finanzielle Schäden zu besorgen wären.

Außerdem ist fraglich, ab welchen **Grenzwerten** ein **objektiver Anschein** angenommen werden soll. Genügt eine **relative Quote** von 5% oder muss die Mehrheit die Inhalte als tatsächliches Geschehen wahrnehmen? Oder gelten **absolute Grenzwerte**?

In Zeiten **viraler Inhaltsverbreitung**, können Inhalte ohne Weiteres durch mehrere Millionen Nutzer*innen binnen kurzer Zeit wahrgenommen werden. Bereits 5% entsprechen somit einer erheblichen, absoluten Zahl von Nutzer*innen. Wird bei der Ermittlung des objektiven Anscheins auf eine **generalistische, globale Betrachtung** abgestellt, oder wird eine **Referenz des Nahfelds der Betroffenen** herangezogen? So ist vorstellbar, dass zwar nur 5% aller Nutzer*innen die Inhalte als „tatsächlich“ wahrnehmen, aber aufgrund abweichender Sozialisation, Bildung und weiterer „weicher Faktoren“, 80% der Nutzer*innen aus dem Nahfeld der Betroffenen.

Zudem bleibt offen, wie die **Feststellung auf einer Zeitachse** die Strafbarkeit beeinflussen. Gemäß dem Motto „der stete Tropfen höhlt den Stein“, mag der originäre Inhalt als solches weder den Anschein erwecken, noch die Schäden begründen.

Dieser Inhalt kann im weiteren Verlauf in einer sich **selbst-verstärkenden Kommunikationsschleife mit Echo-Effekten** eine hohe und **schädigende Eigendynamik** entwickeln, bei dem es den Rezipienten der nachgelagerten Kommunikation gar nicht mehr darauf ankommt, was der Ursprung der sekundären Inhalte tatsächlich war.

Insoweit generiert sich der Anschein des tatsächlichen Geschehens aus der **Vielzahl der sekundär Inhalte**, die (fälschlicherweise) den Eindruck eines tatsächlichen Geschehens auf Basis des offensichtlich nicht tatsächlichen Primär-Inhalts erwecken. **Kausal** für diese schädigenden Sekundär-Inhalte bleibt der **ursprüngliche, schlecht generierte Inhalt**.

Die weiteren **Sekundär-Inhalte erfüllen nicht notwendigerweise Straftatbestände**. Hierdurch bietet sich das **Risikopotential** geschickt **orchestrierter Kampagnen**, um in der Einzeltat eine Strafbarkeit zu vermeiden, in der Summe aber den gleichen, wenn nicht sogar einen intensiveren schädigenden Effekt auszulösen. Ein diese Lücke möglicherweise füllender **Nachweis** des „**vorsätzlich gemeinschaftlichen Handelns**“ dürfte **äußerst schwierig** zu führen sein.

Eine solche **Einschränkung** auf Ebene der „**Qualität**“ des Inhalts erscheint auch **nicht geboten**. Die **Einschränkung**, dass „**ein erheblicher Schaden**“ zu besorgen ist, ist **bereits schwerwiegend**.

Im Übrigen könnte das **Tatbestandsmerkmal** „**unbefugt zugänglich machen**“ **modifiziert** werden. Aktuell genügt bereits die unbefugte Zugänglichmachung gegenüber nur einer Person. Dies wäre aber nur dann geeignet, einen erheblichen Schaden zu begründen, wenn diese eine Person in einer besonderen Beziehung zu etwaigen Opfern stünde. Ansonsten wären erhebliche Schäden nur dann zu besorgen, wenn die Inhalte eine (unbestimmten) Vielzahl von Personen zugänglich gemacht wird. Insoweit erscheint eine sachdienlichere Ausgestaltung mit weniger Umgehungspotential vorstellbar.

5.2 Verlagerung hinsichtlich der räumlichen Tatbegehung

Zunächst wird auf die möglichen Risiken hinsichtlich des Tatortes hingewiesen, soweit sich dies aus der Limitierung der Beschränkung des GGDG-E hinsichtlich der Anbieter ergibt, exemplarisch und entsprechend 2.3.2.

Ergänzend hierzu sei darauf hingewiesen, dass die **Beschränkung auf Internetzugangsdienste erhebliche blinde Flecken** bedeuten kann. Täter*innen, die eher beiläufig eine Straftat begehen, werden hierdurch ermittelt werden können. Dies stellt – hoffentlich – auch die Mehrheit der Täter*innen dar.

Soweit Täter*innen aber einen gewissen Grad der Professionalität erreicht haben, oder aus anderen Gründen die Identifizier- und Nachverfolgbarkeit im Internet einschränken, etwa um ein (Werbe-)Profiling zu vermeiden, ist **nicht notwendigerweise von einer direkten Verbindung zwischen Informationen der Diensteanbieter zu den Informationen der Internetzugangsanbieter** auszugehen.

Soweit etwa **Proxy- oder VPN-Dienste** durch die Täter*innen genutzt würden, müsste zunächst die entsprechende **Dienstkette** nachverfolgt werden, wenn nicht bei den **Zwischendiensten** bereits hinreichende identifizierende Informationen vorlägen. Insoweit sollten auch **derartige Dienste als Adressaten der gerichtlichen Ausunftsanordnungen** aufgenommen werden, um eine Verlagerung der Tathandlungen zu vermeiden (obgleich man die Nutzung derartiger Dienste auch als veränderten modus operandi verstehen kann).

Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt

Mai 2026

Stellungnahme zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 16. April 2026

Rechtsanwalt Frank Ingenrieth, LL.M.