Anke Stelkens

Digitale Gewalt und Persönlichkeitsrechtsverletzungen

Vom analogen zum virtuellen Raum

Der virtuelle Raum ist zur Selbstverständlichkeit geworden. Wer jung ist oder up to date sein will, bewegt sich in sozialen Netzwerken, what`s appt ohne Kosten und schnellstmöglich Kontakte und Termine, informiert und präsentiert sich in Suchmaschinen, organisiert sich blitzschnell betreffend Orte, Wege, Zeiten, Veranstaltungen und das möglichst von unterwegs mit Angabe des Standortes und unter Zugriff auf die Cloud, konsumiert mit wenigen Klicks per Bestellbutton, tindert, vergibt Likes und postet mal eben online eine Meinung oder spielt und chattet in virtuellen Communities. Tut insbesondere eine Frau dies alles nicht (mehr),[1] fühlt es sich bestenfalls alt an, ist sie jedenfalls ausgeschlossen, oft beruflich nicht mehr konkurrenzfähig. Es ist auf Dauer keine Option, sich diesem virtuellen Raum zu entziehen oder sich auf umständlichen zeitintensiven Umwegen zu bewegen.[2]

Die Kehrseite dieses virtuellen Raums, der die Privatsphäre erweitert und bereichert und eine neue Öffentlichkeit geschaffen hat, ist eine immense Verantwortung, die plötzlich übernommen werden muss. Zum einen für jede und jeden selbst, zum anderen für die gesellschaftlichen Auswirkungen, die diese bahnbrechende digitale Umwälzung von Alltagsverhalten mit sich bringt. Und beides fällt schwer.

Und offensichtlich unerträglich erscheint dabei das Phänomen der digitalen Gewalt, die sich wesentlich vom herkömmlichen Verständnis von Gewalt als körperlich direkter Attacke unterscheidet. Shit Storms, Hate Speech, Online-Harassement, Hacked Identities – all das spielt sich doch „nur im Netz" ab. Regeln für einen cyber-zivilen Umgang miteinander zu definieren, rechtssichere Cyberräume und darin Freiheit im Sinne von Bewegungsfreiheit, Meinungsfreiheit, Zugang und Teilhabe zu gewährleisten – nichts weniger als das ist die Herausforderung, vor der unsere Rechtsordnung und auch die internationale Staatengemeinschaft stehen.

Die Euphorie, mit der in den frühen 90er-Jahren die sogenannten „Neuen Medien" begrüßt und das Internet als sich selbst genügender und selbstregulierender Raum gefeiert wurden, ist mittlerweile mehr als verflogen. Nachdem zuerst noch gesetzliche Regelungen für Internetphänomene wie domain-Adressen und Emails gefordert oder Gesetze zu Mediendiensten versus Telediensten geschaffen wurden,[3] setzte sich bald als mehr oder weniger herrschende Meinung im Medienrecht der Denkansatz durch, dass es keiner besonderen Rechtsregelungen für „das Internet" bedürfe. Vielmehr sei dort kein „rechtsfreier Raum", sondern es seien die nationalen Regelungen online genauso wie offline anzuwenden. Eine Argumentation, die nicht von ungefähr zeitlich zusammenfiel mit der Deregulierung der Wirtschaft und dem Neoliberalismus. Bis heute begleitet uns aus dieser Zeit das Haftungsprivileg für Zugangsprovider im weitesten Sinne, welches von den mittlerweile monopolartig agierenden Internetgiganten auch mit Zähnen und Klauen verteidigt wird.

Zwar wurden im StGB das „Ausspähen" und „Abfangen" von Daten unter Strafe gestellt und im Titel „Sachbeschädigung" die neuen Tatbestände „Datenveränderung" und „Computersabotage" aufgenommen, die Strafrahmen stehen jedoch in keinem Verhältnis zu ihrer Gefährlichkeit. Eine Sanktionierung von psychischen und körperlichen Verletzungen durch Aktivitäten im virtuellen Raum ist bis heute im StGB kein Thema.

Auch hat es der Staat bis heute versäumt, eine digitale Infrastruktur zu schaffen, die – ähnlich einer Grundversorgung durch öffentlich-rechtlichen Rundfunk oder auch der Grundinfrastruktur für Straßen – eine Grundversorgung mit digitalen Zugängen, digitaler Information und digitaler Datensicherheit gewährleistet. Vertraut wurde auf die Marktkräfte und

1 Zumeist stoppt frau den Umgang mit digitalen Medien erst nach schlechten Erfahrungen, manchmal auch vorab aus Angst davor, bezeichnend der Titel einer Tagung der Bundesarbeitsgemeinschaft kommunaler Frauenbüros „Dann geh doch nicht ins Internet" am 27.11.2014, Dokumentation siehe auf www.frauenbeauftragte.org/ dort: Service/ Konferenzen und Tagungen.

2 Der Aufruf des Hamburger Datenschutzbeauftragten, doch auf die Nutzung von WhatsApp zu verzichten, erscheint dabei fast schon rührend hilflos, www.abendblatt.de/hamburg/article208371011/Hamburger-Datenschuetzer-Meiden-Sie-WhatsApp.html.

3 Geblieben ist das Telemediengesetz (TMG) mit seinem allgemeinen Begriff der Telemedien für alle Websites und seinem Verweis auf den Rundfunkstaatsvertrag, soweit journalistische und vergleichbare Inhalte übers Internet verbreitet werden. Speziellere Regelungen und eine klare Unterscheidung von kommerziellen Websites (Telediensten im alten TMG) gegenüber Mediendiensten (eher rundfunkähnliche Angebote in einem Mediendienstestaatsvertrag der Länder) erwiesen sich als faktisch unmöglich. Der Umfang von über das TMG hinausgehenden Verpflichtungen der Websitebetreiber, insbesondere der Impressumspflicht, nach den §§ 55 ff. Rundfunkstaatsvertrag ist bis heute rechtlich unscharf und umstritten. Näher dazu z.B. https://www.telemedicus.info/article/2155-Was-sind-vergleichbare-Telemedien.html.

die freie Wirtschaft, was ein sattes Stadt-Land-Gefälle bei den digitalen Datenzugängen zur Folge hatte. Weltweit agierende Firmen sammeln per Data-Mining unsere im Netz hinterlassenen „Fußspuren", um daraus Profile für passgenaue Werbung zu errechnen. Die Profile aller, die sich im Internet ungeschützt bewegen, ermöglichen Zugriffe durch offen agierende oder selbst technisch vor Entdeckung geschützte Angreifer.

Erst langsam setzt sich die Erkenntnis durch, dass der Schutzauftrag des Staates sich auch auf diesen virtuellen Raum erstreckt und der Staat entsprechende Abwehrmechanismen und Schutzräume entwickeln muss. Konsumüberschuldung und erhöhte Privatinsolvenzen brachten durch Regelungen zum Fernabsatz das Widerrufsrecht und zuletzt den „zahlungspflichtig bestellen"-Button in die Webshops, offensichtlich war erweiterter Verbraucher*innen Schutz im virtuellen Raum geboten.

Die Enthüllungen von Edward Snowden schließlich brachten den orwellschen Überwachungsstaat in die öffentliche Diskussion und lösten eine Renaissance im Datenschutzrecht aus, was jetzt im Ergebnis einerseits zur Europäischen Datenschutzgrundverordnung 2016/679 vom 27. April 2016, andererseits aber auch zur Verschärfungen der staatlichen Datenzugriffe für die Terrorabwehr geführt hat. Und die Krise der Massenflucht nach Europa 2015 brachte das Phänomen Hate Speech mit rassistischem Inhalt ganz oben auf die rechtspolitische Agenda.[4] Immerhin, die Weichen stehen insgesamt auf Handeln.

Digitale Gewalt gegen Frauen

Mediale Attacken gegen Frauen und Frauenhass setzten sich derweil in den letzten Jahren im Cyberraum virtuell fort in bisher unermessenem Ausmaß und noch wenig untersucht in Daten und Fakten.[5] Harte Verbalattacken, Vergewaltigungsandrohungen, Revenge Porn, Slut Shaming und massive virtuelle Maskulinistennetzwerke, die feministische Positionen gezielt attackieren, sind die Realität. Frauen werden abgeschreckt, den virtuellen Raum zu nutzen oder feministische Positionen im Netz zu vertreten. Und da dies auch Personen treffen kann, die sich gar nicht im Netz bewegen, wird auch die Vertretung dieser Positionen in der realen Welt massiv erschwert. Denn die Verweigerung der Nutzung der neuen Kommunikationswege schützt eben nicht vor Angriffen im Netz mit unter Umständen extremen Folgen für die eigene Lebensgestaltung und Gesundheit.

Momentan wird dieser extrem frauendiskriminierende Effekt des Internets in der öffentlichen Diskussion in Deutschland eher verharmlost und verdrängt und sich auf rassistische Phänomene und Terrorabwehr, allenfalls noch auf Mobbing unter Jugendlichen, konzentriert.[6] In diesem Sinne klingt auch der gängige Begriff Cyber *Harassement* – wörtlich „*Belästigung*" – eher beschönigend. Denn für Frauen bedingt die allgegenwärtige Masse und die Unausweichlichkeit dieses Harassements im virtuellen Raum – egal ob sie sich nun explizit feministisch äußern oder einfach nur „als Frau" an einem virtuellen Dialog teilnehmen – ein Gewicht, welches im Begriff Belästigung nicht mehr angemessenen Ausdruck findet. Im virtuellen Raum ist eine Frau immer gefährdet und verschärft auf ihre Geschlechterrolle zurückverwiesen und es bleibt ihr nur, sich männlich zu tarnen oder ganz zu tarnen oder technisch abgeschottete Räume zu nutzen, um sich selbst zu schützen. Eine Situation, die wir im öffentlichen Raum eigentlich glaubten, überwunden zu haben.

Frauen sind über sexualisierte Attacken im Netz weit verletzbarer als Männer. Dies ist dem Geschlechterverhältnis aus der realen Welt geschuldet, welches sich im virtuellen Raum fortsetzt. Nacktbilder von Frauen – ob echt oder montiert – oder Vergewaltigungsaufforderungen gefährden eine Frau real, machen sie als potentielles Opfer auch im realen Raum verfügbar. Die Verletzungsintensität ist i.d.R. höher als bei vergleichbar geposteten Nacktbildern oder Bedrohungen von Männern, die unter Umständen in ihrem männlichen Selbstverständnis, in ihrer Potenz von solchen Dialogen sogar noch profitieren können. Soziales Verhalten im virtuellen Raum scheint jedenfalls Hemmschwellen bei diskriminierendem Verhalten vermissen zu lassen, die zumindest im realen öffentlichen Raum ansonsten weitgehend eingehalten werden.[7] Soziale Normen, die gesellschaftlich mühsam erreicht wurden, sind plötzlich nicht nur

4 Bundesministerium für Justiz und Verbraucherschutz: Gemeinsam gegen Hassbotschaften. Von der „Task Force Umgang mit rechtswidrigen Hassbotschaften im Internet" vorgeschlagene Wege zur Bekämpfung von Hassinhalten im Netz, vom 15.12.2015: www.bmjv.de/SharedDocs/Downloads/DE/Artikel/12152015_TaskForceErgebnispapier.html. Frauenfeindliche Hassbotschaften werden hier nicht erwähnt.

5 2015 veröffentlichten die UN einen ersten Report „Cyber Violence Against Women and Girls", siehe www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259; dazu auch Höver, „UN-Report: Es ist Zeit, gegen die Gewalt gegen Mädchen und Frauen im Netz vorzugehen!" im online Magazin „wired", www.wired.de/collection/life/neuer-un-report-schlagt-alarm-zu-online-gewalt-gegen-frauen.

6 So Lembke, „Ein antidiskriminierungsrechtlicher Ansatz gegen Cyber Harassement", in: KJ 3/2016, S.385 ff, S.386.

7 Bock, Harrendorf: „Strafbarkeit und Strafwürdigkeit tatvorbereitender computervermittelter Kommunikation", in ZSTW 2014, S.337 ff mit vielen weiteren Nachweisen auf soziologische Studien zu abweichendem Verhalten im Internet, insbesondere auf die SIDE-Theorie, nach der die Herabsetzung der Hemmschwellen nicht zwingend antisozial wirken muss (auch wenn sie dies betreffend digitale Gewalt gegen Frauen offenbar meist tut).

aufgehoben, sondern bei pseudonymer und anonymer Kommunikation offenbar kontraproduktiv und werden mit besonderer Intensität gebrochen. Wobei sich die Angriffe durch gegenseitiges Sich-Bestätigen noch verstärken.

Mit dieser neuen Dimension von Gewalt gegen Frauen – mit dieser *digitalen Gewalt* – können wir noch gar nicht umgehen. Und noch schlimmer, dieser virtuelle Raum wirkt zurück in den realen Raum und verschärft das Klima, indem er Worte und Taten wieder salonfähig macht, die dort schon nicht mehr denkbar waren.

Zivilrechtliche Abwehrrechte gegen Persönlichkeitsrechtsverletzungen

Das klassische Abwehrinstrument im Zivilrecht steht mit den persönlichkeitsrechtlichen Schadensersatz-, Unterlassungs- und Beseitigungsansprüchen aus dem BGB zur Verfügung.

Das allgemeine Persönlichkeitsrecht (APR), als verfassungsrechtlich geschützte Rechtsposition verdichtet aus Art. 1 und 2 GG, findet sich einfachgesetzlich nach wie vor nicht kodifiziert. Durch die Rechtsprechung anerkannt als „sonstiges Recht" im Sinne von § 823 BGB und als „eigentumsanaloge Rechtsposition" im Sinne des § 1004 BGB wird die Rechtslage aber seit Jahrzehnten von den Zivilgerichten und letztentscheidend vom BVerfG gestaltet. Abzuwägen ist das APR dabei stets gegen die grundsätzlich auf gleicher Augenhöhe stehende Meinungsfreiheit.

Lange tradiert sind vom APR erfasst der Schutz der persönlichen Ehre, das Recht am eigenen bürgerlichen Namen und das Recht am eigenen Bild. Hier finden sich auch schon lange einfachgesetzliche Regelungen. So enthält § 12 BGB einen Unterlassungs- und Beseitigungsanspruch bei Namensverletzungen,[8] die Beleidigungstatbestände der §§ 185 ff. StGB werden als Schutzgesetze i.S.d. § 823 II BGB auch für den zivilrechtlichen Ehrschutz herangezogen und die §§ 22 ff. Kunsturhebergesetz enthalten sowohl den zivilrechtlichen als auch einen strafrechtlichen Schutz für rechtswidrige Personenabbildungen. Eine lange Tradition hat im Medienrecht auch der zivilrechtliche Gegendarstellungsanspruch,[9] ein besonderer Beseitigungsanspruch ursprünglich aus dem Presserecht. Er bietet bei medialen persönlichkeitsrechtsverletzenden Tatsachenbehauptungen unabhängig von deren Wahrheitsgehalt das Recht, zeitnah eine eigene ausgleichende Darstellung der entsprechend verletzten Person an gleichwertiger medialer Stelle zu veröffentlichen. Darüber hinaus wird über das Verständnis als absolutes Recht i.S.d. § 823 BGB heute ein umfassender Schutz für die Privat-, Geheim- und Intimsphäre gewährt. Dazu gehört auch das Recht am gesprochenen und geschriebenen Wort mit seinem Schutz gegen Entstellung oder Unterschiebung von Äußerungen.

Und Eingang gefunden in das APR hat im deutschen Recht umfänglich ein Verständnis vom Schutz personenbezogener Daten. Als Recht auf informationelle Selbstbestimmung ist es vom BVerfG schon seit Jahrzehnten als Teil des APR anerkannt[10] und seit 2008 auch erweitert verstanden als Recht auf Integrität informationstechnischer Systeme.[11] Dieses zuletzt durch das BVerfG anerkannte Computergrundrecht, mit dem der Zugriff auf die heimische Festplatte erschwert wurde, erscheint in Zeiten von cloud computing und globalen Serverfarmen allerdings schon wieder hoffnungslos veraltet. Dabei ist das Verständnis von Datenschutz in Deutschland sehr umfassend und bezieht sich nicht nur auf den Schutz personenbezogener Daten vor dem Zugriff des Staates (öffentliche Stellen), sondern schützt auch jede Person vor Zugriffen sogenannter nicht-öffentlicher Stellen, sprich Unternehmen und sonstiger Dritter.[12] Insoweit ist der Datenschutz auch als Verbraucher*innen schützende Norm im Sinne des § 4 Nr. 11 UWG anerkannt, so dass Persönlichkeitsrechtsverletzungen in Form von datenschutzrechtlichen Verstößen der Unternehmen mit der Verbandsklage angegriffen werden können, was die Verbraucherschutzverbände auch tun. [13]

Diese teils gesetzliche, teils richterrechtliche Ausformung des APR ist nicht abschließend zu verstehen. Es wäre also an das Internetzeitalter anpassbar und

8 Üblich ist es, als Anspruchsgrundlage den § 1004 BGB analog mit zu nennen. Außerdem wird im Rahmen einer erweiterten Auslegung des § 12 BGB der Schutz von persönlichen Kennzeichen im weitesten Sinne judiziert, so gilt er als Auffangvorschrift bezüglich der Grenzen von gewerblichem Rechtsschutz und insbesondere der Abwehrrechte betreffend domain-Missbräuche.

9 Z.B. für Telemedien in § 56 Rundfunkstaatsvertrag, ähnlich in allen Pressegesetzen der Länder und im ARD- und im ZDF-Staatsvertrag.

10 Volkszählungsurteil 1983 BVerfGE 65, 1.

11 Online-Durchsuchung/Computer-Grundrecht 2008, BVerfGE 120, 274.

12 Umfassender zivilrechtlicher Datenschutz hat in den §§ 11 ff. TMG eigene Internetregelungen erhalten und ist ansonsten mitgeregelt im Bundesdatenschutzgesetz, das die Datenverarbeitung der Bundesbehörden regelt und wie die entsprechenden Landesdatenschutzgesetze eigentlich dem öffentlichen Recht zugeordnet wird. Es gilt ein striktes Verbot der Nutzung personenbezogener Daten mit Erlaubnisvorbehalt bei gesetzlicher Ermächtigung oder formunterworfener Einwilligung. Datenschutzgesetze sind Schutzgesetze nach § 823 II BGB.

13 Die Position der Verbraucherschutzverbände wurde gestärkt durch das „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts" v. 17.2.2016, BGBl I Nr. 8 vom 23.02.2016. Aktuell erfolgt eine Abmahnung des VZBV gegen Whats App: Pressemitteilung des VZBV vom 19.09.2016, zuvor gab es schon mehrere teilweise erfolgreiche Verfahren gegen Facebook, www.vzbv.de/pressemitteilung/vzbv-klagt-gegen-facebook.

erweiterbar. In der Vergangenheit haben immer wieder medienrechtliche Verfahren Anstöße für die Modernisierung des Rechtsgebietes gegeben.[14] Das Instrument APR als solches scheint also geeignet, Regeln für den cyber-zivilen Umgang im virtuellen Raum zu schaffen.

Und dennoch – faktisch zielt diese ausgefeilte Abwehr im Internetzeitalter meist ins Leere. Der Weg, den ein Opfer von medialer Attacke zivilrechtlich beschreiten muss, ist aufwendig und lang. Die Verletzungen müssen im Einzelnen nachgewiesen werden. Das bedeutet in der Praxis das Anfertigen von Website-Snapshots und ähnlichem mit gleichzeitiger Dokumentierung des Zeitpunktes der Verletzungshandlung.[15] Dabei ist zeitnahes Handeln gefordert, Gegendarstellungen müssen unverzüglich nach Kenntnis eingefordert werden, einstweiliger Rechtsschutz hat kurze Fristen für die Geltendmachung. Auch wenn das Ignorieren von bloßer „Belästigung" im Einzelfall als cooler erscheint oder der Schock bei einer massiven Drohattacke ein schnelles Wegklicken auslöst – nötig wäre ein aktives Handeln, Abspeichern, Archivieren. Das ist für die einzelne betroffene Person in der Situation meist schon technisch gar nicht geschweige denn emotional zu leisten. Verbreitete Reaktion insbesondere bei Frauen ist denn auch ein „sich Zurückziehen" und „sich Beschränken". Verhaltensweisen, die durch weibliche Sozialisierung in unserer Gesellschaft nach wie vor automatisiert und eingeübt sind.

Um für die verschuldensabhängigen Ansprüche auf Schadensersatz bzw. Schmerzensgeld Identitäten festzustellen, ist es häufig erforderlich, parallel ein Strafverfahren einzuleiten, welches erst Auskunftspflichten des für die Website verantwortlich zeichnenden Diensteanbieters auslöst.[16] Aber auch durch die Strafverfolgungsbehörden sind Identitäten oft nicht zweifelsfrei feststellbar. Die Identität bei anonymer und pseudonymer Nutzung des Internets zu knacken kostet Zeit und Geld und ist teilweise technisch unmöglich gerade da, wo vorsätzliche, eindeutig einen Verletzungstatbestand erfüllende Handlungen vorliegen. Denn je professioneller die Angriffe, desto besser sind sie getarnt.

Und oft gibt es gar nicht „den Täter", oft ist es gerade die massenhafte Aktivität im Netz, das Verlinken, Teilen, Kommentieren, schlicht das „Digitale Weitererzählen", welches den mehr oder weniger vernichtenden „Datensturm" ausmacht, der sich dann auch in der realen Welt ganz massiv als gewaltgleiche Attacke auswirkt.[17] Und lässt sich tatsächlich eine Tat beweisen und eine verantwortliche Person ausfindig machen, so ist auch die Bemessung eines Schmerzensgeldes in Deutschland in der Regel niedrig in Anbetracht der Dimension der Taten.[18] Eine bloße „Tätersuche" wird dem Phänomen digitaler Gewalt in den globalen Öffentlichkeiten und massenhaften Teilöffentlichkeiten also selten gerecht.

Auch der Unterlassungs- und Beseitigungsanspruch, der das rechtswidrige Tun ganz ohne Verschuldensnachweis beenden und tilgen soll und auch gegen vergleichsweise leicht zu identifizierende Forenbetreiber, Plattformen, soziale Netzwerke gerichtet werden kann,[19] geht häufig ins Leere – meist ist es schon im Zeitpunkt der Abmahnung zu spät, noch irgendwelche Auswirkungen zu unterbinden. Über das Institut der sogenannten Störerhaftung nimmt die Rechtsprechung die Internetdiensteanbieter i.S.d. TMG bereits in die Unterlassungs- und Beseitigungspflicht. Überwachungs- und Prüfpflichten für Provider – unterteilt werden sie in haftungsprivilegierte Access- und Hostprovider[20] im Gegensatz zu haftungsverantwortlichen Contentprovidern – bestehen gemäß den Haftungsprivilegierungen der §§ 7-10 TMG dabei nur eingeschränkt. Accessprovider sind nach dem Wortlaut des § 8 TMG für Inhalte nicht verantwortlich, werden aber bisher dennoch von der Rechtsprechung als Störer herangezogen. Hostprovider treffen Unterlassungs- und Beseitigungspflichten gemäß § 10 TMG erst nach positiver Kenntnis oder

14 Angefangen beim Grundsatzurteil 1971 BVerGE 30, 173 (Mephisto) hat sich eine umfangreiche Rspr. entwickelt – themenbezogene Übersicht z.B. auf https://www.telemedicus.info/urteile/Allgemeines-Persoenlichkeitsrecht/- deren aktuellster Fall des Böhmermann-Schmähgedichts noch nicht ausjudiziert ist.

15 Dies kann am einfachsten durch einen verletzungszeitgleichen Snapshot von Datum und Uhrzeit auf einer neutralen Website in einem danebenliegenden Bildschirmfenster erfolgen, z.B. auf www.weltzeituhr.de.

16 Ein Verfahren, welches die Abmahnlobby sich bei urheberrechtlichen Verletzungen durch den erweiterten Auskunftsanspruch über Verkehrsdaten erleichtert hat, § 101 Abs. 9 UrhG. Ein entsprechender Auskunftsanspruch im APR besteht nicht.

17 Für eine „haftungsrechtliche Erfassung des Mobs" über die gesamtschuldnerische Haftung gemäß §§ 830, 840 BGB Lembke, a.a.O., Fn. 6, S. 392.

18 695.000 € Schmerzensgeld – bislang das höchste in Deutschland judizierte Schmerzensgeld für APR-Verletzung im Fall Springerverlag./.Kachelmann – werden in Deutschland als Rekordschadensersatz angesehen. Im anglo-amerikanischen Rechtsraum können Schadensersatzsummen um Größenordnungen höher ausfallen. Denn im US-Regressrecht hat der Schadensersatz grundsätzlich eine Straffunktion (punitive damages), die dem deutschen Recht fehlt.

19 Viele Betreiber wie Facebook, Instagram, Twitter, YouTube, Snapchat bieten hier mittlerweile interne Prozesse zur Meldung von Verletzungshandlungen, die aber natürlich auch durch die jeweilige Interessenlage des Dienstanbieters geprägt sind, Überblick dazu auf www.no-hatespeech.de/de/wissen/.

20 Accessprovider (z.B. Telekom, 1&1, auch WLAN-Anbieter in Internetcafés) bieten nur Zugang zum Internet, Hostprovider (z.B. Facebook, YouTube) bieten den Nutzenden Speichermöglichkeiten für Inhalte. Im Unterschied dazu bieten Contentprovider selber Inhalte an und ermöglichen oft auch, diese zu kommentieren (z.B. zeit-online). Oft vermischen die Anbieter Accessproviding und Hostproviding (z.B. Telekom) und bieten beide Dienstleistungen und zusätzlich noch Contentseiten an.

bei Offensichtlichkeit von Verletzungshandlungen. Hostprovidern werden – im Gegensatz zu Contentprovidern – die Inhalte der Nutzenden grundsätzlich nicht als eigene Inhalte zugerechnet – eine Rechtsposition, die Plattformbetreiber stets für sich in Anspruch nehmen. Insbesondere haften Plattformen mangels Verschulden damit nicht auf Schadensersatz in Form von Schmerzensgeld.[21]

Zwar ist die Rechtsprechung durchaus geneigt, diese Providerhaftung auszudehnen.[22] Insbesondere beim Eigentumsschutz für Urheberrechtsverletzungen wurden hier aufgrund der Klagefreudigkeit der Verwerterindustrie weitreichende Erfolge erzielt,[23] eine Ausdehnung der Haftung für sog. Intermediäre gekoppelt mit einer Lizensierungspflicht bzw. eben Schadensersatzpflicht wird im Bereich der Verletzung geistigen Eigentums durchaus bejaht.[24] Im Bereich des APR ist dagegen keine vergleichbare Rechtsprechungstendenz erkennbar. Bei der Verletzung von Persönlichkeitsrechten soll der Schutz der Meinungsfreiheit und das gesellschaftliche Interesse an einem möglichst unkontrolliert zu nutzenden Internet überwiegen und eine haftungsprivilegierte Bereitstellung von Internetzugängen für eine möglichst breite Nutzungsgemeinde ist politisch gewollt. So ist im Zuge der Reformierung des § 8 TMG sogar von der „Abschaffung der Störerhaftung" für Accessprovider die Rede.[25] Das korrespondiert mit dem politischen Ziel, freien Zugang zum Internet über möglichst flächendeckende Infrastrukturen zu schaffen, die eben nicht staatlich bereitgestellt, sondern privatwirtschaftlich angeboten werden sollen. Hier könnte zwar unterschieden werden zwischen einer Privilegierung von reinen Zugangsprovidern – insbesondere Anbietern von freiem WLAN-Zugang – und der differenzierten Betrachtung von einerseits Host-Providern, die redaktionelle und informierende Plattformen bereitstellen und andererseits Host-Providern, die von den auf ihren Plattformen geteilten oder gehandelten Inhalten mehr oder weniger direkt nur geschäftlich profitieren. Dies erinnert allerdings wieder an die ergebnislose Diskussion zur Unterscheidung zwischen Telediensten und Mediendiensten, die sich als ungeeignet für eine rechtliche Anknüpfung erwiesen hat.[26] Einen zivilrechtlichen Schadensersatzanspruch, der an die Art und Weise anknüpft, in der ein Hosting angeboten wird, gibt es im APR bislang nicht. Gesetzentwürfe zur Ausdehnung der Haftung von Hostprovidern sind umstritten, wobei eine Unterscheidung verschiedener Providertypen nach Art des inhaltlichen Angebots bzw. des geschäftlichen Eigeninteresses politisch wohl angestrebt wird.[27]

Auch das „Recht auf Vergessen werden"[28] bzw. das „Recht auf Löschung", mit dem die Rechtsprechung den Unterlassungs- und Beseitigungsanspruch auf Suchmaschinen erweitert hat, kommen meist zu spät für die betroffenen Menschen. Hiermit kann allenfalls noch eine Genugtuungsfunktion erfüllt werden. Zu schnell verbreiten sich Falschmeldungen und Rufschädigungen im Netz, verselbstständigen sich Gerüchte und vernichten mediale Attacken Personen und Existenzgrundlagen so vollständig, dass kein rechtlicher Stopp mehr hilft.

Tempo und Ausmaß von Persönlichkeitsrechtsverletzungen im globalen Informationszeitalter lassen sich also mit all diesen Instrumenten nicht bekämpfen. Die Einzelnen auf den Rechtsweg zu verweisen, läuft in der Praxis meistens ins Leere. So unverzichtbar diese Ansprüche auch sind, sie sind nicht geeignet, Rechtsgüterschutz und Rechtssicherheit im virtuellen Raum herzustellen, weil sie schlicht nicht schnell genug durchsetzbar sind.

21 Gute Übersicht in diesem Zusammenhang dazu bei Lembke, a.a.O, Fn. 6, S. 394-396.

22 Einzelheiten sind im deutschen Recht umstritten und wurden von den Gerichten unterschiedlich gehandhabt. Zuletzt Grundsätze der sog. Ping-Pong-Haftung im BGH-Urteil v. 25.10.2011 – VI ZR 93/10, BGHZ 191, 219-228.

23 Bei von der „Rechtsordnung missbilligten Geschäftsmodellen" wird urheberrechtlich eine volle Haftung bejaht, „Rapid-Share" BGH, Urteil v. 15.08.2013, Az. I ZR 80/12.

24 Regelmäßige Forderung der Initiative Urheberrecht, siehe http://urheber.info/.

25 Am 27.7.2016 trat das Zweite Gesetz zur Änderung des Telemediengesetzes in Kraft. Erklärtes Ziel des Gesetzes ist es, Anbieter offener WLANs von der Haftung für Rechtsverletzungen der Nutzenden freizustellen. Die Haftungsprivilegierung für Accessprovider gilt nach dem neuen § 8 III TMG nun auch für Anbieter lokaler WLAN-Netze. Allerdings bedeutet dies noch nicht das Ende der Störerhaftung. Mit dem aktuellen McFadden-Urteil des EuGH vom 15.09.2016 – C-484/14 WLAN- werden Zugangsanbieter zwar weitgehend haftungsfrei auch betreffend Unterlassungsansprüche gestellt, aber nur soweit Nutzungen via Passwörtern erfolgen. Eine Entscheidung, die flächendeckendem freien Internetzugang im Sinne einer Infrastruktur aber sicherlich nicht gerecht werden kann. Diskussion dazu auf https://www.telemedicus.info/article/3130-5-Fragen-zum-WLAN-Urteil-des-EuGH.html.

26 Siehe oben Fn. 3.

27 Ablehnend betreffend Ideen des Gesetzgebers zu Haftungserweiterungen angelehnt an die Rspr. zu von der „Rechtsordnung missbilligten Geschäftsmodellen" oder „gefahrgeneigten Diensten" natürlich das im Auftrag des eco – Verband der deutschen Internetwirtschaft e.V. erstellte Gutachten „Rechtliche Bewertung des Gesetzentwurfs zur Neuregelung der Host-Providerhaftung", auf www.eco.de/wp-content/blogs.dir/150913-gutachten-host-providerhaftung-2015000545.pdf.

28 Der EuGH hat 2014 (Rs C-131/12) einen Anspruch gegen Google auf Löschung personenbezogener Daten in Ergebnislisten bejaht und in seiner Abwägungsentscheidung dabei den Schutz personenbezogener Daten gegenüber der allgemeinen Informationsfreiheit von Google als Datenverarbeiter überwiegen lassen, siehe dazu PM 70/14 des EuGH auf http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf., siehe dazu auch Art 12 ff, insbesondere Art 17 der neuen EU-Datenschutzgrundverordnung 2016/679 vom 27. April 2016.

Schutz durch Strafrecht

Das Strafrecht kann Angriffe im virtuellen Raum nicht verhindern und Schäden nicht beseitigen. Es ist aber wegen seiner symbolischen Wirkung, indem es Unrecht als solches benennt, nicht zu unterschätzen, kann im Einzelfall vielleicht sogar abschreckend wirken. Digitale Gewalt gegen Frauen wird bisher im Strafrecht nicht adressiert. Überlegungen zu einem erweiterten strafrechtlichen Gewaltbegriff stehen an. Der Begriff „Digitale Gewalt" wird im allgemeinen Sprachgebrauch bereits gleichgesetzt mit einer Vielzahl von Angriffsformen, bei denen die Anonymität des Internets und die technischen Möglichkeiten des virtuellen Raums bewusst eingesetzt werden.[29] Juristisch dagegen erschöpft sich der Gewaltbegriff in körperlich wirkendem Zwang, der im virtuellen Raum stets fehlt. Diese physische Gewalt gilt grundsätzlich als strafbar.

Es fragt sich, wie die *digitale Verbreitungs- und Wegbereitungs-Gewalt* im virtuellen Raum zu werten ist. Gefährdungen durch digitale Gewalt „nur im Netz" sind vielleicht mittlerweile schlimmer – weil dauerhafter, entgrenzter, die persönliche Intimsphäre weit umfassender verletzend als ein tätlicher Angriff und damit vielleicht sogar in der Wirkung auch körperlich brutaler – als die allseits geächteten Übergriffe im öffentlichen oder privaten realen Raum. Bisher gibt es für solche virtuellen Angriffe keine angemessenen Straftatbestände.[30] Als Gewaltdelikte können virtuelle Angriffe nur verfolgt werden, wenn sich die digitalen Angriffe, was in der Masse der Taten nicht der Fall ist, im realen Raum fortsetzen, z.B. als intendierte Bedrohung oder Nötigung. Hier liegen auch die Grenzen des Gewaltschutzgesetzes.[31] Wird die schädigende Wirkung eines Angriffs in erster Linie durch eine virale Verbreitung erzeugt, wird bei den Einzelnen, die zur Weiterverbreitung beitragen, von mangelnder Erheblichkeit oder fehlendem Vorsatz ausgegangen.

Dabei wäre digitale Gewalt durchaus strafrechtlich fassbar. Angesichts der Tatsache, dass sich ein ständig wachsender Teil unserer Lebensrealität in virtuellen Räumen abspielt, sind Straftatbestände unverzichtbar. Auch wenn eine Strafverfolgung erfolglos bleibt, weil die Ermittlung eines individuell verantwortlich handelnden und identifizierbaren „Täters" bei virtuellen anonymisierten oder auch Schwarmangriffen schwierig ist, kann auf die Klarstellung, dass die Unverletzlichkeit der Person auch im virtuellen Raum zu achten ist, nicht verzichtet werden. Die Schwierigkeit der Täter*innensuche sollte dabei nicht als Argument gegen anonyme Nutzungsmöglichkeiten des Internets instrumentalisiert werden. Vielmehr ist die anonyme Tatbegehung immer das Problem im Strafrecht und die Digitalisierung nur eine weitere Möglichkeit, kriminelle Aktivitäten zu tarnen. Es müsste darüber nachgedacht werden, wie digitale Gewalt in den Tatbeständen der Körperverletzungsdelikte, Sexualstraftaten, Nötigung, Bedrohung und natürlich als Cyber Stalking unter Strafe gestellt werden könnte.[32] Inwieweit hier auch neue Straftatbestände für den virtuellen Raum notwendig sind, wäre zu diskutieren.[33]

Bisher lassen sich virtuelle Angriffe in der Regel nur als Persönlichkeitsrechtsverletzungen verfolgen. Es bleibt bei der Anzeigemöglichkeit der Beleidigungsdelikte der §§ 185 ff. StGB, der Bildrechtsverletzungsdelikte nach § 201a StGB, § 33 KUG und der Datenveränderung nach § 303a StGB, die alle nur auf Antrag verfolgt werden. Die Verfolgung dieser Straftaten liegt mehr oder weniger brach. Ermittlungsaktivitäten müssen mühsam in Gang gesetzt werden. Ein grundsätzliches öffentliches Interesse an der Verfolgung dieser massenweise begangenen Delikte zu bejahen, erscheint hier auch eher keine Lösung zu sein. Denn die Ermittlungsintensität hält sich aufgrund der Vielzahl der Delikte und der technischen Ausstattungsanforderungen, die in umgekehrtem Verhältnis zur Personaldecke und Ausstattung bei Polizei und Staatsanwaltschaft stehen, schlicht schon faktisch in Grenzen. Dies würde sich wohl auch dann nicht ändern, wenn die Ermittlungsaufnahme ohne Anzeigenotwendigkeit im öffentlichen Interesse erfolgen müsste.[34]

Denkansätze zur Prävention durch Datenschutz- und Wettbewerbsrecht

Folgerichtig scheint also der Ruf nach einer effektiven vorbeugenden Gefahrenabwehr für den virtuellen Raum. Und es stellt sich die Frage nach einem angemessenen Ordnungsrahmen für die globalisierte Informationsgesellschaft. Es ist eine Herausforderung, nach Handlungsalternativen zu den bestehenden persönlichkeitsrechtsschützenden Abwehrinstrumenten

29 Eine solche weite Begriffsdefinition benutzt z.B. der bff Frauen gegen Gewalt e.V. https://www.frauen-gegen-gewalt.de/digitale-gewalt-was-ist-das.html.

30 Dazu Lembke, a.a.O., Fn. 6, S. 397/398 mit weiteren Nachweisen.

31 Freudenberg „Gewalt gegen Frauen im Internet – der rechtliche Rahmen und die Gesetzeslücken", in: BAG kommunaler Frauenbüros, a.a.O., Fn. 1, S. 17 f. Sie regt an, in § 1 GewSchG einen Beseitigungsanspruch aufzunehmen.

32 Freudenberg, a.a.O.; Lembke, a.a.O., S. 398.

33 Z.B. der Digitale Hausfriedensbruch, siehe dazu Gesetzesantrag des Landes Hessen: BR-Drs. 338/16 vom 17.06.2016; auch Bock, Harrendorf, a.a.O., Fn. 7.

34 Lembke hält ein öffentliches Interesse an der Strafverfolgung bei Cyber Harassment immer für gegeben, Lembke, a.a.O., Fn. 6, S. 398.

und einem sicherlich erforderlichen strafrechtlichen Abschreckungsrahmen zu suchen.

Die momentan stattfindende massive Ausbeutung unserer Privatsphären durch die datenverarbeitende Industrie kommt einer „kostenlosen Aneignung" von Körperlichkeit gleich, die verwundbar macht. Würde man das APR als „Eigentumsposition" ausgestalten,[35] so hätte das in einer kapitalistischen Wirtschaftsordnung zur Folge, dass dessen Ausbeutung zumindest „zu bezahlen und verhandelbar" sein müsste. Solchen Ausbeutungen und dem freien Verfügen über Körper strikt entgegenzutreten ist eine feministische Grundforderung. Ob eine Kommerzialisierung in Form von immateriellen „Personaldatengütern" in der Informationsgesellschaft wünschenswert ist oder geächtet werden sollte, ist dabei eine Diskussion, die über Gewaltprävention hinausgeht.

Besonders umstritten und heikel ist die Frage, welche Bedeutung dem Datenschutz in diesem Zusammenhang zukommt. Jedenfalls fragwürdig ist die weitverbreitete Ansicht, dass „Datenschutz stets Täterschutz" sei und nicht weiter ausgebaut werden dürfe, eher noch zurückgefahren werden müsse. Dabei ist zu unterscheiden zwischen dem Datenschutz als Abwehrrecht gegen Eingriffe von Seiten des Staates und Rechten auf den Schutz der persönlichen Daten vor dem Zugriff privater Dienstleister.

Die Lockerung des Datenschutzes, um staatliche Zugriffe zu ermöglichen, ist zur Zeit im Gang.[36] Im August 2016 hat Bundesinnenmister de Maizière ein weitreichendes Maßnahmepaket dazu vorgestellt, das u.a. auch die umstrittene Vorratsdatenspeicherung auf soziale Medien und Messenger-Dienste ausweiten soll. Solche Lockerungen von Datenschutz sind vielleicht sogar durchaus angemessen, denn die Verteidigung der Freiheitsrechte der Einzelnen könnte gegenüber dem Interesse des Staates an der Verfolgung Einzelner zurückzutreten haben, wenn es darum geht, die Freiheit aller bzw. die staatlichen freiheitsgewährleistenden Infrastrukturen zu verteidigen. Im Zeitalter von Cybergewalt könnte unsere Freiheit doch in größerem Ausmaß bedroht sein, als wir es im Moment noch ahnen oder wahrhaben wollen. Dabei soll hier sicher nicht einem Überwachungs- oder Zensurstaat oder kurzfristigen Anti-Terror-Maßnahmen das Wort geredet werden und es kann in diesem Beitrag nicht das Für und Wider dieser Maßnahmen dargestellt werden. Es soll nur deutlich gemacht werden, dass der Datenschutz als öffentlich-rechtliches Instrument vom Datenschutz als zivilrechtlichem Instrument strikt abgetrennt diskutiert werden muss.

Denn eingeschränkter Datenschutz im öffentlichen Recht in Form des erleichterten Zugriffs insbesondere der Strafverfolgungs- und Gefahrenabwehrorgane auf personenbezogene Daten seiner Bürger*innen eingebunden in internationale Fahndungsabsprachen muss eben nicht bedeuten, dass der Datenschutz im Sinne des Schutzes personenbezogener Daten gegen den Zugriff durch andere Zivilpersonen – dito international agierende datenverarbeitende Monopolisten – ebenfalls eingeschränkt werden müsste. Es ertönt aber schnell ganz allgemein der Ruf nach Lockerung von Datenschutz, wenn sich aufgrund von anonymer Nutzung des Netzes ein „Täter" zivilrechtlich nicht ermitteln lässt.

Ein geringer zivilrechtlicher Datenschutz kommt dem Selbstverständnis der amerikanischen Internetunternehmen entgegen, die in einem Rechtsraum beheimatet sind, in dem der Datenschutz europäischer Denkungsart schlicht unbekannt ist.[37] In den USA gilt es als Serviceleistung, wenn personenbezogene Daten von Kund*innen aufbereitet und in Form von personenbezogener Werbung genutzt werden. Unser medienrechtliches Trennungsgebot betreffend Werbung und redaktionelle Information ist unbekannt, das Verständnis und das Gewicht von Meinungsfreiheit weit umfassender als hier. Kommerzielle algorithmengestützte Anwendungen für große Datensammlungen personenbezogener Daten zu entwickeln (Big Data, Industrie 4.0) und solche Daten in möglichst großem Umfang auf Vorrat für zukünftige Zwecke und als Investition in die Zukunft zu erheben (Data Mining) gelten als zeitgemäße unternehmerische Leistung.[38] Jegliche rechtliche Einschränkung dieser

35 Ablehnend Hofstetter: „Sie wissen alles", München, 2014, S. 232 ff., personenbezogenen Daten fehle die Objekteigenschaft, die für den Eigentumsbegriff konstituierend sei; anders mit Bejahung einer Fungibilität von Verwertungsrechten an personenbezogenen Daten wohl Kilian: „Strukturwandel der Privatheit" in: Garstka, Coy (Hrsg.), „Wovon – für wen – wozu Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis", Berlin, 2014, S. 195 ff.

36 Überwachungsoffensive: Innenminister de Maizière fordert Vorratsdatenspeicherung für WhatsApp, Twitter & Co. auf: netzpolitik.org/2016/innenminister-de-maiziere-fordert-vorratsdatenspeicherung-fuer-whatsapp-und-soziale-medien/; außerdem dazu „Berliner Erklärung" der Innenminister und -senatoren von CDU und CSU zu Sicherheit und Zusammenhalt in Deutschland 19.08.2016, www.regierung-mv.de/serviceassistent/_php/download.php?datei_id=1577972, S. 4 f.; dagegen recht matt die „Stellungnahme zur Berliner Erklärung" der Bundesbeauftragten für den Datenschutz, www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2016/12_BerlinerErklaerung.html?nn=5217040.

37 Ausführlich dazu Selzer: „Datenschutz in Europa und den USA – Grenzüberschreitender Datenverkehr nach dem Safe Harbor Aus" auf www.sit.fraunhofer.de/fileadmin/dokumente/Presse/FraunhoferSIT-Selzer-SchaderStiftung.pdf?_=1453975039; eindringlich die Forderung nach „Internationalen Algorithmen-Abkommen" von Hofstetter, a.a.O., Fn. 35, S. 296 ff.; auch Stöcker, „Googles gnädige Kontrolleure" auf http://www.spiegel.de/netzwelt/netzpolitik/datenschutz-in-den-usa-und-europa-a-849114.html.

38 Sehr erhellend dazu das Buch der IT-Wirtschaftsjuristin Hofstetter, a.a.O., Fn. 35.

unternehmerischen Tätigkeit wird als unzumutbare Beschränkung verstanden.

Eine Durchsetzung deutscher datenschutzrechtlicher Grundsätze wie Datensparsamkeit und Datenvermeidung, strikte Transparenz, Zweckbindung und Datenvernichtung nach Beendigung des Nutzungsvorgangs ist im virtuellen globalisierten Wirtschaftsraum entsprechend schwer. Es stellt sich also zunächst schon die Aufgabe, das bestehende Datenschutzrecht möglichst durchsetzbar zu machen. Zur Zeit krankt der Datenschutz an einem Vollzugsdefizit und an der Marktmacht der ausländischen Unternehmen, denen gegenüber deutsches Datenschutzrecht schlicht nicht verbindlich ist. Die europäische Datenschutzgrundverordnung 2016/679 vom 27. April 2016 vereint hier die Kräfte, ist aber sicherlich auch erst der Anfang eines weiten Weges.

Die Frage ist, ob sich nicht mit massiv verstärktem zivilrechtlichem Datenschutz gepaart mit entsprechenden technischen, nicht zwingend staatlichen, sondern auch private Diensteanbieter verpflichtenden Infrastrukturmaßnahmen der virtuelle Raum entscheidend absichern, transparenter, gefährdungsfreier und leichter zugänglich gestalten ließe. Und ob sich damit nicht das zur Zeit ausufernde diskriminierende Verhalten im virtuellen Raum in den Griff kriegen ließe. Denn Frauenhass und Gewalt gegen Frauen sind und bleiben allgemeingesellschaftlich ein Problem. Sie sind nicht originär durch das Internet bedingt, sondern nur durch die massive Ausnutzung von technischen Möglichkeiten auch im Sinne von technisch zu einfachen Zugriffen auf personenbezogene Daten von Opfern verschärft. Insoweit hat die zunehmende Viktimisierung von Frauen auch schlicht Indikatorfunktion für Fehlentwicklungen im virtuellen Raum.

Sehr weitgehende Vorschläge finden sich beim Chaos Computer Club,[39] der es für alle Unternehmen verpflichtend machen will, einen sogenannten „Datenbrief" zu erstellen, der Auskunft über gespeicherte personenbezogene Daten gibt. Bisher gibt es im deutschen Datenschutzrecht zwar einen Auskunftsanspruch, der Unternehmen verpflichtet, die personenbezogenen Daten gegenüber Betroffenen offenzulegen.[40] Sobald jedoch „ein Interesse an der Wahrung des Geschäftsgeheimnisses" des Unternehmens überwiegt, läuft dieser Auskunftsanspruch ins Leere. Und Data-Mining ist stets Geschäftsgeheimnis. Ein Datenbrief, der ohne Antrag über die gespeicherten Daten informieren muss, könnte die informationelle Selbstverteidigung stärken und die Anhäufung von personenbezogenen Daten für Unternehmen möglichst unattraktiv machen.

Gefordert wird damit eine Umkehr der bisherigen Praxis, wo Bürger*innen mit ihrem Auskunftsantrag als Bittsteller*innen gegenüber datenspeichernden Stellen auftreten.[41] Es sei an der Zeit, die Asymmetrie zwischen Personen, deren persönliche Daten oft ohne ihr Wissen verarbeitet werden, und Unternehmen, die solche großen Sammlungen anlegen, weiterverarbeiten oder verkaufen, zu beenden. Das würde nicht nur die Weitergabe und den Verkauf der eigenen Daten an potenzielle Täter erschweren, sondern insbesondere auch die Durchsetzung des Anspruchs auf Löschung der Daten wesentlich erleichtern.

Die momentane Praxis der intransparenten Verträge, in denen Personen datenschutzrechtliche Einwilligungserklärungen abgeben, deren Tragweite sie nicht kennen, oder umfänglichen vertraglichen Nutzungen ihrer personenbezogenen Daten in AGB zustimmen, muss beendet werden. Das gilt insbesondere für die große Gruppe der Kinder und Jugendlichen. Es ist zu erwarten, dass solche Zustimmungen zu Nutzungen personenbezogener Daten zurückhaltender erfolgen, wenn Personen wissen, welche Daten wo über sie gespeichert sind und wenn sie davon ausgehen können, dass Datenspeicherungen sparsam zu erfolgen haben. Erhalten Nutzer*innen regelmäßig Auskunft über Datenprofile und können sie deren Löschung veranlassen, dann ist es auch eher möglich, den eigenen Auftritt im virtuellen Raum zu kontrollieren und sich zu schützen. Wichtig in diesem Kontext sind auch entsprechende Bildungsinvestitionen und Medienschulungen.

Eine solchermaßen datenschutzrechtlich unterstützte selbstbestimmte Teilnahme an digitaler Kommunikation wäre zu ergänzen mit allen Nutzenden gleichermaßen zur Verfügung zu stellenden Verschlüsselungstechniken. Der zivilrechtliche Datenschutz braucht ergänzend den verpflichtenden technischen Datenschutz. Datenverschlüsselung und ein Anspruch auf strikte Datensparsamkeit als Mittel zum informationellen Selbstschutz sind ein Grundrecht.[42]

Bei Schaffung dieser Datenschutzinfrastruktur ist nicht nur der Staat sondern auch jedes einzelne datenverarbeitende Unternehmen in die Investitionspflicht zu nehmen. Das erfordert wirtschaftsregulierende Maßnahmen, vor denen gerade im Hinblick

39 https://www.ccc.de/de/datenbrief.
40 § 34 BDSG.

41 Wobei der CCC auch einen weitgehenden öffentlichrechtlichen Datenschutz mit einschließt.
42 Siehe dazu auch den Entwurf einer „Charta der Digitalen Grundrechte der Europäischen Union" auf https://digitalcharta.eu.; dagegen sieht die Initiative „Algorithm Watch" diese Charta als populistisch an, da keine neuen digitalen Grundrechte nötig seien, sondern Transparenz bei den Datenfusionen, um die Grundrechte auch im digitalen Zeitalter wahren zu können, siehe dazu das ADM-Manifest (ADM=algorithm decision making) auf http://algorithmwatch.org/das-adm-manifest-the-adm-manifesto.

auf die wirtschaftspolitische Förderung der Industrie 4.0 politisch gerne zurückgeschreckt werden wird. [43] Gerade hier müssen Jurist*innen interdisziplinär arbeiten, um rechtliche Anforderungen an Datenschutz formulieren zu können. So ist es technisch möglich, Nutzungsdaten extrem sparsam zu erheben.[44] Technischer Datenschutz bedingt einen erhöhten Schutz für alle Personen, die sich im virtuellen Raum bewegen.

Insoweit ist auch der Ruf nach Einschränkung der anonymen Nutzung des Internets abzulehnen. Die anonymen Nutzungsmöglichkeiten machen einen Teil des Selbstverständnisses der Internetgemeinde und damit einer digitalen Informationsgesellschaft erst aus und bilden eben nicht nur für Täter*innen sondern auch für die Opfer digitaler Gewalt gleichermaßen Schutz. Vergleichbar ist das mit der Möglichkeit mit Bargeld zu zahlen und sich nicht bei jedem Konsumvorgang, sprich jeder medialen Nutzung personenbezogen zu outen.

Die Klarnamenpflicht, Lieblingsforderung von Facebook, das die Personenbezogenheit von Daten als sein Grundkapital und seine Kund*innen als Ware ansieht, hat jedenfalls eine Kehrseite. Das gilt auch für den Rechtsgrundsatz der Anbieterkennung des § 5 TMG bzw. § 55 Rundfunkstaatsvertrag. Diese verlangen bei Betrieb einer Website die Angabe des Namens einer natürlichen Person und ihrer Anschrift. Und das erfasst jede auch nur nebenberuflich betriebene Blogseite, zumindest wenn sie sich auch über Werbung finanziert oder mit einem beruflichen Hintergrund oder professionellen Anspruch betrieben wird.[45] Dahinter steht der alte presserechtliche V.i.S.d.P.-Grundsatz,[46] dass die Inanspruchnahme von Meinungsfreiheit, auch von medialer Berufsfreiheit immer durch die Freiheit anderer begrenzt ist, und diesen eine zustellungsfähige Anschrift für rechtliche Schritte wie die klassische Gegendarstellung zur Verfügung gestellt werden muss. Eine E-Mail-Adresse reicht nicht aus. Das kann insbesondere für beruflich als Journalistinnen und Bloggerinnen aber auch als Wissenschaftlerinnen oder Unternehmensberaterinnen – in einer feministischen Gegenöffentlichkeit unverzichtbare Stimmen – mit einer hohen Selbstgefährdung im realen Raum verbunden sein. Hier liegt eines der vielen Hindernisse beim Schutz gegen Cybermobbing und digitale Bedrohungen.

Um einen Selbstschutz gegen Hassattacken zu ermöglichen, ohne zugleich rechtswidrige Angriffe zu sehr zu erleichtern, könnten rechtliche Möglichkeiten geschaffen werden, eine private Adresse im Netz nicht angeben zu müssen, sondern sie z.B. bei einer öffentlichen Stelle zu hinterlegen.[47] Inwieweit hier antidiskriminierungsrechtlich motivierte Lockerungen der Impressumspflichten und ein durch staatliche Schutzstellen vermittelter anonymisierter virtueller Raum garantiert werden müsste, ist durchaus eine Überlegung wert. Die Möglichkeit der Hinterlegung des Klarnamens mit Anschrift bei einer staatlich kontrollierten Stelle, um unter Pseudonym im Netz auftreten zu können, könnte einen staatlichen Schutzschild bilden für geförderte Teilöffentlichkeiten und Counterspeech und eine Aufgabe für Antidiskriminierungsstellen sein. Besteht eine solche Infrastruktur, wird der virtuelle Raum auch für diskriminierungsgefährdete Gruppen wieder betretbar. Das versetzt die Gesellschaft in die Lage, geschützte Gegenöffentlichkeiten im Netz aufzubauen und dem Phänomen digitaler Gewalt so entschlossen entgegenzutreten wie der Gewalt im realen öffentlichen Raum. Das wäre auch für Frauen eine Möglichkeit, sich wieder verstärkt in den virtuellen Dialog einzubringen.

Diskutiert wird auch eine Ausweitung der Host-Providerhaftung.[48] Für im Netz als sogenannte „soziale Medien" bereitgestellte Kommunikationsplattformen soll den Host-Provider eine erweiterte Verantwortung treffen, die über die bisherige Störerhaftung noch hinausgeht. Für auf seinen Plattformen begangene Persönlichkeitsrechtsverletzungen sollen den Host-Provider also nicht mehr nur Unterlassungs- und Beseitigungspflichten mit mehr oder weniger ausgeprägten Prüfpflichten treffen, sondern die Host-Provider soll als „Gefährder" eine Verpflichtung zu pauschalen Schadensersatz- bzw. Schmerzensgeldzahlungen treffen.

Dies würde allerdings das Internet als freiheitlichen Raum für alle und als geringschwellig zugänglichen Raum für gewerblich Handelnde insbesondere auch Medienschaffende in Frage stellen. Eine Errungenschaft des digitalen Zeitalters ist es, dass Meinungsforen, digitale Vernetzung, alle Arten medialer Veröffentlichungen und medialer Teilhabe ohne große Investitionen in Material und Vertrieb revolutionär einfach für alle geworden sind. Diensteanbieter generell zu einer Art virtueller blitzschnel-

43 2016 wiesen nahezu alle geprüften „Smart-Geräte" des „Internets der Dinge" datenschutzrechtliche Lücken auf, dies ergab eine internationale Prüfaktion des Global Privacy Enforcement Networks, siehe dazu PM des Bayerischen Landesamts für Datenschutzaufsicht v. 16.9.2016 auf https://www.lda.bayern.de/media/pm2016_06.pdf.

44 Siehe dazu Zimmermann, Rodewig, „Differential Privacy" in ct Nr.23/2016, S. 28.ff., der Bericht bezieht sich auf die Forschungen der Informatikerin Cynthia Dwork, die schon 2006 ein Verfahren entwickelt hat, mit dem sich Daten bereits beim Erfassungsvorgang anonymisieren lassen.

45 Zur Weite des Impressumsbegriffs und Abgrenzungsfragen siehe www.linksandlaw.info/Impressumspflicht-Notwendige-Angaben.html.

46 V.i.S.d.P. = Verantwortlich im Sinne der Pressegesetze, das bezog sich eigentlich nur auf gedruckte Meinungsäußerungen.

47 Siehe dazu schon die Fachstellungnahme im Rahmen des 40. FJT, AG 3: Digitale Gewalt und Persönlichkeitsrechtsverletzungen im Netz, in: STREIT 2014, S. 94.

48 Siehe dazu Fn. 27.

ler Nachzensur bzw. Redaktion ihrer Plattformen anzuhalten, um eine geschlechtergerechte Teilhabe von Frauen bzw. auch anderer diskriminierter Gruppen zu gewährleisten, und sie andernfalls in Haftung zu nehmen, erscheint nicht wünschenswert und faktisch kaum machbar.

Wenn eine Gefährdungshaftung in den Blick genommen werden soll, wäre höchstens zu überlegen, inwieweit mit einem medienrechtlichen Ansatz, der zwischen „informationsaffinen" Host-Providern und an der Generierung möglichst vieler personenbezogener Daten geschäftlich interessierter, „datenaffiner" Host-Provider unterscheidet, eine Ausdifferenzierung von Haftungsprivilegien im TMG möglich wäre. Auch so ließe sich eine Ausdehnung der zivilrechtlichen Verantwortung hin zu pauschalierten Schadensersatzzahlungen erreichen in einer datenschutzrechtlichen Variante. Es könnte mit einer Transparenzpflicht bei der Verarbeitung und Speicherung personenbezogener Daten eindeutig quantitativ gemessen werden, wer zur Verantwortung gezogen werden soll. Data-Miner, denen es wie Facebook darauf ankommt, große Datenmengen ihrer Nutzer*innen zu hosten und möglichst uneingeschränkt ausbeuten zu können, träfe dann so etwas wie eine Gefährdungshaftung für Persönlichkeitsrechtsverletzungen. Privilegieren ließen sich dagegen Plattformen, die Datensparsamkeit und unverzügliche Datenvernichtung auf ihren Plattformen standardisieren, sich technischer Mittel wie der „differential privacy"[49] bedienen und nur Informations- und Kommunikationshosting anbieten wollen. Wenn frau auf solchen Plattformen eine feministische Meinung vertritt oder bloggt, kann sie dies nämlich unter Pseudonym und ohne Datenspuren tun.

Richtig sind in diesem Zusammenhang auch wettbewerbsrechtliche Überlegungen. Zum einen bieten sich im kollektiven Wettbewerbsrecht Möglichkeiten, den Zugang zu wettbewerbsrelevanten personenbezogenen Daten bei der Prüfung der Marktbeherrschung von Unternehmen ausdrücklich zu berücksichtigen und damit „Datenmonopolisten" bekämpfbar zu machen.[50] Inwieweit sich durch peer-to-peer-Technologien sog. Datenkraken wie Facebook schlicht umgehen lassen,[51] ist daneben wieder eine technische Frage. Das Erleichtern von Meinungsvielfalt und damit ein Erschweren auch von meinungsbeherrschender Weg-

bereitungsgewalt wäre wünschenswert. Hier könnten wirtschaftliche Subventionen lohnend sein, durch die die rechtliche Zerschlagung der Plattformmonopole oder ihre Verzichtbarkeit durch technische Alternativen ermöglicht würden. Schließlich ließe sich die frauenverachtende mediale Bilderflut, die Gewalt in jeder Form begünstigt, durch ein Verbot geschlechtsdiskriminierender Wirtschaftswerbung auch individual-wettbewerbsrechtlich bekämpfen.[52]

Wirtschaftsrechtliche Regulierungsanstrengungen heraufzufahren erscheint also durchaus erstrebenswert. Dabei muss der internationale Aspekt im Auge bleiben. Staatliche Alleingänge, wie es Deutschland beim zivilrechtlichen Datenschutzrecht durchaus versucht hat, bleiben im Zeitalter der Globalisierung weitgehend ineffektiv, wenn sie nicht durch internationale Zusammenarbeit gestärkt werden. Insoweit ist die Europäische Datenschutzgrundverordnung zu begrüßen, auch wenn sie Deutschland datenschutzrechtlich auf einen geringeren Standard zurückwerfen wird. Internationale Abkommen zum zivilrechtlichen Datenschutz stehen aus. Anders als im Bereich des rechtlich fast weltweit abgesicherten geistigen Eigentums stehen hier Verhandlungen noch ganz am Anfang.[53]

Ausblick

Im derzeitigen Informationskapitalismus haben sich Monopole etabliert, die die Freiheit aller bedrohen. Sie verfügen über personenbezogene Daten und über Schlüsseltechnologien zu deren Analyse. Dabei stehen heutige BigData-Anwendungen technisch noch ganz am Anfang. Indem personenbezogene Daten mit mathematischen Modellen ausgewertet werden, wird der Mensch zum reinen Objekt, zur Ware gemacht. Ein Phänomen, das der pornografisierten Darstellung von Frauen entspricht. Als Subjekt Träger*innen von Rechten und Pflichten zu sein, ist aber die Errungenschaft unserer demokratischen freiheitlichen Gesellschaften. Entsprechend fragt es sich, ob die datenverarbeitende Industrie die gesellschaftlich mittlerweile geächtete Atomindustrie als neue Risikotechnologie ablöst.[54] Die aktuelle Weigerung der Industrie, Datenerhebungen und Datenfusionen auch nur annä-

49 Siehe dazu Zimmermann, Rodewig, a.a.O., Fn. 44.

50 In diese Richtung geht jetzt ein Gesetzentwurf des Bundeswirtschaftsministers, siehe PM vom 28.9.2016, http://docs.dpaq.de/11349-pm_neuer_ordnungsrahmen_f_r_den_wettbewerb_in_einer_digitalisierten_welt.pdf.

51 Immer noch sehr hörenswert dazu der CCC-Podcast Chaosradio „Dezentrale Soziale Netzwerke, Facebook ist tot! Hoch – die – internationale – Dezentralität!" auf https://chaosradio.ccc.de/cr168.html.

52 Dazu Völzmann, „Spießigkeit oder Geschlechtergerechtigkeit? – Für ein Verbot sexistischer Werbung" in STREIT 2016, S. 51 ff.

53 Nach dem Ende des Safe-Harbour-Abkommens sind auch die Verhandlungen zur Nachfolgevereinbarung Privacy Shield stark umstritten, siehe dazu Selzer, a.a.O. Fn. 37.

54 So Hofstetter, a.a.O., Fn. 35, S. 172 ff, die lebensbedrohliche Gefahren der neuen Datenfusionstechnologien im „terra forming" der globalen datengetriebenen Finanzmärkte sieht und eine Ächtung des Hochfrequenzhandels anregt.

hernd für die betroffenen Menschen transparent zu machen, weist tatsächlich in diese Richtung. Und Gesetzgeber und Gerichte erscheinen angesichts der globalen Ausbreitung und Vernetzung der Datenindustrie relativ hilflos.

Die Risiken der atomaren Strahlung wurden lange verschwiegen und kleingeredet. Staatliche Stellen forderten die Menschen zunächst auf, sich mit einer Aktentasche gegen atomare Strahlung zu schützen. Aktuell erscheint die gutgemeinte Schirmherrschaft des BMFSFJ für die Youtube/Google-Counterspeech-Kampagne *„nicht egal"*,[55] mit der zum Selbstschutz gegen Hate Speech aufgerufen wird, so wenig hilfreich wie diese Aktentasche. Es hat lange gebraucht, sich die Bedrohung durch die und die gesellschaftlichen Kosten der Atomtechnologie bewusst zu machen und es steht immer noch an, die Auswirkungen wirtschaftspolitischer Entscheidungen der Vergangenheit zu korrigieren. Und gemäß Straßenverkehrsrecht bewegt sich, wer ein für die körperliche Unversehrtheit anderer Verkehrsteilnehmer*innen durch technische Überlegenheit gefährliches Werkzeug – sprich Auto – benutzt, nur zwangsversichert und mit entsprechender Ausbildung auf den Straßen. Das erscheint auf digitalen Autobahnen noch undenkbar. Diesen Weg präventiver Regulierung werden wir angesichts der Gefahren durch digitale Gewalt auch im virtuellen Raum gehen müssen.

55 YouTube Initiative „Hass ist uns #NichtEgal" https://nichtegal.withyoutube.com/ mit Schirmherrschaft des BMFSFJ, siehe dazu auch Kaschel, „YouTubes Anti-Hass-Initiative geht nach hinten los" im online-Magazin wired, https://www.wired.de/collection/life/youtubes-anti-hass-initiative-nichtegal-geht-nach-hinten-los.