Daraus ergeben sich neue Aushandlungsprozesse bezüglich des Schutzes privater Einzelmeinungen vor sozialen und kollektiven Kontrollmechanismen, die sich in (Be-)Drohungen äußern können; des Schutzes der freien Meinungsbildung vor der Dominanz der öffentlichen Meinung; des Schutzes digitaler Öffentlichkeiten vor staatlichen Repressionen, etc. Kurz gesagt: Es geht erneut um die Aushandlung der Frage, welche individuellen Praktiken unter soziale und öffentliche Kontrolle gestellt werden müssen und in welchen Bereichen das Individuum vor der Öffentlichkeit und dem Staat geschützt werden muss und damit auch darum, welches Primat in digitalen Kommunikations- und Handlungskontexten jeweils vorherrschen soll.

Die Abwägung zwischen öffentlicher Kontrolle und individuellen Abwehrrechten im digitalen Raum gleicht dabei einem Drahtseilakt. Es stellt sich einerseits die Frage, inwieweit das Individuum vor Konsequenzen der Verdatung und Digitalisierung im öffentlichen Leben rechtlich geschützt werden kann, ohne dabei gesellschaftliche Interessen – beispielsweise an sicherheits- oder gesundheitsbezogenen Daten – zurückzustellen. Andererseits lässt sich fragen, wie kollektiven Interessen Rechnung getragen werden kann, wenn einzelne Akteure oder das Nebeneinander von (digitalen) Öffentlichkeiten das Potenzial haben, Kollektivinteressen auszuhebeln bzw. sich insgesamt problematische gesellschaftliche Tendenzen im Rahmen der Formierung digitaler Kollektive zeigen.

Diesen Problematiken an der Schnittstelle von individueller Freiheit und kollektivem Interesse widmen sich die Autorinnen dieser Sektion aus unterschiedlichen Perspektiven.

Autorinnenbeiträge

Wulf Loh beschreibt individuelle Anerkennungserkennungskonflikte im Kontext kollektiver Normen aus einer praxistheoretischen Perspektive und benennt Probleme informationeller und dezisionaler Privatheit in digitalen Kontexten als soziale Pathologien. Diese fasst er zunächst als strukturelle Defizite in den Rollenverständnissen im Rahmen von Verdatungspraktiken auf. Hierzu nutzt er das „social-ontological recognitional model of privacy" (SORM), in dem zwei Kategorien von Rollen bzw. Rollenträgerinnen unterschieden werden: Zum einen Trägerinnen konstitutiver Rollen (TkR), die in der Regel als Standardautorität in sozialen Praktiken anerkannt werden, und zum anderen Trägerinnen akzidenteller Rollen (TaR), denen diese Standardautorität nicht zuerkannt wird. Neben dieser sozialontologischen Grundlegung unterscheidet Loh weiter zwischen sozialen

Pathologien erster und zweiter Ordnung. Eine *Pathologie erster Ordnung* liege dann vor, wenn eine Nichtanerkennung der Praxisteilnehmenden als Standardautorität erfolgt und diese Missachtung erkannt und durch die Teilnehmenden gezielt artikuliert wird. Spätestens dann, wenn die Verweigerung der Anerkennung als Standardautorität innerhalb einer bestimmten (Daten-)Praxis allgemein akzeptiert ist – also kein Widerstand mehr gegen die Nicht-Anerkennung erfolgt –, lässt sich nach Loh von einer *Pathologie zweiter Ordnung* sprechen. Sich daraus ergebende Resignationen (z. B. „Google hat ja sowieso alle meine Daten!") könnten sich nach Loh unter Umständen auch in kognitiven Dissonanzen wie dem oft untersuchten Privacy Paradox äußern. Damit unternimmt der Beitrag einen ersten Versuch zur sozialontologischen Klärung von Privatheitsphänomenen, die bislang vor allem kognitions-, motivations-, und medienpsychologisch untersucht wurden.

Christian Thies befasst sich in einem philosophischen Essay mit dem Ressentiment im digitalen Zeitalter und skizziert dabei Dynamiken im Internet, die durch das Kollektiv als anonyme Masse entstehen können. Dabei problematisiert er insbesondere die zunehmende Emotionalisierung digitaler Kommunikation. Im ersten Teil des Beitrags unternimmt Thies zunächst eine Begriffsgenese des Ressentiments, wobei er die negativen sozialen Gefühle Groll und Neid als konstituierend für das Entstehen von Ressentiments betrachtet. Wesentliche Aspekte bei der Genese von Ressentiments seien weiter die Verselbständigung und Ablösung vom eigentlichen Grund oder Objekt der Gefühle und die Tendenz zur Generalisierung und Übertragung auf ganze soziale Gruppen. Eine besondere Gefahr bestehe darin, wenn Ressentiments politisch funktionalisiert würden. In modernen Gesellschaften braue sich dabei ein gefährliches Syndrom zusammen, das aus Ressentiments, kollektivem Narzissmus und der Verehrung autoritärer Führungspersönlichkeiten bestehe. Durch die Digitalisierung erfahre dieses Syndrom noch Aufwind, denn bestimmte Aspekte digitaler Medienangebote hätten das Potenzial, Ressentiments, bereits vorhandenen Hass und Rassismus zu verstärken. Thies geht im zweiten Teil seines Essays den Gründen für diese Verstärkung in der digitalen Welt nach – etwa den gesteigerten Möglichkeiten zu sozialen Vergleichen –, und diskutiert in einem dritten Teil Lösungsansätze.

Anna K. Bernzen nimmt das Verhältnis von Privatheit und Öffentlichkeit im sensiblen Bereich von Gerichtsverhandlungen in den Blick. Hier geht es vor allem um die Live-Berichterstattung aus dem Gerichtssaal, die im Konflikt zwischen Öffentlichkeitsherstellung und einer möglichen Verletzung der Unabhängigkeit der Justiz steht. Bernzen diskutiert das Dilemma, justizielles Handeln einerseits für die Öffentlichkeit transparent und

unmittelbar zugänglich zu machen (Kontrollfunktion der Medien), andererseits Vorabverurteilungen durch die öffentliche Meinung sowie die Beeinflussung der Gerichte in ihrer unabhängigen Urteilsfindung weitgehend zu vermeiden. Bernzen untersucht die derzeit geltenden Regelungen zur Gerichtsöffentlichkeit und schildert aktuelle und durch die Digitalisierung im Bereich der Medienberichterstattung erst möglich gewordene Fallbeispiele und potenzielle Problemkonstellationen. Es wird aufgezeigt, dass die bestehenden Normen Lücken aufweisen, die es zu schließen gelte. Derzeit bediene sich die Praxis dazu der Einschränkungsmöglichkeit mittels sitzungspolizeilicher Maßnahmen. Als alternative Lösung wird von Bernzen eine Gesetzesanpassung vorgeschlagen, die den aktuellen Stand der Technik umfassend berücksichtigt. Dabei wird zwischen reinen Bild- und reinen Ton-Aufnahmen, Bild/Ton-Aufnahmen sowie Textberichten in Echtzeit unterschieden. Bernzen justiert dabei interessengerecht anhand der dargelegten Problemfelder, wobei die Autorin zwar für eine Verschärfung durch neue Verbote, jedoch auch für Lockerungen – etwa im Bereich der Textberichterstattung aus dem Gerichtssaal heraus – plädiert, im Gegensatz zur aktuell verbreiteten Praxis meist umfangreicher Ausschlüsse durch sitzungspolizeiliche Maßnahmen.

Eine andere Perspektive nimmt *Christian Lenk* ein, indem er sich der Thematik von Privatheit und Vertraulichkeit in der Medizin widmet und das Verhältnis zwischen öffentlicher und privater Gesundheitsvorsorge beleuchtet. Das Kollektiv bildet hier keine anonyme Masse, sondern erscheint konkret als Versicherungsgemeinschaft, die in die (finanzielle) Pflicht genommen wird, sobald ein Mitglied erkrankt. Vor allem durch die Digitalisierung – beispielsweise durch die Einführung der elektronischen Patientenakte oder die vermehrte Nutzung von Health- und Tracking-Apps – scheint sich die Diskussion von Patientinnenrechten zu verkomplizieren: Auf der einen Seite wird völlige Transparenz und Zugänglichkeit der Daten zum Zwecke von Forschung und Wissenschaft im öffentlichen Interesse gefordert, auf der anderen Seite steht der unveräußerliche Schutz der Patientinnendaten vor der Öffentlichkeit. Ethische und rechtliche Brisanz besteht nach Lenk insbesondere bei genetischen Daten, beispielsweise bei vererbbaren Krankheiten: Haben Betroffene das Recht, eine vererbbare Erkrankung nicht zu erfahren oder darüber zu schweigen, obwohl nahe Verwandte auch betroffen sein könnten? Dürfen Eltern darüber bestimmen, ob ihr Kind auf eine genetische Erkrankung getestet wird oder nicht? Unterliegt die Diagnose einer vererbbaren Krankheit überhaupt einem Anspruch auf Privatheit oder steht sie im öffentlichen Interesse? An dieser Schnittstelle zwischen Ethik, Recht und Medizin fragt Lenk nach den normativen Grundlagen eines *Rechts auf Nichtwissen*

und diskutiert, wie sich ein solches Recht zum allgemeinen Anspruch auf Privatheit verhält. Anknüpfend an eine Begriffsgenese von Privatheit skizziert Lenk im Artikel theoretische und rechtliche Begründungsansätze eines Rechts auf Nichtwissen am Beispiel des Gendiagnostikgesetzes (GenDG).

2.3 Anonymität und Transparenz, Autonomie und Verantwortung in digitalen Öffentlichkeiten

Durch den derzeitigen Stand der Digitalisierung und Datafizierung alltäglicher, sozialer und politischer Prozesse hat sich nicht nur das Verhältnis zwischen Privatheit und Öffentlichkeit gewandelt, sondern Konfliktfelder für Autonomie und Verantwortung entstehen auch *innerhalb* digitaler Öffentlichkeiten. Entsprechend werden in der dritten Sektion Faktoren der Einflussnahme formgebender Strukturen digitaler Plattformen auf die Konstitution digitaler Öffentlichkeiten diskutiert.

Zwei zentrale Themenkomplexe in diesem Kontext markieren die Begriffe Anonymität und Transparenz. Unter Anonymität kann allgemein eine Handlung oder Äußerung verstanden werden, die keiner Person direkt zugeordnet werden kann.[117] Das Bundesamt für Sicherheit in der Informationstechnik nennt hierzu drei Ausprägungen von Anonymität: Eine Person ist dann anonym, wenn sie Anderen nicht bekannt ist (Nichtbekanntsein), nicht erfahrbar in Erscheinung tritt (Nichtgenanntsein) oder ohne Erkennbarkeit und Zurechenbarkeit handelt (Namenlosigkeit).[118] Anonymität bewahrt das Individuum dabei zunächst vor den sozialen Folgen einer Handlung oder Äußerung wie zum Beispiel in Form sozialer Ächtung oder Beeinflussung. Anonymität übernimmt damit Funktionen dezisionaler Privatheit nach Rössler und schützt vor gesellschaftlicher Einflussnahme. So kann man behaupten, dass freie Meinungsäußerung – im Digitalen wie im Analogen – „ohne ein gesichertes Maß an Privatheit nicht möglich ist“[119] und Anonymität zunächst einmal dazu dient, diesen

117 Vgl. hierzu exemplarisch Thiel (2016: S. 16); zum Verhältnis von Anonymität und Pseudonymität aus datenschutzrechtlicher Perspektive anhand des Grades der Zuordenbarkeit von Informationen zu einem Subjekt, vgl. Härting, NJW 2013, 2065; zu den verschiedenen Erscheinungsformen von Pseudonymität, vgl. Schleipfer, ZD 2020, 284.

118 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2018); vgl. auch Deremetz (2018: S. 12).

119 Keber (2018: S. 272).

Schutz zu gewährleisten.[120] Gleichzeitig kann Anonymität nicht nur einen Nutzen für das Individuum, sondern auch für die Gesellschaft oder das öffentliche Interesse darstellen, wenn beispielsweise durch ‚Whistleblowing' geheime Unterlagen ‚geleakt' werden, die ohne den Schutz der Anonymität nie veröffentlicht worden wären, was gesellschaftlichen Schaden abzuwehren hilft. Das gleiche Prinzip findet man im Journalismus, bei dem der Schutz der Quellen vor Veröffentlichung ein zentrales Element der Pressefreiheit darstellt.[121]

Auf der anderen Seite wird Anonymität im Zuge der Digitalisierung vermehrt auch kritisch betrachtet. So zeigen Hass-Kommentare, Shitstorms sowie anonyme Androhungen von Gewalt im Netz problematische Tendenzen von Anonymität auf. Aufgrund einer erschwerten Rückverfolgung können in digitalen Kontexten Handlungen und Äußerungen stattfinden, die im Schutz des Anonymen selbst das Potenzial haben, die freie Meinungsäußerung zu behindern und gesellschaftliche Strukturen zu destabilisieren. Anonymität wird dadurch im Diskurs zuweilen auch mit einer Gefährdung für demokratische Gesellschaften[122] und Individuen gleichgesetzt, wo sie eigentlich das genaue Gegenteil versprach.

Die Aufhebung oder Einschränkung von Anonymität im Netz wird auch unter dem Begriff der ‚Transparenz' gefordert. Hiermit ist dann die Sichtbarmachung oder das In-Erscheinung-Treten der individuellen Person hinter einer Handlung bzw. Äußerung gemeint.[123] Das Ziel ist dabei häufig, durch die Offenlegung und Sichtbarmachung der Nutzenden das Verhalten im Netz unter stärkere staatliche und gesellschaftliche Kontrolle zu stellen und damit soziale Ordnungen und Verhaltensregeln durchzusetzen, bzw. an bestehendes Recht zu binden. Allerdings sind nicht nur Individuen, sondern auch Unternehmen – insbesondere IT-Konzerne – und Regierungen aufgefordert, im Netz wie auch in ihren wirtschaftlichen Unternehmungen und regierungspolitischem Handeln so transparent wie möglich zu agieren, sei es, dass Algorithmen einsehbar sein sollen, sei es, dass die Verarbeitung von Nutzendendaten so transparent wie möglich gehalten werden soll.

120 So auch Berger (2018: S. 21).

121 Vgl. § 53 Abs. 1 S. 1 Nr. 5 StPO, sowie den in ständiger Rechtsprechung des EGMR durch Art. 10 EMRK bestehenden Schutz journalistischer Quellen, vgl. EGMR, Urt. vom 22.11.2007 — Az. 64752/01 (Rs. *Koen Voskuil* vs. Niederlande); Urt. vom 27.11.2007 — Az. 20477/05 (Rs. *Tillack* vs. Belgien).

122 Vgl. Thiel (2016: S. 19).

123 Vgl. Matzner (2018: S. 88).

Transparenz fungiert dabei zuweilen sogar als Gegenbegriff zur (staatlichen) Überwachung, wenn sie als Form sozialer Kontrolle der staatlichen Macht und als ein Bottom-up-Prozess verstanden wird, während Überwachung als ein Top-Down-Prinzip erscheint und als Werkzeug der ‚Mächtigen'.[124] Aus der einseitigen Überwachung der Bürgerinnen wird dann durch das Mittel der Transparenz eine gegenseitige Überwachung und Kontrolle.[125] Transparenz kann so auf der einen Seite zwar als Schutz der Bürgerinnen vor dem Staat oder anderen Machtinstanzen verstanden werden, auf der anderen Seite wird Transparenz durch die stattfindende Selbstveröffentlichung im Digitalen nunmehr allerdings auch von ihnen selbst gefordert.

Eine umfassende gesellschaftliche Transparenz birgt wiederum Gefahren für demokratische Gesellschaften und individuelle Freiheitsrechte. So wird Transparenz in der Kritik mit einer möglichen Totalüberwachung der Gesellschaft gleichgesetzt.[126] Der Konflikt zwischen Sichtbarkeit und Anonymität wird zudem durch strukturelle Machtgefälle gerahmt. Laut Matzner bedeute dies,

> dass solch eine ‚transparente' Gesellschaft für diejenigen mehr Probleme verursachen würde, die sich oft an den schwächeren Enden solcher Machtbeziehungen finden. Die umfassende Forderung nach Offenheit und Transparenz wäre somit eine Moral für Starke. Und tatsächlich stammen solche Vorschläge oft von erfolgreichen, weißen Geschäftsmännern.[127]

Als Strukturgeber des Verhältnisses zwischen Anonymität und Transparenz im Netz wirken zum einen der Staat, welcher die Kommunikation gewissen Regularien unterwirft, und zum anderen die Plattformbetreiber selbst. Gerade die Plattformbetreiber gestalten die soziale Interaktion durch die rahmensetzende Funktion ihrer Angebote, sie entscheiden über Partizipationsmöglichkeiten innerhalb ihrer Plattformen. Dabei wird

---

124 Vgl. Heller (2011: S. 110 f.).

125 Heller etwa entwirft die totale Transparenzgesellschaft als positives Gegengewicht zur staatlichen Überwachung, denn wenn „die Überwachung schon total wird und alle erfasst, dann soll sie wenigstens auch allen zur Verfügung stehen. Dann lässt sie sich nämlich nicht nur von der Macht gegen uns einsetzen, sondern auch von uns gegen die Macht. Die totale Überwachung wird zur totalen Transparenz." (Heller 2011: S. 111). Siehe als dazu konträre Position auch Han (2012).

126 Vgl. hierzu Han (2012).

127 Matzner (2018: S. 87 f.).