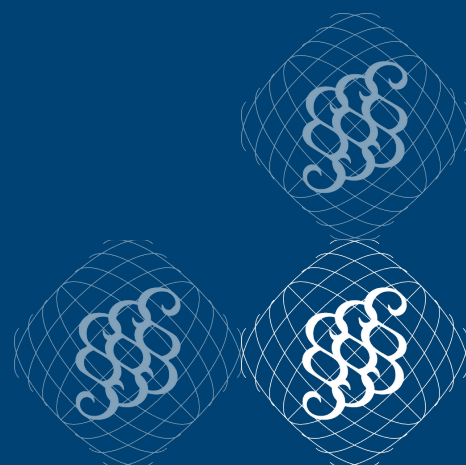
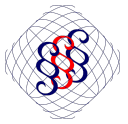




Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt

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





1 Executive Summary

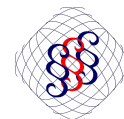
2 Einordnung, Prämissen und die veränderte Realität digitaler 3 Gewalt

4 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.

13 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.

20 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.

28 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.



33 Defizite in der methodischen Fundierung und Zielbestimmung

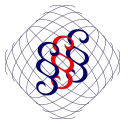
34 Die systematische Untersuchung offenbart, dass der Ref-E trotz seines explizit proklamierten
35 „ganzheitlichen Anspruchs“ diesem Anspruch wohl nicht gerecht wird. Der Gesetzgeber listet
36 zwar einen breiten Katalog an Phänomenen auf – wie Hate Speech, Doxing, Cyberflashing,
37 Cybergrooming, bildbasierte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

43 Zudem fehlt eine klare Definition und dogmatische Priorisierung der primären gesetzgeberi-
44 schen Schutzziele. Es wird nicht sauber unterschieden, ob das vorrangige Ziel die **präventive**
45 **Vermeidung** künftiger Delikte, die **schnelle Beseitigung** (Löschung, Sperrung) von Inhalten
46 oder die **nachträgliche Sanktionierung** der Täter*innen ist. Da je nach Primärziel gänzlich
47 unterschiedliche regulatorische Instrumente zielführend sind, führt dieses methodische Ver-
48 säumnis zu weitgehenden Fehllenkungen und im Ergebnis geringen Effekten der vorgeschlage-
49 nen Regelungen.

50 Grundlegende Kritik bzgl. des präventiven Ansatz

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

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



67 Strukturelle Mängel des GGDG-E und verfahrenstechnische 68 Hürden

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

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

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

82 ■ **Beweiswürdigungsprobleme bei nachträglicher Manipulation:** Löschen oder verändern
83 Täter*innen ihre Inhalte oder Personalien im Nachgang einer Tat, führt die starre Orientie-
84 rung an einem bloßen „Live-Inhalt“ zum Zeitpunkt der behördlichen Abfrage zu unauflösba-
85 ren Widersprüchen zwischen den Beweisen der Betroffenen und den Auskünften des Anbie-
86 ters. Dies führt im Rahmen der gerichtlichen Beweiswürdigung zu erheblichen **Nachteilen zu**
87 **Lasten der Opfer** digitaler Gewalt, obwohl die Modifikation direkt auf die Manipulation der
88 Täter*innen zurückzuführen ist. Ein effektiver Auskunftsanspruch muss daher zwingend
89 auch verfahrensrelevante Nebeninformationen und Historisierungsdaten (z. B. Reichweiten-
90 konfigurationen, Interaktionsdaten, Änderungshistorien) umfassen.

91 Ignoranz technischer Realitäten bei der Identitätsfeststellung (§ 92 2 Abs. 2 GGDG-E)

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

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



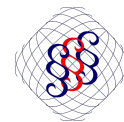
- 99 ▪ **Account-Hacking:** Das unbefugte Kapern oder Hacken von legitimen Nutzerkonten wird pro-
100 zessual nicht adäquat abgefangen.
- 101 ▪ **Fehlerhafte Zeitstempel und IP-Übertragungsfehler:** Die automatisierte Abfrage von IP-
102 Adressen kann unter asynchronen Aktualisierungsverzögerungen in den Zuweisungsdaten-
103 banken der Internetzugangsanbieter sowie unter fehlerhaften Zeitstempeln bei den Diens-
104 teanbietern leiden. Schon minimale Abweichungen führen zur Zuordnung völlig unbeteiligter
105 Personen.
- 106 ▪ **Identitätsdiebstahl und Fake-Accounts:** Das gezielte Agieren unter falschem Namen oder
107 mittels gefälschter Profile hebt die einfache Abfrage gespeicherter Personalien aus.

108 Um diesen Mängeln zu begegnen, bedarf es engmaschigerer Verfahren. Die gerichtliche Siche-
109 rung und Identitätsfeststellung sollte innerhalb eines straffen, maximal 48 Stunden umfassen-
110 den Gesamtverfahrens direkt über die Gerichte abgewickelt werden, anstatt Anbieter zu
111 „Schutzpatronen der Rechtsstaatlichkeit“ zu stilisieren und mit unnötigen Rechtsmitteln
112 auszustatten.

113 Kritik an eingeschränkten strafrechtlichen Tatbeständen am 114 Beispiel des § 202e StGB-E

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

124 Die Stellungnahme legt daher einen **modifizierten Formulierungsvorschlag** vor: Die Strafbar-
125 keit sollte primär an die Unbefugtheit der Überwachungshandlung und den gezielten Einsatz
126 von Informations- oder Kommunikationstechnik anknüpfen. Zudem wird eine gesetzliche Ver-
127 mutungswirkungen und Regelbeispiele vorgeschlagen.



128 Differenzierter Umgang mit Anonymität, KI-Bots und innovative 129 Sanktionsinstrumente

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

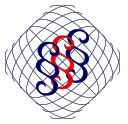
135 Je höher der Grad der Anonymität eines Profils ist, desto niedriger müssen die Hürden für
136 **Unmittelbarkeitsautomatismen** (Inhalts- und Account-Sperren) angesetzt werden.

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

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

150 Verlagerung der Tatorte und Tatformen

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



159 sowie verfahrenstechnische Verzögerungen ungelöst lässt, steht zu befürchten, dass die vorge-
160 schlagenen Regelungen zu keiner nachhaltigen Eindämmung, sondern lediglich zu einer inhalt-
161 lichen und räumlichen Verlagerung digitaler Gewalt führen:

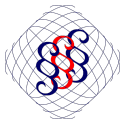
162 ■ **Inhaltliche Verlagerung (Anpassung des modus operandi):** Da die im Entwurf vorgesehe-
163 nen Effizienz- und Effektivitätsgewinne des GGDG-E starr an eng umgrenzte Katalogtaten
164 gekoppelt sind, wird für potenzielle Täter*innen ein erheblicher Anreiz geschaffen, ihre Ver-
165 haltensmuster gezielt anzupassen. Durch das bewusste Ausnutzen verbleibender Rege-
166 lungs- und Durchsetzungslücken können Schutzmechanismen systematisch umgangen wer-
167 den, wodurch der beabsichtigte Opferschutz im Ergebnis ins Leere läuft.

168 ■ **Räumliche Verlagerung (Ausweichen auf alternative Plattformen und Infrastrukturen):**
169 Durch die sachlich nicht gerechtfertigte Beschränkung folgenschwerer zivilrechtlicher Maß-
170 nahmen (wie Account-Sperren) auf klassische „Soziale Netzwerke“ verlagert sich das Tatge-
171 schehen absehbar auf professionelle Plattformen, Messenger-Dienste oder Gaming-Netz-
172 werke, die vom Schutzbereich der §§ 1 und 4 GGDG-E unberücksichtigt bleiben. Zudem nut-
173 zen professionell agierende Täter*innen zunehmend **Proxy- oder VPN-Dienste**, um ihre
174 Nachverfolgbarkeit einzuschränken und ein Profiling zu vermeiden. Da der Entwurf es ver-
175 säumt, derartige Intermediäre und Dienstketten konsequent als Adressaten gerichtlicher
176 Auskunftsanordnungen einzubeziehen, droht eine vollständige Verschiebung der Tathand-
177 lungen in nach dem GGDG-E regulatorisch unzugängliche Räume.

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

183 Defizite im Opferschutz: Prozessuale Beschleunigung, finanzielle 184 Risikominimierung und innovative Sanktionsinstrumente

185 Um das proklamierte Ziel eines effektiven Präventivkonzepts zu erreichen, greift der Referen-
186 tenentwurf prozessual und sanktionsrechtlich zu kurz. Aus kriminalpsychologischer Sicht erfor-
187 dert Abschreckung vor allem **Schnelligkeit und Konsequenz**. Daher fordert die Stellungnahme
188 die Verpflichtung von Plattformanbietern zu **vollautomatisierten Verfahren** zur Beweissiche-
189 rung und Identitätsextraktion. Dieses Erstverfahren ist durch **engmaschige Fristen zu**
190 **beschleunigen**: Eine Informationsweiterleitung an Nutzer*innen muss binnen 24 Stunden
191 erfolgen, die Rückmeldefrist zur Inhaltsverteidigung ist auf 72 Stunden zu begrenzen, und das
192 gerichtliche Identitätsfeststellungsverfahren darf insgesamt maximal 48 Stunden umfassen.



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

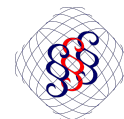
- 196 ■ Dies betrifft etwa die gezielte **Unterbindung von Finanzströmen** zur Austrocknung der Täter-
197 Monetarisierung, die **Rücksetzung digitaler Netzwerke** oder die **algorithmische Verbrei-**
198 **tungsmacht** künftiger Inhalte zu reduzieren.
- 199 ■ Im Bereich der **Strafvollstreckung** regt die Stellungnahme an, das präventive Potenzial,
200 dass bereits von Bewährungsweisungen gemäß § 56c StGB bekannt ist, konsequent auszu-
201 schöpfen, festzuschreiben und weiterzuentwickeln. (Wiederholungs-)Tätern kann die **Nut-**
202 **zung bestimmter Plattformkategorien oder ein unbeaufsichtigter Internetzugang** unter-
203 sagt werden.

204 Im Rahmen finanzieller Wirkkraft, wird eine Optimierung der **Verfahrenskosten** aneregt. Ange-
205 sichts der Ubiquität und Dauerhaftigkeit digitaler Gewalt verlangt die Stellungnahme zudem
206 eine klarstellende Norm zum **Ersatz von Folgeschäden**: Täter*innen sollte verpflichtet werden,
207 die Kosten für professionelle Monitoring-Services zu erstatten. Nur so kann eine Sekundärver-
208 breitung (auch im Darknet) wirksam unterbunden werden, ohne Betroffene im Wege der Eigen-
209 recherche einer permanenten **Retraumatisierung** auszusetzen.

210 Strukturell sollte diese Rechtsdurchsetzung durch **spezialisierte Ermittlungseinheiten und**
211 **Schwerpunktstaatsanwaltschaften** flankiert sowie die unzureichende ‚Textform‘ durch foren-
212 sisch verwertbare, maschinenlesbare Datenstandards ersetzt werden

213 **Fazit und Kernempfehlungen**

214 Der vorliegende Referentenentwurf bedarf einer fundamentalen materiell-rechtlichen und pro-
215 zessualen Überarbeitung. Um digitale Gewalt wirksam und nachhaltig zu bekämpfen, muss der
216 Gesetzgeber von rein symbolischen Strafverschärfungen Abstand nehmen. Stattdessen müs-
217 sen die **prozessuale Schnelligkeit, forensisch verwertbare Datenstandards, plattformüber-**
218 **greifende Geltungsbereiche** sowie **reichweitenbezogene Sanktionsinstrumente** (Netzwer-
219 krücksetzungen und Monetarisierungsverbote) in den Mittelpunkt gestellt werden. Ohne diese
220 Präzisierungen droht das Gesetz zu einem stumpfen Schwert im Kampf gegen die dynami-
221 schen Phänomene digitaler Gewalt zu werden.



222 Über den Autor

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

229 Seine Erfahrung sammelte Frank Ingenrieth während seines beruflichen Werdegangs, inklusive
 230 seiner Ausbildung, in internationalen Großkanzleien, datenschutzrechtlicher Aufsichtsbehör-
 231 den, internationaler Konzerne, gemeinnütziger Organisationen. Er veröffentlicht regelmäßig,
 232 entweder im Rahmen von juristischer Fachliteratur, Fachkommentare, sowie in Form von Dis-
 233 kussionsrunden und Panels².

234 Diese Stellungnahme wurde unabhängig und ohne Auftrag durch etwaige Mandant*innen
 235 erstellt. Die Stellungnahme und die Anmerkungen basieren auf der langjährigen praktischen
 236 Erfahrung des Autors in der Entwicklung und Durchsetzung von Konformitätsbewertungspro-
 237 grammen, inklusive solcher Prüfprogramme, die aufgrund ihrer rechtlichen Vermutungswirkun-
 238 gen behördlicher Anerkennung bedürfen.

239 Pflicht- und Kontaktinformationen des Autors

240	Richard-Sorge-Straße 69a	245	Steuer-Nummer 14/358/01684,
241	10249 BERLIN	246	FA Friedrichshain-Kreuzberg.
242	Fon +49 30 985 387 95	247	Ich optiere gem. § 19 UstG als Kleinunterneh- mer.
243	Fax +49 30 521 036 88	248	
244	E-Mail office@ingenrieth-online.de	249	IBAN DE22 5002 4024 7497 0388 01

250 Zuständige Kammer

251 Rechtsanwaltskammer Berlin, Littenstraße 9,
 252 10179 Berlin

253 In Deutschland verliehene

254 Berufsbezeichnung

255 Rechtsanwalt

wesentliche **berufsrechtliche Regelungen**

- Bundesrechtsanwaltsordnung
- Berufsordnung
- Rechtsanwaltsvergütungsgesetz.

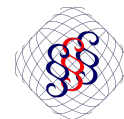
260 Diese und weitere können auf der [Webseite](#)
 261 [der Rechtsanwaltskammer Berlin](#) abgerufen
 262 werden.

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:

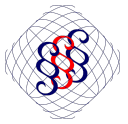
<https://ingenrieth-online.de/de/publikationen>.



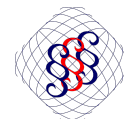
263	Inhaltsverzeichnis	
264	Executive Summary	2
265	Einordnung, Prämissen und die veränderte Realität digitaler Gewalt.....	2
266	Defizite in der methodischen Fundierung und Zielbestimmung.....	3
267	Grundlegende Kritik bzgl. des präventiven Ansatz.....	3
268	Strukturelle Mängel des GGDG-E und verfahrenstechnische Hürden.....	4
269	Ignoranz technischer Realitäten bei der Identitätsfeststellung (§ 2 Abs. 2 GGDG-E).....	4
270	Kritik an eingeschränkten strafrechtlichen Tatbeständen am Beispiel des § 202e StGB-E.....	5
271	Differenzierter Umgang mit Anonymität, KI-Bots und innovative Sanktionsinstrumente.....	6
272	Verlagerung der Tatorte und Tatformen.....	6
273	Defizite im Opferschutz: Prozessuale Beschleunigung, finanzielle Risikominimierung und innovative Sanktionsinstrumente.....	7
274		
275	Fazit und Kernempfehlungen.....	8
276	Über den Autor	9
277	Inhaltsverzeichnis	10
278	1 Einordnung, Prämissen	13
279	1.1 Prämissen und thematischer Fokus.....	14
280	1.2 Im Ref-E angesprochene Phänomene, Begriffsbestimmung.....	15
281	1.3 Gesetzgebungskompetenzen, Ganzheitlichkeit.....	17
282	2 Analyse der Ganzheitlichkeit	18
283	2.1 Präventivmaßnahmen.....	19
284	2.2 Schnelle Beseitigung digitaler Gewalt.....	21
285	2.2.1 Konkretisierungspotential der Rechtsmittel durch Anbieter.....	23
286	2.2.2 Konkretisierungs- und Effektivierungspotential 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
287	2.2.3 Kostenerleichterung für das Auskunftsverfahren; Regelbeispiele des Umfangs der Beseitigungsansprüche.....	26
288		
289	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
303		
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



310 1 Einordnung, Prämissen

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

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

318 Konkret heißt es:

319 ***Zugleich hat die digitale Transformation einen neuen, virtuellen Raum zur Begehung von Rechtsguts-***
320 ***verletzungen mit digitalen Mitteln eröffnet und damit neue Formen der Gewalt – die „digitale Gewalt“***
321 ***– ermöglicht.⁷***

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

325 ***Dieser Entwurf zielt darauf ab, den Schutz vor digitaler Gewalt rechtsgebietsübergreifend zu verbes-***
326 ***sern.⁹***

327 Sowie

328 ***Die Bekämpfung digitaler Gewalt erfordert ein ganzheitliches Vorgehen.¹⁰***

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

3 Abruflbar 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.

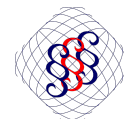
8 Abschnitt A Ref-E, S. 1, Ref-E Begründung, Abschnitt A I, S. 19.

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.



333 1.1 Prämissen und thematischer Fokus

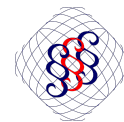
334 Diese Generalität des Ref-E verlangt eine Einordnung der Stellungnahme vor dem Hintergrund
335 der vom Ref-E adressierten Sachverhalte. Eine Umfänglichkeit hinsichtlich jedweder Thematik
336 ist im Hinblick auf die erforderlichen Ressourcen nicht zu leisten. Entsprechend bedarf diese
337 Stellungnahme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

338 Die inhaltlichen Einschränkungen betreffen die juristischen Einzelfalltiefe. Diese Stellung-
339 nahme widmet sich vordergründig der **methodischen Analyse** und der **potentiellen strukturel-**
340 **len Regelungslücken**.

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

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

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



368 1.2 Im Ref-E angesprochene Phänomene, Begriffsbestimmung

369 Das Ref-E spricht selbst einen weitreichenden Katalog an Phänomenen an, die als „digitale
370 Gewalt“ verstanden werden. Dies umfasst beispielsweise¹³

- 371 ▪ **„Hate Speech“** (abwertende, bedrohliche, gewaltverherrlichende oder zu Straftaten auf-
372 rufende Beiträge in sozialen Netzwerken, Blogs oder Foren),
- 373 ▪ **„Doxing“** (das unerlaubte Veröffentlichen personenbezogener Daten wie Adresse oder
374 Telefonnummer),
- 375 ▪ **„Cyberflashing“** (das unerwünschte Zusenden von Bildmaterial, das Gewalttätigkeiten
376 und/oder Pornographie („Dick Pics“) enthält),
- 377 ▪ **„Cybergrooming“** (das gezielte Ansprechen und Manipulieren Minderjähriger im Internet,
378 um sexuelle Kontakte anzubahnen oder sexuelle Handlungen zu fördern),
- 379 ▪ **bildbasierte sexualisierte Gewalt,**
- 380 ▪ **„Cyberstalking“** (das Verfolgen, Belästigen und/oder Überwachen einer Person mit digitalen
381 Technologien),
- 382 ▪ **„Cybermobbing“** (das Beleidigen, Bedrohen, Bloßstellen oder Belästigen über digitale Kom-
383 munikationsmedien) und der Identitätsmissbrauch (das Kommunizieren unter einem Fake-
384 Profil zum Nachteil einer real existierenden Person).

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

388 | ***Digitale Gewalt unterscheidet sich in ihrer Wirkung und ihrer Wirkweite grundlegend von analoger
389 Gewalt.¹⁵***

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

392 Zugleich werden auch Gemeinsamkeiten und Interdependenzen erwähnt:

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

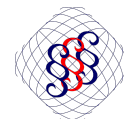
13 Abschnitt A Ref-E, S. 1.

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.



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

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

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

407 Zugleich ergeben sich aus dem ganzheitlichen Anspruch des Ref-E auch Fragestellungen im
408 Rahmen der **Konsistenz und der Begrenzung staatlichen Eingreifens**. Denn nicht jeder indivi-
409 duell unliebsame Sachverhalt begründet einen gesellschaftlich unliebsamen Sachverhalt, der
410 staatlicher Regulierung verlangt. Grundrechtsverpflichtet ist zunächst nur der Staat. Es gehört
411 aber zu den vornehmen Pflichten eines Staats, die in den Grundrechten zum Ausdruck kom-
412 menden Werte in seine allgemeinen Gesetze zu überführen und somit Wirkung grundrechtli-
413 cher Werte auch zwischen Privaten zu begründen.¹⁹ Zugleich ist der Staat im Rahmen seiner
414 vornehmen Pflicht, die grundrechtlichen Werte einfachgesetzlich zu effektuieren, wiederum
415 selbst an die Grundrechte, und mithin den **Verhältnismäßigkeitsgrundsatz**, gebunden.

- 416 ■ Nicht jeder Sachverhalt, der abstrakt-generell regelungsfähig ist, ist automatisch
417 regelungspflichtig.
- 418 ■ Nicht jeder Sachverhalt, der abstrakt-generell regelungsfähig ist, ist automatisch
419 regelungsberechtigt.

420 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.



421 1.3 Gesetzgebungskompetenzen, Ganzheitlichkeit

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

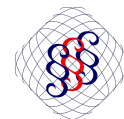
424 Insofern ist es nachvollziehbar, dass diese unterschiedlichen Sachverhalte ebenso eine Viel-
425 zahl von Themenfeldern und Rechtsgebieten betreffen. Insoweit ist zu erwarten, dass sich
426 effektive Maßnahmen aus einem **Konglomerat aus Regelungen** in unterschiedlichsten The-
427 menfeldern und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

430 Insbesondere im Rahmen der Regulierung der „Dienste der Informationsgesellschaft“ sowie
431 der „Telekommunikationsdienste“ ist aufgrund des Europäischen Binnenmarktes davon auszu-
432 gehen, dass die Kompetenz **des nationalen Gesetzgeber** erheblich durch absolute oder konkurrierende
433 Gesetzgebungskompetenzen der **Europäischen Union** limitiert sein dürfte.
434 Zugleich ist davon auszugehen, dass im Rahmen der Medienregulierung zumindest in Deutsch-
435 land die Gesetzgebungskompetenz ganz oder teilweise nicht dem **Bund**, sondern den **Ländern**
436 zugewiesen ist.

437 Im Rahmen der Stellungnahme wird nicht im Detail darauf eingegangen werden, ob das den
438 Ref-E bzw. dessen finalen Gesetzesbeschluss zu verantwortende Organ die tatsächliche
439 Gesetzgebungskompetenz besitzt. Es wird auch nicht darauf eingegangen werden, ob für
440 etwaige Alternativvorschläge die Gesetzgebungskompetenz vorläge. Vielmehr wird methodisch
441 und systematisch untersucht, ob der Ref-E den avisierten ganzheitlichen Anspruch erfüllt. Die
442 Frage der Gesetzgebungskompetenz stellt sich erst im Anschluss, nachdem eine sachdienliche
443 Analyse der derzeitigen Sachlage stattgefunden hat. Nachdem der Ref-E selbst auch bereits
444 auf weitere Gesetzgebungsvorhaben verweist, welche das Gesamtkonzept vervollständigen sol-
445 len²⁰, wäre eine solche Darstellung und Ganzheitlichkeit auch methodisch vorstellbar gewesen
446 im Falle abweichender Gesetzgebungskompetenzen.

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

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



2 Analyse der Ganzheitlichkeit

455
456 Der Ref-E behauptet das Phänomen der „digitalen Gewalt“ ganzheitlich zu adressieren. Letzt-
457 lich beschränkt sich der Ref-E jedoch auch zwei wesentliche Regelungsbereiche, nämlich das
458 **Strafrecht** und das **Zivilrecht**.

459 Der Ref-E nennt eine Vielzahl von konkreten Phänomenen der „digitalen Gewalt“ Zugleich lässt
460 der Ref-E eine strukturierte Analyse dahingehend vermissen, für welche dieser Phänomene tat-
461 sächlich eine regulatorische Lücke existiert. Eine solche Analyse ist dem Ref-E allenfalls mittel-
462 bar zu entnehmen. Etwa immer dann, wenn der Ref-E zu den Phänomenen bereits existierende
463 Schutznormen anführt und keine eigenen, neuen Schutznormen etabliert. Im Ergebnis sieht
464 der Ref-E nur begrenzt neue strafrechtliche Normen vor, § 201b StGB-E²¹ und § 202e StGB-E
465 werden ergänzt, § 184k StGB-E wird ersetzt.²²

466 Die „Ersetzung“ von § 184k StGB-E ist eher eine editorielle Erleichterung. Bereits der aktuelle
467 § 184k StGB hat die „Verletzung des Intimbereichs durch Bildaufnahmen“ zum Regelungsgen-
468 stand. Die Gesetzesbegründung führt aus, dass § 184k StGB-E eine Konsolidierung der Straf-
469 tatbestände verfolge und bestehende Schutzlücken schließe.²³

470 Neu eingeführt wird zudem das GGDG-E, welches die zivilrechtliche Durchsetzung der Ansprü-
471 che erleichtern soll.

472 Dabei stellen sich indessen mehrere Fragen:

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

474 Ist Ziel die **schnelle Beseitigung** (Löschung, Sperrung oder sonstige Verhinderung der Verbrei-
475 tung) von digitalen Gewaltinhalten?

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

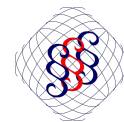
477 Je nach Primärziel sind andere Maßnahmen zielführend.

478 Da der Ref-E eine solche methodische Unterscheidung erst gar nicht aufweist, ist zu vermuten
479 dass bei der Ausarbeitung des Ref-E die nötigen Vorüberlegungen nicht stattgefunden haben.
480 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.



481 2.1 Präventivmaßnahmen

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

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

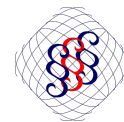
489 Einerseits ist zu begrüßen, dass der Entwurf klarstellt, was ohnehin klar sein sollte: das Verhal-
490 ten im Digitalen Raum unterliegt ebenfalls den rechtlichen Normen, wie das Verhalten im Ana-
491 logen Raum. Sollte diese Grundregel der Gesellschaft noch nicht bekannt gewesen sein, kann
492 der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

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

495 Ein Gesichtspunkt könnte eine mangelnde Ausprägung zentraler Werte und Normen im Rah-
496 men der **persönlichen Entwicklung** sein. Eine ähnliche Zielrichtung hätte die Frage, ob allen
497 Täter*innen²⁴, gerade im Bereich der Kinder und Jugendlichen, der Unrechtsgehalt ihrer Hand-
498 lungen bewusst ist. Ob etwaige Präventionsmaßnahmen im Bereich der Kinder- und Jugend-
499 arbeit zielführend(er) wären, obliegt den Stellungnahmen der diesbezüglichen Fachverbände.
500 Ein weiterer Gesichtspunkt könnte eine wachsende **Perspektivlosigkeit** der Täter*innen sein,
501 die digitale Gewalt als **Frustrationsventil** nutzen. Inwieweit hier begleitende Präventionsmaß-
502 nahmen im Rahmen der persönlichen Perspektivplanung besser geeignet wären, obliegt den
503 Stellungnahmen der diesbezüglichen Fachverbände. Ebenfalls vorstellbar ist, dass die Aus-
504 übung Digitaler Gewalt eine Folge individueller **Traumata** und individueller **Fehlvorbilder** ist.
505 Inwieweit hier begleitende Präventionsmaßnahmen zur Bewältigung erlittener Traumata und
506 Erkenntnis der eigenen Fehlvorbilder zielführender sein könnten, obliegt den Stellungnahmen
507 der diesbezüglichen Fachverbände. Für einen Ref-E, der einen ganzheitlichen Anspruch prokla-
508 miert, fällt jedoch auf, dass diese Dimension unbeachtet bleibt.

509 Soweit der abstrakte Präventionscharakter von Sanktionsnormen in Anrechnung gebracht wird,
510 und aus diesen Gründen sowohl die strafrechtliche als auch zivilrechtliche Durchsetzung von
511 gestärkt werden soll, ist zu erkennen, dass sich die Vorschläge im Wesentlichen auf das mate-
512 rielle 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.



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

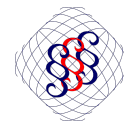
518 Aus psychologischer Sicht erscheint der zügige Abschluss des „Erstverfahrens“ besonders
519 wichtig. Hierzu genügt bereits die Erkenntnis, dass „digitale Handlungen“ verfolgt werden kön-
520 nen. Die konkrete Schärfe der „**Erstsanktion**“ erscheint weniger ausschlaggebend. Soweit
521 etwaige Rechtsmittel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

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

- 531 ■ Der Ref-E gibt an, die Gesamtheit der Tathandlungen bzgl. „Tatmittel Internet“ als Grundlage
532 heranzuziehen, das sind nach eigenen Angaben aus den Jahren 2022/2023 97.000.²⁵
- 533 ■ Von den Tathandlungen wurden laut Ref-E bereits 83.000 Fälle aufgeklärt auf Grundlage der
534 bisherigen Rechtslage – bzw. der Rechtslage in den Jahren 2022/2023, das entspricht
535 einer Aufklärungsquote von 85,57%.
- 536 ■ Durch den Ref-E wird eine Steigerung der Aufklärungsquote von 10% der bisher nicht aufge-
537 klärten Fälle (14.000) erwartet, also einer Aufklärung von weiteren 1.400 Fällen. Das ent-
538 spricht ca. 1,5% aller Tathandlungen, und würde zu einer Gesamtaufklärungsquote von
539 87,01% führen.

540 Jede aufgeklärte Tathandlung ist ein Fortschritt, und es sollte eine Verbesserung nicht des-
541 wegen aufgegeben werden, weil die angestrebte Regelung nicht perfekt ist: „Das Bessere ist
542 der Feind des Guten“. Es ist auffällig, dass der ganzheitliche Anspruch des Ref-E in Wider-
543 spruch zu dem doch minimalen Mehrwerten steht. Es ist jedenfalls nicht ersichtlich, wie sich
544 aus einer relativen Steigerung der Aufklärungsquote von 1,5% eine hinreichende Steigerung
545 des **Sanktionsdrucks** ergeben sollte, die tatsächlich präventive Auswirkungen haben könnte.

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



546 2.2 Schnelle Beseitigung digitaler Gewalt

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

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

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

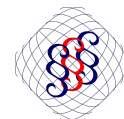
558 Vielmehr scheint der Ref-E Auffassungen zur „Erforderlichkeit der Anonymität im Internet“ zu
559 perpetuieren, die im Ergebnis so nicht zwingend sind, siehe hierzu vertiefend 4.

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

563 An keiner Stelle sieht der Ref-E **Vermutungswirkungen** im Sinne der Betroffenen vor, die
564 zumindest eine vorläufige, schnelle Beseitigung der digitalen Gewalt begründenden Umstände
565 zur Folge hat. Im Gegenteil, selbst die nun vorgesehenen Regelungen zur Account-Sperre
566 (§ 4 GGDG-E) führen im Ergebnis zu einer erheblichen **Verzögerung des Verfahrens**.

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

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



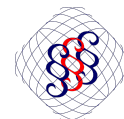
575 ▪ Betroffene müssen im Rahmen der einstweiligen Anordnung bzw. im Rahmen außergerichtli-
576 cher Verfahren eine Unterlassungserklärung herbeiführen; welches eine Verzögerung von
577 weiteren zwei Wochen oder mehr nach sich ziehen kann. Inwieweit der Auffangtatbestand
578 „anderen Umstände“ zeitliche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

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

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

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

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



594 2.2.1 Konkretisierungspotential der Rechtsmittel durch Anbieter

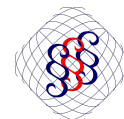
595 Der **Grundrechtsschutz** der vermeintlichen Täter*innen ist durch den **Richtervorbehalt**
596 gewährt. Die dem Gesetz innewohnende Skepsis gegenüber der Rechtmäßigkeit der richterli-
597 chen Anordnung ist bedenkenswert. Es ist zwar dem Rechtsstaat immanent, dass gerichtliche
598 Entscheidungen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

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

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

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

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



626 2.2.2 Konkretisierungs- und Effektivierungspotential durch engma- 627 schige Fristen

628 Soweit nicht der **Ausnahmefall** vorliegt, dass anonyme Nutzer*innen unrechtmäßig Gegen-
629 stand eines Informationsanspruchs werden und trotz eines Richtervorbehalts diesem unzuläs-
630 sigen Informationsbegehren auch stattgegeben wurde, ist davon auszugehen, dass tatsächlich
631 eine rechtswidrige Handlung vorliegt. In diesem Fall ist nicht nachvollziehbar, warum das
632 GGDG-E keine strafferen Verfahrensfristen vorsieht.

633 2.2.2.1 Fristen für Nutzer*innen zur Verteidigung eigener Rechte

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

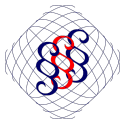
641 Die Weiterleitung von Informationen an Nutzer*innen hat **sofort** zu erfolgen, jedenfalls nicht
642 später als **24 Std.** nach Erhalt durch die Anbieter.

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

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

649 Eine Anzeige dahingehend, dass der angegriffene Inhalt weiterhin zugänglich bleiben muss,
650 sollte binnen **72 Std.** für Nutzer*innen möglich sein. Eine Anzeige dahingehend, dass Rechts-
651 mittel gegen die Aufdeckung der Identität eingelegt werden, kann hiervon unabhängig die übli-
652 chen Rechtsmittelfristen vorsehen.

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



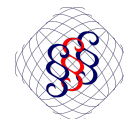
656 2.2.2.2 Fristen und Verfahren zur Sicherung der für die Aufdeckung der Identität 657 erforderlichen Informationen

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

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

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

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



677 2.2.3 Kostenerleichterung für das Auskunftsverfahren; Regelbeispiele 678 des Umfangs der Beseitigungsansprüche

679 Soweit die Gesetzesbegründung ausführt, dass auf einen **Gebührentatbestand** für das Aus-
680 kunftsverfahren verzichtet werden, sind die dortigen Gründe nur teilweise nachvollziehbar.

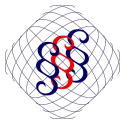
681 Einerseits ist zwar zu begrüßen, dass Betroffene, die aufgrund der Erfahrung durch digitale
682 Gewalt bereits Nachteile erfahren, von unnötigen Kosten zur Durchsetzung der eigenen Ansprü-
683 che befreit sein sollten. Soweit es sich hierbei also um einen psychologischen Effekt handeln
684 sollte, endet dieser bereits bei den **Folgeverfahren**. Etwaige Unterlassungs- oder Schaden-
685 ersatzansprüche unterlägen den auch sonst geltenden Regeln des Zivilprozesses. Je nach
686 Höhe des erlittenen Schadens, ist das damit einhergehende Kostenrisiko, und die zu leisten-
687 den Kostenvorschüsse, signifikant.

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

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

697 Diese Risiken könnten durch zielgerichtete Regelungen mitigiert werden.

- 698 ■ Verbleibt der Auskunftsanspruch **fruchtlos**, da **keine hinreichenden Informationen** ermittelt
699 werden konnten, so könnte das Gesetz vorsehen, dass in diesen Fällen die Kosten des Ver-
700 fahrens durch den Staat zu tragen sind.
- 701 ■ Verbleibt der Auskunftsanspruch **fruchtlos**, da dieser **nicht hinreichend glaubhaft** gemacht
702 wurde, so ist durchaus vorstellbar, dass die Betroffenen (einen Teil der/) die Kosten zu tra-
703 gen haben; schließlich liegt die Ursache der Fruchtlosigkeit in ihrer eigenen Einflussphäre.
- 704 ■ Ist ein Auskunftsanspruch erfolgreich, aber die Betroffenen **verzichten auf einen zivilrechtli-**
705 **chen Folgeprozess**, so ist durchaus vorstellbar, dass die Betroffenen (einen Teil der/) die
706 Kosten zu tragen haben;
- 707 ■ Wird im **Folgeverfahren** festgestellt, dass die **angegriffenen Inhalte nicht rechtswidrig**
708 waren, so ist durchaus vorstellbar, dass die Betroffenen keine oder allenfalls einen Teil der
709 Kosten zu tragen haben; schließlich hat das Gericht im Auskunftsverfahren ebenfalls die
710 Ansprüche für überwiegend wahrscheinlich (glaubhaft) eingeschätzt.



711 ▪ Wird im **Folgeverfahren** die Rechtswidrigkeit festgestellt, könnte der **Kostenanspruch auf**
712 **den Staat** übergehen, und durch diesen durchgesetzt werden; auf den ansonsten möglichen
713 Rückgriff auf die Klägerpartei bei Zahlungsausfall der Beklagtenpartei könnte explizit ver-
714 zichtet werden.

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

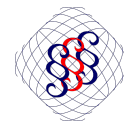
723 Aus ähnlichen Überlegungen lässt das GGDG-E bzw. der gesamte Ref-E **Potentiale verpuffen**,
724 die einen **nachhaltigen Schutz** der **Betroffenen** vor den **Konsequenzen der rechtswidrigen**
725 **Inhalte** etabliert. Es ist bisher keine etablierte Rechtsfolge, dass im Falle einer rechtswidrigen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

730 Dabei sind es neben der eigentlichen Tathandlung gerade die **Langzeitfolgen**, die auch der
731 Ref-E als besonders schwerwiegend und die Betroffenen belastend darstellt. Zugleich kann es
732 nicht von den Betroffenen verlangt werden, sich selbst ständig mit der „historischen Tat“ aus-
733 einanderzusetzen, in diese selbst aktiv das Internet – und möglicherweise Darknet – auf ent-
734 sprechende Vervielfältigungen der Inhalte durchforsten.

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

- 739 ▪ eine **Allgemeinklausel**, die die konkrete angemessenen Auftragsdauer in das Ermessen des
740 Gerichts stellt
- 741 ▪ **Regelbeispiele**, bei welchen Tathandlungen eine Angemessenheit der Auftragsdauer vermu-
742 tet wird.

743 Eine Regelung zu den **angemessenen Vergütungssätzen** der Dienste erscheint nicht erforder-
744 lich, da dies durch die Täter*innen im Rahmen eines eigenen Gerichtsverfahrens festgestellt
745 werden kann.



746 2.3 Sanktionierung digitaler Gewalt

747 Soweit der Ref-E eine effektive **Sanktionierung** in den Fokus nimmt, ergeben sich auch Fra-
748 gen. Einerseits lässt die Gesetzesbegründung im Rahmen der zu erwartenden Erfüllungsauf-
749 wände erkennen, dass lediglich eine Verbesserung der Aufklärungsquote im strafrechtlichen
750 Bereich von 1.5% erwartet wird.²⁷

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

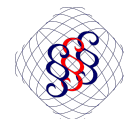
759 Auffällig ist andererseits, dass sich im Gesetz keine Maßnahmen dahingehend finden, die eine
760 **effizientere Bearbeitung der Verfahren** begründen könnte, etwa im Sinne von **spezialisierten**
761 **Ermittlungseinheiten, Schwerpunktstaatsanwaltschaften** oder **Schwerpunktgerichten**. Eine
762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

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

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

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

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



776 Beide Aspekte sind der deutschen Rechtsordnung nicht fremd.

777 ■ Die **Untersagung des Internetanschlusses** ist nach Auffassung der Rechtsprechung als
778 Bewährungsaufgabe, konkret in Form der Bewährungsweisung § 56c StGB, zulässig.²⁸

779 ■ Eine gezielte **Untersagung der Nutzung von Sozialen Netzwerken** wurde in der Vergangen-
780 heit durch die Strafverfolgungsbehörden auch angestrebt.

781 Dies hat die Rechtsprechung aber teils als unzulässig betrachtet, wobei die dafür angeführ-
782 ten Gründe erwähnenswert sind, nämlich (1) vermeintlich leichte Umgehungsmöglichkeit, (2)
783 Mehrpersonenhaushalt und damit einhergehende Unsicherheiten, wer den Anschluss und
784 das in Rede stehende Endgerät benutzt haben könnte, und – das war wohl der primäre
785 Grund – (3) eine mangelnde Definition, was denn ein Soziales Netzwerk und was eine „Nut-
786 zung“ dessen sei.²⁹ Alle genannten Gründe können durch entsprechende gesetzliche Ausge-
787 staltung ausgeräumt werden.

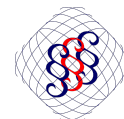
788 Eine solche gesetzliche Ausgestaltung könnte inzwischen auch geboten sein. Die etwa vom LG
789 Nürnberg-Fürth geäußerte These, dass verurteilte Straftäter*innen spätestens durch die Verur-
790 teilung über das Unrecht der begangenen Tathandlung Bescheid wüssten, und daher eine Wie-
791 derholung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

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

795 Insoweit erscheint – jedenfalls für nachweisliche Wiederholungstäter*innen – ein **Schutz-**
796 **pfllicht des Staates** dahingehend vertretbar, dass er diesen Täter*innen in angemessener
797 Weise die **Mittel für eine weitere Tatwiederholung entzieht**. Dies gilt umso mehr, soweit für
798 diese Täter*innen psychiatrische Erkrankungen – etwa Suchtkrankheiten oder Zwangsstörungen
799 – 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.



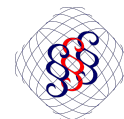
800 2.3.1 Beschränkung der Anwendbarkeit, Regelkatalog § 1 GGDG-E

801 Es ist nachvollziehbar, dass Betroffene nicht in allen Fällen eine **strafrechtliche Sanktion** der
802 Täter*innen anstreben, etwa je persönlichem (**Nähe-Verhältnis**) zwischen Täter*innen und
803 Betroffenen oder in Anbetracht des **Alters der Täter*innen**, bei denen Betroffene und deren
804 gesetzliche Vertreter erkennen können, dass die Täter*innen die Auswirkung des eigenen Han-
805 delns nicht haben umfänglich absehen können und die real eingetretenen Konsequenzen ehr-
806 lich und nachhaltig bereuen. Eine strafrechtliche Verfolgung, die möglicherweise negative Aus-
807 wirkungen auf den weiteren persönlichen und beruflichen Werdegang der Person hat, ist nicht
808 für alle Betroffene das Ziel. Diese Gedankengänge sind auch den Wertungen des StGB zu ent-
809 nehmen, da viele der Tatbestände als absolute oder relative Antragsdelikte ausgestaltet sind.

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

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



836 2.3.2 Beschränkung der Anwendbarkeit, Anbieter §§ 1, 4 GGDG-E

837 Insoweit das GGDG-E in dessen Begriffsbestimmungen **einzelne Formen der Anbieter** geson-
838 dert regelt, ist der Gesetzesbegründung zu entnehmen, dass hierdurch die Anwendbarkeit
839 bewusst eingeschränkt werden sollte. Einerseits aufgrund vermuteter Umstände, dass
840 bestimmte Dienste technisch für eine Tatbegehung nicht in Betracht kommen. Andererseits
841 um bestimmte Dienste auszuschließen, bei denen die Tatbegehung derzeit allenfalls als Rand-
842 phänomen wahrgenommen wird.³¹

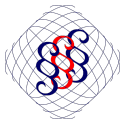
843 Diese Unterscheidung erschien dem Gesetzgeber notwendig, um im Rahmen der **Account-**
844 **Sperre** gesonderte Regelungen zu treffen. Denn diese Account-Sperre findet lediglich für Nut-
845 zerkonten in **Sozialen Netzwerken** statt.

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

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

863 ***Soziale Netzwerke im Sinne dieses Gesetzes sind Online-Plattformen im Sinne des Artikels 3 Buch-***
864 ***stabe i der Verordnung (EU) 2022/2065, deren Hauptzweck oder wesentliche Funktion darin besteht,***
865 ***dass ihre Nutzer miteinander kommunizieren und interagieren, indem sie Inhalte mit anderen Nutzern***
866 ***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.



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

871 Derartige zukunftsgerichtete Überlegungen sind dem Ref-E auch nicht fremd. So heißt es in der
872 Gesetzesbegründung³²:

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

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

882 2.3.2.1 Plattformen mit besonderen Schutzbedarfen der Nutzer*innen

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

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

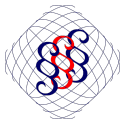
889 2.3.2.1.1 Plattformen im beruflichen, professionellen Kontext

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

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

896 Hierbei ist der Primärzweck der Plattform, dass die Veranstalter die eigene Veranstaltung
897 bewerben, und deren Operationalisierung erleichtern, etwa durch digitale Anmelde- und Regis-
898 trierungsprozesse, durch zentrale digitalen Agenden. Die wesentlichen Inhalte – Existenz der
899 Veranstaltung, sowie Untereinheiten – etwa konkrete Ereignisse entlang des Veranstaltungsab-
900 laufs – werden nicht von allen Nutzer*innen frei angelegt, sondern durch den Veranstalter.
901 Nutzer*innen haben sodann etwa die Möglichkeit, generell zur Veranstaltung, oder zu den ein-
902 zeln Ereignissen zu kommentieren.

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



903 Ebenfalls etabliert sich, dass den Teilnehmer*innen neben diesem Primärzweck die Möglich-
904 keit eingeräumt wird, niederschwellig mit weiteren Teilnehmer*innen der Veranstaltung in **pri-**
905 **vate, bilaterale Kommunikation** einzutreten, etwa um bilaterale Gespräche zur Geschäfts-
906 anbahnung zu vereinbaren.

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

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

916 **2.3.2.1.2 Gaming-Plattformen**

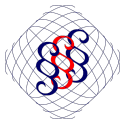
917 Hinsichtlich Gaming-Plattformen gilt entsprechendes. In diesem Fall ist zu beachten, dass die
918 **besonders vulnerable Gruppe** höchstwahrscheinlich Kinder und Jugendliche sind, und die
919 diese Gruppen gegenüber begangenen **Straftaten möglicherweise besonders schwerwie-**
920 **gend** sind.

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

926 **2.3.2.2 Weitere Plattformen**

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

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



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

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

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

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

954 **2.3.2.3 Fazit**

955 Das Gesetz sollte auf die **einschränkenden Definitionen** verzichten. Ein Nutzerkonto ist für
956 jede Plattform von Relevanz, nicht nur für Soziale Netzwerke. Dies ergibt sich auch bereits aus
957 § 2 GGDG-E.

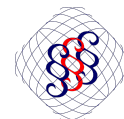
958 Informationspflichtig sind die zu den Nutzer*innen gespeicherten Personalien, § 2 Abs. 2 Nr. 1
959 lit. a) GGDG-E, neben den sonstigen Informationen, z.B. die IP-Adresse, § 2 Abs. 2 Nr. 1
960 lit. b) GGDG-E. § 2 GGDG-E findet auf jegliche Online-Plattformen Anwendung, unabhängig ob
961 es sich um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

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

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

968 Somit stellt sich die Frage, ob diese Referenz dort bewusst eine Einschränkung der Anwend-
969 barkeit auf Soziale Netzwerke beabsichtigt, oder ob dies ein der unnötigen begrifflichen Ein-
970 schränkung geschuldeter Redaktionsfehler ist.

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



972 2.3.3 Beweissicherung und Verwertbarkeit im Strafverfahren

973 § 3 Abs. 4 S. 2 GGDG-E ist insoweit unklar, durch wen die Informationen an die Strafverfol-
974 gungsbehörden weitergeleitet werden dürfen.

975 2.3.3.1 Anbieter als Regelungsadressat

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

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

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

990 2.3.3.2 Gericht als Regelungsadressat

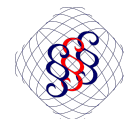
991 Wenn die **Strafverfolgungsbehörden** von dem bereits durchgeführten oder laufenden Identi-
992 tätsfeststellung gem. GGDG-E wissen, ist es wesentlich naheliegender, dass sich die Strafver-
993 folgungsbehörden die **Akten vom zuständigen Zivilgericht** übermitteln lassen. In diesem Fall
994 würde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

995 2.3.3.3 Betroffene als Regelungsadressat

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

1000 Laut Gesetzesbegründung soll eine Sicherung des angegriffenen Inhalts durch den Dienstean-
1001 bieter erfolgen und an das Zivilgericht übermittelt werden, um die Betroffenen von etwaigen
1002 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.



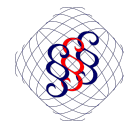
1003 im – rechtlich deutlich schwerwiegenderen – Strafverfahren wieder aufkommen, wenn die
1004 Inhalte vom Zivilgericht zunächst an die Betroffenen ginge, um von dort wieder an die Strafver-
1005 folgungsbehörden weitergeleitet würde.

1006 **2.3.3.4 Generelle Zielsetzung der Norm – Datenschutz oder Sicherung der** 1007 **Beweisverwertung**

1008 Irritierend ist die Wortwahl der „Übermittlung“ und welches Ziel hiermit verfolgt wird. Die Wort-
1009 wahl lässt darauf schließen, dass eine datenschutzrechtliche Erlaubnisnorm geschaffen wer-
1010 den sollte. Hierbei bliebe auch unklar, wer sich letztlich auf diese Erlaubnisnorm berufen dürfte
1011 – ungeachtet der Frage, ob es dieser Norm überhaupt bedurft hätte.

1012 Vor diesem Hintergrund der Uneindeutigkeit des Regelungsziels, scheint zudem vorstellbar,
1013 dass der Gesetzgeber mit dieser Vorschrift sicherstellen wollte, dass die im Rahmen des **zivil-**
1014 **rechtlichen Verfahrens** erhobenen und **gesicherten Beweise** tatsächlich in einem **nachgela-**
1015 **gerten Strafverfahren verwendet** werden dürfen, wenn zum Zeitpunkt des Strafverfahren eine
1016 neuerliche Beweissicherung nicht mehr möglich wäre, vgl. auch die Effekte und die Zielsetzung
1017 aus § 3 Abs. 5 GGDG-E.

1018 Insoweit ist anzumerken, dass im Strafrecht gem. § 250 StPO der **Unmittelbarkeitsgrundsatz**
1019 statuiert wird. Hiernach sind jegliche Beweise – soweit möglich – unmittelbar im Hauptsache-
1020 verfahren zu erheben. Sollte der **Gesetzgeber Risiken** hinsichtlich der Vereinbarkeit der nach
1021 GGDG-E erhobenen Beweise mit dem strafrechtlichen Unmittelbarkeitsgrundsatz erkannt
1022 haben, so sollte § 3 Abs. 4 S. 2 GGDG-E **dringend diesbezüglich nachgeschärft** werden.



1023 2.4 Unzulänglichkeit der Informationen nach § 2 Abs. 2 GGDG-E

1024 Das GGDG-E stellt in § 2 fest, welche Informationen durch Anbieter bereitgestellt werden müs-
1025 sen. Hierbei wird, in Ansehung des ganzheitlichen Charakters, davon ausgegangen, dass dies
1026 auch die Entsprechung der im Übrigen durch die Strafverfolgungsbehörden unmittelbar als für
1027 die Erhebung zulässig betrachteter Informationen betrifft.

1028 Zumindest ist in Anrechnung zu bringen, dass das GGDG-E den Zweck verfolgt, die **Informati-**
1029 **onserhebung** und **Beweissicherung** zu **beschleunigen**, und etwa Verzögerungen aufgrund der
1030 hohen Belastung Strafverfolgungsbehörden sowie der Prüfanforderungen im Rahmen der
1031 Strafverfahren zu vermeiden. Zumindest erklärt sich vor diesem Hintergrund die Regelung des
1032 § 3 Abs. 4 S. 2 GGDG-E, auch wenn hier Klarstellungen erforderlich sein dürften.³⁴

1033 In Ansehung von § 3 Abs. 4 S. 2 GGDG-E erscheint eine solche Beschleunigung auch effektiv,
1034 da die Informationserhebung und die Beweissicherung höchst effizient erfolgen könnte. Hierzu
1035 sollten aber die **Fristen** und die **Effekte der Rechtsmittel** noch einmal sachdienlich überprüft
1036 und angepasst werden, vgl. 2.2.1 und 2.2.2.

1037 Und dennoch bestehen **Bedenken**, ob das konkrete Verfahren hinsichtlich der betroffenen
1038 Informationen ausreicht. Während zivilrechtlich der Grundsatz „in dubio pro reo“ nicht gilt, ver-
1039 hindern im Strafrecht etwaige Zweifel an der Täterschaft eine etwaige Verurteilung. Insoweit
1040 sollte das GGDG-E etwaige Schutzbehauptungen antizipieren, um in den anschließenden oder
1041 parallelen Strafverfahren eine Verurteilung zu ermöglichen.

- 1042 ■ § 2 Abs. 2 Nr. 1 GGDG-E sieht vor, dass die Personalien, soweit gespeichert, die IP-
1043 Adresse verbunden mit dem angegriffenen Inhalt und die IP-Adresse des letzten Login
1044 bereitzustellen sind, inklusive der Zeitstempel und der für die Zeitstempel gültigen Zeitzone.
- 1045 ■ § 2 Abs. 2 Nr. 2 GGDG-E sieht vor, dass die Personalien bereitzustellen sind, die der
1046 Nutzer*in der IP-Adresse zum genannten Zeitpunkt zugewiesen war.

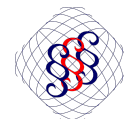
1047 Hierbei ist positiv hervorzuheben, dass in § 2 Abs. 2 Nr. 1 und Nr. 2 GGDG-E neben der rei-
1048 nen IP-Adresse auch die Port-Nummer erwähnt wird. Gerade im Falle von IPv4-Adressen ist
1049 diese notwendig, wenn sich mehrere Nutzerzugänge eine IP-Adresse³⁵ teilen. Dies ist ins-
1050 besondere im Falle von mobilen Zugängen der Fall, einer immer wichtigeren Zugangsform.

- 1051 ■ § 2 Abs. 2 Nr. 3 GGDG-E eine Kopie des angegriffenen Inhalts.

1052 Dennoch bleiben Möglichkeiten zumindest **theoretischer Schutzbehauptungen**, die nachträg-
1053 lich aufgrund des Zeitablaufs und voraussichtlich unwiderruflich gelöschter Informationen bei
1054 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.



1055 2.4.1 Nutzung des Anschlusses durch (unbekannte) Dritte oder 1056 Verwandte

1057 In diesen Fällen ist **trotz Kenntnis der IP-Adresse** nicht final geklärt, welche natürliche Person
1058 die Tathandlung begangen hat. Diese Zuweisung auf eine **konkrete Person** ist allerdings für
1059 eine strafrechtliche Verurteilung notwendig.

1060 Eine Widerlegung dieser Schutzbehauptung ist allenfalls möglich, soweit die **Endgeräte** der
1061 Verdächtigen **beschlagnahmt** und **forensisch ausgewertet** werden. Je nach in Rede stehender
1062 Tat könnte dies als unverhältnismäßig eingestuft werden.

1063 Einerseits könnte rechtlich die Schwelle der **Verhältnismäßigkeit** überschritten sein, anderer-
1064 seits könnten die Strafverfolgungsbehörden im Rahmen des **Opportunitätsprinzips** die ohne-
1065 hin knappen Ressourcen auf andere – schwerwiegendere – Straftaten verwenden wollen.

1066 Fällt die strafrechtliche Ermittlung – und eine damit einhergehende Möglichkeit der Beschlag-
1067 nahmung und / forensischen Auswertung – zeitlich auseinander zur zivilrechtlichen Anfrage, ist
1068 zudem davon auszugehen, dass etwaige Beweise auf den Endgeräten – mit mehr oder weniger
1069 Erfolg – in der **Zwischenzeit vernichtet** werden. Insofern bestehen erhebliche Bedenken, ob
1070 die bloße Kenntnis über den vermeintlichen Anschluss im Falle von **Mehrpersonenhaushalten**
1071 und / oder anderweitig von mehreren Personen genutzten Internetzugängen ausreicht.

1072 Zwar ist zu erwarten, dass ein aktives Nutzerkonto etwa in Sozialen Medien weitere Informatio-
1073 nen – etwa Bilder – der Täter*in beinhalten. Dies ist aber mit Nichten zwingend. Einerseits
1074 sind auch in Sozialen Netzwerken inzwischen viele Nutzer*innen sehr **bewusst** unter **Pseud-**
1075 **onym ohne Bild** aktiv. Zudem ist nicht ausgeschlossen, dass für die Ausübung digitaler Gewalt
1076 dedizierte „**Hetz-Accounts**“ angelegt wurden, und diese Accounts in Ansehung der Identifikati-
1077 onsrisiken möglichst auf die Identifikation ermöglichende Informationen verzichten.

1078 Spätestens wenn aber **Online-Plattformen** betroffenen sind, **die nicht Soziale Netzwerke**
1079 **sind**, ist die Ausgestaltung der im Nutzerkonto hinterlegten weiteren Informationen höchst
1080 variabel. Insoweit vorauszusetzen, dass im Falle der Schutzbehauptung aus den im Nutzer-
1081 konto (öffentlich) zugänglichen Informationen auf die Täter*in geschlossen werden kann,
1082 erscheint fahrlässig und naiv.

1083 An dieser Stelle sei auf den – wohl ungewollten – begrifflichen **Zirkelschluss des Gesetzes**
1084 hingewiesen. Durch die Verwendung des Begriffs Nutzerkonto in § 2 Abs. 2 Nr. 1 GGDG-E fin-
1085 det dieser aufgrund des Wortlauts von § 1 Abs. 7 GGDG-E nur auf Soziale Netzwerke Anwen-
1086 dung. Ein Einschränkung, die als **Redaktionsversehen** betrachtet wird, da ausweislich der
1087 Gesetzesbegründung die Klarstellungen zu Sozialen Netzwerken aufgrund der Regelungen zur
1088 Account-Sperre aufgenommen wurden, nicht jedoch um etwaige Einschränkungen der Aus-
1089 kunftspflichten zu begründen.



1090 Es wird daher empfohlen, neben der IP-Adresse auch **andere bei den Anbieter vorhandene**
1091 **Informationen zum Gegenstand der Auskunft** zu machen, soweit diese geeignet sind, die kon-
1092 kreten Nutzer*innen zu identifizieren.

1093 Zu diesen Informationen gehören möglicherweise etwaige

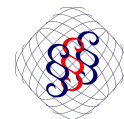
- 1094 ■ **Mac-Adressen** der genutzten Endgeräte,
- 1095 ■ **sonstige Informationen**, die etwa im Rahmen des Fingerprintings erstellt wurden, oder
- 1096 ■ etwaige **Geräte-Ids oder Session-Ids**, die dem Nutzerkonto und der Tathandlung zugeschrie-
1097 ben sind.

1098 Insbesondere die langfristige Zuweisung von **Geräte- und Session-Ids** sind inzwischen eine
1099 Gute Praxis im Rahmen der IT-Sicherheitsmaßnahmen der Online-Plattformen. Nutzer*innen
1100 können die „aktiv eingeloggt“ Geräte bzw. Login-Sessions im Nutzerkonto einsehen, teil-
1101 weise sogar mit einer weit zurückreichenden Historie.

1102 Diese weiteren Merkmale sind ein relevanter Baustein, um einer Schutzbehauptung es gäbe
1103 „weitere Nutzer*innen des Internetanschlusses“ entgegenzutreten.

1104 Auch diese Informationen sind keine Garantie, um diese Schutzbehauptung gänzlich erfolglos
1105 zu machen, insbesondere, wenn und soweit die Täter*innen etwaige nachgelagerte Ermitt-
1106 lungsmaßnahmen **antizipieren** und **Gegenmaßnahmen** bereits bei Begehung der Tat treffen
1107 bzw. wenn das zivilrechtliche Verfahren und etwaige Sicherungsmaßnahmen bei den
1108 Täter*innen zeitlich auseinanderfallen.

1109 In diesen Fällen tritt neben der **geringfügigen kriminellen Energie** einer möglicherweise
1110 begangenen **Spontan-Tat** eine koordinierte und **hohe kriminelle Energie**, mit vorsätzlichen
1111 **Planungsbewusstsein** und **nachträglicher Verdeckungsabsicht**. Dies lässt erwarten, dass
1112 Straftaten von erheblicher Schwere im Raum stehen, und es sich um kein (relatives) Antrags-
1113 delikt mehr handelt. In diesen Fällen erfolgt die Informationsabfrage hoffentlich ohnehin pri-
1114 mär durch die Strafverfolgungsbehörden, sodass jedenfalls die Risiken nachträglicher Ver-
1115 deckungshandlungen, wie etwa einer Beweisvernichtung, deutlich reduziert sind.



1116 2.4.2 Hack des Nutzerkontos

1117 Soweit die Schutzbehauptung eines „Hacks der Nutzerkontos“ vorgetragen wird, gelten
1118 zunächst die Ausführung in 2.4.1 entsprechend. Insbesondere die Kenntnis der Geräte- und
1119 Login-Session könnten hinreichende Anhaltspunkte bieten, diese Schutzbehauptung zu
1120 erschüttern.

1121 Ergänzend müssten sich im Falle eines Hacks weitere **Unregelmäßigkeiten** in den **Internetzu-**
1122 **gängen** finden, die für die Verwendung des Nutzerkontos genutzt wurden, soweit der Hack
1123 einen „Fernzugriff“ auf das Nutzerkonto zur Folge hatte.

1124 Sind keine **Unregelmäßigkeiten** im Rahmen der **IP-Adressen** noch der **Geräte- und Session-**
1125 **Ids** erkennbar, käme allenfalls ein Hack durch auf dem Endgerät installierte Malware in
1126 Betracht, die einen validen Login der vermeintlichen Täter*innen aufgreift, und somit die Tat-
1127 handlung remote über den validen Login der vermeintlichen Täter*innen und deren Endgeräte
1128 begangen wird. In diesen Fällen sollte aber eine **forensische Untersuchung** der in Verdacht
1129 stehenden Endgeräte eben solche **Malware** nachweisen können.

1130 Dies führt zu weiteren Überlegungen. Der **Auskunftsanspruch** ist derzeit **nicht geeignet**, eine
1131 **Plausibilisierung der Informationen** durchzuführen, oder Erkenntnislücken aus den nahezu
1132 zufällig gewählten Zeitpunkten der IP-Adressen zu schließen.

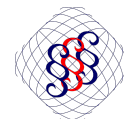
1133 Die Gesetzesbegründung stellt selbst fest, dass es vorstellbar ist, dass – gerade im Falle der
1134 Verwendung von mobilen Endgeräten – Täter*innen zum Zeitpunkt der Tathandlung und/oder
1135 des letzten Logins in einem **öffentlichen Netzwerk** eingeloggt waren. In diesem Fall würde eine
1136 Identifizierung ohne weitere Informationen, vgl. in 2.4.1, vermutlich sofort ins Leere laufen.

1137 Insoweit wird empfohlen, die Auskunftspflicht um **weitere Zeitpunkte zu erweitern**. Sowohl in
1138 die **Vergangenheit**, als auch in die **Zukunft**. Soweit der Gesetzgeber die konkreten Werte nicht
1139 festlegen möchte, kann dies auch in das Ermessen des mit der Entscheidung befassten
1140 Gerichts gestellt werden.

1141 Vorstellbar scheint:

1142 n-IP-Adressen unmittelbar vor und nach der in Rede stehenden **Tathandlung**; wobei ein maxi-
1143 malar Wert von n=5 sehr zielführend erscheint

1144 ■ IP-Adressen der n **letzten Zugriffe / Aktivitäten des Nutzerkontos**; wobei ein maximaler
1145 Wert von n=5 sehr zielführend erscheint; wobei in Abweichung zum aktuellen Wortlaut von
1146 § 2 Abs. 2 Nr. 1 lit. c) GGDG-E klargestellt werden sollte, dass es sich um eine unmittelbare
1147 (menschliche) Nutzung handeln muss; soweit Online-Plattformen Interaktions-API bereitstel-
1148 len, könnte die „letzte“ IP-Adresse ansonsten die IP-Adresse eines API-Proxies sein.



1149 2.4.3 Übertragungsfehler der IP-Adressen; fehlerhafte Zeitstempel

1150 Eine bereits aus den urheberrechtlichen Streitigkeiten bekannte Schutzbehauptung betrifft
1151 etwaige „**Übertragungsfehler**“.

1152 Diese Übertragungsfehler seien entweder eine Folge menschlichen Versagens – falsch kopiert,
1153 falsch abgeschrieben, in der Zeile verrutscht. Oder eine Folge technischer Fehler, wie etwa
1154 einem fehlerhaften Zeitstempel. Dieser fehlerhafte Zeitstempel hätte dazu geführt, dass auf-
1155 grund der dynamischen IP-Adresse der falsche Internetanschluss identifiziert wurde.

1156 Diese Schutzbehauptung lässt sich insoweit entkräften, wenn wenige, aber in Summe hocheffi-
1157 ziente Maßnahmen getroffen werden.

1158 2.4.3.1 (voll)-automatisierung der Abfragen

– 1159 Jedenfalls die Behauptung menschlichen Versagens aufgrund von Übertragungsfehlern kann
1160 durch eine weitreichende **Automatisierung** entkräftet werden.

1161 Fehler könnten bei einer Automatisierung am Anfang entstehen, weil etwa die falsche „Nut-
1162 zeraktivität“ als Referenzpunkt gesetzt wird. Dies würde aber aufgrund der bereitgestellten
1163 Informationen (Kopie) gem. § 2 Abs. 2 Nr. 3 GGDG-E erkennbar sein.

1164 Fehler könnten im Übrigen aufgrund eines grundsätzlichen Fehlers in der Automatisierungs-
1165 logik entstehen. Derartige behauptete Fehler können leicht durch eine Prüfung der implemen-
1166 tierten Logiken entweder verifiziert oder falsifiziert werden.

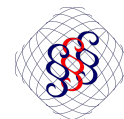
1167 2.4.3.2 falscher Zeitstempel bei Diensteanbieter

1168 Vorstellbar erscheint die Behauptung, dass der durch den Diensteanbieter bereitgestellte Zeit-
1169 stempel fehlerhaft sei.

1170 Der **Zeitstempel** folgt in der Regel der **Server-Zeit**. Diese kann, wie jede andere Uhr, falsch
1171 eingestellt sein. Dies wird heutzutage eigentlich durch regelmäßige **Synchronisation** mit Zeit-
1172 servern vermieden. Es ist aber nicht ausgeschlossen, dass derartige Synchronisationsvorgänge
1173 fehlerbehaftet sind, oder sich die Serverzeit zwischen den jeweiligen Synchronisationsvorgän-
1174 gen verstellt hat.

1175 Gerade in komplexen Systemstrukturen haben die Plattformbetreiber ein hohes **Eigeninter-**
1176 **esse**, dass die Server-Zeit auf allen (eigenen) Servern identisch ist und diese auch synchron
1177 mit weiteren (externen) Servern ist, da deren eigene Funktionalität in höchstem Maße von kor-
1178 rekten Zeitstempeln abhängig ist.

1179 Trotzdem ist nicht ausgeschlossen, dass einer derartige Schutzbehauptung vorgetragen
1180 wird. Möglicherweise verfängt dieser Vortrag, da die zur Auskunft verpflichtete Online-Plattform
1181 relativ klein ist, und kein besonderes Eigeninteresse an einer korrekten Server-Zeit hat.



1182 In diesen Fällen wäre es dennoch ziemlich einfach dieser Schutzbehauptung entgegen zutre-
1183 ten, nämlich indem neben dem Zeitstempel (und Zeitzone) zwei **weitere Informationen**
1184 bereitgestellt werden:

- 1185 ■ **implementierte Maßnahmen** zur Synchronisation der Server-Zeit, inklusive Bestätigung /
1186 relevanter Teilauszug aus den erfolgreichen **Synchronisations-Protokollen**
- 1187 ■ ein **aktueller Zeitstempel** zum Zeitpunkt der Informationsermittlung nebst einem **zeitgleich**
1188 von einem **offiziellen Zeitserver abgerufenen Zeitstempel** .

1189 Die erste Information lässt erkennen, ob grundsätzlich die Validität der Zeitstempel vorausge-
1190 setzt werden kann.

1191 Die zweite Informationen sichert diese Vermutung der ersten Information ergänzend ab. Sollte
1192 wider Erwarten eine Abweichung auftreten können (oder sollten keine Prozesse zur Sicherung
1193 der Validität des Zeitstempels implementiert sein), ließen die aktuellen Zeitstempel Rücksch-
1194 lüsse über das einschlägige Zeitfenster zu, um welches der Zeitstempel des Logeintrags „feh-
1195 lerhaft“ sein könnte. Diese Information einer **Eventualabweichung** könnte für eine **erweiterte**
1196 **Sicherung** bei den Internetzugangsanbietern genutzt werden.

1197 **2.4.3.3 falscher Zeitstempel bei Internetzugangsanbieter**

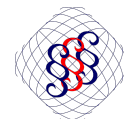
1198 Auch **Internetzugangsanbieter** können dem Vorwurf ausgesetzt sein, dass deren Zeitstempel
1199 fehlerhaft seien. Insoweit gelten zunächst die Ausführungen zu 2.4.3.2 entsprechend.

1200 Ergänzend können auch hier **vorsorgliche Sicherungsmechanismen** etabliert werden. So
1201 könnten die Internetzugangsanbieter stets verpflichtet werden, neben den Zuordnungen für
1202 den konkreten Zeitstempel alle weiteren Zuordnungen zu der IP-Adresse in einem Zeitraum n
1203 ebenfalls in den eigenen System zu sichern. Der konkrete Zeitraum n gälte es auf Basis der
1204 vorstellbaren Abweichungen zu ermitteln; eine Zeitspanne von mehr als 5min erscheint aber
1205 besonders rechtfertigungsbedürftig, bringt man in Ansatz, dass Telekommunikationsanbieter,
1206 von denen Internetzugangsanbieter eine Untergruppe sind, besondere Sorgfaltspflichten in die-
1207 sem Bereich treffen.

1208 Unabhängig der „**Regelabweichung**“ sind etwaige **Streubreiten** aufgrund der in 2.4.3.2
1209 erkannten möglicherweise fehlerhaften Zeitstempel ergänzend zu berücksichtigen.

1210 Es ist hervorzuheben, dass auch im Sinne der **grundrechtlichen** Überlegungen der **Fehliden-**
1211 **tifikation Sicherungsmechanismen** im Verfahren vorgesehen werden sollten.

- 1212 ■ Internetzugangsanbieter sollten zwar verpflichtet sein, die **weiteren Zuordnungen** zu
1213 **sichern**; die übermittelten **Personalien** sollten aber in der Regel nur **einen konkreten**, vom
1214 Gericht bei der Anfrage **identifizierten Zeitstempel betreffen**.



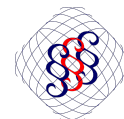
- 1215 ▪ Soweit das **Gericht** in den von den Diensteanbietern erhaltenen Informationen relevante
1216 **Unschärfen erkennt**, die eine Begrenzung auf einen konkreten Zeitstempel verunmöglicht,
1217 soll das Gericht den Umfang der erstmalig zu übermittelnden Daten **verhältnismäßig erwei-**
1218 **tern** können, soweit diese bereits Gegenstand der erweiterten Sicherung der Informationen
1219 durch die Internetzugangsanbieter sind;
- 1220 ▪ Es ist sicherzustellen, dass im Falle von bereits durch das Gericht **erkannte Unschärfen**, die
1221 **Plausibilitätsprüfung** der zutreffenden Identität **durch** das **Gericht** erfolgt, und etwaige Per-
1222 sonalien **unbeteiligter Dritter** zunächst nicht Gegenstand der Akte(nteile) werden, auf die
1223 die weiteren Verfahrensbeteiligten Zugriff haben.
- 1224 ▪ Das **Gericht** hat darauf **hinzuweisen**, wenn die Identifikation aufgrund der IP-Adresse nicht
1225 ein-eindeutig war, sondern aufgrund der **Korrelation mehrerer Personalien** und **Zeitstem-**
1226 **pel** abgeleitet bzw. plausibilisiert wurde. Für diesen Fall soll es den vermeintlichen
1227 **Täter*innen** ermöglicht werden, diese abgeleitete **Identifikation** unter Wahrung der Rechte
1228 unbeteiligter Dritter angemessen in Zweifel zu ziehen und zum **Gegenstand einer Überprü-**
1229 **fung** machen zu können.

1230 **2.4.3.4 (asynchrone) „Aktualisierungsverzögerungen“ der Zuweisungsdatenbank** 1231 **bei Internetzugangsanbietern bzw. der gespeicherten Logfiles der Diensteanbieter**

1232 Es ist eine Schutzbehauptung vorstellbar, in dem Täter*innen behaupten, dass die Zuweisung
1233 der Personalien deswegen fehlerhaft sei, weil die Zuweisungsdatenbank der Internetzugangs-
1234 anbieter einen minimalen zeitlichen Verzug aufweise, oder weil die Speicherung des Logein-
1235 trags bei den Diensteanbietern einen minimalen Verzug aufweise.

1236 Hierbei ist zu berücksichtigen, dass gerade im Bereich des mobilen Internets eine neue Zuwei-
1237 sung bereits durch Wechsel der Funkzelle erfolgen kann und dass Zeitstempel bis auf die Milli-
1238 sekunde exakt sind. Zumindest in der Theorie ist möglich, dass die Abweichung von nur einer
1239 Millisekunde zu einer Abweichung in den ausgelesenen Personalien führen könnte.

1240 Dieser **theoretischen Schutzbehauptung** könnte mit entsprechender Ergänzung der zu
1241 sichernden Informationen entgegen getreten werden. Insoweit wird auf 2.4.3.2 und 2.4.3.3
1242 verwiesen. Im **Zusammenspiel des Vorgesagten** wäre auch diese – sicherlich höchst theoretische –
1243 Schutzbehauptung in den meisten Fällen entkräftet.



1244 2.4.4 Fake-Account, Identitätsdiebstahl

1245 Der Ref-E erkennt an, dass es durchaus eine neue **Gefährdungslage** des **Identitätsmiss-**
1246 **brauchs** durch „**Fake-Accounts**“ gibt.

1247 2.4.4.1 Abfrage von Bestandsdaten, Verhältnis zur IP-Adressen

1248 Die Gesetzesbegründung lässt hierbei erkennen, dass der Gesetzgeber sich bei der Abfrage
1249 der Bestandsdaten bei Internetzugangsanbietern im Wesentlichen auf die **ladungsfähige**
1250 **Anschrift** fokussiert hat, aber wohl nicht die Risiken eines Identitätsdiebstahls berücksichtigt.³⁶

1251 So heißt es dort:

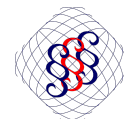
1252 *In einem zweiten Schritt sind regelmäßig die bei dem Anbieter von Internetzugangsdiensten hinterleg-*
1253 *ten Bestandsdaten erforderlich, wenn die bei dem Diensteanbieter hinterlegten Daten nicht zur Iden-*
1254 *tifizierung des Nutzers, dem die Rechtsverletzung vorgeworfen wird, ausreichen. Nutzerkonten bei*
1255 *Diensteanbietern werden häufig unter Pseudonymen ohne Angabe einer ladungsfähigen Anschrift*
1256 *erstellt; in der Regel genügt die Angabe eines (fiktiven) Namens und einer E-Mail-Adresse. Folglich*
1257 *reicht die Mitteilung der bei dem Diensteanbieter vorhandenen Daten zur Identifizierung in der Regel*
1258 *nicht aus. Um eine effektive Rechtsverfolgung und den grundrechtlich gebotenen Rechtsschutz zu*
1259 *ermöglichen, ist daher die Zuordnung der beim Diensteanbieter protokollierten dynamischen IP-*
1260 *Adresse durch den jeweiligen Internetzugangsanbieter unter Berücksichtigung des exakten Zeitstem-*
1261 *pels zwingend erforderlich, da eine Identifizierung auf anderem Wege regelmäßig ausscheidet.*

1262 Dabei ist der Gesetzgeber selbst **inkonsistent**. Einerseits schränkt er die Erforderlichkeit auf
1263 die Fälle ein, in denen die Personalien der Diensteanbieter nicht genügen. Insoweit scheint der
1264 Gesetzgeber hier eine gedankliche Bedingung für die Zulässigkeit der Abfrage bei Internet-
1265 diensteanbietern zu etablieren: „Nur wenn die Personalien nicht genügen, dann darf auch die
1266 IP-Adresse herangezogen werden.“ Zugleich erwähnt die Gesetzesbegründung, dass diese
1267 ergänzenden Informationen für eine grundrechtlich gebotene Rechtsverfolgung zwingend
1268 seien. Entweder ist etwas zwingend (in allen Fällen), oder eine im Einzelfall erforderliche Infor-
1269 mation je nach Faktenlage.

1270 Der **Richtervorbehalt** für jede einzelne Anordnung verlangt, dass das Gericht somit nach der
1271 Anordnung gegenüber den Diensteanbietern eine weitere Anordnung gegenüber den Inter-
1272 netzugangsanbietern erlassen muss. Aufgrund des „**Erforderlichkeitsgebots**“ in § 2
1273 Abs. 1 GGDG-E, das für diese zweite Anordnung erneut zu prüfen sei, ergibt sich aus der Geset-
1274 zesbegründung, dass Gerichte eine Anordnung nach § 2 Abs. 2 Nr. 2 GGDG-E dann ablehnen
1275 können oder gar sollten, wenn die Diensteanbieter bereits einen umfassenden (aber **nicht**
1276 **verifizierten) Datensatz** übermittelt haben.

1277 Die Erkenntnis eines **Identitätsmissbrauchs** würde zwar sodann eine nachgelagerte Abfrage
1278 ermöglichen. Zu diesem Zeitpunkt ist aber davon auszugehen, dass zur **Tathandlung keine**
1279 **notwendigen Informationen mehr vorliegen**. Hinsichtlich einer zeitlichen Beschleunigung des
1280 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.



1281 Im Übrigen sollte inhaltlich klargestellt werden, dass es in **allen Fällen zwingend** ist, auch die
1282 **Identitätsdaten mit Hilfe der IP-Adresse** zumindest **zu plausibilisieren**. Insoweit wird auch auf
1283 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
1284 ergänzende Informationen als erforderlich erweisen.

1285 Insoweit wird auch ausdrücklich empfohlen, die **Beweissicherung** nach § 3 GGDG-E **nicht ein-**
1286 **zuschränken**, sondern auf alle Informationen nach § 2 Abs. 2 GGDG-E zu erstrecken, inklusive
1287 der für die Ermittlung der Informationen möglicherweise anfallenden **Zwischeninformationen**.

1288 Soweit der Gesetzgeber lediglich die **Zustellung erleichtern** wollte, läge es im Ermessen und in
1289 den Möglichkeiten des Gesetzgebers, die förmliche Zustellung, soweit erforderlich, anzupassen
1290 und eine Zustellung etwa an die hinterlegte E-Mailadresse genügen zu lassen. Ein solcher
1291 Ansatz ist § 5 und § 6 GGDG-E auch zu entnehmen, wobei sich § 5 Abs. 3 GGDG-E nur auf
1292 formlose Dokumente bezieht. § 6 Abs. 2 GGDG-E kann aber als eine Modifikation der förmli-
1293 chen Zugangsregeln verstanden werden. Anstelle die Täter*innen unmittelbar über die Eröff-
1294 nung des Verfahrens zu informieren, etabliert § 6 Abs. 2 GGDG-E ein Auffangverfahren. Hierbei
1295 werden die Diensteanbieter zu Ersatzzustellbevollmächtigten und Ersatzempfangsberechtig-
1296 ten, ähnlich eines Rechtsbeistands. Über die Sinnhaftigkeit, Diensteanbieter derart intensiv in
1297 das Verfahren einzubinden, lässt sich streiten, und es wird auf 2.2.1 verwiesen.

1298 Insoweit sollte einerseits das Verfahren dahingehend präzisiert werden, sodass sich etwaige
1299 Kunstgriffe des derzeitigen Ref-E erübrigen.

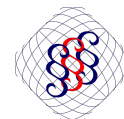
1300 **2.4.4.2 weitere sinnvolle Informationen und Anbieter**

1301 Es ist je nach Diensteanbieter vorstellbar, dass entweder die Nutzer*innen selbst diese Online-
1302 Plattform zur **Monetarisierung** nutzen, oder aber auf der Online-Plattform etwaige **kosten-**
1303 **pflichtige Premium-Dienste** in Anspruch nehmen, oder aber die Online-Plattform selbst **Zah-**
1304 **lungsdienste** bereitstellt.

1305 Insofern ist davon auszugehen, dass Nutzer*innen auch etwaige **Zahlungsinformationen** mit
1306 dem Nutzungskonto verknüpft haben oder Zahlungsinformationen (**Kreditkartendaten** oder
1307 **Kontodaten**) hinterlegt haben.

1308 Insoweit sollte überlegt werden, den **Informationsanspruch** auf derartige Informationen **auszu-**
1309 **dehnen** und auch entsprechend **weitere Anbieter** für eine Informationsbereitstellung zu ver-
1310 pflichten. Soweit „**Gutschein- oder Zahlungskarten**“ für etwaige Zahlungen an den Dienstean-
1311 bieter genutzt werden, sind auch diese teilweise rückverfolgbar; jedenfalls, soweit diese nicht
1312 lokal durch Bargeld erworben wurden.³⁷ Auch im Digitalen gilt: folgt man dem Geldfluss, findet
1313 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.



1314 2.4.5 Nachträgliche Änderungen der Inhalte und Personalien durch 1315 Täter*in

1316 § 2 Abs. 2 Nr. 3 GGDG-E schreibt vor, dass der angegriffene Inhalt durch die Diensteanbieter in
1317 **Kopie** an Betroffene zu übermitteln sei; insoweit besteht auch eine teilweise Redundanz zu
1318 den Regelungen des § 3 Abs. 1 GGDG-E.

1319 Die Gesetzesbegründung gibt zu verstehen, dass diese Norm insbesondere notwendig
1320 erscheint, um etwaigen Behauptungen der Täter*innen entgegen zu treten, dass die **Betroffene**
1321 **nen** die Inhalte nachträglich selbst **manipuliert** hätten.³⁸

1322 2.4.5.1 Redundanz und Wirkungslosigkeit der §§2 und 3 GGDG-E

1323 Zunächst ist festzuhalten, dass die **Redundanzen** der §§ 2 und 3 GGDG-E unnötig sind. Der
1324 durch § 2 GGDG-E intendierte Zweck einer Vermeidung der Manipulationsvorwürfe ist in dem
1325 Moment obsolet, in dem die Kopie der Inhalte wieder in den alleinigen Verfügungsbereich der
1326 Betroffenen übergeht.

1327 2.4.5.1.1 Verwaltung der gesicherten Informationen durch das Gericht

1328 Insoweit ist die Regelung des § 3 GGDG-E durchaus zu begrüßen, dass eine **Kopie der ange-**
1329 **griffenen Inhalte** zu erstellen ist. Die Regelung lässt zunächst offen, was mit der Kopie der
1330 Informationen erfolgen soll; ob diese etwa unmittelbar an das Gericht zu übermitteln sind, oder
1331 ob die Informationen bis auf Weiteres im Verfügungsbereich der Diensteanbieter verbleiben
1332 sollen, oder ggf. sogar beides erwartet wird.

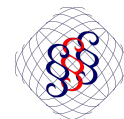
1333 § 3 Abs. 2 GGDG-E schafft insoweit Klarheit, da Diensteanbieter angeordnet werden, die Infor-
1334 mationen dem Gericht „**in Textform**“ zu übermitteln. Positiv ist, dass hierdurch die Informatio-
1335 nen ab diesem Zeitpunkt (auch) dem Gericht vorliegen und durch das Gericht verwaltet wer-
1336 den. Etwaige Manipulationen durch an dem Verfahren Beteiligte sind somit wohl grundsätzlich
1337 auszuschließen.

1338 2.4.5.1.2 Beweiswert der durch das Gericht verwalteten Informationen

1339 Insoweit ist aber die Gesetzesbegründung **inkonsistent**: Gegenstand des erhöhten **Beweiswer-**
1340 **tes** sollten und können eigentlich nur die bei Gericht eingegangenen und durch das Gericht
1341 verwalteten Informationen haben. So heißt es konkret:

1342 *Zwar werden Betroffene in aller Regel ihrem Antrag einen Screenshot beifügen, der die behauptete*
1343 *Rechtsverletzung beweisen soll. Allerdings kann es vorkommen, dass der rechtsverletzende Inhalt bis*
1344 *zur Entscheidung des Gerichts gelöscht wird. In einem solchen Fall ist der Beweisführer regelmäßig*
1345 *dem Vorwurf ausgesetzt, den Screenshot gefälscht oder manipuliert zu haben. Diesem Einwand kann*
1346 *mit der vom Diensteanbieter erstellten Kopie entgegengetreten werden, sodass ein Gericht dem*
1347 *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.



1348 Warum die durch die Diensteanbieter erstellte Kopie dem durch die Betroffenen erstellten
1349 Screenshot einen erhöhten Beweiswert ermöglichen soll, ist nicht nachvollziehbar. Zumal die
1350 Gesetzesbegründung offenlässt, was in den Fällen passiert, in denen ein Widerspruch zwi-
1351 schen Screenshot der Betroffenen und durch den Diensteanbieter gesicherten Informationen
1352 festgestellt wird.

1353 Im Falle eines Widerspruchs ist – nach jetziger Formulierung des Gesetzes – eigentlich davon
1354 auszugehen, dass den durch den **Diensteanbieter gesicherten** und an das Gericht **übermittel-**
1355 **ten** Informationen der **höhere Beweiswert** im Rahmen einer Beweismwürdigung zukommen
1356 würde.

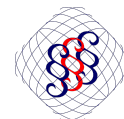
1357 Denn einerseits sind die bei der Sicherung beteiligten Parteien nicht Beteiligte des Verfahrens,
1358 somit sollten diese also – in der Regel – keine **Interessenkonflikte** haben, die eine eigenständ-
1359 ige Manipulation der Informationen erwarten ließe.³⁹ Im Anschluss werden die Informationen
1360 durch das Gericht verwaltet. Die **Rechtsstaatlichkeitsprinzipien** verlangen an dieser Stelle
1361 bereits, dass die Informationen nicht durch das Gericht manipuliert werden. Betroffene müss-
1362 ten also vermutlich erhebliche Umstände vortragen, die den durch das Gericht gesicherten
1363 Beweiswert erschüttern könnten; realistisch kann davon ausgegangen werden, dass Betrof-
1364 fene diese Hürde nicht überwinden können.

1365 Denn man muss diese Überlegung auch von der anderen Seite her anstellen: Wenn die Infor-
1366 mationen des Diensteanbieters und der Screenshot sich nicht widersprechen, muss auch die
1367 **Möglichkeit** für Täter*innen bestehen, sich **effektiv zu verteidigen**. Insoweit müssten auch
1368 die Täter*innen den Beweiswert der gesicherten Informationen anzweifeln können.

1369 Wenn also Betroffene den **Beweiswert** im Falle von Widersprüchen aus Sicht des Gesetz-
1370 gbers leicht **erschüttern** könnten, so könnten Täter*innen den Beweiswert vermutlich ebenso
1371 leicht im Falle konsistenter Informationen erschüttern.

1372 Das würde im Ergebnis aber bedeuten, dass die **Beweissicherung** derzeit an **mindestens** einer
1373 Stelle einen **erheblichen Konstruktionsfehler** aufweisen müsste, und die gesetzliche **Rege-**
1374 **lung** derzeit also den **intendierten Zweck nicht erreichen kann**. Einige Schwachstellen im
1375 Rahmen der Beweissicherung sollen im Folgenden dargestellt werden, deren Auflösung durch
1376 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.



1377 2.4.5.1.3 Für forensische Untersuchungen ungeeignetes Datenformat

1378 Das Gesetz schreibt vor, dass die Informationen an das Gericht „in **Textform**“ übermittelt wer-
1379 den sollen, § 3 Abs. 2 GGDG-E. Hierbei lässt weder das Gesetz, noch die Gesetzesbegründung
1380 erkennen, wie „Textform“ in diesem Kontext zu verstehen ist. Textform ist per definitionem in
1381 Abgrenzung zur Schriftform zu verstehen. D.h., es kommt nur darauf an, dass der Inhalt lesbar
1382 ist und auf einem dauerhaften Datenträger erfolgt, und zwar dergestalt, dass es möglich ist,
1383 eine auf dem Datenträger befindliche Erklärung so aufzubewahren oder zu speichern, dass
1384 diese während eines für ihren Zweck angemessenen Zeitraums zugänglich ist, und die Erklä-
1385 rung unverändert wiedergegeben werden kann.

1386 Insoweit wird auf etwaige qualifizierende Merkmale der Urheberschaft der Erklärung im Ver-
1387 gleich zur Schriftform verzichtet. Textform ist insoweit also keine weitere Ausgestaltung des
1388 Datenformats, oder eine Sicherstellung in der Gestalt, dass eine weitere Analyse der übermit-
1389 telten Informationen ermöglicht wird.

1390 Nach den obigen Ausführungen, wäre eine **Übermittlung der Informationen im Rohformat**,
1391 also als exportierte Zeilen der log-Dateien, als exportierte Datensätze der Datenbank, oder als
1392 eine – alle Quellen inkludierende – HTML-Datei, oder eine sonstige ausführbare Datei **vorstell-**
1393 **bar**. Hierbei ist nicht sichergestellt, dass die übermittelten **Dateiformate ohne proprietäre**
1394 Software ausgelesen werden können. **Ebenso** würde es aber auch **genügen**, wenn die Informa-
1395 tionen durch die Diensteanbieter in Form von **(virtuellen) Screenshots** an das Gericht übermit-
1396 telt würden.

1397 **Bloße (virtuelle) Screenshots** verhindern jegliche, künftige **forensische Untersuchung** der
1398 Informationen auf etwaige Manipulationen oder sonstige, ggf. verfahrensrelevante Zusammen-
1399 hänge. Die Übermittlung in Form **proprietärer Formate** würde es den Diensteanbietern ermög-
1400 lichen, den Anordnungen Folge zu leisten, ohne dass die Gerichte (oder Betroffenen) im
1401 Anschluss mit angemessenem Aufwand die Informationen verwenden könnten; es stünde
1402 sogar zu befürchten, dass die Diensteanbieter an dieser Stelle ein **profitables Geschäft** wittern
1403 dahingehend, dass für die Verwertung der bereitgestellten Informationen durch die Dienstean-
1404 bieter lizenzierte Dienstleistungen in Anspruch genommen werden müssten.

1405 Insoweit wird empfohlen, das GGDG-E nachzuschärfen, um die für die **rechtsstaatliche** und
1406 **effektive Verfahrensführung notwendigen Informationen** jedenfalls bei Gericht vorrätig zu
1407 halten.

1408 Zwar ist vorstellbar, dass dem Gericht zunächst nur durch die Diensteanbieter erstellte (virtu-
1409 elle) Screenshots bereitgestellt werden, und weitere Informationen nur dann durch das Gericht
1410 abgerufen werden können, wenn dies im Verlauf des Verfahrens erforderlich wird. Dieser
1411 Ansatz birgt aber das **Risiko**, dass die **Informationen bei einer privaten Stelle vorgehalten**



1412 werden, und somit diese private Stelle einerseits für diese Sicherung **kompensatorische Maß-**
1413 **nahmen** erwartet oder aber, die private Stelle – absichtlich oder unabsichtlich – die **Informati-**
1414 **onen verliert** oder **verändert**.

1415 2.4.5.1.4 Unzureichender Sicherungszeitraum

1416 § 3 Abs. 1 GGDG-E stellt sicher, dass die Informationen bei Anbietern bis zum **Abschluss des**
1417 **Verfahrens** vorgehalten werden müssen. Das GGDG-E enthält insoweit keine weiteren Klarstel-
1418 lungen, auf welches Verfahren sich die Regelung bezieht.

1419 Vorstellbar ist:

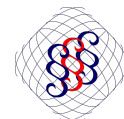
- 1420 ■ ausschließlich das **zivilrechtliche Auskunftsverfahren** gem. GGDG-E
- 1421 ■ einschließlich etwaiger **zivilrechtlicher Verfahren im Anschluss**, wobei es zu klären gälte,
1422 was passiert, wenn ein solches zivilrechtliches Verfahren nicht „sofort“, „in definierter ange-
1423 messener Zeit“, „während der Verjährungsfristen“ durch die Betroffenen angestrengt wird
- 1424 ■ einschließlich etwaiger **strafrechtlicher Verfahren im Anschluss**, wobei sich ähnliche Frage-
1425 stellungen wie für etwaige zivilrechtliche Verfahren stellen.

1426 § 3 Abs. 5 GGDG-E lässt hier eine eindeutige Wertung erkennen, nämlich dahingehend, dass
1427 ausschließlich das **zivilrechtliche Auskunftsverfahren** gem. GGDG-E gemeint sein soll. Hierbei
1428 kann § 3 Abs. 5 S. 2 GGDG-E sogar so verstanden werden, dass die Anbieter die eigene Kopie
1429 mit Erfüllung der Auskunft sofort irreversibel zu löschen haben, und zwar ungeachtet, ob das
1430 Verfahren rechtskräftig abgeschlossen wurde. Letzteres ist insoweit nachvollziehbar, da gem.
1431 § 5 Abs. 4 GGDG-E Entscheidungen erst mit Rechtskraft wirksam werden, was aus anderen
1432 Gründen möglicherweise und unnötig das Verfahrensziel gefährdet, vgl. 2.2.2.

1433 Aber selbst, wenn man diese **Rechtskraftregelung** für **erforderlich** hält, ist davon auszugehen,
1434 dass die Beteiligten erst zu diesem Zeitpunkt **erstmalig** die von den Anbietern bereitgestellten
1435 Informationen **erhalten** und einsehen können. Sollten die Beteiligten, hier insbesondere die
1436 Betroffenen, **Zweifel** an den übermittelten Informationen anzeigen, könnten diese aufgrund
1437 der unmittelbaren **irreversiblen Löschung nicht mehr** im Rahmen des Verfahrens **ausgeräumt**
1438 **werden**.

1439 Insoweit sind dringend **Klarstellungen** angeraten, die sowohl

- 1440 ■ eine vollständige **Überführung** der Informationen in einem **Format** an das Gericht sicher-
1441 stellt, die auch anschließende (**forensische**) **Untersuchungen** der Informationen
1442 **ermöglichen**



1443 ■ insoweit diese Informationen, die nach § 3 GGDG-E nicht mehr lediglich Informationen dar-
1444 stellen, sondern wohl **gerichtlich erhobene Beweise**, diese auch in **Folgeverfahren** im
1445 jeweils gebotenen Umfang **zur Verfügung** stehen, vgl. auch **Klarstellungsbedarf für straf-**
1446 **rechtliche Verfahren** unter 2.3.3.

1447 2.4.5.1.5 Unzureichender Sicherungsumfang

1448 Die von der Sicherung umfassten Informationen sind **inhaltlich** gegenüber dem Informations-
1449 anspruch **beschränkt**, jedenfalls lässt die derzeitige Formulierung Spielraum dahingehend,
1450 dass wichtige (**Zwischen-)**Informationen nicht von einer **Sicherungsanordnung** umfasst
1451 wären.

1452 Beispielhaft ist hier insbesondere auf § 3 Abs. 3 GGDG-E verwiesen. Hiernach sind die Informa-
1453 tion aus § 2 Abs. 2 Nr. 1 lit. b) und c) einem **Anschlussinhaber** zuzuordnen, und sodann die
1454 anhand der Zuordnung nach § 2 Abs. 2 Nr. 2 GGDG-E **erlangten Daten** zu speichern.

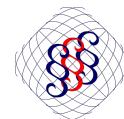
1455 Insofern beschränkt sich die **Speicheranordnung** dem reinen Wortlaut lediglich auf die **Per-**
1456 **sonalien**. Das ergibt sich auch aus der Gesetzesbegründung. Etwaige **Zwischeninformationen**
1457 wären allenfalls auf Basis einer noch nicht verabschiedeten, getrennten Aktualisierung des
1458 TKG möglich. Wobei auch an dieser Stelle die Gesetzesbegründung offenlässt, ob lediglich die
1459 Zwischenspeicherung der Bestandsdaten, oder die Zwischenspeicherung aller zur Ermittlung
1460 erforderlichen Umstände gemeint ist. So heißt es in der Gesetzesbegründung:

1461 *§ 174 Absatz 1 Satz 3 in Verbindung mit Absatz 5 Nummer 9 TKG-E, der die in § 2 Absatz 1 Satz 1 gere-*
1462 *gelte Befugnis zur Datenverarbeitung ergänzt, berechtigt den Internetzugangsdienst, hierbei – neben*
1463 *sämtlichen unternehmensinternen Datenquellen – auch die nach § 177 Absatz 1 TKG-E vorsorglich*
1464 *gespeicherten Daten zu verwenden und das Ergebnis der Zuordnung in einem Zwischenschritt der*
1465 *Bestandsdatenauskunft betriebsintern zu speichern.*

1466 An dieser Stelle sollte sichergestellt werden, dass die **Verfahren des GGDG-E** auch ohne
1467 Annahme etwaiger **sonstiger Gesetzesvorhaben** effektiv und effizient funktionieren.

1468 Der vom Gesetzgeber angesprochene, weitere Gesetzesentwurf betrifft die mögliche Wieder-
1469 einföhrung einer allgemeinen **Vorratsdatenspeicherung**. Der Erfolg des Gesetzesvorhabens
1470 und eine verfassungsrechtliche Bestandskraft kann derzeit jedenfalls als höchst umstritten
1471 angesehen werden. Das GGDG-E sollte insoweit dessen Effektivität nicht von diesem weiteren
1472 Gesetzesvorhaben abhängig machen.

1473 Die für das GGDG-E **erforderliche Datenverarbeitung** betrifft gerade **nicht** eine etwaige **Vor-**
1474 **ratsdatenspeicherung**. Vielmehr sind aufgrund eines konkreten Tatvorwurfs angefallene Infor-
1475 mationen zu sichern; etwaige darüber hinausgehende Informationen (vgl. die weiteren Ausführ-
1476 ungen in diesem Abschnitt 2.4) wären jedenfalls **deutlich geringeren verfassungsrechtlichen**
1477 **Bedenken** ausgesetzt, da ein wesentlich **stärkerer Bezug** zu einer **rechtswidrigen Handlung**
1478 bestünde. Es wird insoweit dringend empfohlen, das GGDG-E an dieser Stelle um **eigene**
1479 **Rechtfertigungsgrundlagen** zu **ergänzen**.



1480 Hierbei sollte auch sichergestellt werden, dass **nicht nur** das **Ergebnis** der Zuordnung Gegen-
1481 stand der Speicher- und Übermittlungsanordnung ist, **sondern auch** die bei der Zuordnung
1482 **angefallenen** bzw. **genutzten Zwischeninformationen**. Diese Zwischeninformationen sind
1483 möglicherweise erforderlich, um im Anschluss im Sinne eines rechtsstaatlichen Verfahrens,
1484 Bedenken bezüglich etwaiger Zuordnungsfehler auszuräumen.

1485 **2.4.5.2 Unzureichender Informationsanspruch**

1486 Im Übrigen erscheint auch der **Informationsumfang dem Grunde** nach bereits nicht ausrei-
1487 chend im Falle nachträglicher Änderung der Informationen.

1488 Der Informationsanspruch gem. § 2 Abs. 2 GGDG-E, und somit eine darauf basierende Siche-
1489 rungsanordnung gem. § 3 GGDG-E, bezieht sich lediglich auf die Informationen, wie diese **zum**
1490 **Zeitpunkt des Eingangs der Anordnung** als „**live-Zustand**“ bei den Anbietern vorhanden ist.

1491 Hierdurch bestehen sowohl für die Personalien als auch für die rechtsverletzenden Inhalte
1492 Durchsetzungsrisiken.

1493 **2.4.5.2.1 nachträglich geänderte oder gelöschte Personalien**

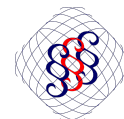
1494 Dieses Phänomen betrifft vermutlich stärker Diensteanbieter, und weniger Internetzugangs-
1495 anbieter, obgleich es theoretisch in beiden Fällen möglich ist.

1496 Soweit Täter*innen zum Zeitpunkt der Tat kein vollständig anonymes Nutzerkonto unterhalten
1497 haben, könnten die Reaktionen auf die rechtswidrigen Inhalte Bedenken seitens der
1498 Täter*innen über die Rechtmäßigkeit auslösen, die im Ergebnis in der Sorge münden, Gegen-
1499 stand von zivil- oder strafrechtlichen Verfahren zu werden.

1500 Es ist somit damit zu rechnen, dass Täter*innen in diesem Moment anfangen, etwaige sie
1501 **identifizierende Informationen** aus den vergangenen **Nutzeraktivitäten** sowie aus dem im
1502 **Nutzerkonto** unmittelbar hinterlegten Daten **zu ändern**, entweder indem diese ersatzlos **ent-**
1503 **fernt** werden, soweit möglich, oder durch **anonymisierte (Fake)-Informationen ersetzt** werden.

1504 Blicke der Informationsanspruch auf die zum Zeitpunkt der Anfrage vorgehaltenen Informatio-
1505 nen beschränkt, entstünde hierdurch eine die Durchsetzung massiv gefährdende
1506 Erkenntnislücke.

1507 Deshalb sollte **klargestellt** werden, dass die Anbieter **auch verpflichtet** sind, auch **historische**
1508 **Informationen** jedenfalls zu **sichern** und an das Gericht zu **übermitteln**. Betroffenen sind –
1509 soweit erforderlich – ebenfalls diese historischen Informationen zur Verfügung zu stellen.



1510 2.4.5.2 nachträglich geänderte oder gelöschte Inhalte

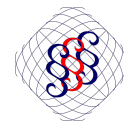
1511 Aus den gleichen Überlegungen wie zuvor, ist damit zu rechnen, dass Täter*innen **rechtswid-**
1512 **rige Inhalte nachträglich editieren, löschen, deren (öffentliche) Zugänglichkeit einschrän-**
1513 **ken, oder in sonstiger Art und Weise im Vergleich zur ursprünglichen Tathandlung**
1514 **verändern.**

1515 Derzeit ist lediglich eine **Kopie der angegriffenen Inhalte** zu übermitteln. Hierbei verbleibt der
1516 Ref-E unklar, was eine hinreichende „Kopie“ darstellt. Zielführend scheint es allerdings nur,
1517 wenn hiervon auch **alle – potentiell tatbestandlich relevanten – Nebeninformationen**
1518 umfasst sind, d.h., der konkrete **Inhalt**, der **Zeitstempel** der Veröffentlichung, die bei der Veröf-
1519 fentlichung ausgewählte **Reichweite**, insbesondere soweit die Reichweite eingeschränkt
1520 wurde, zum Zeitpunkt der Veröffentlichung **ermöglichte Interaktionen**, insbesondere soweit
1521 diese eingeschränkt wurden, etc.

1522 Neben diesen „**Nebeninformationen**“, ist auch eine **Historie** zu all den Informationen mögli-
1523 cherweise verfahrensrelevant. Denn soweit die rechtswidrigen Inhalte etwa im Nachgang ent-
1524 fernt würden, so würde eine Kopie des „**live-Inhalts**“ zum Zeitpunkt der Informationsbereitstel-
1525 lung den rechtswidrigen Inhalt nicht mehr beinhalten. Dies führt sodann zu **Widersprüchen** in
1526 den von den Betroffenen vorgelegten Tatsachen und den durch die Diensteanbieter bereitge-
1527 stellten Tatsachen, mit möglicherweise **negativen Folgen im Rahmen der Beweiswürdigung**,
1528 vgl. 2.4.5.1.2. Dabei läge in diesem Fall **keine Manipulation durch die Betroffenen** vor, son-
1529 dern eine Manipulation durch Täter*innen. Die **gesetzliche Regelung** würde aber möglicher-
1530 weise eine **Vermutung der Manipulation durch Betroffene statuieren** und somit das Gegen-
1531 teil des intendierten Gesetzeszwecks zur Folge haben.

1532 Neben der **Historie der eigentlichen Inhalte** ist auch eine **Historie zu den Nebeninformatio-**
1533 **nen** möglicherweise verfahrensrelevant. Soweit etwa tatbestandlich eine „Veröffentlichung“
1534 voraussetzt ist, und ein Inhalt ursprünglich tatsächlich „jeder Nutzer*in“ der Online-Plattform
1535 zugänglich gemacht wurde, hätte zum Zeitpunkt der Tatbegehung eine Veröffentlichung vorge-
1536 legen. Wäre die Reichweite nachträglich durch Täter*innen eingeschränkt worden, zwar auf
1537 eine handvoll enger Freunde, stünde das Tatbestandsmerkmal „Veröffentlichung“ in Zweifel.
1538 Insoweit wäre auch hier eine Information lediglich auf Basis des „live-Zustands“ geeignet, die
1539 Durchsetzung zu verunmöglichen.

1540 Ergänzend ist klarzustellen, dass die Information durch Diensteanbieter **auch etwaige als**
1541 **gelöscht oder gesperrt markierte Inhalte** betrifft. Vereinfacht kann formuliert werden: Diens-
1542 teanbieter sollten verpflichtet sein, alle zu den Inhalten vorhandenen Informationen bereitzustel-
1543 len bzw. jedenfalls zu sichern, soweit diese noch bei den Diensteanbietern vorhanden sind und
1544 soweit diese Informationen nicht ansonsten irrelevante Daten zu weiteren Nutzerkonten und/
1545 oder deren Interaktionen mit dem Inhalt betrifft.



1546 2.4.6 Mangelnde Informationen als Durchsetzungsdefizit sind mögli- 1547 ches Defizit der Rechtsstaatlichkeit

1548 Einerseits sind die fehlenden Informationen, wie in diesem Abschnitt 2.4 erläutert, ein Risiko
1549 für die Durchsetzbarkeit. Informationen und Zustände, die nicht zu Beginn des Verfahrens und
1550 möglichst umfassend erhoben und gesichert werden, können im weiteren Verlauf des Verfah-
1551 rens möglicherweise nicht mehr nachträglich festgestellt werden.

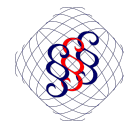
1552 Diese Lücke kann einerseits als **Durchsetzungsdefizit** betrachtet werden, da dies Täter*innen
1553 ermöglichen könnte, hinreichende Zweifel zu etablieren.

1554 Andererseits kann man dies auch als ein **potentielles Defizit der Rechtsstaatlichkeit** verste-
1555 hen. Einerseits können die vorgenannten Aspekte als bloße Schutzbehauptungen abgetan wer-
1556 den. Andererseits können – in den zuvor benannten Situationen oder in ähnlich gelagerten
1557 Sachverhalten – sich durchaus Fehler im Verfahren befunden haben.

1558 Auf diese diese Fehler hinzuweisen und diese ggf. auch nachzuweisen zu können, ist Teil des
1559 **rechtsstaatlich und grundrechtlich geschützten Rechts auf Verteidigung**. Diese Verteidigung
1560 kann sich möglicherweise aber nur darauf beschränken, Umstände in Zweifel zu ziehen oder
1561 mit Unwissen zu bestreiten. Während im Strafrecht der Grundsatz des in dubio pro reo gilt, ist
1562 dieser in der Intensität im Zivilrecht nicht einschlägig.

1563 Im **Zivilrecht** gilt grundsätzlich, dass diejenige Partei, die sich auf einen Umstand (positiv)
1564 berufen möchte, diesen Umstand auch **beweisen** muss. Das Zivilrecht kennt hiervon auch
1565 Abweichungen, etwa die die **Substantiierungspflicht** und die sekundäre **Darlegungslast**. Es ist
1566 daher nicht ausgeschlossen, dass im Ergebnis die Vermutungswirkungen aus den gem.
1567 § 2 Abs. 2 GGDG-E erhobenen Informationen gegen die Täter*innen wirken, und eine hinrei-
1568 chende Verteidigung ins Leere läuft.

1569 Je nachhaltiger und verlässlicher die Darlegung der klagenden Partei ist, umso stichhaltiger
1570 muss dieser Vortrag bestritten werden. Ein bloßes Bestreiten mit **Nicht-Wissen** oder Bestreiten
1571 „**ins Blaue**“ ist unzulässig. Ein Bestreiten mit Nicht-Wissen ist jedoch dann möglich, wenn die
1572 Partei selbst keine Möglichkeiten der weiteren Substantiierung hat. Dies kann man in den hier
1573 zu erwartenden Fällen wohl annehmen. Die Täter*innen haben keine Möglichkeiten, selbst die
1574 in den Systemen der Anbieter hinterlegten Informationen zu erheben. Die **Pflicht zur Mitwir-**
1575 **kung der Anbieter** mag zwar gegeben sein – wobei auch das streitig gestellt werden kann –,
1576 der Zeitablauf wird aber in der Regel dafür Sorgen, dass Anbieter einen **Großteil der relevan-**
1577 **ten Informationen gelöscht** haben werden. Insofern würde zwar ein **unsubstantiiertes**
1578 **Bestreiten** genügen, und die klagende Partei müsste weiteren **substantiierten Vortrag** leisten.
1579 Jedoch spricht für die klagende Partei, dass diess den gleichen **Unmöglichkeiten** gegenüber-
1580 steht, sich aber auf gerichtlich erhobene und gesicherte Informationen berufen kann.



1581 2.5 Beispielhafte Ausführungen zu § 202e StGB-E

1582 § 202e StGB-E wie im Ref-E vorgesehen, enthält nicht **nachvollziehbare Tatbestandsein-**
1583 **schränkungen**, die dem Ziel der Norm höchstwahrscheinlich zuwiderlaufen. Insoweit lässt sich
1584 auch nicht erkennen, wie die vorgeschlagene Regelung dem ganzheitlichen Ansatz zuträglich
1585 sei. Im Gegenteil, die Norm verliert sich in Einschränkungen, um einen ganzheitlichen Effekt zu
1586 vermeiden.

1587 Der Ref-E stellt fest, dass die Auswirkungen „digitaler Gewalt“ sowohl auf psychischer als auch
1588 physischer Ebene signifikant sein können.⁴⁰ Das Bundesverfassungsgericht hat in seinem
1589 „Volkszählungsurteil“⁴¹ das Grundrecht auf „Informationelle Selbstbestimmung“ etabliert, wel-
1590 ches feststellt:

1591 *Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in*
1592 *bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommu-*
1593 *nikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich*
1594 *gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.⁴²*

1595 Das BVerfG leitet hieraus ab:

1596 *Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft*
1597 *gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltens-*
1598 *weisen aufzufallen.⁴³*

1599 Dies mündet in der durch das BVerfG abstrakt-generellen Risikobetrachtung:

1600 *Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern*
1601 *auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Hand-*
1602 *lungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemein-*
1603 *wesens ist.⁴⁴*

1604 Mithin ist somit schon 1983 festgestellt worden, dass sich bereits aus einer **bloßen Unsicher-**
1605 **heit**, ob eine Überwachung stattfindet oder nicht, **erhebliche Einschränkungen** für jedes Indivi-
1606 duum ergeben können. Der **psychologische Effekt** der rein **potentiellen Nachteile und Risi-**
1607 **ken**, schlägt über in **reale, physische Nachteile**. Dies betrifft sowohl die Selbstbeschränkung
1608 eigenen Handelns, als auch möglicherweise die Materialisierung körperlicher, physischer Sym-
1609 ptome aufgrund der psychologischen Belastung.

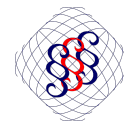
40 Abschnitt A I, S. 19, 20, Abschnitt A I 1, S. 21.

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.



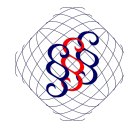
1610 2.5.1 Zweifel am Bestimmtheitsgebot; Aufhebung des eigenen Schutz- 1611 ziels durch zu weitreichende Tatbestandseinschränkung

1612 Begrifflich umfasst bereits der Begriff „**Überwachung**“ eine **Signifikanz**, die über eine verein-
1613 zelte Verarbeitung von Informationen hinausgeht. Eine Überwachung setzt voraus, dass die
1614 Informationen **qualitativ** hinreichend erhoben werden, um Rückschlüsse ziehen zu können.
1615 Das umfasst sowohl die **zeitliche Perspektive** (Erhebungsfrequenz) und die **qualitative Per-**
1616 **spektive** (welche Informationen sind betroffen). Die Aufnahme der dem Begriff „Überwachung“
1617 immanenten Attribute „wiederholt oder ständig“ in den Gesetzestext erschiene nur dann nach-
1618 vollziehbar, soweit der Gesetzgeber diese beiden Dimensionen im Rahmen von Regelbeispielen
1619 näher ausgestaltet hätte. Ohne die Aufnahme von Regelbeispielen wird ein ohnehin unbestimmter
1620 Rechtsbegriff „Überwachung“ durch zwei weitere unbestimmte Rechtsbegriffe „wiederholt“ und
1621 „ständig“ ergänzt. Dies lässt zumindest Zweifel aufkommen, ob und inwieweit dies letztlich dem
1622 Bestimmtheitsgebot strafrechtlicher Normen genügt.

1623 Die sodann ergänzende Beschränkung auf Fälle, in denen ein **schwerer Schaden wahrschein-**
1624 **lich** ist, läuft dem Zweck erst recht zu wider. Wie das BVerfG bereits feststellt, genügt bereits
1625 eine bloße Ungewissheit, um nachteilige Effekte im Verhalten der betroffenen Person zu
1626 begründen. Das Gesetz etabliert hier erneut **unbestimmte Rechtsbegriffe**, die letztlich die Ein-
1627 haltung des **Bestimmtheitsgebots zweifelhaft** erscheinen lassen. Weder ist geregelt, auf wel-
1628 cher Basis eine „Wahrscheinlichkeit“ zu ermitteln sei, noch ist definiert, was ein „schwerer
1629 Schaden“ im Sinne der Norm sei.

1630 Im Ergebnis lässt sich somit festhalten:

- 1631 ■ § 202e StGB-E begründet möglicherweise **keinen ergänzenden Schutz**, da dessen Anwend-
1632 barkeit an den verfassungsrechtlichen Hürden des **Bestimmtheitsgebots** scheitern
1633 könnten.
- 1634 ■ Selbst wenn § 202e StGB-E die verfassungsrechtlichen Hürden überwände, sind die **ein-**
1635 **fachgesetzlichen Einschränkung** des Tatbestands derart **weitreichend**, dass eine **straf-**
1636 **rechtliche Verfolgung** allenfalls in **Ausnahmefällen** in Betracht kommt. Dies steht im **Wider-**
1637 **spruch** zum im Ref-E festgestellten **Handlungsdrucks** aufgrund wachsender Fallzahlen.
- 1638 ■ Soweit eine strafrechtliche Verfolgung als **ultima ratio** auf Ausnahmefälle beschränkt wurde,
1639 so verbliebe dennoch eine **Schutzlücke**, da den Betroffenen auch zivilrechtlich vor der Her-
1640 ausforderung stünden, dass diese nicht ohne Weiteres herausfinden können, durch wen die
1641 unbefugte Überwachung stattfindet.
- 1642 ■ Das GGDG-E umfasst aber weder § 202e StGB-E im Regelkatalog, § 1 Abs. 1 Nr. 2 GGDG-
1643 E, noch adressiert es die Anbieter etwaiger Überwachungs-Hard- und Software.



1644 2.5.2 Modifizierter Vorschlag

1645 Vor diesem Hintergrund wird **konzeptionell eine modifizierte Formulierung** vorgeschlagen.
1646 Der Ref-E anerkennt, dass eine unbefugte Überwachung des Aufenthaltsorts oder Tätigkeiten
1647 einer Person gesellschaftlich zu missbilligen ist. Zugleich anerkennt der Ref-E, dass es einen
1648 relevanten Anstieg des Erwerbs und der unbefugten Verwendung von Produkten (Hard- und
1649 Software) gibt, die eine solche Überwachung ermöglichen.⁴⁵ Hieraus ergäbe sich logisch, dass
1650 es einen erheblichen gesetzgeberischen Druck gibt, dieser Dynamik entgegen zu treten.
1651 Sowohl im Sinne des Individualrechtsschutzes als auch im Sinne der für eine demokratische
1652 Gesellschaft immanente individuelle Freiheit als Voraussetzung einer funktionierenden demokrati-
1653 schen Grundordnung.

1654 Insoweit sollte zunächst auf eine **unnötige Einschränkung** des Tatbestandsmerkmals „Über-
1655 wachung“ **verzichtet** werden (vgl. neuer Abs. (1)). Wie zuvor dargelegt, ist es dem Begriff „Über-
1656 wachung“ bereits immanent, dass es sich um einen sich wiederholenden Vorgang handelt.
1657 „Ständig“ ist aber nur die maximal größte Frequenz einer Wiederholung.

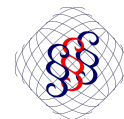
1658 Soweit die Gesetzesbegründung ausführt, dass diese Einschränkung deshalb notwendig sei,
1659 damit die Verarbeitung von Informationen aus bzw. das Nachschlagen von Social Media Profi-
1660 len oder anderweitig berechtigterweise zugänglichen Quellen ausgeschlossen wird, erscheint
1661 dies nicht überzeugend. Der Umstand der Überwachung und der sich daraus ergebende psy-
1662 chische Druck auf die Betroffenen hat nur bedingt eine Konnexität mit dem berechtigten
1663 Zugang zu den für die Überwachung erforderlichen Informationen. Insoweit kann der **unbe-
1664 rechtigte Zugriff** auf Informationen als **Voraussetzung des Tatbestandsmerkmals „unbefugt“**
1665 definiert werden (vgl. neuer Abs. (2)).

1666 Wenn überhaupt erscheint der Umkehrschluss zudem naheliegender: wurden für die Über-
1667 wachung Informationen genutzt, die lediglich unberechtigterweise zugänglich sind, bedürfte es
1668 keiner weiteren Wiederholung oder anderer Nachweise der tatsächlichen Überwachung. Um
1669 jedoch eine uferlose Strafbarkeit durch lediglich einmaliges, unberechtigtes Abrufen von Infor-
1670 mationen zu vermeiden, erscheint hier ein derartiger Automatismus nicht zielführend. Aller-
1671 dings, wenn für die **Informationsbeschaffung gezielt Soft- oder Hardware** installiert wurde⁴⁶,
1672 erscheint es vertretbar, **von der Installationshandlung auf den Überwachungszweck zu
1673 schließen** (vgl. neuer Abs. (4)).

1674 Doch auch die Verarbeitung von **Informationen, auf die berechtigterweise zugegriffen wer-
1675 den kann**, ist geeignet eine unbefugte Überwachung zu begründen, aus der sich erhebliche
1676 Nachteile für die Betroffenen in deren Lebensführung ergeben. Insoweit sollte auch diese
1677 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.



1678 Betroffenen **erhebliche Nachteile** zu befürchten sind. Die Nachteile können die freie, allge-
1679 meine **Lebensführung** betreffen, da sich Betroffene aufgrund des **Überwachungsdrucks** ein-
1680 schränken, oder weil zu befürchten steht, dass die Überwachung tatsächlich in physische Über-
1681 griffe münden könnte (vgl. neuer Abs. (3)). Soweit einer berechtigten **Aufforderung zur Unter-**
1682 **lassung** nicht Folge geleistet wird, erscheint es vertretbar, die erhebliche Beeinträchtigung zu
1683 vermuten. Die Ergänzung einer „berechtigten Aufforderung“ erscheint notwendig, um einen
1684 Strafbarkeitsreflex für ansonsten durch die Rechtsordnung gebilligtes Verhalten zu vermeiden.

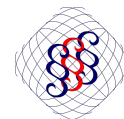
1685 **§ 202e StGB-E (modifiziert)**

1686 *(1) Wer den Aufenthaltsort oder die Tätigkeit einer anderen Person mittels Informations- oder Kom-*
1687 *munikationstechnik unbefugt überwacht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Gelds-*
1688 *trafe bestraft.*

1689 *(2) Eine mangelnde Befugnis setzt neben dem mangelnden Einverständnis durch die andere Person*
1690 *oder mangelnder Befugnisnorm, die Verarbeitung von ansonsten nicht berechtigterweise zugängli-*
1691 *cher Informationen voraus.*

1692 *(3) Die Verarbeitung von ansonsten berechtigterweise zugänglicher Informationen begründet in*
1693 *Abweichung von Abs. 2 eine Strafbarkeit, wenn eine ansonsten unbefugte Überwachung stattfindet*
1694 *und die andere Person hierdurch in ihrer allgemeinen Lebensführung wesentlich beeinträchtigt wird*
1695 *oder die Handlung wahrscheinlich dazu führt, dass dieser Person ein Schaden zugefügt wird. Eine*
1696 *wesentliche Beeinträchtigung ist jedenfalls dann gegeben, wenn die Überwachung nach Satz 1 trotz*
1697 *berechtigter Aufforderung zur Unterlassung fortgesetzt wird.*

1698 *(4) Ungeachtet der tatsächlichen Verarbeitung hinsichtlich der Häufigkeit, Dauer oder inhaltlichen*
1699 *Qualität, liegt eine Überwachung jedenfalls dann vor, wenn unbefugt Hard- oder Software installiert*
1700 *wurde, die eine Informationsbeschaffung zum Zwecke der Überwachung ermöglicht.*



1701 3 Strukturelle Perpetuierung einer unnötigen definitori- 1702 schen Komplexität

1703 Für einen ganzheitlichen Ansatz, wie dies der Ref-E laut eigener Aussage verfolgt, wäre zu
1704 erwarten, dass die einzelnen Fallgruppen systematisch aufgearbeitet und die jeweiligen Kern-
1705 elemente der Fallgruppen in die gesetzlichen Regelungen überführt wird.

1706 Hierbei ist es dem gesetzgeberischen Prozess stets immanent, dass Gemeinsamkeiten in **all-**
1707 **gemeine Regelungen** vorgezogen werden. Ein Unterfall dieser Methodik sind **zentrale**
1708 **Begriffsbestimmungen**, soweit diese Begriffe wiederholt in den gesetzlichen Bestimmungen
1709 auftauchen.

1710 Einerseits erhöht eine Zentralisierung der Begriffsbestimmungen die **Lesbarkeit**, da mehrere
1711 Aspekte in einen definierten Begriff zusammengeführt werden können. Andererseits erhöht es
1712 auch die **Flexibilität, Aktualisierbarkeit** und **Umfänglichkeit** der gesetzlichen Regelungen.
1713 Verändern sich die gesellschaftlichen oder rechtlichen Rahmenbedingungen und bedürfen ein-
1714 zeln Definitionen einer Anpassungen, so ist dies nur an einer Stelle erforderlich, und alle wei-
1715 teren Normen aktualisieren sich automatisch. Sollte im Ausnahmefall eine Aktualisierung für
1716 eine konkrete Rechtsnorm nicht erforderlich sein, sondern sogar negativ Effekte nach sich zie-
1717 hen, kann dies für diese eine Rechtsnorm im Wege eine lex specialis Regelung adressiert
1718 werden.

1719 Der Ref-E lässt **Potentiale** durch zentrale Begriffsbestimmungen **ungenutzt**. Im Ergebnis
1720 scheint dies sogar zu ungewollten Regelungslücken zu führen.

1721 Beispielhaft werden die Regelungen der §§ 184 ff. , sowie 201b StGB herangezogen.

1722 Etwaige Fallgruppen sind

1723 **A)**

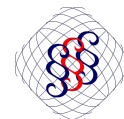
1724 1. künstlich generierte oder manipulierte Inhalte – ohne und ohne besondere Ehrverletzung

1725 2. künstlich generierte oder manipulierte Inhalte – mit offensichtlichen objektiven sexualisier-
1726 ten Inhalten

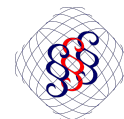
1727 3. künstlich generierte oder manipulierte Inhalte – mit aus Sicht bestimmter Erzeuger und
1728 Empfängerkreise sexualisierten Inhalten

1729 **B)**

1730 1. fiktive Inhalte entsprechend A), die aufgrund einzelner Inhalte Rückschlüsse auf konkrete
1731 Betroffene zulassen



- 1732 **C)**
- 1733 1. tatsächliche Inhalte entsprechend A), die konkrete Betroffene zum Inhalt haben, während
1734 diese auch für informierte Kreise erkennbar sind bzw. bleiben
- 1735 2. tatsächliche Inhalte entsprechend A), ohne dass diese konkrete Betroffene zum Inhalt
1736 haben, und diese auch für informierte Kreise nicht erkennbar sind oder erkennbar werden
- 1737 In allen Fällen von A) bis C) gilt, dass diese unterschiedliche Qualitäten aufweisen können,
1738 etwa aufgrund Inhalte
- 1739 ■ allgemeiner Qualität
 - 1740 ■ besonders verwerflicher Qualität (vgl. 184a StGB)
 - 1741 ■ besonderes verwerflicher Qualität aufgrund des tatsächlichen Alters der Betroffenen
 - 1742 ■ besonders verwerflicher Qualität aufgrund der bewusst erzeugten Wirkung über das Alter
1743 der Betroffenen
- 1744 Nun sollte davon ausgegangen werden können, dass das Gesetz jedenfalls hinsichtlich der
1745 objektiv **offensichtlich sexualisierten Körperregionen** eine einheitliche Wertung aufweist. Ein
1746 Vergleich der Regelungen §§ 184b, 184c, und 184k StGB lässt daran **Zweifel** aufkommen.
- 1747 So heißt es in § 184b Abs. 1 Nr. 1 lit. c) sowie in § 184c Abs. 1 Nr. 1 lit. c):
- 1748 | ***die sexuell aufreizende Wiedergabe der unbedeckten Genitalien oder des unbedeckten Gesäßes***
- 1749 Im neuen § 184k Abs. 1 Nr. 2 StGB-E heißt es:
- 1750 | ***die unbedeckten Genitalien, das unbedeckte Gesäß oder die unbedeckte weibliche Brust einer
1751 anderen Person abbildet***
- 1752 Eine solche inhaltliche Abweichung gab es in der Form auch schon in der gültigen Fassung des
1753 § 184k Abs. 1 Nr. 1 StGB.
- 1754 Soweit für Erwachsene ergänzende Körperregionen deshalb für erforderlich gehalten werden,
1755 um etwaige **Urlaubsfotos** der von §§ 184b oder 184c StGB erfassten Betroffenenkreise nicht
1756 unter Strafe zu stellen, erscheint dies nicht überzeugend. Die jeweilige litera der Regelung ver-
1757 langt ausdrücklich, dass eine „**sexuell aufreizende Wiedergabe**“ erforderlich ist. Insofern ist
1758 trifft die Regelung bereits anderweitig Sicherungsmaßnahmen, um ein nicht-verwerfliches Han-
1759 deln von einer Strafe auszuschließen; zumal es fraglich wäre, warum das nicht-verwerfliche
1760 Handeln nur einzelne Körperregionen betreffen können sollte. Vielmehr ist davon auszugehen,
1761 dass der Gesetzgeber hier eine **systematisch Vorgehensweise vermissen** lässt, weil die
1762 Beschäftigung der Thematik möglicherweise Tabuthemen betrifft oder höchst unterschiedliche



1763 gesellschaftliche moralische Vorstellungen betreffen könnte. Doch eine Diversität der morali-
1764 schen gesellschaftlichen Vorstellungen sollte nicht dazu führen, dass sich am Ende ein **inkon-**
1765 **sistentes Schutzkonzept** ergibt. Hiervon ist den potentiellen Opfern nicht geholfen.

1766 An dieser Stelle sei zudem darauf hingewiesen, dass die Abweichung nicht in der – wohl noch
1767 eher – nachvollziehbaren Weise erfolgt, dass ergänzende körperliche Schutzregionen für die
1768 **besonders vulnerablen Gruppen** der §§ 184b und 184c StGB geregelt wurden. Im Gegenteil,
1769 den besonders vulnerablen Gruppen wird der **geringere Umfang besonders geschützter Kör-**
1770 **perregionen** gewährt.

1771 Im entsprechenden Abschnitt des StGB existiert bereits eine Norm, die konkrete Begriffsbe-
1772 stimmungen beinhaltet, **§ 184h StGB**. Insoweit ist es auch kein Argument, dass es der bisheri-
1773 gen Systematik des StGB zuwiderliefe, in einem Abschnitt **ergänzende Begriffsbestimmungen**
1774 zentral zu regeln.

1775 Begriffsbestimmungen könnten und sollten etwa umfassen:

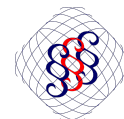
- 1776 ■ „tatsächliches Geschehen“, „wirklichkeitsnahes Geschehen“, „fiktives Geschehen“
- 1777 ■ „besonders geschützte Körperregionen“
- 1778 ■ „nackt“ bzw. „(un-)bekleidet“
- 1779 ■ „sexuell aufreizend“, „in sexuell bestimmter Weise“

1780 Hieraus ergibt sich eine weitere Inkonsistenz der genutzten Begrifflichkeiten, die zu nicht not-
1781 wendigerweise nachvollziehbaren Wertungsunterschieden führt.

1782 §§ 184b Abs. 1 Nr. 1 lit. c) und 184c Abs. 1 Nr. 1 lit. c) verwenden jeweils die Formulierung
1783 **„sexuell aufreizende Wiedergabe“**. § 184k Abs. 1 Nr. 3 verwendet **„in sexuell bestimmter**
1784 **Weise“**.

1785 Einerseits zeigt die Gesetzesbegründung, die im Kontext von „in sexuell bestimmter Weise“ auf
1786 § 184i StGB verweist, dass eine zentrale Norm für relevante Begriffe sachdienlich sein könnte,
1787 da sich die Begrifflichkeiten über mehrere Normen hinweg wiederholen und der Gesetzgeber
1788 offenkundig ein sich einheitlich entwickelndes oder entwickeltes Verständnis zu Grunde legen
1789 möchte.

1790 Andererseits ist für die beiden zuvor genannten Formulierungen festzuhalten, dass rein dem
1791 Wortlaut nach, **„sexuell aufreizend“** im Vergleich zu **„sexuell bestimmt“** die wohl höheren
1792 Anforderungen stellen müsste. „Sexuell aufreizend“ hat eine **ausschließlich objektive Kompo-**
1793 **nente**, während „sexuell bestimmt“ eine **starke subjektive Komponente** beinhaltet. Auf diese
1794 subjektive Komponente kann aus objektiven Kriterien zurückgeschlossen werden, was auch



1795 der Gesetzesbegründung zu entnehmen ist.⁴⁷ „Sexuell aufreizende“ Inhalte sind aufgrund ihrer
1796 objektiven Aspekte immer auch „sexuell bestimmt“, während der Umkehrschluss nicht immer
1797 zulässig sein dürfte.

1798 Und hieraus resultiert ein **Wertungswiderspruch**, der den Ganzheitlichen Anspruch des Ref-E
1799 in Zweifel zieht. Dieser Wertungswiderspruch könnte zudem bei konsistenter Verwendung von
1800 definierten Begriffen vermieden werden.

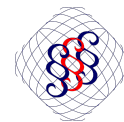
1801 „**Sexuell bestimmt**“ findet Verwendung bei der Abbildung **von bekleideten besonders schüt-**
1802 **zenswerten Körperregionen**. „**Sexuell aufreizend**“ hingegen, findet **bei unbekleideten (!)**
1803 **besonders schützenswerten Körperregionen** Anwendung. „**Sexuell bestimmt**“ findet insoweit
1804 für **alle Altersgruppen** Anwendung, „**sexuell aufreizend**“ lediglich bei der **besonders vulnera-**
1805 **blen Gruppe** der von §§ 184b und 184c Betroffenen.

1806 Unbenommen, ob die Beschränkung der **Tatbestandsvoraussetzungen** in § 201b Abs. 3 StGB
1807 gF, bzw. § 184 Abs. 2 StGB-E auf eine **Entgeltlichkeit** sachdienlich ist, ist die durch das Gesetz
1808 verwendete Wortwahl inkonsistent. Während §§ 184b Abs. 1 und 184c Abs. 1 StGB sowie
1809 § 184 Abs. 1 StGB-E jeweils von bekleidet, unbekleidet sowie „ganz oder teilweise unbeklei-
1810 det“ spricht, verwendet § 184 Abs. 2 StGB-E „**die Nacktheit**“ eine anderen Person. Begrifflich
1811 entspräche dies, dass diese andere – abgebildete – Person „ganz unbekleidet“ wäre. Hierauf
1812 kommt es aber wohl nicht an, da davon ausgegangen werden kann, dass der Gesetzgeber in
1813 diesem Falle die gleiche Formulierung verwendet hätte. Somit könnte genügen, dass die
1814 andere Person „teilweise unbekleidet“ abgebildet wird.⁴⁸ Auch dies scheint nicht die Intention,
1815 denn dann hätte der Gesetzgeber es wohl so formuliert. Denn neben der Abweichung
1816 „(un-)bekleidet“ tritt die weitere Abweichung „**abbilden**“ und „**zum Gegenstand**“ haben. Der
1817 Gesetzgeber könnte hierdurch eine Intention der Darstellung zum Ausdruck bringen wollen. Es
1818 käme dann nicht nur darauf an, dass eine (teilweise) unbekleidete Person abgebildet ist, son-
1819 dern das Bild muss gerade wegen oder zum Zwecke dieser „Nacktheit“ erstellt oder angebo-
1820 ten/verschafft werden. Die (teilweise) unbekleidete Person wird somit **objektifiziert**. Insoweit
1821 stellt sich die Frage, wo der Unterschied gegenüber der Formulierung „in sexuell bestimmter
1822 Weise“ läge, oder ob es nicht gerade doch – aufgrund des Entgeltumstands – auf die bloße
1823 Abbildung ankommen solle.

1824 In § 201b StGB-E bleibt offen, ob ein „mittels Computerprogramms erstellter Inhalt, der den
1825 **Anschein eines tatsächlichen Geschehens** erweckt“ einer Erstellung eines „**wirklichkeits-**
1826 **nahen Geschehens**“ entspricht, oder die abweichende Formulierung **materielle Unterschiede**
1827 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.

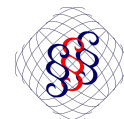


1828 Soweit die Gesetzesbegründung zum Ausdruck bringt, dass konkrete **Regelbeispiele** zu vermeiden seien, da diese die **Rechtssprechung** daran **hindern** würden, auf künftige, neuere Formen **flexibel zu reagieren**, erscheint diese Auffassung höchst fragwürdig.

1831 Das **Bestimmtheitsgebot** verlangt, dass das Gesetz aus sich heraus verständlich 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 alsbald aufgelöst** werden, insbesondere im Wege der Rechtssprechung. Betrifft es einen bereits **bekanntem Regelungsbereich**, wird eine Ausnahme des Bestimmtheitsgebots dahingehend akzeptiert, dass die unbestimmten Rechtsbegriffe ja bereits durch die **Rechtssprechung hinreichend Kontur** erhalten hätten.

1839 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 Rechtssprechung, der Gesetzgeber im nächst möglichen Zeitpunkt die der Rechtssprechung zu entnehmende Kontuierung in das Gesetz aufnehmen müsste.

1843 Jedenfalls ist es der Rechtssprechung nicht möglich, eine stetige Rechtssprechung ohne Weiteres auf gänzliche unerwartete Fälle zu erweitern oder in ihrer Aussage gänzlich umzukehren. Jedenfalls, kann diese neuerlich Rechtsprechung wenn nur Wirkung für dann zukünftige Tat handlungen betreffen. Im Übrigen wird die Rechtssprechung unbestimmte Rechtsbegriffe auch gegenüber ihrer eigenen Rechtssprechung 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 Rechtswidrigkeit ihres künftigen Handelns absehen könnten.



1856 4 Annahme eines Rechts auf anonyme 1857 Meinungsäußerung

1858 Der Ref-E perpetuiert das Dogma eines Anrechts auf anonyme Meinungsäußerung und
1859 anonyme Nutzung von Online-Plattformen. Ein solcher grundrechtlicher Anspruch kann nicht
1860 erkannt werden.

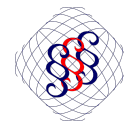
1861 Hierbei ist zu unterscheiden zwischen einer **pseudonymen** und einer **anonymen** Nutzung. In
1862 der Tat erscheint es geboten, zumindest eine pseudonyme Nutzung erlauben zu müssen. Dies
1863 entspricht auch der analogen Welt. Eine echte „Anonymität“ ist dort ebenfalls nicht gegeben,
1864 sondern allenfalls eine Pseudonymität. Zugleich scheint es aber auch nicht geboten, eine
1865 „anonyme Nutzung“ per se zu verbieten, soweit die damit einhergehenden Risiken anderweitig
1866 mitigiert werden.

1867 Das Dogma des grundrechtlichen Anrechts auf anonyme Meinungsäußerung basiert bereits
1868 auf einem **Zirkelschluss**. Dieser Zirkelschluss wird in Zeiten von Künstlicher Intelligenz, KI-
1869 Agenten und (Social Media)-Bots umso relevanter.

1870 **Anonymität verhindert bereits die Prüfung, ob der persönliche Anwendungsbereich der in**
1871 **Rede stehenden Grundrechte** überhaupt betroffen ist. Nicht jedes Grundrecht wird hinsicht-
1872 lich des persönlichen Anwendungsbereichs uneingeschränkt. Zudem kennt – wenn auch in der
1873 Praxis seltenst bis gar nicht relevant – das Grundgesetz auch die sogenannte **Grundrechtsver-**
1874 **wirkung**. Ob eine solche einschlägig ist, kann ebenfalls nicht geprüft werden, wenn es einen
1875 grundrechtlichen Anspruch auf Anonymität gäbe.

1876 In Zeiten von Künstlicher Intelligenz erscheint zudem der **Rückschluss unzulässig**, dass eine
1877 „**Accountaktivität**“ zwingend **von einem Menschen** ausgeübt werden muss. Zutreffend ist,
1878 dass auch eine etwaige **KI-gestützte Aktivität oder ein (Social-Media)-Bot** am Ende der Ver-
1879 antwortungskette eine natürliche Person benötigt, die den automatisierten Prozess in Gang
1880 setzt. Fraglich ist aber, ob in diesen Fällen dem „Bot“ aufgrund eines mittelbaren Bezugs zu
1881 einer natürlichen Person die grundrechtlichen Schutzmechanismen gewährt werden müssen.
1882 Insoweit ist auch fraglich, ob die gesetzliche Vermutung, ein anonymer, rechtswidrig agierender
1883 Account ist grundsätzlich unmittelbar einem Grundrechtsträger zugeordnet, noch aufrecht
1884 erhalten werden kann.

1885 Dies vorangestellt, könnten engmaschige und effizientere **Verfahrensregelungen** den **Schutz**
1886 **der Betroffenen verbessern**. Hierbei ist zu beachten, dass Ziel dieser Regelungen nicht die
1887 Versagung der Möglichkeiten auf Anonymität ist. Es ist aber die Frage zu stellen, ob mit den



1888 Vorteilen der Anonymität auf der einen Seite, nicht auch Nachteile auf der anderen Seite hinzu-
1889 nehmen sind. Es gibt ein Recht auf freie Meinungsäußerung, aber nicht notwendigerweise ein
1890 Recht auf die effizienteste Form der freien Meinungsäußerung.

1891 Vorstellbar sind daher nachstehende **Regelungsdimensionen**:

- 1892 ■ gesetzlich normierter Abstufungen des Schutzbedarfs von Nutzerkonten, je nach Anonymität
- 1893 ■ Möglichkeiten des anonymen Nutzer*innen unter Aufgabe der Anonymität die eigene Rechts-
1894 position effektiv zu verteidigen
- 1895 ■ Klare Verfahrensfristen und Vermutungswirkungen (z.T. siehe auch 2.2.2)

1896 **Abstufungen des Schutzbedarfs** können sich etwa entlang der nachstehenden Varianten
1897 bewegen:

- 1898 ■ vollständig anonymes Profil, bei dem weder im Nutzerkonto noch in den Aktivitäten Rückschlüsse
1899 auf die dahinterstehende Nutzer*in gezogen werden können, und welches – mit Aus-
1900 nahme der rechtswidrigen Handlungen – keine sonstigen Aktivitäten aufweist; eine Ver-
1901 mutung, dass dieses Nutzerkonto durch KI oder einen Bot gesteuert wird, ist begründet.
- 1902 ■ vollständig anonymes Profil, die Aktivitäten sind aber nicht auf rechtswidrige Handlungen
1903 beschränkt; die Aktivitäten sind aber ansonsten weiterhin nicht geeignet eine Vermutung zu
1904 etablieren, dass die dahinterstehende Nutzer*in ein Mensch ist; die Vermutung, dass dieses
1905 Nutzerkonto durch KI oder einen Bot gesteuert wird, bleibt begründet.
- 1906 ■ vollständig anonymes Profil, die Aktivitäten sind hinreichend divers und mit Bezug zum rea-
1907 len Leben, dass weder vermutet werden kann, dass das Nutzerkonto durch KI oder einen
1908 Bot gesteuert wird, noch vermutet werden kann, dass das Nutzerkonto durch einen Men-
1909 schen gesteuert werden kann;
- 1910 ■ anonymes Profil, bei dem die Aktivitäten starke Bezüge in die reale Welt aufweisen, etwa
1911 aufgrund durchgeführter Transaktionen, geposteter Inhalte (Bilder, Videos) von tatsächli-
1912 chen Umständen, etc.; die Inhalte genügen aber nicht, um mit vertretbarem Aufwand die
1913 Aktivitäten zu korrelieren und hieraus die Identität der dahinterstehenden Nutzer*in
1914 abzuleiten;
- 1915 ■ pseudonymes Profil, bei dem Nutzer*innen nicht unter dem eigenen Klarnamen auftreten,
1916 aber entweder im Nutzerkonto ihre (vermeintlichen) Klardaten angegeben haben, oder die
1917 geposteten Inhalte Rückschlüsse auf die reale Person ermöglichen, etwa durch Aktivitäten,
1918 die das Gesicht der Nutzer*in beinhaltet, konkrete ggf. auch regelmäßige Aufenthaltsorte zu
1919 bestimmten Zeitpunkten, etc.



1920 ▪ Unverifiziertes Klarnamenprofil, bei dem Nutzer*innen selbst unter dem vermeintlichen Klar-
1921 namen auftreten, ein Fake-Account aber mangels Verifikation nicht ausgeschlossen ist.

1922 ▪ pseudonymes verifiziertes Profil, bei dem Nutzer*innen nicht unter dem eigenen Klarnamen
1923 auftreten, sich aber gegenüber dem Dienstanbieter verifiziert haben, d.h., die im Nutzer-
1924 konto hinterlegten Identifikationsdaten (Klarnamen, Adresse, etc.) nicht nur selbst behaupten,
1925 sondern nach einem definierten Prozess gegenüber dem Dienstanbieter bestätigt
1926 haben.

1927 ▪ Verifiziertes Klarnamenprofil

1928 Es ist naheliegend, dass der **gewährte Schutz für verifizierte Profile am höchsten** sein sollte;
1929 sodann kann der Schutz – teils auch im Interesse der Nutzer*innen – abgeschwächt werden.

1930 Hierbei sollten zwei Elemente in den Fokus genommen werden:

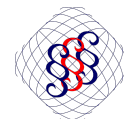
1931 ▪ Schutz vor digitaler Gewalt durch möglichst unmittelbare Entfernung der rechtsverletzenden
1932 Inhalte

1933 ▪ Schutz vor digitaler Gewalt durch Sanktionierung der Täter*innen

1934 Bei digitaler Gewalt kann das aus der Liegenschaftspflege bekannte „broken window“ Phäno-
1935 men übertragen werden. Das „broken window“-Phänomen besagt, dass eine Liegenschaft wei-
1936 terem Vandalismus umso schneller ausgesetzt ist, sobald die Liegenschaft bereits Schäden
1937 (broken window) aufweist; denn in diesem Moment ist ersichtlich, dass die Liegenschaft nicht
1938 mehr bewohnt oder gepflegt wird; mithin das Risiko „erwischt zu werden“ augenscheinlich
1939 gesunken ist.

1940 Im Falle von digitaler Gewalt bedeutet dies: ist der „**Damm**“ **erst einmal gebrochen**, dass
1941 Betroffene im digitalen Raum etwaigen Schmähungen oder sonstigen Rechtsverletzungen
1942 ausgesetzt sind, also „der erste Stein geworfen wurde“, so **senkt dies auch die Hemm-**
1943 **schwelle** weiterer Täter*innen, und ein ganze **Welle von Rechtsgutsverletzungen kann sich**
1944 **Bahn brechen** (Shitstorm). Es ist daher von großer Bedeutung, die individuellen rechtsgutsver-
1945 letzenden Inhalte **möglichst schnell aus der Öffentlichkeit zu entfernen** und somit das Risiko
1946 der Nachahmung zu reduzieren.

1947 Eine **Sanktionierung** soll und darf deswegen nicht gänzlich hintangestellt werden. Hierzu sind
1948 etwaige Beweis-sichernde Maßnahmen zu treffen. Die **Sanktionierung von anonymen KI-Bots**
1949 wird aber ohnehin in den meisten Fällen ins Leere laufen. Deswegen erscheint es im Sinne
1950 einer ganzheitlichen Betrachtung zielführend, diese **beiden Dimensionen zu trennen**, und
1951 auch anhand der Anonymität der Nutzerkonten abgestuften Schutzbedarfe zu effektuieren.



1952 Im Ergebnis wird **vorgeschlagen**, ein **Konzept zu prüfen** und in einer **Überarbeitung des**
1953 **Gesetzes** aufzunehmen, welches **nachstehende Eckpunkte** berücksichtigt.

1954 ■ Je höher der Grad der Anonymität, desto höher der Grad an **Unmittelbarkeitsautomatismen**
1955 hinsichtlich der zur Verfügung stehenden Maßnahmen, insbesondere hinsichtlich der
1956 Inhalts- und Account-Sperren.

1957 ■ Als mögliche **Erweiterungen des Anordnungskanons** sollte in Betracht gezogen werden

1958 ■ etwaige Sperren der über die Nutzerkonten erfolgenden **Geldflüsse**, jedenfalls, soweit die
1959 Nutzerkonten auch dazu genutzt werden, die eigenen Inhalte zu monetarisieren.

1960 ■ die **Löschung** von Accounts

1961 ■ die **Rücksetzung** der durch das Nutzerkonto **aufgebauten „Netzwerke“**, etwa in Form von
1962 Follower*innen, „Freunden“, Kontakten, etc.;

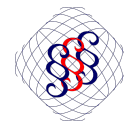
1963 ■ für die Verbreitung von rechtswidrigen Inhalten, ist ein Netzwerk erforderlich; eine Rück-
1964 setzung des Netzwerks würde die Breitenwirkung der (künftigen) rechtswidrigen Inhalte
1965 betreffen bzw. die Verbreitung jedenfalls gegenüber den weiteren Nutzer*innen einer
1966 Online-Plattform auflösen, die lediglich aus – längst – vergessenen Gründen einen Ver-
1967 bindung zu dem betroffenen Nutzerkonto aufweisen;

1968 ■ die „Netzwerkgröße“ ist zudem ein Faktor, sowohl für die „objektive“ öffentliche Wahr-
1969 nehmung der über einen Account geteilten Inhalte, als auch für die auf Online-Plattfor-
1970 men erfolgte „Gewichtung“ der Inhalte im Rahmen der Feed-Algorithmen

1971 ■ **Untersagung der „Empfehlung“** der Inhalte durch die Online-Plattform

1972 Ein Nebeneffekt sowohl der Erweiterung der Maßnahmen als auch einen erhöhten Grad der
1973 Automatismen wäre, dass die ebenfalls inzwischen über Automatismen erstellten Nutzerkon-
1974 ten und ganze Nutzerkonten-Netzwerke zur gegenseitigen „Wirkungsbestärkung“ auf lange
1975 Sicht ausgetrocknet werden könnten; bzw. deren Betrieb mit deutlichen höheren Aufwänden
1976 verbunden wäre.

1977 **Derartige Ansätze erscheinen zudem weniger eingriffsintensiv als parallele Diskussionen**
1978 **über eine Vorratsdatenspeicherung oder eine Klarnamenpflicht.**



1979 5 Verlagerung der Tatbegehung und Tathandlung

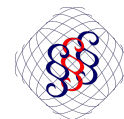
1980 In Folge der unnötigen definitorischen Einschränkungen und Unklarheiten, ist der Ref-E selbst
1981 bereits **Geburtshelfer für neue Phänomene**.

1982 Dies liegt im Wesentlichen daran, dass es der Ref-E versäumt, eine klare Linie zu etablieren,
1983 die einen Gleichlauf zwischen analoger und digitaler Welt zur Folge hätte.

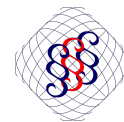
1984 Im Wesentlichen würden für eine **materielle Betrachtung** als Leitlinie folgende drei Prämissen
1985 genügen:

- 1986 ■ die Straftatbestände der analogen Welt werden hinreichend geschlossen, etwa im Bereich
1987 der Nachstellung, der Bereich des Besitz, Herstellung und Verbreitung besonders verwerfli-
1988 cher tatsächlicher, wirklichkeitsnaher oder fiktiver Inhalte⁴⁹, etc.
- 1989 ■ die Implementierung des logischen Grundsatzes, dass es für die Strafbarkeit einer strafbe-
1990 wehrten Handlung irrelevant sein muss, über welches Medium diese Tathandlung begangen
1991 wird
- 1992 ■ erst im dritten Schritt werden etwaige Besonderheiten der digitalen Kommunikation in
1993 Ansatz gebracht, nämlich in zwei Dimensionen,
 - 1994 ■ eine Verringerung der Strafbarkeitsschwelle oder eine Verschärfung der (Mindest-)Straf-
1995 rahmen, oder sonstige, die negativen Folgen der Tathandlung mitigierender Maßnahmen,
1996 etwa aufgrund größerer Streubreite der Inhalte, erleichterter Tatbegehung, verringerte
1997 Reversibilität von Tathandlungen bzw. intensivere Langzeitauswirkungen der Tathandlun-
1998 gen, etc.
 - 1999 ■ eine Erhöhung der Strafbarkeitsschwelle oder eine Verringerung der (Mindest-)Strafrah-
2000 men, etwa aufgrund Umstände, die bei gleicher objektiver Tathandlung, einen geringeren
2001 Unwertgehalt erkennen lassen, die Reversibilität erleichtert ist bzw. die Langzeitwirkungen
2002 geringer sind, etc.

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



- 2003 Neben der materiellen Betrachtung sind selbstredend etwaige **Besonderheiten der Durchsetz-**
2004 **barkeit** zu beachten. Auch hier können die Prämissen auf wenige Aspekte kondensiert werden
- 2005 ■ Bestehen Erkenntnisdefizite im Rahmen der Ermittlung und/oder Beweissicherung im Ver-
2006 gleich zur analogen Welt?
- 2007 ■ Resultieren etwaige Erkenntnisdefizite aus auf Grund für die demokratische Rechtsordnung
2008 notwendigen Zugewinnen im Vergleich zur bisher gültigen analogen Welt?
- 2009 ■ Können im Einzelfall etwaige Erkenntnisdefizite unter Beibehaltung der Zugewinne für die
2010 demokratische Rechtsordnung durch rechtsstaatliche Verfahren behoben werden?
- 2011 ■ Sind aufgrund der Flüchtigkeit des Digitalen beschleunigte Verfahren erforderlich?
- 2012 ■ Existieren etwaige Nachweisdefizite im Falle von Schutzbehauptungen?
- 2013 Der Ref-E versäumt es eine in Absehung des Mediums der Tat einheitliche Definition zu eta-
2014 blieren, vgl. auch 3.
- 2015 Zudem versäumt der Ref-E, die für eine Durchsetzbarkeit bestehenden Erkenntnisdefizite auf-
2016 grund effizienter Verfahren hinsichtlich ihres zeitlichen Ablaufes oder ihres inhaltlichen
2017 Erkenntnisgewinns zu überwinden, vgl. auch 2.2.2 und 2.4.
- 2018 Es steht somit zu befürchten, dass sich die Tathandlungen sowohl inhaltlich als auch räumlich
2019 lediglich verlagern könnten.
- 2020 Eine **inhaltliche Verlagerung** bedeutet, dass die Tathandlungen sich hinsichtlich der **modus**
2021 **operandi** anpassen, und neu geschaffene oder beibehaltene Regelungs- oder Durchsetzungs-
2022 lücken ausnutzen.
- 2023 Eine **räumliche Verlagerung** bedeutet, dass die Tathandlungen sich hinsichtlich der „räumli-
2024 chen“ Tatumstände verlagern, also im digitalen Raum dahingehend, dass **andere oder ganz**
2025 **neue Formen der Online-Plattformen** in den Fokus rücken, oder **andere (Sekundär-)Funktio-**
2026 **nalitäten** der Plattformen zur Tatbegehung genutzt werden.
- 2027 In beiden Fällen der Verlagerung ist zu befürchten, dass der **Schutzeffekt für die Betroffenen**
2028 **ausbleibt**, oder jedenfalls deutlich geringer ausfällt. Mithin steht zu befürchten, dass die dem
2029 ganzheitlichen Ansatz des Ref-E innewohnende Hoffnung, die „**Verrohungstendenz**“ digitaler
2030 Räume auszubremsen oder im besten Fall umzukehren, sich nicht zeitnah erfüllt.



2031 5.1 Verlagerung hinsichtlich des modus operandi

2032 Einerseits wird auf die möglichen Risiken hinsichtlich des Tatortes hingewiesen, soweit auch
2033 dies den modus operandi beeinflusst. Siehe hierzu exemplarisch und entsprechend 2.3.2.

2034 Ebenso ist für den modus operandi relevant, dass derzeit nur bestimmte Katalogtaten von den
2035 durch den Ref-E erhofften Effizienz- und Effektivitätsgewinnen durch das GGDG-E profitieren.
2036 Auch dies kann den modus operandi dahingehend beeinflussen, dass die **Tathandlungen sich**
2037 **künftig bewusst in den Grauzonen zwischen den Katalogtaten bewegen** werden, vgl. 2.3.1.

2038 Im Übrigen wird nachstehend auf die Normen §§ 184 ff. StGB-E, sowie § 201b StGB-E einge-
2039 gangen, und warum keine ganzheitliche Überarbeitung, wie diese der Ref-E für sich behauptet,
2040 erkannt werden kann. Soweit sachdienlich wird hierzu auch auf die exemplarischen Ausführun-
2041 gen unter 3 verwiesen.

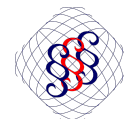
2042 Besonders augenscheinlich sind die **unterschiedlich relevanten Körperregionen**. Es ist daher
2043 davon auszugehen, dass (professionelle) Täter*innen die sich verschobenen Grenzlinien
2044 gezielt ausnutzen werden.

2045 Insoweit ist – wie bereits unter 3 ausgeführt – nicht nachvollziehbar, warum sich gerade der
2046 **Schutz bei besonders vulnerablen Gruppen** geringer darstellt.

2047 Grundsätzlich ist auch nicht nachzuvollziehen, warum die **Strafbarkeit** einer sexuell bestimm-
2048 ten **Objektifizierung** überhaupt von **besonders schützenswerten Körperregionen** abhängig
2049 sein sollte. Es mag ein angepasster Strafrahmen geboten sein. Die Annahme eines abweichenden
2050 Unwertgehalts, der eine Strafbarkeit gänzlich verneint, erschiene vor dem Hintergrund des
2051 Ref-E und dessen Überlegungen in der Gesetzesbegründung inkonsistent.

2052 Dieser **Schutzbedarf** erscheint **unabhängig des Alters der Personen** gegeben, wobei beson-
2053 ders vulnerable Gruppen ggf. einen qualifizierten Strafrahmen rechtfertigen könnten.

2054 Insoweit ist auch die **Entgeltlichkeit** des § 184k Abs. 2 StGB-E **fragwürdig**. Nachvollziehbar
2055 erschiene ein **Rückgriff auf die sexuell bestimmte Weise**, und eine gesetzliche Liste von
2056 Regelbeispielen, etwa die Verbreitung auf, oder der Bezug über **spezialisierte Online-Plattfor-**
2057 **men, Chat-Gruppen** oder in Fällen, in denen sich aufgrund des **konkreten Kommunikations-**
2058 **Kontexts** zu den Inhalten, die Intention der Täter*innen eindeutig erkennen lässt.



2059 Im Weiteren erscheint der Rückgriff auf ein **fiktives, tatsächliches** und **wirklichkeitsnahes**
2060 **Geschehen inkonsistent.**

2061 Aus § 184b Abs. 1 aE StGB(-E) ergibt sich, dass für die höchst schützenswerte Gruppe der
2062 Betroffenen nach § 184b StGB auch fiktive Inhalte strafbar sein sollen. Dort heißt es nämlich

2063 *Gibt der [,,] Inhalt in den Fällen von Absatz 1 Satz 1 Nummer 1 und 4 kein tatsächliches oder wirk-*
2064 *lichkeitsnahes Geschehen wieder, so ist auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu*
2065 *erkennen.*

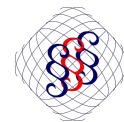
2066 Eine entsprechende Regelung fehlt aber in § 184c StGB-E, wobei nicht erkennbar ist, woraus
2067 sich dieser **Wertungswiderspruch** ergibt. Vorstellbar sind etwaige – internationale – (audiovi-
2068 suelle) Medien, die zum Teil auch auf eine (weitreichende) Tradition in deren Herkunftskultu-
2069 ren aufbauen. Sollte dies der einzige Grund sein, eine ganze Kategorie der Tathandlungen für
2070 die betroffene Gruppe nach § 184c StGB unreguliert zu lassen, scheint eine **zielgerichtete**
2071 **Ausnahme möglich** und wohl im Sinne des **Opferschutzes** zielführender, wenn nicht gar
2072 **geboten.**

2073 § 201b StGB-E umfasst „einen mittels eines Computerprogramms erstellten oder veränderten
2074 Inhalt, der den Anschein erweckt, ein tatsächliches Geschehen in Bezug auf eine andere Per-
2075 son wiederzugeben“.

2076 Also mit anderen Worten die künstliche Generation eines Inhalts mit einem wirklichkeitsnahen
2077 Geschehen oder die Manipulation eines Inhaltes mit einem tatsächlichen Geschehen.

2078 Die abweichende Formulierung „**den Anschein erweckt**“ lässt **Zweifel**, ob dieser Gleichlauf zur
2079 hier vorgeschlagenen „mit anderen Worten“-Formulierung gewünscht ist. Laut Gesetzesbegrün-
2080 dung könnte ein solches **abweichendes Verständnis gewünscht** sein. Es soll laut Gesetzes-
2081 begründung nicht nur darauf ankommen, ob wirklichkeitsnahe Inhalte neu oder durch Manipu-
2082 lation erstellt wurden, sondern auch, ob ein objektiver Dritter diese als tatsächliches Gesche-
2083 hen wahrnehmen würde.

2084 Es kommt also auf die **Qualität der Inhalte** an, wiederum gemessen am **objektivierten Erfolg**
2085 der tatsächlichen „**Fehlwahrnehmung**“. Mit anderen Worten: eine **Strafbarkeit** der inhaltlich
2086 verwerflichsten Inhalte wäre wohl auch dann nach dieser Norm **ausgeschlossen**, wenn
2087 Täter*innen in den – etwa bildlichen – Inhalt einen sichtbaren Hinweis „**mit KI erstellt**“ einbin-
2088 den. Ob dies ausreicht, um den „**erheblichen Schaden**“ von Betroffenen abzuwenden ist frag-
2089 lich, zumindest, wenn man die parallelen Diskussionen über den erforderlichen Umfang zur
2090 transparenten Darstellung von Produktplatzierungen, Werbung, oder ähnlichem berücksichtigt.



2091 Hierbei mag angeführt werden, dass in diesen besonders krassen Fällen wohl etwaige **Spezial-**
2092 **normen** einschlägig wären, die den hohen Unwertgehalt adressieren. Dies ist aber in **Zweifel**
2093 zu ziehen, aufgrund der hier bereits **ausgeführten Inkonsistenzen**. Ergänzend ist etwa zu
2094 berücksichtigen, dass der **Unwertgehalt von § 184a StGB weiterhin auf tatsächliche**
2095 **Geschehen begrenzt** ist.

2096 Zudem lässt eine solche Betrachtung die **Wirkung auf die Betroffenen** außer Acht. Der **psy-**
2097 **chologische Effekt** auf Betroffene, dass Dritte den Inhalt wahrgenommen haben (könnten),
2098 und das Dritte (im Einzelfall) nicht verstanden haben, dass es sich um künstliche / manipu-
2099 lierte Inhalte handelt, ist nicht zu unterschätzen. Allein dieser psychologische Effekt kann die
2100 Betroffenen in ihrer weiteren Lebensführung einschränken, ohne das im Übrigen erhebliche,
2101 physische oder finanzielle Schäden zu besorgen wären.

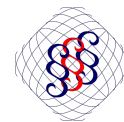
2102 Außerdem ist fraglich, ab welchen **Grenzwerten** ein **objektiver Anschein** angenommen werden
2103 soll. Genügt eine **relative Quote** von 5% oder muss die Mehrheit die Inhalte als tatsächliches
2104 Geschehen wahrnehmen? Oder gelten **absolute Grenzwerte**?

2105 In Zeiten **viraler Inhaltsverbreitung**, können Inhalte ohne Weiteres durch mehrere Millionen
2106 Nutzer*innen binnen kurzer Zeit wahrgenommen werden. Bereits 5% entsprechen somit einer
2107 erheblichen, absoluten Zahl von Nutzer*innen. Wird bei der Ermittlung des objektiven
2108 Anscheins auf eine **generalistische, globale Betrachtung** abgestellt, oder wird eine **Referenz**
2109 **des Nahfelds der Betroffenen** herangezogen? So ist vorstellbar, dass zwar nur 5% aller Nut-
2110 zer*innen die Inhalte als „tatsächlich“ wahrnehmen, aber aufgrund abweichender Sozialisa-
2111 tion, Bildung und weiterer „weicher Faktoren“, 80% der Nutzer*innen aus dem Nahfeld der
2112 Betroffenen.

2113 Zudem bleibt offen, wie die **Feststellung auf einer Zeitachse** die Strafbarkeit beeinflussen.
2114 Gemäß dem Motto „der stete Tropfen höhlt den Stein“, mag der originäre Inhalt als solches
2115 weder den Anschein erwecken, noch die Schäden begründen.

2116 Dieser Inhalt kann im weiteren Verlauf in einer sich **selbst-verstärkenden Kommunikations-**
2117 **schleife mit Echo-Effekten** eine hohe und **schädigende Eigendynamik** entwickeln, bei dem es
2118 den Rezipienten der nachgelagerten Kommunikation gar nicht mehr darauf ankommt, was der
2119 Ursprung der sekundären Inhalte tatsächlich war.

2120 Insoweit generiert sich der Anschein des tatsächlichen Geschehens aus der **Vielzahl der**
2121 **sekundär Inhalte**, die (fälschlicherweise) den Eindruck eines tatsächlichen Geschehens auf
2122 Basis des offensichtlich nicht tatsächlichen Primär-Inhalts erwecken. **Kausal** für diese schädi-
2123 genden Sekundär-Inhalte bleibt der **ursprüngliche, schlecht generierte Inhalt**.



2124 Die weiteren **Sekundär-Inhalte erfüllen nicht notwendigerweise Straftatbestände**. Hierdurch
2125 bietet sich das **Risikopotential** geschickt **orchestrierter Kampagnen**, um in der Einzeltat eine
2126 Strafbarkeit zu vermeiden, in der Summe aber den gleichen, wenn nicht sogar einen intensive-
2127 ren schädigenden Effekt auszulösen. Ein diese Lücke möglicherweise füllender **Nachweis** des
2128 „**vorsätzlich gemeinschaftlichen Handelns**“ dürfte **äußerst schwierig** zu führen sein.

2129 Eine solche **Einschränkung** auf Ebene der „**Qualität**“ des Inhalts erscheint auch **nicht gebo-**
2130 **ten**. Die **Einschränkung**, dass „**ein erheblicher Schaden**“ zu besorgen ist, ist **bereits**
2131 **schwerwiegend**.

2132 Im Übrigen könnte das **Tatbestandsmerkmal** „**unbefugt zugänglich machen**“ **modifiziert** wer-
2133 den. Aktuell genügt bereits die unbefugte Zugänglichmachung gegenüber nur einer Person.
2134 Dies wäre aber nur dann geeignet, einen erheblichen Schaden zu begründen, wenn diese eine
2135 Person in einer besonderen Beziehung zu etwaigen Opfern stünde. Ansonsten wären erhebli-
2136 che Schäden nur dann zu besorgen, wenn die Inhalte eine (unbestimmten) Vielzahl von Per-
2137 sonen zugänglich gemacht wird. Insoweit erscheint eine sachdienlichere Ausgestaltung mit
2138 weniger Umgehungspotential vorstellbar.

2139 5.2 Verlagerung hinsichtlich der räumlichen Tatbegehung

2140 Zunächst wird auf die möglichen Risiken hinsichtlich des Tatortes hingewiesen, soweit sich
2141 dies aus der Limitierung der Beschränkung des GGdG-E hinsichtlich der Anbieter ergibt, exem-
2142 plarisch und entsprechend 2.3.2.

2143 Ergänzend hierzu sei darauf hingewiesen, dass die **Beschränkung auf Internetzugangs-**
2144 **dienste erhebliche blinde Flecken** bedeuten kann. Täter*innen, die eher beiläufig eine Straf-
2145 tat begehen, werden hierdurch ermittelt werden können. Dies stellt – hoffentlich – auch die
2146 Mehrheit der Täter*innen dar.

2147 Soweit Täter*innen aber einen gewissen Grad der Professionalität erreicht haben, oder aus
2148 anderen Gründen die Identifizier- und Nachverfolgbarkeit im Internet einschränken, etwa um
2149 ein (Werbe-)Profiling zu vermeiden, ist **nicht notwendigerweise von einer direkten Verbin-**
2150 **dung zwischen Informationen der Diensteanbieter zu den Informationen der Internetzu-**
2151 **gangsanbieter** auszugehen.

2152 Soweit etwa **Proxy- oder VPN-Dienste** durch die Täter*innen genutzt würden, müsste zunächst
2153 die entsprechende **Dienstkette** nachverfolgt werden, wenn nicht bei den **Zwischendiensten**
2154 bereits hinreichende identifizierende Informationen vorlägen. Insoweit sollten auch **derartige**
2155 **Dienste als Adressaten der gerichtlichen Ausunftsanordnungen** aufgenommen werden, um
2156 eine Verlagerung der Tathandlungen zu vermeiden (obgleich man die Nutzung derartiger
2157 Dienste auch als veränderten modus operandi verstehen kann).

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

