Anonymität im Internet

Interdisziplinäre Rückschlüsse auf Freiheit und Verantwortung bei der Ausgestaltung von Kommunikationsräumen*

Hans-Christian Gräfe und Andrea Hamm

1. Gängige Annahmen über Anonymität

„Die anonyme Nutzung ist dem Internet immanent."[1] So lautet eine unter Juristinnen bekannte und weit verbreitete Behauptung, die sich hinterfragen lassen muss. Die Wirklichkeit im Internet zeigt ein hinreichend anderes Bild. Unternehmen, die hinter den Kulissen immense Umsätze mit personalisierter Werbung erwirtschaften, registrieren nicht nur die Webseiten, die wir besuchen, sondern erfassen als Metadaten auch jede unserer Mausbewegungen, jeden Tastendruck und jede Änderung der Scrollposition.[2] Anhand ihrer individuellen Verhaltensmuster können Internetnutzende nicht nur identifiziert, sondern auch Aussagen über ihre Gewohnheiten und politischen Überzeugungen, ihre gesundheitliche und finanzielle Situation, ihre Persönlichkeit und vieles mehr getroffen werden.[3]

Nichtsdestotrotz kann das Recht auf anonymes Surfen aus dem Grundgesetz abgeleitet werden und ist einfachgesetzlich bereichsspezifisch geschützt. Wie dies verfassungsrechtlich einzuordnen ist, und inwiefern zwischen aktiver und passiver Nutzung des Internets, also zwischen dem aktiven Verbreiten von Online-Inhalten oder dem passiven Rezipieren solcher, unterschieden werden muss, ist sich die Rechtswissenschaft (selbstverständlich) nicht ganz einig. Die Ansätze dafür unterscheiden, ob es sich um Individualkommunikation oder Massenkommunikation handelt. Doch in Zeiten sozialer Netzwerke hilft diese Einteilung nicht immer weiter. Aus kommunikationswissenschaftlicher Sicht lösen sich im digitalen Raum die Konzepte von Konsumierenden und Produzierenden von Nachrichteninhalten zu sogenannten *Produsers* (aus dem Engl. von *produce* und

---

* Stand April 2020.

1 BGH, Urteil vom 23.06.2009 – VI ZR 196/08, Rn. 38; MMR 2009, S. 612.

2 Vgl. Raschke et al. (2019: S. 3–17).

3 Vgl. Acquisti et al. (2015: S. 509–514).

use) auf.[4] Eine passive Leserin eines Online-Mediums kann zu einer aktiven Verteilerin dieser Inhalte auf sozialen Netzwerken werden. Daher ist es unmöglich, Kommunikation im Internet eindeutig der Individualkommunikation oder der Massenkommunikation zuzuordnen.

Welche Rolle Anonymität für Selbstbestimmung und Verantwortung in digitalen Kontexten spielt, ist seit jeher umstritten. Zum einen handelt es sich um einen sehr abstrakten, auslegungsbedürftigen Begriff. Zum anderen ist die Bedeutung von Anonymität dem gesellschaftlichen Wandel unterworfen. Ob und wie weit Anonymität zu schützen ist, beurteilt die Gesellschaft insbesondere anhand von gegenwärtigen Ereignissen. So stieß beispielsweise in der Zeit nach den Grausamkeiten des Dritten Reichs die Beibehaltung der Fingerabdrücke auf Personalausweisen auf einhellige Ablehnung.[5] In der Zeit nach den Terroranschlägen in den USA vom 11. September 2001 ging die öffentliche Debatte in eine andere Richtung: Das *Recht auf informationelle Selbstbestimmung* sei nicht der Regelfall; die *Informationsfreiheit* sei die Grundlage der Kommunikation – verstanden in dem Sinne, dass die Informationsbeschränkung der Rechtfertigung bedürfe, da sie bei der Informationssystemgestaltung die Belange des Systembetreibers vernachlässigen würde.[6]

Die beiden Phänomene, die bei der derzeitigen Diskussion um Anonymität im Internet am relevantesten erscheinen, weil sie in diesem Zusammenhang immer wieder diskutiert werden, bilden einen Gegensatz. Der sogenannte *Cambridge-Analytica-Skandal* hat der Gesellschaft vor Augen geführt, dass wir uns auf sozialen Netzwerken nicht unbeobachtet bewegen – mithin nicht großartig anonym. So suggerierten die Versprechungen Cambridge Analyticas eine gläserne Userin, die im Internet gezielt angesprochen und beeinflusst werden könne[7] – insofern das absolute Gegenteil zur Vorstellung der anonymen Internetnutzenden aus dem Eingangszitat des Bundesgerichtshofs in seiner *Spickmich*-Entscheidung. Trotzdem würde – so eine häufig geäußerte Befürchtung – die Kommunikation auf sozialen Netzwerken aufgrund von Anonymität verrohen, was z. B. die Debatte um Hatespeech zeigt.[8] Anonymität im Internet würde demnach als Brandbe-

4 Vgl. Bruns (2009).
5 Vgl. Denninger (2003: S. 43), mit Verweis auf Dürig (1958). In: Maunz/Dürig, GG, Art. 1 Abs. l Rn. 37.
6 Vgl. Denninger (2003: S. 47), mit Verweis auf Aulehner (1998: S. 302, S. 487, S. 567).
7 Vgl. Gräfe, PinG 2019, 5 (8).
8 Vgl. von Kempis (24.10.2018).

schleuniger für Persönlichkeitsrechtsverletzungen dienen.[9] Daher werden in der Politik immer wieder De-Anonymisierungen und weitere Befugnisse zur Überwachung gefordert und umgesetzt, z. B. beim Ruf nach Vorratsdatenspeicherung oder der letzten Novelle des *Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten* (BKA-Gesetz).[10]

Außerdem zeigen verschiedene Online-Phänomene, dass Anonymität im Internet eine Bedrohung für den demokratisch-liberalen Diskurs darstellen kann: Politische Akteure bedienen sich dubioser Online-Kommunikationsmethoden, z. B. gefälschter Nachrichtenwebseiten, Social Bots oder Trollen, um auf illegitime Weise politisch werben zu können oder Falschinformationen in Umlauf zu bringen.[11] Trolle können einen sinnhaften Meinungsaustausch verhindern und unter Pseudonym gezielt Hatespeech verbreiten, um den demokratischen Diskurs zu stören oder ganz zu verhindern.[12] Zumindest besteht die Furcht, dass es so sein könnte.[13]

Dem entgegen steht, dass das anonyme Surfen ebenso als fördernd für die Gesellschaft angesehen werden kann, da es in der Lage ist, die Privatheit der Bürgerinnen zu stärken.[14] Darüber hinaus kann durch anonymes Teilen von Inhalten im Internet der normativ-deliberative, gesellschaftliche Diskurs gestärkt werden. Im Deckmantel des Schutzes der eigenen Persönlichkeit können Meinungen freier – oder überhaupt erst – artikuliert und wahrgenommen werden.[15] In solchen Fällen kann Anonymität Benachteiligte schützen, z. B. können sich Opfer von Straftaten anonym beraten und helfen lassen[16] oder psychisch belastete Patientinnen können sich vernetzen.[17] Auch das Hinweisgeben bei strukturellem Fehlverhalten (sogenanntes *Whistleblowing*) wird erleichtert, wenn Whistleblowerinnen anonymisiert in Aktion treten können, wenn es nicht sogar erst durch Anonymität ermöglicht wird.[18] All diese Punkte sind wichtig für eine funktionierende Demokratie, um beispielsweise vorhandene gesellschaftliche Missstände aufzudecken – wie im Rahmen der sogenannten *Panama Pa-*

9 Vgl. Palzer, AfP 2017, 199 (200) mit weiteren Nachweisen.
10 Vgl. Bäcker (08.06.2017).
11 Vgl. Hamm/Gräfe (07.05.2019).
12 Vgl. Aro (2016).
13 Vgl. Janisch (09.10.2019).
14 Vgl. Rost, DuD 2003, S. 155.
15 Vgl. entspr. OLG Hamm, Urteil vom 03.08.2011 – I-3 U 196/10.
16 Vgl. z. B. anonyme Online-Beratung des Weißer Ring e.V.
17 Vgl. Kang (2017).
18 Vgl. Santoro/Kumar (2018: S. 41).

pers[19] – oder um Themen enttabuisieren zu können sowie um die Medien als sogenannte *vierte Gewalt* zu stärken und investigativen Journalismus zu ermöglichen. Aus kommunikationswissenschaftlicher Sicht ist es unmöglich, festzumachen, ob anonyme Internetnutzende nach demokratieförderlichen oder -bedrohenden Motiven handeln, da eine solche Bewertung nie pauschal, sondern nur im Einzelfall erfolgen kann.

Der Beitrag möchte die angesprochenen und weitere Probleme im Zusammenhang mit passiver und aktiver anonymer Nutzung des Internets darstellen, bewerten und zu weiteren Überlegungen anregen. Neben der allgemeinen grundrechtlichen Einordnung sollen vor allem einzelne Phänomene im Zusammenhang mit anonymer Internetnutzung aufgegriffen werden. Aus kommunikationswissenschaftlicher Perspektive wird dabei zu fragen sein, welche Vor- und Nachteile in anonymer Online-Kommunikation liegen bzw. welche Veränderungen damit einhergehen. Aus rechtlicher Sicht ergibt sich die Frage, wie die gegensätzlichen Interessen in Kommunikationsumgebungen zu gewichten sein werden. Dabei geht es ausdrücklich nicht nur um rechtliche Perspektiven zum Schutz personenbezogener Daten, sondern allgemeiner darum, wie sich Anonymität in das für das Medienrecht typische Spannungsfeld zwischen Meinungsfreiheit und Persönlichkeitsschutz einordnen lässt. Die Bewertung der Einzelfragen lässt einen Rückschluss auf die allgemeine Frage zu: Wie steht es derzeit um ein Grundrecht auf Anonymität im Internet?

2. *Anonymität aus kommunikations- und rechtswissenschaftlicher Perspektive*

Das Thema Anonymität im Internet soll zunächst aus beiden genannten Perspektiven beleuchtet werden. So lassen sich interdisziplinäre Rückschlüsse ziehen und Ansätze finden, wie Online-Anonymität rechtlich und gesellschaftlich bewertet werden muss. Betrachtet werden einzelne Online-Phänomene wie die Nutzung von Medienintermediären wie sozialen Netzwerken. Obwohl der Fokus also auf Online-Umgebungen liegt, lässt sich Anonymität im Internet nicht unter Ausschluss der Auswirkungen auf die sinnlich erfassbare, reale Welt betrachten. Gerade bei der Betrachtung von Kommunikation und der ihr zugrunde liegenden Kommunikationsfreiheiten besteht keine trennscharfe Linie zwischen Online- und realer Welt. Die Vorstellung eines sogenannten *digitalen Dualismus*, also der Trennung von

19 Vgl. Obermayer et al. (o. J.).

Realität und Medialität,[20] würde die Betrachtung verfälschen, da vielfältige Verflechtungen zwischen beiden Sphären bestehen.

2.1 Kommunikationswissenschaftlicher Hintergrund von Anonymität

Aus kommunikationswissenschaftlicher Sicht muss Anonymität immer situativ und im jeweiligen Kontext betrachtet werden. Im Folgenden wird exemplarisch erklärt, wie sich Anonymität auf investigativen Journalismus und Aggressivität in sozialen Netzwerken auswirken kann. Darüber hinaus muss zwischen einer vertikalen und horizontalen Anonymität unterschieden werden, um eine weitere Bewertung vornehmen zu können.

2.1.1 Investigativer Journalismus

Anonymität spielt eine wichtige Rolle für den investigativen Journalismus. Die Aufdeckung von Missständen erfolgt meist unter der Voraussetzung, dass Hinweisgebende dem Quellenschutz unterliegen und nicht öffentlich identifiziert werden können. Denn Journalistinnen haben als sogenannte *Berufsgeheimnisträgerinnen* gem. § 53 Abs. 1 Nr. 5 Strafprozessordnung (StPO) das Recht, vor Gericht und den Strafverfolgungsbehörden ihre Quellen nicht offenlegen zu müssen. Dieses Recht auf Quellenschutz leitet sich aus der *Medienfreiheit* des Art. 5 Abs. 1 GG ab und ist in Ziffer 5 des Pressekodex spezifiziert: „Die Presse wahrt das Berufsgeheimnis, macht vom Zeugnisverweigerungsrecht Gebrauch und gibt Informantinnen ohne deren ausdrückliche Zustimmung nicht preis. Die vereinbarte Vertraulichkeit ist grundsätzlich zu wahren." Obwohl Informantinnen sich mitunter rechtswidrig verhalten, wenn sie den Medien Informationen zukommen lassen, erleichtern sie den Medien, ihrem normativen Auftrag als *vierte Gewalt* im Staat nachzukommen, welche die anderen drei Gewalten öffentlichkeitswirksam überwacht. Der Quellenschutz und die somit intentional gewahrte Anonymität kann folglich als wichtiger Bestandteil für die aufklärerische Pressearbeit gesehen werden. Auch der Europäische Gerichtshof für Menschenrechte (EGMR) betrachtet den Schutz journalistischer Quellen als Grundvoraussetzung der *Pressefreiheit* nach Art. 10 EMRK.[21]

20 Vgl. Ebner (15.10.2019).
21 Vgl. EGMR, Urteil vom 27.03.1996 – 17488/90 (Goodwin/UK).

2.1.2 Aggressives Verhalten in sozialen Netzwerken

In sozialen Medien können Menschen ihre öffentlich sichtbare Identität auf eigenen Wunsch verbergen oder ändern. Die bestehende Literatur über das Online-Verhalten geht davon aus, dass eine auf diese Weise hergestellte Pseudonymität[22] einer der Hauptfaktoren ist, der soziale Zurückhaltungen, wie beispielsweise Höflichkeit, aufhebt und zur Ansprache tabuisierter Themen oder Einnahme von scheinbaren Minderheitenmeinungen führt.[23] Im Allgemeinen erzeugt Anonymität das Phänomen des/der sogenannten *Fremden im Zug*, bei dem Menschen spontan persönliche Selbstauskünfte mitteilen.[24] Da sie kein Wiedersehen mit diesen Personen erwarten würden, haben sie keine Angst vor Risiken oder Konsequenzen, die sich aus dem Gesagten ergeben könnten.

Unter Online-Aggression versteht man demgegenüber ein irrationales und illegitimes Verhalten, das durch zugrundeliegende Persönlichkeitsmerkmale wie mangelndes Einfühlungsvermögen und fehlende soziale Fähigkeiten, Narzissmus, Impulsivität, Gefühlssucht, emotionale Regulationsprobleme oder psychologische Symptome wie Einsamkeit, Depression und Angst verursacht wird.[25] Da Online-Aggression scheinbar von niederen Antrieben geleitet wird, liegt die Vermutung nahe, Menschen würden sich schämen, unter ihrem richtigen Namen derart aggressiv aufzutreten. Die empirischen Beweise für einen solchen Zusammenhang sind jedoch knapp und es wurde bisher kein eindeutiger Ursache-Wirkungs-Bezug zwischen Anonymität und Aggression nachgewiesen.[26] Im Gegenteil fand die Studie von Rost et al. (2016) heraus, dass nicht-anonyme Nutzerinnen, die also mit ihrem Klarnamen agierten, deutlich aggressiver auftraten als anonyme Nutzerinnen. Auch offline gibt es Beispiele dafür, dass vollständig identifizierbare Menschen aggressiv öffentlich auftreten. Besonders hervorzuheben ist ein Beitrag aus der Sendung *Kontraste* vom 4. Juli 2019, in welchem Pegida-Demonstrationsteilnehmende vor laufender Kamera entsetz-

22 Zur Unterscheidung von Anonymität, Pseudonymität und deren Rückverfolgbarkeit vgl. Froomkin (1995).
23 Vgl. Hollenbaugh/Everett (2013); Moore et al. (2012); Suler (2004).
24 Vgl. Bargh et al. (2002: S. 35). Siehe hier vor allem Simmels „Exkurs über den Fremden". Vgl. Simmel (1908: S. 509–512).
25 Vgl. Rost et al. (2016: S. 2).
26 Vgl. Ebd.

liche Ansichten mitteilen[27], scheinbar ohne sich über ihre Identifizierbarkeit oder über spätere Konsequenzen ihrer Äußerungen zu sorgen.[28]

2.1.3 Vertikale und horizontale Anonymität

Bei der Bewertung des angenommenen schleichenden Abbaus von Anonymität im Netz ist es hilfreich, zwischen horizontaler und vertikaler Anonymität zu unterscheiden.[29] Horizontale Anonymität bezieht sich auf unpersönliche Nahbeziehungen sowie auf das Vorhandensein vieler öffentlicher Räume. Man kann sie als Nicht-Identifizierbarkeit zwischen *Peers*[30] verstehen, z. B. unter anonymen Reisenden an Bahnhöfen, anonymen Besucherinnen in Konzerthallen oder unter Nutzenden sozialer Netzwerke. Horizontale Anonymität ist eher schwach ausgeprägt in kleinen Gemeinden oder Netzwerken, in denen sich alle kennen, und stark ausgeprägt in modernen Millionenstädten.

Vertikale Anonymität hingegen benennt die Nicht-Identifizierbarkeit von Individuen durch höhere Instanzen wie private wirtschaftliche Akteure oder Staaten. Vertikale Anonymität besteht beispielsweise nicht, wenn Konzertorganisationen ihre Besucherinnen über personalisierte oder gar RFID-unterstützende[31] Tickets am Einlass oder während des ganzen Konzertbesuchs nachverfolgen können. Sie besteht auch nicht, wenn Nutzende sozialer Netzwerke (potenziell) jederzeit durch die Plattformbetreiber identifiziert werden können, was insbesondere bei vorgeschriebener Klarnamenregistrierung gilt.

In den meisten Online-Situationen ist vertikale Anonymität aufgelöst, und zwar durch Login-Verfahren und Registrierungen oder indirekte Identifizierbarkeit basierend auf Big Data und Metadaten.[32] Dennoch ist durch das Surfen unter Pseudonym eine relative horizontale Anonymität ge-

27 Befragte werden zum Mordfall Walter Lübke befragt und schätzen die Tat u. a. als ‚normal' und ‚menschliche Reaktion' ein.
28 Vgl. mja/dpa (05.07.2019).
29 Vgl. Thiel (2016: S. 14 f.).
30 Von engl. *peer*: Ebenbürtiger, Gleichgestellter oder -altriger.
31 Die Radiofrequenz-Identifikation (RFID) nutzt elektromagnetische Felder, um an Objekten angebrachte Tags automatisch zu identifizieren und zu verfolgen. Da RFID-Etiketten an Bargeld, Kleidung und Besitztümern angebracht oder Tieren und Menschen implantiert werden können, wirft die damit gegebene Möglichkeit des Auslesens personengebundener Informationen ohne Zustimmung ernsthafte Bedenken hinsichtlich des Datenschutzes auf.
32 Vgl. Sarunski, DuD 2016, 424 (424 f.).

währt, die verhindert, dass Nutzende von ihren *Peers* identifiziert werden können.

Horizontale Anonymität mag in vielen Situationen ausreichend sein, wenn es darum geht, eine pluralistische Online-Diskussion zu erhalten. Jedoch ist sie gewiss nicht ausreichend, wenn es um demokratische Korrekturprozesse geht. Insbesondere investigativer Journalismus und der inbegriffene Quellenschutz sowie Whistleblowing richten sich gegen höhere Instanzen, seien es private Akteure oder Staaten. Durch das hohe Risiko für die Beteiligten führt eine vollständige und manifestierte Auflösung der vertikalen Anonymität letztendlich dazu, dass Kommunikationsräume im Internet nicht mehr für diese demokratieerhaltenden Maßnahmen zur Verfügung stehen.[33]

Allerdings muss festgehalten werden, dass Nutzerinnen im Online-Bereich kaum mehr selbstbestimmt entscheiden können, anonym in Erscheinung zu treten. Der „digitale Strukturwandel von Öffentlichkeit“[34] hat in der näheren Vergangenheit zu einer kontinuierlichen Reduktion von vertikaler Anonymität im Internet geführt und tut dies auch weiterhin. Durch computervermittelte Prozesse werden zahlreiche Datenspuren hinterlassen, die eine (verzögerte) Identifikation der handelnden Akteure erleichtern.[35] Über diese Tatsache scheinen sich Internetnutzende in vielen Fällen von Web-Tracking durch Metadaten jedoch gar nicht bewusst zu sein.[36]

2.2 Rechtliche Einordnung von Anonymität

Der juristische Ansatz „Anonymität ist kein Wert an sich“[37] erscheint nach Betrachtung der oben genannten Erkenntnisse aus der Kommunikationswissenschaft also zunächst zutreffend. Jedoch ist Anonymität in bestimmten Kontexten die Voraussetzung für wertvolle und schützenswerte Mechanismen demokratischer Gesellschaften. Um die verschiedenen Probleme rund um die anonyme Nutzung des Internets und sozialer Netzwerke zu betrachten, ist zunächst eine verfassungsrechtliche Einordnung vonnöten. Bei der Nutzung des Internets spielen dann vor allem einfachgesetzliche,

33 Diese Bewertung gilt für das konventionelle Internet. Wie es sich bei dem Einsatz von identitätsverschleiernden Technologien verhält (z. B. dem TOR-Netzwerk), wird in Abschnitt 3.3 erläutert.
34 Thiel (2016: S. 9 f.).
35 Vgl. entspr. Sarunski, DuD 2016, 424 (424 f.).
36 Vgl. Thode et al. (2015: S. 445–456).
37 Hornung/Wagner, CR 2019, 565 (566).

europarechtlich geprägte sowie von Medienintermediären gesetzte Normen eine Rolle. Außerdem muss im Hinterkopf behalten werden, dass das juristische Verständnis von Horizontalität und Vertikalität ein anderes ist, als soeben kommunikationswissenschaftlich dargestellt. Danach gilt, sehr grob vereinfacht, eine Über- und Unterordnung – mithin Vertikalität – nach der sogenannten *modifizierten Subjektstheorie*[38] im öffentlichen Recht, während wir im Privatrecht von einer Gleichordnung der Rechtssubjekte sprechen. Die Privatautonomie wird qua Gesetz nur dort eingeschränkt, wo wir durch gestörte Machtverhältnisse ein zu großes Abweichen von diesem Gleichordnungsgedanken ausmachen.[39]

2.2.1 Verfassungsrechtliche Einordnung

Ein Grundrecht auf Anonymität im Internet findet sich im Grundgesetzkatalog nicht. Auch ist es vom Bundesverfassungsgericht noch nicht explizit festgestellt worden. Allerdings hängt die anonyme Nutzung des Internets mit mehreren ausdrücklich genannten bzw. anerkannten Grundrechtspositionen – je nach Fallgestaltung – eng zusammen. Infrage kommen insbesondere das Grundrecht auf *informationelle Selbstbestimmung*, welches als Teil des *Allgemeinen Persönlichkeitsrechts* aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG abgeleitet wird,[40] das Grundrecht auf *Meinungs- und Informationsfreiheit* aus Art. 5 Abs. 1 S. 1 GG und das Grundrecht auf *Versammlungsfreiheit* aus Art. 8 Abs. 1 GG.[41]

---

38 Die modifizierte Subjektstheorie prägt die juristische Lehre bei der Bestimmung, ob ein Rechtsverhältnis öffentlich-rechtlicher oder privatrechtlicher Natur ist. Eigentlich ist sie gerade eine Abkehr von der sogenannten Subordinationslehre, die von einem Unterordnungsverhältnis der Bürgerinnen gegenüber dem Staat ausgeht. Allerdings gesteht auch die modifizierte Subjektstheorie Trägern hoheitlicher Gewalt Durchgriffsrechte gegenüber Bürgerinnen zu, wenn und soweit sie sich im Rahmen ihrer hoheitlichen Befugnisse bewegen. Insofern ist es zu sehr vereinfacht, von einer generellen Unterordnung der Bürgerinnen unter den Staat im Sinne der Subordinationstheorie zu sprechen. Im Rahmen der freiheitlich demokratisch gestalteten Rechtsordnung ist der Staat in konkret geregelten Verhältnissen aber doch berechtigt, ‚von oben' durchzugreifen; zur Vertiefung s. Papier (2019). In: Maunz/Dürig, GG, Art. 34, Rn. 126–131 mit weiteren Nachweisen.

39 So etwa im Verbraucherschutz- oder Arbeitsrecht.

40 Vgl. BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 (Volkszählung), BVerfGE 65, 1.

41 Die ebenfalls zu beachtenden Art. 10 und 13 GG und das aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG abgeleitete Grundrecht auf *Gewährleis-*

Das Recht auf anonymes Surfen wird von einem Teil der Literatur vor allem aus dem *allgemeinen Persönlichkeitsrecht (APR)* abgeleitet.[42] Das *APR* schützt Einzelne gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten. Dieses Grundrecht auf *informationelle Selbstbestimmung* gewährleistet insoweit die Befugnis Einzelner, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen. In Bezug auf Anonymität ergibt *informationelle Selbstbestimmung* nur Sinn, wenn sie dahingehend ausgeübt werden kann, dass gar keine Daten offenbart werden, auch nicht die Identitätsdaten.[43] Wenn die einzelne Person entscheiden darf, welche Informationen über sie bekannt sein dürfen, dann muss sie auch das Recht haben, dass keine Informationen über sie bekannt sein sollen.

Die aus dem *APR* abgeleitete Anonymität unterliegt damit den Einschränkungen des Art. 2 Abs. 2 S. 3 GG. Sie kann durch Gesetz eingeschränkt werden, aber natürlich nur im Rahmen der sogenannten *Wechselwirkungslehre*.[44] Danach kann ein Gesetz zwar die Anonymität begrenzen, muss seinerseits aber im freiheitlich demokratischen Staat so ausgelegt werden, dass das *APR* möglichst weit reicht.[45] Die grundlegende Bedeutung der Anonymität als Ausprägung des *APR* begrenzt also ihrerseits ein einschränkendes Gesetz. Wer anonym bleiben möchte, kann sich grundsätzlich auf Art. 2 Abs. 1 GG berufen und es ist Sache der ‚anderen Seite', die Schranken dieses Rechts darzutun.[46]

Nun sind speziell die Freiheitsgrundrechte in ihrer Urkonstruktion Abwehrrechte gegen den Staat, wirken also in vertikaler Ebene. Zwischen Privaten – juristisch betrachtet also in horizontaler Ebene – wirken sie nach herrschender Meinung nur mittelbar und nicht direkt. Das bedeutet, dass die Grundrechte gegenüber Privaten vor allem in der Auslegung allgemeiner Gesetze eine Rolle spielen und insbesondere über die sogenannten *Generalklauseln* wirken. Das wiederum heißt, dass gegenüber Medienintermediären nicht ohne weiteres ein Grundrecht auf Anonymität geltend gemacht werden könnte. Wohl aber kommt es, wie grundsätzlich alle Grundrechte, z. B. bei Uneinigkeit über Nutzungsbedingungen, bei der

---

tung der Vertraulichkeit und Integrität informationstechnischer Systeme werden aus Gründen der Stringenz hier nicht betrachtet.

42 Vgl. so Denninger (2003: S. 50); Kersten, JuS 2017, 193 (195) mit weiteren Nachweisen.

43 Vgl. Bäumler (2003: S. 5).

44 Vgl. Grabenwarter (2019). In: Maunz/Dürig, GG, Art. 5, Rn. 139–147.

45 Vgl. St. RSpr. d. BVerfG seit BVerfG, Urt. v. 15.01.1958 – 1 BvR 400/51 (Lüth).

46 Vgl. Bäumler (2003: S. 5).

Heranziehung der gesetzlichen Regelungen zur Geltung. Hier ist als erstes an das AGB-Recht zu denken. Über §§ 305 Abs. 2, 305 c Abs. 1, 306 Abs. 2, 3, 307 Abs. 1 BGB als Einfallstore für die Wertvorstellungen des Grundgesetzes lässt sich sicherlich diskutieren. § 307 Abs. 1 S. 1 BGB ist inhaltsgleich mit dem alten § 9 Abs. 1 AGB-Gesetz, der die Überschrift ‚Generalklausel' trug. Auch wenn amtliche Überschriften für das BGB erst nach Art. 1 Abs. 2 des Schuldrechtsmodernisierungsgesetzes endgültig eingeführt wurden und § 307 Abs. 1 BGB die amtliche Überschrift ‚Inhaltskontrolle' trägt, mittelt er doch Grundrechtswirkung.[47]

Bei *mittelbarer Drittwirkung* bleibt es aber nicht. Schließlich entfließt das *APR* nicht nur Art. 2 Abs. 1 GG, sondern auch der unveräußerlichen *Menschenwürde* des Art. 1 Abs. 1 GG. Die Menschwürde prägt das deutsche Grundgesetz und ist von der *Ewigkeitsgarantie* des Art. 79 Abs. 3 GG umfasst. Ewigkeit steht dabei für die Bestehensdauer des Grundgesetzes an sich.

> Die Menschenwürde verwirft jede selbstzweckhafte Überhöhung des staatlichen Herrschaftsverbandes und wurde anerkannt als *oberstes Konstitutionsprinzip* der Rechtsordnung (Wintrich), als *Staatsfundamentalnorm* (Nawiasky), als *höchster Rechtswert* (Nipperdey) und als *Wurzel aller Grundrechte* (Isensee).[48]

Insofern bildet Art. 1 Abs. 1 GG das über allem stehende Super-Grundrecht, wohingegen ein Super-Grundrecht auf Sicherheit nicht existiert.[49] Die Anonymität ist also einerseits als Ausprägung des *APR* besonders schützenswert und wird andererseits in Zeiten von privaten informationsmittelnden wie -sammelnden Medienintermediären ausgehöhlt. Aufgrund des Menschenwürde-Kernes muss der Gesetzgeber – auch auf Kosten grundrechtlich verbürgter Rechte Dritter – das *APR* im Wege einfachgesetzlicher Ausgestaltung schützen, gerade wenn sich der Staat aus wichtigen Feldern der Gesellschaft zurückzieht und der Wirtschaft vergleichsweise weiten Entfaltungsraum lässt.[50]

---

47 Vgl. Art. 1 Abs. 2 sowie Anlage zu Art. 1 Abs. 2 des Gesetzes zur Modernisierung des Schuldrechts vom 26.11.01 (Bundesgesetzblatt Jahrgang 2001 Teil I Nr. 61, ausgegeben zu Bonn am 29.11.2001, S. 3170, S. 3189).

48 Herdegen (2019). In: Maunz/Dürig, GG, Art. 1, Rn. 1 und Rn. 4 mit weiteren Nachweisen (Herv. i. Orig.).

49 Ablehnend ebenfalls Papier, NJW 2017, 3025 (3030).

50 Vgl. Di Fabio (2019). In: Maunz/Dürig, GG, Art. 2 Abs. 1, Rn. 135; siehe ebenso Kap. 2.2.2.

Nach anderer Auffassung folgt der Grundsatz der Anonymität im Internet vor allem aus der *Meinungsfreiheit*.[51] Der Bundesgerichtshof sieht in seiner *Spickmich*-Entscheidung die aktive, anonyme Nutzung einer Bewertungsplattform als von der *Meinungsäußerungsfreiheit* umfasst an:

> Die anonyme Nutzung ist dem Internet immanent. […]. Eine Beschränkung der Meinungsäußerungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugeordnet werden können, ist mit Art. 5 Abs. 1 S. 1 GG nicht vereinbar. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde […] die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegengewirkt werden.[52]

Soweit es demnach um die aktive – aber anonyme – Teilnahme an Online-Kommunikation gehe, gerate der Persönlichkeitskern der *Kommunikationsgrundrechte* ins Blickfeld. Die grundrechtlich geschützte Meinungsfreiheit als unmittelbarster Ausdruck der menschlichen Persönlichkeit in der Gesellschaft verleihe den Einzelnen das Recht, autonom darüber zu entscheiden, ob sie ihre Identität in der Kommunikation zu erkennen geben.[53] Nach Gersdorf müsse aber für die Frage, welchem Grundrecht die passive Nutzung des Internets (anonymes Surfen, Versand bzw. Empfang anonymer bzw. pseudonymer Mails etc.) unterliegt, zwischen Individualkommunikation und Massenkommunikation unterschieden werden:

> Die anonyme bzw. pseudonyme Teilnahme an Individualkommunikation ist Ausdruck des Grundrechts auf informationelle Selbstbestimmung. Demgegenüber ist das Recht, sich in anonymer bzw. pseudonymer Form aus allgemein zugänglichen Quellen zu informieren, also an der Massenkommunikation als Rezipient teilzunehmen (Surfen etc.), Ausdruck der grundrechtlich geschützten Informationsfreiheit […].

---

51 Vgl. Pille, NJW 2018, 3545 (3546); faktische Behinderungen der Anonymität der Rezipierenden unter Art. 5 Abs. 1 GG grundrechtsthematisch anerkennend ebenfalls Denninger (2003: S. 50); Kersten, JuS 2017, 193 (196) mit weiteren Nachweisen.

52 BGH, Urteil vom 23.06.2009 – VI ZR 196/08 (Spickmich), Rn. 38; MMR 2009, S. 512.

53 Vgl. Gersdorf (2019), Informations- und MedienR, Art. 2 GG, Rn. 6 mit Verweis auf BVerfG, Urt. v. 15.01.1958 – 1 BvR 400/51 (Lüth) und BVerfG, Beschl. v. 09.10.1991 – 1 BvR 221/90.

> Allenfalls ergänzend kann insoweit auch auf das Grundrecht auf informationelle Selbstbestimmung zurückgegriffen werden.[54]

Die Informationsfreiheit ist dabei wie die anderen Grundrechte des Art. 5 Abs. 1 GG ein Abwehrrecht. Sie darf insofern nicht derart missdeutet werden, dass sie das Recht beinhaltet, Andere aus der selbstgewählten Anonymität – im Sinne einer absoluten Informationsfreiheit – herauszureißen. Die Unterscheidung zwischen Individual- und Massenkommunikation ist in Fällen von *Produsern* (auf Videoportalen, Blogs etc.) aber nicht immer möglich. Das ändert per se nichts an der von Gersdorf festgestellten Unterscheidung, sondern führt dazu, dass *informationelle Selbstbestimmung* und *Informationsfreiheit* gleichzeitig einschlägig sein müssen.

Nach wie vor hochumstritten ist die Frage, ob sich ein Recht auf Anonymität im Internet aus der *Versammlungsfreiheit* des Art. 8 Abs. 1 GG ableiten lässt.[55] Denn die Möglichkeit, anonym an Versammlungen teilzunehmen, ist besonders schutzwürdig. Eine Identifizierung könnte hier in besonderer Weise von der Ausübung des Grundrechts abschrecken.[56] Dies hat u. a. das OVG Nordrhein-Westfalen bestätigt, indem es entschieden hat, dass Foto-/Videoaufnahmen einer Demonstration und deren anschließende Veröffentlichung in sozialen Netzwerken durch die Polizei unzulässig seien.[57] Erstaunlicherweise wird die einfachgesetzliche Konkretisierung der Friedlichkeit des Art. 8 Abs. 1 GG durch das sogenannte *Vermummungsverbot* gem. § 17a Abs. 2 Bundes-Versammlungsgesetz immer wieder als Argument für die Einführung einer Klarnamenpflicht herangeführt.[58] Es ist sich allerdings vor Augen zu führen, dass dafür erst einmal ein Online-Versammlungsrecht anerkannt werden muss. Im Weiteren müsste das digitale Vermummungsverbot im Sinne des Art. 8 Abs. 1 GG anhand der *Friedlichkeit* ausgelegt werden. Das Ergebnis kann online wie offline nur das sein, dass eine friedliche Vermummung stets zulässig ist.[59]

Zusammenfassend spielt für Anonymität im Internet eben nicht allein Art. 8 Abs. 1 GG eine Rolle, sondern auch das *APR* sowie vor allem *die Meinungs- und Informationsfreiheit*. Selbst bei dem lückenhaften und ober-

---

54 Ebd.

55 Vgl. ausführlich und i. E. bejahend Kersten, JuS 2017, 193 (198); Schloemann (26.9.2019).

56 Vgl. BVerfG, Beschl. v. 17.02.2009 – 1 BvR 2492/08 (Bayerisches Versammlungsgesetz).

57 Vgl. OVG Nordrhein-Westfalen, Urt. v. 17.09.2019 – 15 A 4753/18.

58 Vgl. zuletzt Papier (30.10.2019).

59 Vgl. Kersten, JuS 2017, 193 (199) mit Verweis auf Höfling (2018). In: Maunz/Dürig, GG, Art. 8 Rn. 70 mit weiteren Nachweisen.

flächlich bleibenden Versuch[60] einer verfassungsrechtlichen Einordnung des Begriffs Anonymität fallen zwei Punkte auf:

Anonymität ist eingeordnet in den jeweiligen Kontext zu verstehen und nicht synonym zu *informationeller Selbstbestimmung*. Dies sollte bei jeglicher Debatte über gesetzliche Bestimmungen, die Anonymität regeln, beachtet werden. Das ist insofern wichtig, als dass das Datenschutzrecht personenbezogene Daten ex-ante vor Schäden schützen will, während im Äußerungsrecht typischerweise erst in einer ex-post Abwägung festgestellt wird, ob Grundrechtspositionen geschädigt wurden.

Denn auch der typische Gegensatz medienrechtlicher Sachverhalte und Probleme zwischen den Medienfreiheiten des Art. 5 Abs. 1 GG auf der einen Seite und dem Persönlichkeitsschutz auf der anderen Seite besteht hier so nicht. Vielmehr spielt Anonymität auf beiden Seiten eine große Rolle. Entscheidend für die Beurteilung ist die konkrete Kommunikationssituation im jeweiligen Kontext. So dient Anonymität einerseits gerade dem Persönlichkeitsschutz, wenn negative Konsequenzen durch eine Offenlegung der Person drohen. In der gleichen Situation dient sie der praktischen Ermöglichung der Rezeption von Informationen bei den Empfangenden, also der *Informationsfreiheit*. Anderseits ermöglicht sie gewisse Aussagen erst, dient also primär der *Meinungsäußerungsfreiheit*.

Festzuhalten bleibt, dass es sich um eine grundrechtliche Gemengelage handelt, wenn wir Anonymität verfassungsrechtlich betrachten. Ein absolutes Grundrecht auf Anonymität kann aufgrund der Gegensätzlichkeiten der Schutzbereiche demnach schon gar nicht bestehen. Vielmehr muss es Sache des Gesetzgebers sein, den grundrechtlichen Schutzbereich für Anonymität möglichst weit offen zu halten, um den verschiedenen Grundrechtspositionen größtmögliche Wirkung zu verschaffen und sie dann miteinander in Ausgleich zu bringen. Die Regulierungsfrage kann deshalb nur lauten, wie relative Anonymität gegenüber dem Staat und gegenüber Privaten auszugestalten ist.

2.2.2 Europäisches Recht: EMRK, EU-GRCh, DS-GVO und ePrivacy

Eine Besonderheit der Europäischen Menschrechtskonvention (EMRK) sowie der ihr z. T. nachempfundenen EU-Grundrechtecharta (EU-GRCh) ist, dass Privatheit dort explizit geregelt wird. Art. 8 Abs. 1 EMRK schützt die Achtung des Privat- und Familienlebens, der Wohnung und Korrespon-

60 Eine ausführliche Betrachtung findet sich bei Kersten, JuS 2017, 193.

denz. Art. 7 EU-GRCh regelt, dass jede Person „das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation" hat. Hierin finden sich also gebündelt Schutzgüter, die im deutschen Grundgesetz in verschiedenen Artikeln normiert sind. So regelt Art. 13 GG die *Unverletzlichkeit der Wohnung* und Art. 10 GG schützt das *Post- und Fernmeldegeheimnis*, mithin die Kommunikationsübermittlung. Art. 8 EU-GRCh ist als explizites *Datenschutzgrundrecht* ausformuliert, im Gegensatz zur Herleitung der *informationellen Selbstbestimmung* als Teil des *Allgemeinen Persönlichkeitsrechts* aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Ausgehend von der Idee, dass Privatheit nicht ausschließlich in der eigenen Wohnung stattfindet,[61] kann insofern für Anonymität im Internet wohl zusätzlich auch explizit an Regelungen zum Privatheitsschutz angeknüpft werden. Die *Freiheit der Meinungsäußerung* und *Informationsfreiheit* regelt Art. 11 Abs. 1 EU-GRCh.

Die potenziell unterschiedliche Ableitung eines Rechts auf Anonymität im europäischen Recht ist also ähnlich zum unter Kapitel 2.2.1 Dargestellten, aber noch einmal vielschichtiger. Insbesondere die – wenn auch graduelle und nicht eindeutige – Unterscheidung zwischen Privatheit und *informationeller Selbstbestimmung* taugt allgemein dazu, die derzeitige Debatte um die Schutzgüter des Datenschutzes zu bereichern – ohne den verengenden Blick durch die DS-GVO. Auf sekundärrechtlicher Ebene ist diese Unterscheidung durch die *Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation* (ePrivacy-Richtlinie) ausgedrückt. Die ePrivacy-Richtlinie regelt besondere Schutzpflichten für die Privatheit der Kommunikation auf elektronischem Wege und hat deshalb auch einen eigenen Anwendungsbereich neben der DS-GVO.[62] EPrivacy bedeutet, dass Anbieter nicht nur personenbezogene Daten schützen müssen, sondern auch das Fernmeldegeheimnis.[63] Die ePrivacy-Richtlinie wurde 2009 novelliert (durch Richtlinie 2009/136/EG, seitdem Cookie-Richtlinie genannt) und sollte eigentlich bereits durch die ePrivacy-Verordnung abgelöst und dabei ausgeweitet wer-

61 Zur Sphärentheorie des BVerfG, insb. zur Privatsphäre s. BVerfG, Urt. v. 15.12.1999 – 1 BvR 653/96, BVerfGE 101, 361; vgl. auch Hohmann-Dennhardt, NJW 2006, 545 (546 f.). Eine vertiefte juristische Auseinandersetzung über die Abgrenzung von Privatheit und Öffentlichkeit in Online-Kommunikationsräumen würde hier den Umfang sprengen und muss zukünftigen Publikationen vorbehalten bleiben.

62 Vgl. Art. 95 DS-GVO.

63 Vgl. Assion (08.04.2020: ab 01:17:04).

den.[64] Zu den schon auf europäischer Ebene bestehenden Problemen kommt hinzu, dass es umstritten ist, ob bzw. wie weit die ePrivacy-Richtlinie in deutsches Recht umgesetzt wurde.[65]

Dass ePrivacy mehr als der bloße Schutz personenbezogener Daten ist, erkennt denn auch der EuGH. In seinem Urteil vom 1. Oktober 2019 zum Setzen von Cookies nimmt er Stellung zu Art. 5 Abs. 3 ePrivacy-Richtlinie:

> Es macht insoweit keinen Unterschied, ob es sich bei den im Gerät des Nutzers gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht. Das Unionsrecht soll den Nutzer nämlich vor jedem Eingriff in seine Privatsphäre schützen, insbesondere gegen die Gefahr, dass ‚Hidden Identifiers' oder ähnliche Instrumente in sein Gerät eindringen.[66]

Dies lässt sich sehr verkürzt so interpretieren, dass der Schutz gegen Identifizierung im Internet auch gegenüber anderen Privaten zu gelten habe.[67] Der EuGH stärkt damit das Konzept einer relativen Anonymität als Voraussetzung für Online-Kommunikation.

2.2.3 Klarnamenregistrierung und Recht auf Pseudonym

Die Grenzen und die Ausformung des Rechts auf Anonymität lassen sich an § 13 Abs. 6 Telemediengesetz (TMG) verdeutlichen. Danach müssen Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonymen ermöglichen, soweit dies technisch möglich und zumutbar ist. Die Anbieter dürfen aber von Nutzenden eine Registrierung unter richtigem Namen verlangen, um sie beispielsweise bei Rechtsverstößen identifizieren zu können. Eine sogenannte *Klarnamenregistrierung* ist also zulässig. Soziale Netzwerke hätten also schon jetzt das Potenzial, dafür zu sorgen, dass Verstöße gegen die Rechtsordnung, die pseudonym geschehen, nicht sanktionslos bleiben – auch wenn § 15 Abs. 3 TMG regelt, dass Dienstean-

64 Vgl. zum aktuellen Stand Schleipfer (12.12.2019).

65 Vgl. Engeler/Marosi, CR 2019, 707 (711) mit Verweis auf eine Übersicht über die Literatur bei Rauer/Ettig, ZD 2016, 423 (424).

66 Pressemitteilung Nr. 125/19 d. EuGH zu EuGH, Urt. v. 01.10.2019 – C-673/17 (Planet49).

67 Ob der EuGH mit der Entscheidung ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einführen wollte, bleibt zu diskutieren. Bejahend wohl Assion, Editorial NJW Heft 43/2019; ablehnend wohl Engeler/Marosi, CR 2019, 707 (710).

bieter die pseudonymen Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammenführen dürfen. Für Klarnamenregistrierung und pseudonyme Nutzung würde insofern ein Trennungsgebot mit einem Verbot der Zusammenführung gelten.[68] Ob die datenschutzrechtlichen Vorschriften des Telemediengesetzes seit der Geltung der Datenschutz-Grundverordnung (DS-GVO) nicht mehr angewendet werden können, ist im Detail umstritten.[69] Allerdings ist die Norm im Wesentlichen inhaltsgleich zu § 4 Abs. 6 Teledienstedatenschutzgesetz von 2001 bzw. 1997[70] und somit älter als die ePrivacy Richtlinie von 2002, die die Datenschutz-Richtlinie von 1995 ergänzte. Geändert wurde sie trotz zahlreicher Novellen des TMG nicht. Richtigerweise kann in 13 Abs. 6 TMG also durchaus eine Konkretisierung des alten Grundsatzes der Datensparsamkeit gesehen werden,[71] den auch Art. 5 Abs. 1c DS-GVO vorsieht. Zwar kann es besondere Gründe geben, das Recht auf Pseudonym in einem Online-Dienst aufzuheben. Bei einem allgemein zugänglichen und thematisch unbegrenzten sozialen Netzwerk, das alle Lebensbereiche abbilden will, erscheint das aber sehr abwegig.[72]

3. Problemlagen für Anonymität im Internet

Anonymität wird im Internet insbesondere in zwei Zusammenhängen zum Sündenbock gemacht. Häufig wird angenommen, dass Hatespeech auf sozialen Netzwerken anonym verbreitet würde.[73] Ebenso schnell wirkt die anonyme Infrastruktur des TOR-Netzwerkes suspekt, weil Kriminelle das Netzwerk zum Handel von Drogen, Waffen und noch Schlimmerem verwenden.[74] In diesem Kapitel soll daher ein allgemeiner Blick auf das Spannungsfeld geworfen werden, in welchem über Anonymität diskutiert wird. Anhand der Nutzung sozialer Netzwerke und von TOR wird die Darstellung konkretisiert.

---

68 Vgl. Härting, NJW 2013, 2065 (2067).
69 Insb. sind zwei Verfahren beim OLG München anhängig: OLG München – 18 U 5493/19 Pre; vgl. ZD-Aktuell 2020, 07285.
70 Vgl. Spindler/Schmitz, TMG § 13 Rn. 61.
71 Vgl. Caspar, ZRP 2015, 233 f.
72 Anders auch nicht LG Frankfurt/Main, 03.09.2020 – 2–03 O 282/19 zur Identitätsprüfung: Dort ging es um die Nutzung eines Profils ohne Fake-Check und nicht um pseudonyme Nutzung.
73 Vgl. Froomkin (1995).
74 Vgl. Hanfeld (16.01.2015).

3.1 Das Spannungsfeld

Während Anonymität untereinander im Großstadtleben durchaus normal ist, ist es im Internet genau umgekehrt.[75] Jede Nutzung von *smart devices* kann nachvollzogen werden. Der Unterschied in der subjektiven Empfindung von Anonymität liegt wohl darin begründet, dass die relative Anonymität bspw. in der U-Bahn von jedem nachvollzogen werden kann, während ein Großteil des Bewusstseins für Web-Tracking zu fehlen scheint. Anderenfalls wäre die Aufregung um den Cambridge Analytica-Skandal nicht so groß gewesen. Schließlich behauptete der Dienst, persönliches Verhalten aufgrund online gesammelter Daten vorhersagen zu können, er versprach sogenannte *Predictive Behavioural Analytics*.[76]

Wenn ein Bewusstsein für die vorhandene oder fehlende Anonymität vorhanden ist, lässt sich die Anonymitätsproblematik nur im Zusammenhang mit einer Zurechnungs- oder Nichtzurechnungsproblematik von Verhalten verstehen: Jede ausdifferenzierte Gesellschaft hat nach Denninger einen funktionsspezifischen Bedarf an Zurechnung, aber auch an Nichtzurechnung. Werde erstere mit Hilfe von Kategorien wie *Kompetenz* und *Verantwortlichkeit* gesteuert, so könne letztere durch die Institutionalisierung von relativer Anonymität befriedigt und wirksam erhalten werden.[77] Das bedeutet, dass es entscheidend ist, wer Anonymität bzw. Pseudonymität aufheben kann und/oder darf. Das Spannungsfeld liegt damit nicht zwischen den Extremen absoluter Anonymität – vertikal gegenüber dem Staat und horizontal gegenüber den Mitmenschen und Unternehmen – auf der einen Seite und Totalüberwachung auf der anderen Seite, sondern darin, wie wir eine relativ anonyme Nutzung des Internets im liberalen Grundrechtsstaat kontinentaleuropäischer Prägung des frühen 21. Jahrhunderts verstehen und inwieweit sie gewährleistet und umgesetzt werden muss. Deshalb müssen wir uns die Fragen stellen: Wem geben wir die Kompetenz, relative Anonymität aufzuheben, um Verantwortlichkeit zu gewährleisten? Geben wir überhaupt jemandem die Kompetenz, Anonymität aufzuheben?

75 S. Kap. 2.1.3.
76 Vgl. Hindman (30.03.2018).
77 Vgl. Denninger (2003: S. 43).

3.2 Soziale Medien

Soziale Netzwerke haben die Art, wie wir kommunizieren, verändert. Der Philosoph Julian Nida-Rümelin nimmt an, dass durch die jetzige Gestaltung digitaler Medienintermediäre die drei allgemeinen Grundvoraussetzungen von Kommunikation wie Wahrhaftigkeit, Vertrauen und Realitätsbezug gefährdet seien.[78] Er führt dies darauf zurück, dass soziale Netzwerke anhand ökonomischer, aus dem Marketing stammender Kriterien gestaltet sind. Und in der Tat erleben wir eine Veränderung des Diskurses und diskutieren in Bezug auf Online-Kommunikationskanäle über dubiose Mittel wie Trolling, Fake News, Bots und nicht zuletzt über die Zunahme von Hatespeech. Es wird dabei wie folgt argumentiert: Durch Anonymität geförderte Verrohung sei unbestreitbar![79] Die Lösung für diese Probleme sehen manche – in unangebrachter Verengung des Problems – in der Einführung einer Klarnamenpflicht, die in der netzpolitischen Debatte einem ‚Stehaufmännchen' gleicht.[80]

3.2.1 Verrohung durch Anonymität?

Dass Anonymität automatisch zu einer Verrohung oder zu unsozialem Verhalten führt, ist eine populäre, aber keinesfalls empirisch belegte Vermutung. Denn Anonymität kann auch soziales Verhalten fördern.[81] Chui argumentiert, dass die Denkweise ‚Verrohung durch Anonymität' zu simpel sei, da sie einzelne Zusammenhänge nicht ausreichend berücksichtige.[82] Anonymität allein reiche nicht aus, um unsoziales Verhalten hervorzurufen: Dies erfordere bereits die Motivation, unsozial zu handeln. Eine solche Motivation, unsoziales Verhalten an den Tag zu legen, beinhalte wiederum vielschichtige Motive, die sich sowohl auf die eigene Person (z. B. sozioökonomische Hintergründe und den Grad der Wertschätzung der Anonymität) als auch auf andere Personen beziehen (z. B. Gruppennormen). Diesbezüglich wurden weitere Faktoren herausgearbeitet, die das Auftreten von unsozialem Verhalten beeinflussen:

78 Vgl. Nida-Rümelin (23.10.2019); vgl. auch die Grundvoraussetzungen von Kommunikation nach Habermas (1981).
79 Vgl. Pille, NJW 2018, 3545 (3546).
80 Vgl. Schwander, ZRP 2019, 207 (207).
81 Vgl. Kang (2017).
82 Vgl. Chui (2014).

- der gewählte Medienkanal (z. B. Spiele, Foren, virtuelle Welten, Chatrooms),
- das Vorhandensein weiterer Motivationen (politisch und soziologisch), und
- der Grad der Anonymität durch den Medienkanal.[83]

All diese Faktoren, zusammen mit den individuellen Merkmalen einer Person, beeinflussen die Art und Weise, wie Anonymität von dieser Person wahrgenommen und ob sie sozial oder unsozial genutzt wird.[84]

Auch von der Empfängerseite der Kommunikation her betrachtet, lassen sich empirisch keine klaren Zusammenhänge belegen. Graf et. al. haben sich gefragt, ob anonyme unzivilisierte[85] Kommentare die gleiche Wirkung haben wie nicht-anonyme unzivilisierte Kommentare, und wie sich das Vorhandensein oder Fehlen von Anonymität auf die Wahrnehmung durch das Publikum auswirkt (sowohl bei demokratischen als auch antidemokratischen Inhalten). Im Rahmen eines Experiments mit 170 Personen wurde herausgefunden, dass Teilnehmende, die unzivilisierten Kommentaren ausgesetzt waren, die Kommentierenden weniger positiv sahen und gleichzeitig den Informationen im Kommentar weniger Vertrauen entgegenbrachten. Die Anonymität der Kommentierenden hatte jedoch keinen Einfluss auf das Interesse der Lesenden an der Diskussion, ihren Zuspruch gegenüber den Kommentaren oder den Kommentierenden und auf ihr Vertrauen in die enthaltenen Informationen. Lediglich die (Un-)Zivilisiertheit der Kommentare – unabhängig von ihrer Anonymität – hat die Gesamtwahrnehmung der Teilnehmenden über den Inhalt der Online-Diskussion beeinflusst. Die Autoren kommen zu dem Schluss, dass Online-Medien aktuell über die möglichen Auswirkungen unzivilisierter Online-Kommentare auf den größeren öffentlichen Diskurs oder auf die Verbreitung von Informationen zu sehr besorgt sein könnten.[86]

Sowohl die Studie von Chui als auch die Studie von Graf et. al zeigen folglich, dass es zu vereinfacht ist, kausal von Anonymität auf eine Verrohung der Kommunikation (wie unsoziales Verhalten oder unzivilisierte Kommentare) zu schließen. Im Gegenteil: Es konnte gezeigt werden, dass unzivilisierten Kommentaren weniger vertraut wird und dass andere per-

83 Vgl. ebd.
84 Vgl. ebd.
85 „We operationalized civil and uncivil treatment levels with the inclusion or exclusion of name calling, aspersions, using synonyms for lying directed at someone, vulgarities, and pejorative words for speech“ (Graf et al. 2017: S. 536).
86 Vgl. Graf et al. (2017).

sönliche Merkmale ausschlaggebender dafür sind, wie Anonymität eingesetzt wird – nicht das Merkmal der anonymen Kommunikation als solche. Einzelne Studien, die Zusammenhänge von Anonymität und Aggression untersucht haben[87] können vor diesem Hintergrund als ungenau und zu vereinfacht kritisiert werden, da sie nur eine erklärende Variable betrachten (anonym oder nicht-anonym), auf persönliche Motive oder Merkmale wird nicht vertieft eingegangen.

3.2.2 Hatespeech als Problem

In der Rechtsordnung finden sich eine ganze Reihe von Belegen dafür, dass Anonymität nach diesen Vorgaben generell eher die Regel, die Identifizierung eher die Ausnahme ist.[88] Der bereits zitierte § 13 Abs. 6 Telemediengesetz (TMG) normiert, dass Diensteanbieter die anonyme bzw. pseudonyme Nutzung ihrer Webseiten ermöglichen und darüber informieren müssen. Ein Zwang zur Nutzung eines Dienstes unter Klarnamen wird damit ausgeschlossen. Das schließt allerdings nicht aus, dass der Diensteanbieter im internen Verhältnis zu den Nutzenden deren Daten abfordern kann.[89]

Aus dieser Rechtslage hatte sich vor allem das Problem ergeben, wann die Diensteanbieter die Nutzendendaten herausgeben müssen. Lange Jahre argumentierte die Literatur, dass die Einführung eines Auskunftsanspruches bei Persönlichkeitsrechtsverletzungen nach immaterialgüterrechtlichem Vorbild wünschenswert und verfassungsrechtlich geboten sei.[90]

Geregelt sind die Herausgabefälle nun in § 14 Abs. 2–5 sowie § 15 Abs. 5 TMG. Im Zuge des NetzDG wurde u. a. die Herausgabe der Stamm- und Nutzungsdaten zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte, die von § 1 Abs. 3 NetzDG erfasst werden, eingeführt.[91] Aufsehen erregt hat in diesem Zusammenhang eine Entscheidung des Landgerichts Berlin. Die Politikerin Renate Künast begehrte Auskunft über Daten mehrerer Facebooknutzender gem. § 14 Abs. 3, 4 TMG i.V.m. § 1 Abs. 3 Netz-

87 Vgl. Santana (2013); Ybarra/Zimmerman (2014).
88 Vgl. Bäumler (2003: S. 3).
89 Vgl. Müller-Broich, TMG, § 13 Rn. 10 unter Verweis auf OLG Hamburg, Urt. v. 04.02.2009 – 5 U 180/07.
90 Vgl. Palzer, AfP 2017, 199 (202); Gersdorf, MMR 2017, 439 (440); Paschke/Halder, MMR 2016, 723 (726 f.); Spindler (2012: S. 58 f.).
91 Vgl. Conrad/Hausen (2019), IT- und Datenschutzrecht, § 36 Rn. 53.

DG i.V.m § 185 Strafgesetzbuch (Beleidigung), die sie auf ihrer Facebookseite z. T. sehr drastisch, aggressiv und sexualisiert ‚kommentiert' hatten. Das Landgericht verweigerte das Begehren mit der Begründung, dass sämtliche Aussagen von der Meinungsfreiheit gedeckt seien, da sie sich auf Aussagen über sexuelle Freiheiten bezogen hätten, die die Politikerin Dekaden früher im Parlament gemacht hatte.[92]

Die falsche Antwort auf das berechtigte Entsetzen über die Aussagen derartiger Facebook-Hetzender ist, wiederum über einen Klarnamenzwang zu diskutieren.[93] Die Klarnamenpflicht im Internet stellt weder die Übertragung offline bereits geltender Maßstäbe auf die Online-Welt dar, noch lässt sie sich mit dem Begriff des *digitalen Vermummungsverbots* adäquat beschreiben.[94] Weiterhin ist es äußerst fraglich, ob sie überhaupt ein *geeignetes Mittel* gegen Verrohung der Online-Kommunikation darstellt (siehe Kapitel 3.2.1). Vor dem verfassungsrechtlichen Hintergrund (siehe Kapitel 2.2.1) und aus kommunikationswissenschaftlichen Erkenntnissen (siehe Kapitel 2.1) ergibt sich, dass Anonymität einerseits in den Schutzgütern der Verfassung tief und weitverzweigt verwurzelt ist und andererseits auch nicht so einfach als Brandbeschleuniger für Persönlichkeitsrechtsverletzungen angesehen werden kann. Es besteht daher eine staatliche Pflicht zum Schutz von Anonymität. Das bedeutet nicht, dass es nicht dringend ist, den Schutz vor Hatespeech zu verbessern. Denn anhand der bisherigen Ausführungen lässt sich feststellen, dass Hatespeech das eigentliche Problem darstellt und nicht Anonymität. Um das Problem Hatespeech zu bewältigen, braucht es passendere Werkzeuge, die relative Anonymität sinnvoll ausgestaltet lassen. Diese müssen in einer ausgewogenen Ausgestaltung der *Kompetenz*, Pseudonymität zu lüften und somit *Verantwortlichkeit* herzustellen, liegen.

Das Problem beim Künast-Prozess und ähnlich gelagerten Fällen ist der fehlende Ausgleich zwischen dem konzeptionell unterschiedlich ausgestalteten Schutz des Datenschutzrechts und des Äußerungsrechts. Während das Verbot mit Erlaubnisvorbehalt das Datenschutzrecht prägt, also eine ‚strenge' ex-ante Einschätzung erfolgt, muss im Äußerungsrecht – zumeist erst ex-post – durch Abwägung der einschlägigen Rechtsgüter festgestellt

92 Vgl. LG Berlin, Beschl. v. 09.09.2019 – 27 AR 17/19; das Landgericht selbst und das Kammergericht haben den Beschluss teilweise zu Gunsten der Politikerin korrigiert und einige der streitgegenständlichen Kommentare als Beleidigung im Sinne von § 185 Strafgesetzbuch (StGB) eingestuft und deshalb Nutzendendaten herausgegeben. Vgl. KG Berlin, Beschl. v. 11.03.2020 – 10 W 13/20.

93 Vgl. zur Diskussion entspr. Buermeyer (19.06.2019) sowie Kaufhold (30.07.2019).

94 Vgl. Schwander, ZRP 2019, 207 (209).

werden, ob etwas zulässig war oder nicht. Dies führt zu der derzeitigen Situation, dass der Anspruch nach § 14 Abs. 4 TMG auf Auskunft über die Nutzungsdaten nur ein vorbereitender Anspruch ist, der große Unterschiede zu Ansprüchen auf Unterlassung von Äußerungen und auf andere Leistungen (z. B. Geldentschädigung) aufweist.[95] Erst nach Herausgabe der Daten können diese Ansprüche überhaupt geltend gemacht werden. Dieses zweistufige Modell hat sich im Rahmen der Immaterialgüterrechte bewährt, bereitet im Äußerungsrecht aber Bauchschmerzen, wie der Fall Künast zeigt.

Eine Erweiterung der schon bestehenden Datenherausgabepflichten des TMG sieht so nun auch der *Regierungsentwurf zur Bekämpfung des Rechtsextremismus und der Hasskriminalität* vor.[96] Die darin geregelte Pflicht zur Weitergabe von Nutzendenpasswörtern unter bestimmten Umständen, erscheint auf den ersten Blick äußerst fragwürdig.[97] Das NetzDG wiederum soll vor allem durch den *Gesetzentwurf der Bundesregierung zur Änderung des Netzwerkdurchsetzungsgesetzes*[98] erweitert werden. Danach sollen die erfassten Anbieter strafbare Kommentare direkt an die Behörden weitergeben, damit Ermittlerinnen die Täterinnen hinter den Posts leichter enttarnen können, wo sie bisher an der mangelnden Kooperation mit den Tech-Konzernen scheitern.[99] Dieser Ansatz ist dann zu begrüßen, wenn er differenziert ausgestaltet wird. Das bedeutet, dass z. B. im Rahmen von Äußerungsdelikten (wie im Fall Künast) die Netzwerke nicht von selbst, aber auf Anzeige hin tätig werden. Dies allerdings derart, dass sie die umstrittenen Aussagen samt Parteien – mithin also jede Menge personenbezogene Daten – an die Ermittlungsbehörden übergeben. Denn dorthin gehört die Prüfung, ob sich rechtliche Konsequenzen ergeben. Vor dem Straf- oder Zivilgericht kann dann im Anschluss geklärt werden, ob hier die Meinungsfreiheit einschlägig ist oder nicht. Die Parteien sind sich dort bekannt und der öffentliche Diskurs darüber vollzieht sich anhand der altbekannten Maßstäbe.

---

95 So auch das KG in seinem Beschluss (Volltext liegt noch nicht vor), s. LTO, Kammergericht stuft weitere Kommentare als Beleidigung ein (24.03.2020). KG Berlin vom 11.03.2020, Az. 10 W 13/20.

96 Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 19.02.2020, nicht zu verwechseln mit dem Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes vom 01.04.2020.

97 Eine ausführliche Betrachtung würde den Rahmen sprengen; vgl. aber Reuter (19.12.2019) zum Referentenentwurf.

98 Siehe Fn. 96.

99 Vgl. Hoppenstedt (30.09.2019).

3.3 ‚Anonyme' Infrastruktur

Eine allgegenwärtige Frage lautet: Warum verwenden Menschen beim Surfen im Internet Technologien zur Bewahrung von Anonymität? Dient diese nur kriminellen Aktivitäten wie Drogen- und Menschenhandel oder dem Austausch von Kinderpornografie? Oder benötigen Menschen Technologien wie das TOR-Netzwerk zur Wahrung ihrer Grundrechte und zum Schutz vor Verfolgung? Einzelfälle deuten darauf hin, dass Menschen oft auf die Nutzung von Online-Anonymitätsdiensten wie dem TOR-Netzwerk zurückgreifen, weil sie besorgt darüber sind, dass ihre Regierung ihre bürgerlichen und politischen Rechte verletzt oder verletzen könnte. Das ist insbesondere in hoch repressiven Regimen der Fall. Jardine konnte diesen Zusammenhang in einer ökonometrischen Analyse über die Nutzung des TOR-Netzes von 2011 bis 2013 belegen.[100] Es wurde ermittelt, dass das Verhältnis zwischen politischer Repression und der Nutzung des TOR-Netzes U-förmig ist: Politische Repressionen treiben die Nutzung von TOR am stärksten voran, sowohl in hochgradig repressiven Kontexten (wie in China und Usbekistan) als auch in sehr liberalen (wie in Kanada oder USA). Die Form dieser Beziehung ergibt sich im liberalen Kontext plausibel aus der bloßen Möglichkeit der Menschen, TOR zu nutzen, und in hoch repressiven Regimen aufgrund des Bedürfnisses, mit Hilfe von Technologien zur Gewährung von Anonymität grundlegende politische Rechte auszudrücken.

Jardine schlussfolgert, dass die TOR-Technologie für politische Dissidenten und diejenigen, die versuchen, ihre grundlegenden politischen Rechte auszuüben, nützlich ist. Relativ gesehen deuten die Ergebnisse darauf hin, dass das TOR-Netzwerk wahrscheinlich anfälliger für Missbrauch in liberalen Ländern ist, in denen die bloße Möglichkeit, TOR zu nutzen, die zugrundeliegende Motivation für die Nutzung ist; in repressiven Regimen hingegen, loggen sich Menschen möglicherweise vor allem dann in das Netzwerk ein, wenn sie dies tun müssen, um sich vor Sanktionen zu schützen.[101]

Wir sollten nicht vergessen: Drogen-, Menschenhandel und Handel von Kinderpornografie können auch offline im öffentlichen Raum anonym stattfinden. Es erschiene uns in Europa übertrieben, aus Gründen der Verbrechensbekämpfung vorzuschlagen, alle Bürgerinnen sofort nach Verlassen ihres Wohnhauses zu kontrollieren, um sie bei Betreten des öffentli-

100 Vgl. Jardine (2018).
101 Vgl. Jardine (2018: S. 451).

chen Raumes identifizierbar zu machen. Um dennoch gegen Kriminalität vorzugehen, unternimmt die Polizei gezielte Kontrollen und Durchsuchungen. Eine ähnliche Vorgehensweise muss auch für den Online-Raum umsetzbar sein, in dem Handelsplätze im Darknet infiltriert oder beobachtet werden.[102] Anonymität im gesamten öffentlichen Online-Raum zu verhindern wie in China,[103] würde einer allgemeinen und zeitlich unbegrenzten Ausgangssperre oder einer lückenlosen Überwachung gleichkommen. Dies wäre ohne Zweifel eine zu starke Eingrenzung der Grundrechte mit der unzureichenden Begründung des Schutzes vor Kriminalität.

Mit Einführung des § 126a Strafgesetzbuch (StGB) will der deutsche Gesetzgeber deshalb das Betreiben zugangsbeschränkter Handelsplattformen für illegale Waren und Dienstleistungen im Internet unter Strafe stellen.[104] Die Regelung soll es den Strafverfolgungsbehörden erleichtern, gegen kriminelle Machenschaften im anonymen Internet vorzugehen. Im Gesetzesentwurf wird mehrfach explizit das TOR-Netzwerk erwähnt, obwohl sich illegale Online-Handelsplätze zunehmend auch über verschlüsselte Messenger-Dienste organisieren, da die Eintrittsschwelle hier viel geringer ist.[105] Der Gesetzesentwurf wird insbesondere kritisiert, weil ‚gefährlich weite Regelungen geschaffen würden, deren praktischer Nutzen zweifelhaft' sei.[106]

4. Schlussbetrachtung: Wir brauchen Anonymität

Die Frage, ob Anonymität ein Wert an sich ist oder nicht, ist im Allgemeinen zu kurz gegriffen. Vielmehr ist Anonymität in einigen Fällen die Voraussetzung für wertvolle und schützenswerte Mechanismen von demokratischen Prozessen in Gesellschaften. Gleichzeitig kann sie in anderen Fällen zu unsozialen oder gar kriminellen Handlungen führen. Somit bildet Anonymität eine Voraussetzung für ein Verhalten, welches tendenziell

102 So wurden bereits durch gezielte Polizei- und Geheimdienstarbeit große illegale Online-Marktplätze ausgeschaltet, vgl. The Economist (21.07.2017).
103 Vgl. The Economist (31.05.2018); Schwan (07.09.2009).
104 Vgl. Bundesrat Drucksache 33/19 (Beschluss), Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen, 15.03.2019.
105 Vgl. Cuntz (12.11.2019).
106 Vgl. Bäcker/Golla (21.03.2019); zur derzeitigen Rechtslage entspr. Thiesen, MMR 2014, 803.

entgegengerichtet zu bestehenden sozialen Normen sein kann. Je nach Kontext kann es sich förderlich oder missgünstig auf gesellschaftliches Handeln auswirken (z. B. Schutz journalistischer Quellen, Enttabuisierungskampagnen, Schwarzmärkte).

Es besteht ein großer zusammenhängender grundrechtlicher Schutzbereich für Anonymität, der sich aus gewichtigen und zum Teil überlappenden Grundrechtspositionen ergibt. Anonymität ist ein zentraler Bestandteil des liberalen Verfassungsstaates, um grundrechtliche Freiheiten zu gewährleisten und demokratische Legitimation zu sichern.[107] Das bedeutet aber natürlich nicht, dass Anonymität absolut geschützt wäre. Technologischer Fortschritt führt ständig dazu, die (rechtlichen) Grenzen von Anonymität neu bestimmen zu müssen. Heutzutage besteht ein großes Bedürfnis, die horizontale Anonymität der Offlinewelt in die digitale Lebenswelt zu übertragen bzw. das bestehende Konzept relativer Anonymität nicht auszuhöhlen. Eine Aufteilung der Welt in Online und Offline erscheint dabei generell als überholt. Vielmehr ergibt sich aus der spezifischen Lebenssituation der zu betrachtende Fall aus spezieller Kommunikationsform und -umgebung. An der jeweiligen Schutzbedürftigkeit muss dann auch das Schutzniveau bemessen werden, welches für Grundrechtsausübungen von vorneherein bestehen muss.

Beim interdisziplinären Diskurs hat man sich dabei vor Augen zu führen, dass ein jeweils unterschiedliches Verständnis von vertikaler und horizontaler Anonymität besteht. Die juristische horizontale Ebene bezieht sich auf das Gleichordnungsverhältnis der Akteure im Privatrecht und schließt sowohl das Verhältnis zu anderen Usern als auch zum sozialen Netzwerk mit ein. In der Kommunikationswissenschaft und anderen Sozialwissenschaften versteht sich ein horizontales Verhältnis als Verhältnis gegenüber anderen Nutzenden und gegenüber dem Netzwerkanbieter liegt ein vertikales Verhältnis vor. Es muss aber beiden gegenüber relative Anonymität gewahrt bleiben. Autonomen Personen muss das Recht zugestanden bleiben, sich zurückzuhalten und sich auch vor oder in Beziehungen zu distanzieren.[108] Die Möglichkeit und Fähigkeit zur Distanznahme, zur Bildung und Wahrung von Kommunikationsbarrieren, ist dabei das Wesentliche der Anonymität.[109]

107 Vgl. Kersten, JuS 2017, 193 (194).
108 Vgl. Rössler (2001: S. 193).
109 Vgl. Denninger (2003: S. 50).

4.1 Staatliche Schutzpflicht

Aus der Grundrechtslage folgt eine staatliche Schutzpflicht[110] zur Aufrechterhaltung relativer Anonymität – im doppelten Wortsinn: Relativ in Abgrenzung zu absolut, als auch relativ im Sinne von horizontaler, also privatrechtlicher Beziehung. Wir brauchen ausgewogene Regeln für relative Anonymität. Was staatliche Überwachung, also das eigentlich vertikale Verhältnis angeht, bedeutet das: Es sind ausformulierte Eingriffsnormen und keine generalklauselartigen weichen Normen notwendig. Was marktmächtige Netzwerkanbieter angeht, bedeutet das: Die Gewährleistung relativer Anonymität der Nutzerinnen untereinander und nur die vorhersehbare Herausnahme aus dieser Konstellation aufgrund staatlicher Regeln (und nur dieser) zum Interessenausgleich sollte gelten. Wichtig ist die Konstellation gerade im Lichte des Art. 5 Abs. 1 GG zu betrachten und nicht nur vom Standpunkt der informationellen Selbstbestimmung aus. Die Spannung zwischen dem Individuum und der Gemeinschaft hat das Grundgesetz im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden, als die Einzelnen Einschränkungen ihrer Grundrechte zur Sicherung von Gemeinschaftsgütern hinnehmen müssen.[111] Positiv ließe sich unterstellen, dass dies ein Grund für den Fortbestand des § 13 Abs. 6 TMG ist, der einige Gesetzes-Novellen überstanden hat und eben als Grundvoraussetzung für die Internetnutzung angesehen wird.

Außerdem muss relative Anonymität gegenüber den Netzwerkanbietern überprüfbar von diesen geachtet werden, und das über das derzeitige Datenschutzregime hinaus. Dies sagt uns auch der Blick auf das europäische Recht. Das Europäische Unionsrechts schützt die *elektronische Privatsphäre* der Nutzerinnen vor jedem Eingriff – auch durch Private.[112] Diese These lässt sich stützen, indem eine Parallele zum sogenannten *Right To Be Forgotten* gezogen wird,[113] welches auch kein Recht des Löschens oder Tilgens von Information beinhaltet, sondern lediglich ein *Recht auf erschwerte Auffindbarkeit* bestimmt,[114] also auf ein *relatives Vergessenwerden*.

110 Interessanterweise wurde die Lehre der staatlichen Schutzpflicht für die Grundrechte aus der Argumentation für ein Grundrecht auf Sicherheit entwickelt, vgl. Isensee (1983).
111 Vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83.
112 Vgl. EuGH, Urt. v. 01.10.2019 – C-673/17.
113 Vgl. EuGH, Urt. v. 13.05.2014 – C-131/12.
114 Vgl. Palzer, AfP 2017, 199 (200).

4.2 Instrumente nutzen und verbessern

Daneben müssen die Rechtsprechung und Strafverfolgung befähigt werden, die bestehenden Instrumente besser nutzen zu können. Damit die Generalklauseln zum Grundrechtsschutz besser zur Geltung kommen, müssen die versprochenen Aufstockungen von Gerichtsstellen geschehen, digitale Möglichkeiten zur Klage geschaffen und dabei generell Medienbrüche vermieden werden. Das gilt ebenso für die Strafverfolgung. Schwerpunktstaatsanwaltschaften für Cybercrime und Cybermobbing und die Möglichkeit, digital Anzeigen bei der Polizei einzureichen, sind hierbei unseres Erachtens ein guter Anfang. Denn wie der Ausgleich zwischen Privatheit und Äußerungsrecht am besten gelingt, wird Forschung und Gesellschaft noch einige Zeit beschäftigen. Dabei sollte keinesfalls die Möglichkeit, seine Meinung anonym äußern zu können, generell eingeschränkt werden.

Wir werden aber nicht darum herumkommen, Auskunftsansprüche fortzuentwickeln, besser zu gestalten und gegenüber den Netzwerken durchzusetzen. Praktisch uneingeschränkte Anonymität lässt den Schutz der Freiheit des Einen zum Schutz vor der Verantwortung gegenüber dem Anderen verkommen.[115] Weder Privatheit noch Versammlungs-, Meinungs- oder Informationsfreiheit verhindern, sich auf den Grundsatz der Eigenverantwortlichkeit zu besinnen. Dass derzeit Pseudonymität auf den sozialen Netzwerken, also relative horizontale Anonymität gegenüber *Peers*, nicht vor den Netzwerkanbietern und ihren Werbepartnern schützt – und eventuell gar nicht schützen kann[116] – steht auf einem anderen Blatt. Auch hier besteht großer Forschungs- und Regelungsbedarf.

4.3 Richtiger Fokus

Gegen unsoziales Verhalten im Online-Diskurs schlagen Kümpel und Rieger folgende Maßnahmen vor: „(1) Community Management und Moderation, (2) das Ausüben von Gegenrede, (3) die Produktion und Distribution von Gegenbotschaften sowie (4) die Förderung von Medienkompetenz".[117] Diese Punkte können allesamt umgesetzt werden, ohne die Online-Anonymität generell einzuschränken.

115 Vgl. Palzer, AfP 2017, 199 (199).
116 Entspr. wohl auch Hornung/Wagner, CR 2019, 565 (566).
117 Kümpel/Rieger (2019: S. 32).

Es scheint unseres Erachtens nicht angebracht, Anonymität als Sündenbock heranzuziehen, wenn wir über die Probleme diskutieren, die wir mit Online-Medien haben. Denn das führt zur wiederkehrenden, unangebrachten Verkürzung verschiedener Probleme – eben auf Anonymität. Dabei spielen auch die jeweilige gesellschaftliche Situation und die zugehörigen Narrative eine Rolle: Wer im Kontext vom Cambridge-Analytica-Skandal und chinesischer Totalüberwachung aus Sorge um die Demokratie grundsätzlich *für* mehr Online-Anonymität stimmen würde, stimmt möglicherweise im Kontext von Terroranschlägen und Kriminalität wie Drogen- und Menschenhandel *gegen* mehr Online-Anonymität.

Die Schwierigkeit ist aber, dass durch die technisch bedingte, allgemeine Reduzierung von Online-Anonymität die einzelnen Fälle nicht mehr in ihrem jeweiligen Kontext bewertet, sondern alle Nutzenden grundsätzlich identifizierbarer werden. Demokratieförderliche Prozesse, welche Anonymität voraussetzen, geraten in Gefahr, wenngleich ungeklärt ist, ob kriminelle oder terroristische Aktivitäten tatsächlich durch die eingeschränkte Anonymität reduziert werden können. Zusammenfassend gilt: Wenn Demokratien bei komplexen Problemstellungen vorschnell gegen Anonymität im Netz vorgehen, offerieren sie damit oft eine zu einfache Antwort auf verschiedene komplizierte Fragen.

Literaturverzeichnis

Acquisti, Alessandro et al. (2015): „Privacy and Human Behavior in the Age of Information". In: Science 347 (6221), S. 509–14. DOI: https://doi.org/10.1126/science.aaa1465 [Abruf am: 16.04.2020].

Aro, Jessikka (2016): „The Cyberspace War: Propaganda and Trolling as Warfare Tools". In: European View 15 (1), S. 121–132. DOI: 10.1007/s12290–016–0395–5 [Abruf am: 16.04.2020].

Assion, Simon (2019): Informationelle Integrität des Endgeräts". In: Neue Juristische Wochenschrift (NJW), Editorial zu Ausgabe 43/2019.

Assion, Simon (2020): „Die Einwilligung zum/im Datenschutz und bei E-Privacy (Cookies)". In: Stiegler, Frank (Hrsg.): Legal Bits Podcast, Folge 31 vom 08.04.2020, ab 74:45 Min. URL: https://www.stiegler-legal.com/blog/blog-podcast_folge_31 [Abruf am: 16.04.2020].

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.) (2019): Handbuch IT- und Datenschutzrecht. München: C.H. Beck.

Aulehner, Josef (1998): Polizeiliche Gefahren- und Informationsvorsorge: Grundlagen, Rechts- und Vollzugsstrukturen, dargestellt auch im Hinblick auf die deutsche Beteiligung an einem Europäischen Polizeiamt (EUROPOL). Berlin: Duncker & Humblot.

Bargh, John. A./McKenna, Katelyn. Y. A./Fitzsimons, Grainne M. (2002): „Can You See the Real Me? Activation and Expression of the ‚True Self' on the Internet". In: Journal of Social Issues 58 (1), S. 33–48. DOI: https://doi.org/10.1111/1540-4560.00247 [Abruf am: 13.11.2019].

Bäcker, Matthias (2017): „Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz". In: Verfassungsblog (08.06.2017). DOI: https://dx.doi.org/10.17176/20170608-215340 [Abruf am: 31.10.2019].

Bäcker, Matthias/Golla, Sebastian (2019): „Strafrecht in der Finsternis: Zu dem Vorhaben eines „Darknet-Tatbestands". In: Verfassungsblog (21.03.2019). DOI: https://doi.org/10.17176/20190324-201805-0 [Abruf am: 31.10.2019].

Bäumler, Helmut (2003): „Anonymität – Erscheinungsformen und verfassungsrechtliche Fundierung". In: Bäumler, Helmut/v. Mutius, Albert (Hrsg.): Anonymität im Internet. Wiesbaden: Springer Vieweg, S. 1–11.

Bruns, Axel (2009): „From Prosumer to Produser: Understanding User-Led Content Creation". In: Transforming Audiences. URL: http://eprints.qut.edu.au/27370/ [Abruf am: 13.11.2019].

Buermeyer, Ulf (2019): „Statt Klarnamen: Digitales Gewaltschutzgesetz". In: Tagesspiegel (19.06.2019). URL: https://background.tagesspiegel.de/statt-klarnamen-digitales-gewaltschutzgesetz [Abruf am: 13.11.2019].

Caspar, Johannes (2015): „Klarnamenpflicht versus Recht auf pseudonyme Nutzung". In: Zeitschrift für Rechtspolitik (ZRP) 8, S. 233–236.

Chui, Rebecca (2014): „A Multi-faceted Approach to Anonymity Online: Examining the Relations between Anonymity and Antisocial Behavior". In: Journal of Virtual Worlds Research 7 (2), S. 1–13. DOI: https://doi.org/10.4101/jvwr.v7i2.7073 [Abruf am: 13.11.2019].

Cuntz, Christoph (2019): „Verdacht auf geplanten Anschlag: Durchsuchungen in Offenbach". In: Allgemeine Zeitung (12.11.2019). URL: https://www.allgemeine-zeitung.de//lokales/rhein-main/verdacht-auf-geplanten-anschlag-durchsuchungen-in-offenbach_20682241 [Abruf am: 17.11.2019].

Denninger, Eberhard (2003): „Anonymität – Erscheinungsformen und verfassungsrechtliche Fundierung". In: Bäumler, Helmut/v. Mutius, Albert (Hrsg.): Anonymität im Internet. Wiesbaden: Springer Vieweg, S. 41–51.

Ebner, Julia (2019): „Die Gefahr des gamifizierten Terrors". In: Tagesspiegel (15.10.2019). URL: https://background.tagesspiegel.de/digitalisierung/die-gefahr-des-gamifizierten-terrors [Abruf am: 13.11.2019].

Engeler, Malte/Marosi, Johannes (2019): „Planet49: Neues vom EuGH zu Cookies, Tracking und ePrivacy". In: Computer und Recht (CR) 35 (11), S. 707–713.

The Economist (2017): Two of the biggest dark-web markets have been shut down (21. 07.2017). URL: https://www.economist.com/graphic-detail/2017/07/21/two-of-the-biggest-dark-web-markets-have-been-shut-down [Abruf am: 1.11.2019].

The Economist (2018): Does China's digital police state have echoes in the West? (31.05.2018). URL: https://www.economist.com/leaders/2018/05/31/does-chinas-digital-police-state-have-echoes-in-the-west [Abruf am: 13.11.2019].

Froomkin, A. Michael (1995): „Anonymity and Its Enmities". In: Journal of Online Law art. 4. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715621 [Abruf am: 01.07.2020].

Gersdorf, Hubertus/Paal, Boris (Hrsg.) (2019): Beck'scher Online-Kommentar Informations- und Medienrecht. München: C.H. Beck.

Gersdorf, Hubertus (2017): „Hate Speech in sozialen Netzwerken". In: Multimedia und Recht (MMR) 20 (7), S. 439–447.

Graf, Joseph et al. (2017): „The Role of Civility and Anonymity on Perceptions of Online Comments". In: Mass Communication & Society 20 (4), S. 526–549. DOI: https://doi.org/10.1080/15205436.2016.1274763 [Abruf am: 01.04.2020].

Gräfe, Hans-Christian (2019): „Webtracking und Microtargeting als Gefahr für Demokratie und Medien". In: Privacy in Germany (PinG) 7 (1), S. 5–12.

Habermas, Jürgen (1981): Theorie des kommunikativen Handelns. Frankfurt am Main: Suhrkamp.

Härting, Niko (2013): „Anonymität und Pseudonymität im Datenschutzrecht". In: Neue Juristische Wochenschrift (NJW) 66 (29), S. 2065–2071.

Hamm, Andrea/Gräfe, Hans-Christian (2019): „Social Bots, Trolle & Meinungsfreiheit: Illegitime Kommunikation im Netz". In: Media Convention Berlin 2019 (07.05.2019). URL: https://19.mediaconventionberlin.com/de/session/social-bots-trolle-meinungsfreiheit-illegitime-kommunikation-im-netz [Abruf am: 13.11.2019].

Hanfeld, Michael (2015): „Internetkriminalität: Drogen frei Haus, Panzer für Selbstabholer". In: FAZ.NET (16.01.2015). URL: https://www.faz.net/aktuell/feuilleton/medien/mann-vor-gericht-mafia-geschaefte-ueber-silk-road-13374656.html [Abruf am: 01.04.2020].

Hindman, Matthew (2018): „This is how Cambridge Analytica's Facebook targeting model really worked – according to the person who built it". In: niemanlab.org (30.03.2018). URL: https://www.niemanlab.org/2018/03/this-is-how-cambridge-analyticas-facebook-targeting-model-really-worked-according-to-the-person-who-built-it/ [Abruf am: 01.04.2020].

Hohmann-Dennhardt, Christine (2006): „Freiräume – Zum Schutz der Privatheit". In: Neue Juristische Wochenschrift (NJW) 59 (9), S. 545–549.

Hornung, Gerrit/Wagner, Bernd (2019): „Der schleichende Personenbezug". In: Computer und Recht (CR) 35 (9), S. 565–574.

Hollenbaugh, Erin E./Everett, Marcia K. (2013): „The Effects of Anonymity on Self-Disclosure in Blogs: An Application of the Online Disinhibition Effect: Anonymity and self-disclosure". In: Journal of Computer-Mediated Communication 18 (3), S. 283–302. DOI: dx.doi.org/10.1111/jcc4.12008 [Abruf am: 13.11.2019].

Hoppenstedt, Max (2019): „Lambrecht will Gesetz gegen Online-Hetze verschärfen". In: Süddeutsche.de (30.09.2019). URL: https://www.sueddeutsche.de/digital/netzdg-lambrecht-youtube-facebook-twitter-1.4622150 [Abruf am: 13.11.2019].

Isensee, Josef (1983): Das Grundrecht auf Sicherheit – Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Berlin: De Gruyter. DOI: https://doi.org/10.1515/9783110893243 [Abruf am: 01.04.2020].

Janisch, Wolfgang (2019): „Hassbotschaften – Herabwürdigung als Waffe". In: Süddeutsche.de (09.10.2019). URL: https://www.sueddeutsche.de/kultur/renate-kuenast-hate-speech-bundesverfassungsgericht-1.4633159 [Abruf am: 13.11.2019].

Jardine, Eric (2018): „Tor, what is it good for? Political repression and the use of online ano-nymity-granting technologies". In: New Media & Society 20 (2), S. 435–452. DOI: dx.doi.org/10.1177/1461444816639976 [Abruf am: 13.11.2019].

Kang, Katie K. (2017): „Anonymity and Interaction in an Online Breast Cancer Social Support Group". In: Communication Studies 68 (4), S. 403–421. DOI: dx.doi.org/10.1080/10510974.2017.1340902 [Abruf am: 13.11.2019].

Kaufhold, Sylvia (2019): „Anonymität, Klarnamenpflicht und Meinungsvielfalt im Internet – alles eine Frage der Vertragsfreiheit". In: Beck-Blog (30.07.2019). URL: https://community.beck.de/2019/07/30/anonymitaet-klarnamenpflicht-und-meinungsvielfalt-im-internet-alles-eine-frage-der-vertragsfreiheit [Abruf am: 13.11.2019].

von Kempis, Franzi (2018): „Melden und anzeigen: Das hilft gegen den Hass im Internet". In: t-online.com (24.10.2018). URL: https://www.t-online.de/digital/internet/id_84659880/hate-speech-das-hilft-gegen-den-hass-im-internet.html [Abruf am: 01.04.2020].

Kersten, Jens (2017): „Anonymität in der liberalen Demokratie". In: Juristische Schulung (JuS) 57 (3), S. 193–203.

Kümpel, Anna Sophie/Rieger, Diana (2019): Wandel der Sprach- und Debattenkultur in sozialen Online-Medien. Ein Literaturüberblick zu Ursachen und Wirkungen von inziviler Kommunikation. Berlin: Konrad-Adenauer-Stiftung. URL: https://www.kas.de/documents/252038/4521287/Wandel+der+Sprach-+und+Debattenkultur+in+sozialen+Online-Medien.pdf/6a76553c-7c30-b843-b2c8-449ba18c814e?version=1.0&t=1560853247556 [Abruf am: 13.11.2019].

Künast, Renate/Winkelmeier-Becker, Elisabeth (2019): „Härtere Strafen für Beleidigungen im Internet?". In: Deutsche Richterzeitung (DRiZ) 97 (9), S. 296–297.

Legal Tribune Online (2020): „Künasts Beschwerde gegen ‚Drecks Fotze'-Entscheidung Kammergericht stuft weitere Kommentare als Beleidigung ein". In: Legal Tribune Online (LTO) (24.03.2020). URL: https://www.lto.de/recht/nachrichten/n/kg-10w13-20-kommentare-facebook-renate-kuenast-beleidigung-meinungsfreiheit/ [Abruf am: 01.04.2020].

Maunz, Theodor/Dürig, Günter (Hrsg.) (2009): Grundgesetz Kommentar. München: C.H. Beck.

Maunz, Theodor/Dürig, Günter (Hrsg.) (2019): Grundgesetz Kommentar. München: C.H. Beck.

Moore, Michael J. et al. (2012): „Anonymity and roles associated with aggressive posts in an online forum". In: Computers in Human Behavior 28 (3), S. 861–867. DOI: 10.1016/j.chb.2011.12.005 [Abruf am: 13.11.2019].

mja/dpa (2019): „ARD-Magazin ‚Kontraste': Justiz ermittelt nach Aussagen von Pegida-Demonstranten über Lübcke". In: RP ONLINE (05.07.2019.). URL: https://rp-online.de/politik/deutschland/kontraste-ard-magazin-deckt-aussagen-von-pegida-demonstranten-zu-mordfall-walter-luebcke-auf_aid-40391153. [Abruf am: 4.11.2019].

Müller-Broich, Jan (Hrsg.) (2012): Telemediengesetz. Frankfurt: Nomos.

Nida-Rümelin, Julian (2019): „Zur Ethik der Kommunikation in der digitalen Lebenswelt". In: Medientage München (23.10.2019). URL: https://medientage.de/workshop_item/zur-ethik-der-kommunikation-in-der-digitalen-lebenswelt/ [Abruf am: 13.11.2019].

Obermayer, Bastian et al. (o. J.): „Das sind die Panama Papers". In: Süddeutsche.de. URL: https://panamapapers.sueddeutsche.de/articles/56ff9a28a1bb8d3c3495ae13/ [Abruf am: 16.04.2020].

Palzer, Christoph (2017): „Persönlichkeitsschutz im Internet – Vom schmalen Grat zwischen ‚Wohlstandsverwahrlosung' und effektiver Rechtsdurchsetzung". In: AfP – Zeitschrift für Medien- und Kommunikationsrecht (AfP) 48 (3), S. 199–203.

Papier, Hans-Jürgen (2017): „Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft". In: Neue Juristische Wochenschrift (NJW) 70 (42), S. 3025–3031.

Papier, Hans-Jürgen (2019): „Der Rechtsstaat zieht sich hier schon bedenklich zurück". In: Stern (30.10.2019). URL: https://www.stern.de/politik/deutschland/ex-verfassungsrichter-hans-juergen-papier-warnt-im-stern-vor-erosion-des-rechtsstaats-8975080.html [Abruf am: 13.11.2019].

Paschke, Anna/Halder, Christoph (2016): „Auskunftsansprüche bei digitalen Persönlichkeitsrechtsverletzungen". In: Multimedia und Recht (MMR) 19 (11), S. 723–727.

Pille, Jens-Ullrich (2018): „Der Grundsatz der Eigenverantwortlichkeit im Internet". In: Neue Juristische Wochenschrift (NJW) 71 (49), S. 3545–3550.

Pruszkiewicz, Katarzyna/Cieśla, Wojciech (2019): „Diese Reporterin hat sechs Monate in einer polnischen Troll-Farm gearbeitet". In: Buzzfeed (31.10.2019). URL: https://www.buzzfeed.com/de/katarzynapruszkiewicz/verdeckt-trolle-online-recherche [Abruf am: 13.11.2019].

Raschke, Philip et al. (2019): „Towards Real-Time Web Tracking Detection with T.EX – The Transparency Extension". In: Naldi, Maurizio et al. (Hrsg.): Privacy Technologies and Policy, S. 3–17. DOI: dx.doi.org/10.1007/978–3–030–21752–5_1 [Abruf am: 13.11.2019].

Rauer, Nils/Ettig, Diana (2016): „Aktuelle Entwicklungen zum rechtskonformen Einsatz von Cookies. Die Rechtslage auf dem Prüfstand von Kommission und Gerichten". In: Zeitschrift für Datenschutz (ZD) 6 (9), S. 423–427.

Reuter, Markus (2019): „NetzDG-Erweiterung: Wie der Staat mit Gummiparagrafen Zugriff auf die Accounts der Bürger:innen erhalten will". In: Netzpolitik.org (19.12.2019). URL: https://netzpolitik.org/2019/wie-der-staat-mit-gummiparagrafen-zugriff-auf-die-accounts-der-buergerinnen-erhalten-will/ [Abruf am: 01.04.2020].

Rössler, Beate (2001): Der Wert des Privaten. Berlin: Suhrkamp.

Rost, Martin (2003): „Zur gesellschaftlichen Funktion von Anonymität". In: Datenschutz und Datensicherheit (DuD) 27 (3), S. 155–158.

Rost, Katja/Stahel, Lea/Frey, Bruno S. (2016): „Digital Social Norm Enforcement: Online Fire-storms in Social Media". In: PLOS ONE 11 (6). DOI: dx.doi.org/10.1371/journal.pone.0155923 [Abruf am: 01.04.2020].

Santana, Arthur D. (2014): „Virtuous or Vitriolic". In: Journalism Practice 8 (1), S. 18–33. DOI: https://doi.org/10.1080/17512786.2013.813194_[Abruf am: 13.11.2019].

Santoro, Daniele/Kumar, Manohar (2018): Speaking Truth to Power – A Theory of Whistleblowing. Cham: Springer International.

Sarunski, Maik (2016): „Big Data – Ende der Anonymität? Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern". In: Datenschutz und Datensicherheit (DuD) 40 (7), S. 424–27. DOI: https://doi.org/10.1007/s11623-016-0630-x [Abruf am: 17.04.2020].

Schleipfer, Stefan (2019): „ePrivacy-VO-Reset: Kommt jetzt eine bessere Tracking-Regelung?". In: CR-online.de Blog (12.12.2019). URL: https://www.cr-online.de/blog/2019/12/12/eprivacy-vo-reset-kommt-jetzt-eine-bessere-tracking-regelung/ [Abruf am: 13.01.2020].

Schloemann, Johann (2019): „Junger Wissenschaftler – Klicks und Mobs". In: Süddeutsche.de (26.09.2019). URL: https://www.sueddeutsche.de/kultur/niklas-rakowski-wissenschaftler-1.4617051 [Abruf am: 13.11.2019].

Schwan, Ben (2009): „Chinesische Nachrichtenseiten: Anonyme Kommentare verboten". In: taz (07.09.2009). URL: https://taz.de/!5156653/ [Abruf am: 13.11.2019].

Schwander, Timo (2019): „Das digitale Vermummungsverbot – eine irreführende Analogie". In: Zeitschrift für Rechtspolitik (ZRP) 52 (7), S. 207–209.

Simmel, Georg (1908): Soziologie. Untersuchungen über die Formen der Vergesellschaftung. Berlin: Duncker & Humblodt.

Spindler, Gerald (2012): „Gutachten F zum 69. Deutschen Juristentag, Persönlichkeitsrechte im Internet". In: Ständige Deputation des Deutschen Juristentages (Hrsg.): Verhandlungen des 69. Deutschen Juristentages. München: C.H. Beck.

Spindler, Gerald/Schmitz, Peter/Liesching, Marc (Hrsg.) (2018): Telemediengesetz. München: C.H. Beck.

Suler, John (2004): „The Online Disinhibition Effect". In: CyberPsychology & Behavior 7 (3), S. 321–326. DOI: dx.doi.org/10.1089/1094931041291295 [Abruf am: 13.11.2019].

Thiel, Thorsten (2016): „Anonymität und der digitale Strukturwandel der Öffentlichkeit". In: Zeitschrift für Menschenrechte 10 (1), S. 9–24. URL: https://www.academia.edu/35718224/Anonymit%C3%A4t_und_der_digitale_Strukturwandel_der_%C3%96ffentlichkeit [Abruf am: 17.11.2019].

Thiesen, Michael (2014): „Wie hoch ist der Preis der Anonymität? Haftungsrisiken beim Betrieb eines TOR-Servers". In: Multimedia und Recht (MMR) 17 (12), S. 803–809.

Thode, Wiebke/Griesbaum, Joachim/Mandl, Thomas (2015): „‚I Would Have Never Allowed It': User Perception Of Third-Party Tracking And Implications For Display Advertising". In: Proc. 14th International Symposium on Information Science. DOI: https://doi.org/10.5281/ZENODO.17971 [Abruf am: 16.04.2020].

Ybarra, Gabriel/Zimmerman, Adam (2014): „Online Aggression: The Influences of Anonymity and Social Modeling". In: Psychology of Popular Media Culture 5 (2), S. 181–193. DOI: https://doi.org/10.1037/ppm0000038 [Abruf am: 13.11.2019].