DFG Graduiertenkolleg
Privatheit und Digitalisierung

UNIVERSITÄT PASSAU

Anonymität

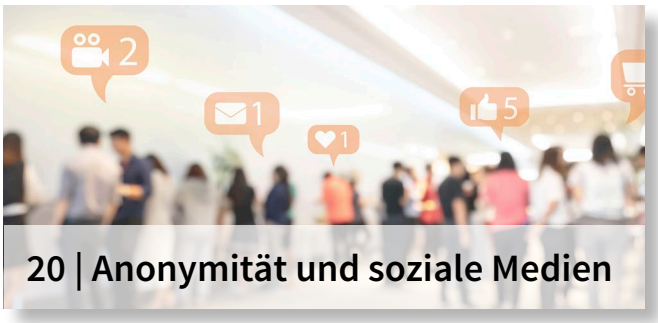
AUSGABE NR. 11, DEZEMBER 2018

Inhalt

3 | Zwischen Troll und Teilhabe

11 | Soziale Funktionen von Anonymität

17 | Interview: »Wir sind alle Exhibitionisten im digitalen Raum«

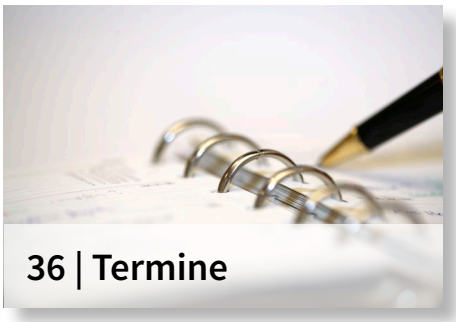


20 | Anonymität und soziale Medien

25 | Kameras im Stadtgebiet

30 | Nationale Sicherheit zum Preis der Anonymität

34 | Publikationen



36 | Termine

37 | Das Kolleg auf Reisen

47 | Impressum

Liebe Leserinnen und Leser,

nachdem im Spätsommer dieses Jahres die Debatte um eine gesetzliche Klarnamenpflicht in sozialen Netzwerken erneut ins Rollen gebracht wurde, kochten die kontroversen Meinungen zum Thema Anonymität im Internet wieder einmal hoch.[1] Hier wurde deutlich, welche unterschiedlichen Positionen die Gesellschaft bezüglich dieser ambivalenten Thematik gerade im Kontext der Digitalisierung durchziehen. Argumente, die in Anonymität eine Stärkung von Partizipation und Aufrichtigkeit sehen, werden in diesem Zusammenhang oftmals gegen Argumente abgewogen, die einen Anstieg gesellschaftlicher Enthemmung durch Anonymisierung befürchten.

Dazu thematisieren **Lea Watzinger** und **Patrick Herget** in ihrem Beitrag zunächst die grundlegenden Zusammenhänge von Anonymität und Privatheit. Dabei zeigen sie Begriffsdimensionen und Ambivalenzen des Anonymitätsbegriffes auf und verorten ihn sodann in der interdisziplinären Privatheitsforschung. **Anne Derametz** beleuchtet die soziale Funktion von Anonymität und stellt dar, inwiefern Anonymität auf verschiedenen gesellschaftlichen Ebenen notwendig für ein friedliches und funktionierendes Miteinander ist. Dem folgt ein Interview mit **Prof. Dr. Thomas Knieper**, der in Passau den Lehrstuhl für Computervermittelte Kommunikation innehat. Er gibt im Gespräch mit Patrick Herget und Lea Watzinger einen Überblick hinsichtlich des potentiellen Missbrauchs von Anonymität und kommt zu dem Schluss, dass das Netz kein rechtsfreier Raum sei – Anonymität im Internet sei daher nur mit Vorsicht als solche zu bezeichnen. **Franz X. Berger** blickt im Anschluss aus juristischer Perspektive auf soziale Netzwerke und zeigt auf, dass es ein Grundrecht auf Anonymität gibt. Im Folgenden erörtert er die daraus erwachsenden Konflikte zwischen dem Schutz der Persönlichkeit und der freien Meinungsäußerung als Herausforderungen für Recht und Gesellschaft. **Hermann Jakobi** setzt sich danach kritisch mit der zunehmenden Überwachungswut im öffentlichen Raum auseinander. Vergleichend geht er dabei auf die rechtlichen Systematiken für die Errichtung von öffentlicher Videoüberwachung am Beispiel von Krasnojarsk und München ein. Ebenfalls bezugnehmend auf Russland hebt **Elizaveta Saponchik** in ihrem Artikel die Bedeutung anonymer Kommunikation am Beispiel des Dienstes ›Telegram‹ hervor und zeigt auf, welche juristischen Konflikte sich in Bezug auf die Nutzung anonymer Kommunikationsdienste in Russland ergeben.

Anschließend daran sind interessante Publikations- und Veranstaltungshinweise im Kontext von Privatheit und Digitalisierung aufgelistet. Zum Schluss finden Sie Berichte zu den Veranstaltungen und Exkursionen des Kollegs im Sommersemester 2018: Neben einem Bericht zur interdisziplinären Ringvorlesung »Narrative der Überwachung« und zur Kooperationstagung mit dem DFG-Forschungsprojekt »American Literature and the Transformation of Privacy« in Frankfurt, blickt **Lea Raabe** auf eine Exkursion des Kollegs nach Stuttgart zurück, wo eine Kooperation mit der Hochschule der Medien aufgebaut wird. **Marcel Schlegel** fasst die wichtigsten Erkenntnisse der *Amsterdam Privacy Conference 2018* zusammen, auf der eine Abordnung des Kollegs ein eigenes Panel bestritt.

Wir wünschen Ihnen viel Spaß bei der vorweihnachtlichen Lektüre!

Lea Watzinger
Wissenschaftliche Mitarbeiterin am DFG-Graduiertenkolleg 1681/2 »Privatheit und Digitalisierung«.

Patrick Herget
Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg 1681/2 »Privatheit und Digitalisierung«.

1 Vgl. exemplarisch Mack, Daniel: Wird Zeit für eine gesetzliche Klarnamenpflicht auf Facebook, Twitter, Instagram und Co. Auf: *Twitter* vom 14.09.2018. Online: https://twitter.com/danielmack/status/1040520176691752961?lang=de (20.11.2018).

Zwischen Troll und Teilhabe

Anonymität und Privatheit im Internet

von Lea Watzinger und Patrick Herget

Anonym sein, namenlos, identitätslos, körperlos, ohne Verantwortung übernehmen zu müssen für das eigene Handeln, in der Masse aufgehen, endlich ehrlich sagen, was man denkt… Mit ›Anonymität‹ verbinden sich viele Vorstellungen, die gerade im Internet zu widersprüchlichen Phänomenen führen: Sogenannte ›Trolle‹ können Hass und Ärger verbreiten, aber es können auch RegimekritikerInnen ihre Meinungsfreiheit ausüben; das ›Darknet‹ ist Umschlagplatz für zahlreiche anonyme illegale Aktivitäten, aber das Gefühl der Anonymität hilft auch, sich z.B. in Selbsthilfeforen über tabuisierte Themen auszutauschen.

Dabei gilt das Internet generell seit seiner Entwicklung als Ort der Anonymität, dem diese bereits als Grundstruktur eigen ist.[1] Gleichzeitig ermöglicht die digitale, vernetzte Kommunikation nicht nur Anonymität, sondern auch Techniken, ebendiese einzuschränken, da digitale Kommunikation immer datenvermittelt ist und daher ausgelesen und nachvollzogen werden kann.[2] Das Internet scheint also sowohl Anonymität zu ermöglichen und zu fördern als auch zu verhindern. Dementsprechend ist die Unsicherheit bei NutzerInnen und BürgerInnen zum Thema Datenschutz, Überwachung und Wahrung der eigenen Anonymität hoch. Niemand weiß genau, welche eigenen persönlichen Daten für wen verfügbar sind; Enthüllungen, Datenlecks und -leaks werden regelmäßig in der Öffentlichkeit verhandelt.

In diesem Artikel wollen wir im ersten Teil eine Reflexion der verschiedenen Begriffsdimensionen vornehmen, um überhaupt das diffuse Phänomen der Anonymität näher zu bestimmen. Im zweiten Teil werden verschiedene Perspektiven beleuchtet, aus denen die Bedeutungen von Anonymität für die demokratische Gesellschaft im Kontext des digitalen Strukturwandels erörtert werden. Zudem hängen Fragen der Anonymität eng mit solchen der Privatheit zusammen: Ziel ist es daher herauszuarbeiten, inwiefern diese beiden Konzepte miteinander verflochten sind. Zuletzt soll am Beispiel der App ›Blind‹ aufgezeigt werden, wie sich diese Verflechtung zunächst auf das Individuum, aber in der Folge auch auf einer kollektiven gesamtgesellschaftlichen Ebene auswirkt.

Anonym wem gegenüber eigentlich?

Um die Widersprüchlichkeit des Anonymitätsbegriffs zu klären, muss man verschiedene Ebenen der Anonymität voneinander unterscheiden und fragen: anonym wem gegenüber eigentlich? Hier lässt sich zwischen horizontaler und vertikaler Anonymität unterscheiden.[3]

Auf horizontaler Ebene anonym sind wir unter Gleichgestellten, also wenn unser Gegenüber nicht weiß, wer wir sind. Dies ist der Fall, wenn wir unter einem Pseudonym etwas posten und der Bezug zu unserer ›wahren Identität‹, also unserem Klarnamen, nicht gegeben ist. Diese Form der Anonymität ist auch im analogen Leben existent, hier unter Umständen sogar als der Normalfall, etwa in der Großstadt: Die allermeisten Leute, die mir begegnen, am Nachbartisch im Café sitzen oder in der U-Bahn, sind mir unbekannt, sie sind für mich ›Anonyme‹, so wie ich für sie. Sie gehen in einer Masse an Menschen, die ich jeden Tag streife, unter. Selbst wenn ich die Aufmerksamkeit auf mich ziehe, etwa, weil ich laut bin, grell gekleidet oder ein Pony mit dabeihabe, bin ich noch anonym. Ich gehe zwar nicht mehr in der Masse unter, aber wer ich bin, meinen Namen, den kennt trotzdem keiner. Allerdings werde ich, sofern ich mein Pony überallhin mitnehme, wiedererkannt, genauso wie wenn ich im Netz immer unter demselben Pseudonym poste. Und wer mich einmal erkennt und meinen Klarnamen weiß, kann dieses Wissen auf verschiedene Kontexte anwenden und so meine Identität in Erfahrung bringen. Im Internet lässt sich nun eine solche Anonymität auf horizontaler Ebene relativ leicht bewahren. Sofern ich meinen Namen nicht selbst angebe, bleibt der Bezug zur realen Person für meine KommunikationspartnerInnen unbekannt. Ich erfahre von meinem Gegenüber erstmal nur, was es mir selbst offenbart. Auf manchen Webseiten darf ich ein Pseudonym angeben, wie z.B. auf Twitter, auf manchen allerdings nicht, wie etwa auf Facebook, wo die Nutzungsrichtlinien dies untersagen.

Die Unterscheidung zwischen Anonymität und Pseudonymität ist auch aus juristischer Perspektive relevant[4] – in der Alltagssprache verwenden wir beide Begriffe jedoch meist synonym. Im juristischen Kontext wird von Pseudonymität gesprochen, obwohl wir damit in der Alltagsprache oft Anonymität meinem. Bei der Pseudonymisierung und Anonymisierung werden persönliche Daten um individuelle Identifikationsmerkmale bereinigt. Nach altem Rechtsstand, vor Inkrafttreten der DS-GVO, war der Begriff der Anonymisierung in § 3 Abs. 6 BDSG (a.F.) definiert: »Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.« Im Rahmen der DS-GVO wird Anonymität lediglich in Erwägungsgrund 26 der Verordnung erwähnt. Dieser erläutert, dass pseudonyme Informationen als Informationen über eine identifizierbare Person zu betrachten sind, anonyme Informationen hingegen nicht den Grundsätzen des Datenschutzrechts unterliegen.[5] Der Begriff der Pseudonymisierung, welcher bisher in § 3 Abs. 6a BDSG (a.F.) bestimmt wurde, wird nun in Art. 4 Nr. 5 DS-GVO als »die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezoge-

1 Vgl. z.B. Brodnig, Ingrid: *Der unsichtbare Mensch*. Wien: Czernin 2013.

2 Vgl. Matzner, Tobias: Anonymität. In: Heesen, Jessica (Hg.): *Handbuch Medien- und Informationsethik*. Stuttgart: Metzler 2016, S. 248–254.

3 Vgl. Thiel, Thorsten: Anonymität und Demokratie. In: *Forschungsjournal Soziale Bewegungen*. Bd. 30, Nr. 2, 2017, S. 153.

4 Vgl. Härting, Niko: Anonymität und Pseudonymität im Datenschutzrecht. In: *NJW*. Bd. 66, Nr. 29, 2013, S. 2065–2071.

5 Vgl. Schmitz, Barbara: Der Abschied vom Personenbezug. In: *ZD*. Nr. 1, 2018, S. 5–8. Dazu auch: Kühling, Jochen/Klar, Manuel/Sackmann, Florian: *Datenschutzrecht*. Heidelberg: CF Müller 2018, S. 120.

nen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden« definiert. Jedoch muss an dieser Stelle angemerkt werden, dass eine De-Anonymisierung selbst vermeintlich ›anonymer‹ Daten in der Praxis, z.B. durch Korrelation, oft leichter möglich ist als gedacht.[6]

Vertikale Anonymität hingegen bezieht sich auf ein Machtverhältnis. Bin ich als Individuum für eine übergeordnete Instanz identifizierbar, nachverfolgbar, sind meine Daten zweifelsfrei zuordenbar? Auf vertikaler Ebene im digitalen Raum anonym zu bleiben ist zwar machbar, erfordert jedoch technische Vorkehrungen und Know-how wie die Nutzung spezieller Software. Zum Vergleich im analogen Kontext (ohne ubiquitäre Videoüberwachung): Ich spaziere durch die Stadt – weiß der Staat, wer ich bin? Erst in dem Moment, in dem ich aktiv von der Polizei danach gefragt werde, und das nur wenn ein hinreichender Grund zur Personenkontrolle vorliegt. Ich bin also im Normalfall auch in vertikaler Hinsicht erst einmal anonym, bis meine Anonymität aufgehoben wird. Im Café in der Großstadt bin ich deshalb grundsätzlich nicht nur auf horizontaler Ebene, wie oben gezeigt, anonym, sondern auch auf vertikaler Ebene. Wenn ich allerdings einen Tisch bestelle, erfährt die Kellnerin meinen Namen – wobei ich hier noch auf ein Pseudonym zurückgreifen kann. Wenn ich jedoch mit der Karte bezahle, sieht sie meinen richtigen Namen. Diese Daten können, etwa im Falle einer Ermittlung, auch von Behörden abgefragt werden.

Im Netz werden wir von den digitalen Café-Betreibern, etwa von Facebook und Google, jederzeit identifiziert, es ist schließlich ihr Kerngeschäft, uns auf diese Weise Werbung zu zeigen. Und der Staat hat – in Deutschland nur mittels richterlichem Beschluss – Zugriff auf Verbindungsdaten und so die Möglichkeit, unseren PC-Zugriff auf das Internet mit uns als NutzerIn in Verbindung zu bringen. Die Telekommunikationsanbieter sind in diesem Bild also so etwas, wie die Augen der PolizistInnen, die meinen Ausweis lesen. Gleichzeitig ist die vertikale De-Anonymisierung im digitalen Raum schwieriger als man denken mag, was die Tiefe des Darknets und die vielen strafrechtlich relevanten Kommunikationen zeigen, die kaum verfolgt werden (können).

6 Vgl. Mayer-Schönberger, Viktor/Cukier, Kenneth: *Big Data. Die Revolution, die unser Leben verändern wird.* München: Redline 2013, S. 67–94.

Diese beiden Dimensionen – horizontal und vertikal – sind der Anonymität inhärent, sie werden im Internet aber besonders sichtbar und widersprüchlich. Was hier hinzukommt, ist das Fehlen der Körperlichkeit von Kommunikation und daher von vielen Informationen aus der analogen Welt, wie etwa Statur und Aussehen meines Gegenübers, seine Mimik, Reaktion, seine Emotionen.[7] Solche Informationen sind zwar nicht Teil des Namens, aber der Identität einer Person, die eben neben dem Namen noch persönliche Informationen über diese fasst. Diese Aspekte fallen im Netz weg. Im Netz wird die Person auf ihren Namen – oder im Falle von dessen Fehlen auf ein Pseudonym – reduziert, sie hat kaum zusätzliche Identitätsmerkmale. Anonymität ist im Internet also in vielen Fällen Körper- und Namenlosigkeit. Dabei ist es wichtig zu unterscheiden, ob die teilweise negativen Aspekte der digital vermittelten Kommunikation wie Hass und Beleidigungen mit Anonymität als Namenlosigkeit zu erklären sind oder eher mit Anonymität als Körperlosigkeit, also dem Fehlen einer direkten menschlichen Reaktion.[8] Wird die Enthemmung in der digitalen Kommunikation dadurch beschleunigt, dass ich nicht weiß, wer es ist, oder dadurch, dass ich mein Gegenüber nicht sehe, es nicht fühlen kann?

Was macht das Gefühl der Anonymität mit uns?

Diese komplexe Anonymitäts-Situation im digitalen Umfeld zeigt verschiedene Konsequenzen zwischen »Enthemmung« und »Aufrichtigkeit«[9]: Als kollektives Phänomen können Einzelne in einer Masse aufgehen und damit nicht als Individuen zur Rechenschaft gezogen werden. Gleichzeitig kann Anonymität als Katalysator für soziales Handeln fungieren und eine Solidarität ermöglichen, die unter Nutzung des Klarnamens nicht denkbar wäre – etwa, wenn es um sensible Themen geht.[10] Hinzu kommt im digitalen Strukturwandel eine gewisse Zeitsensibilität von Anonymität: Durch die ständige Ansammlung von Daten und deren Verfügbarkeit lösen sich digitale Interaktionen nicht mehr auf, sondern bleiben nachvollziehbar[11] und so kann sich durch eine spätere Verknüpfung oder Auswertung von Daten eine vormals bestandene Anonymität im Nachhinein auflösen und die anonymen Daten können einer Identität zugeordnet werden.[12]

7 Vgl. Brodnig 2013, S. 71 f.

8 Vgl. Matzner 2016, S. 248.

9 Vgl. Thiel 2017, S. 156.

10 Vgl. Helm, Paula: Transparenz und Anonymität: Potentiale, Grenzen, Irrtümer. In*: Forschungsjournal Soziale Bewegungen.* Bd. 30, Nr. 2, 2017, S. 142–151.

11 Vgl. z.B.: Ulrike Meyer-Timpe: Das Internet vergisst nichts. In: *Zeit online* vom 02.08.2011. Online: https://www.zeit.de/zeit-wissen/2011/05/Internet-Daten-Ewigkeit (17.11.2018).

12 Vgl. auch Matzner 2016, S. 249.

Was macht das Gefühl der Anonymität nun mit uns? Die eine These lautet, dass horizontale Anonymität zu einer sozialen und kommunikativen Enthemmung führe,[13] eben weil die Körperlichkeit des Gegenübers verloren gehe und wir so vergäßen, dass der oder die Andere ein realer Mensch aus Fleisch und Blut, mit Herz und Seele ist – man erliegt der Illusion der eigenen Anonymität. Trolle nutzen diese scheinbare Namen- und Körperlosigkeit und entziehen sich so ihrer Verantwortung, zum Gesagten bzw. Geposteten zu stehen. Juristische wie soziale Konsequenzen bleiben häufig abstrakt. Wenn nun allerdings Anonymität in vertikaler Hinsicht tatsächlich aufgelöst wird und die Polizei Strafbefehl wegen Beleidigung oder Volksverhetzung erlässt, wird die bloße Illusion von Anonymität deutlich.

Anonymität kann auch ein Gefühl der Unsichtbarkeit vermitteln, das einen der Verantwortung entzieht und daher zu verbotenem Verhalten verleiten mag. Diese Vorstellung hat bereits Platon ausgeführt, wenn er die Legende vom Hirten Gyges erzählt, der durch einen magischen Ring am Finger unsichtbar werden kann, sodann Verbrechen zu seinen eigenen Gunsten begeht und so schließlich zum König wird.[14] Der Ring verleiht Gyges gewissermaßen eine vertikale Anonymität, da er durch die Fähigkeit zur punktuellen Unsichtbarkeit nicht verfolgbar ist. Aber auch die Anonymität als Normalfall auf horizontaler Ebene ist elementar für das Funktionieren dieses Tricks, da so kaum einer den Betrug, den er mit dem Ring begeht, bemerken kann.

Horizontale Anonymität im Netz kann wiederum auch zu einer Wahrhaftigkeit und Ehrlichkeit führen, die im gesellschaftlichen Korsett moralischer Normen kaum eine Chance hätte (man denke an heikle Themen wie z.B. Drogenkonsum): Anonymität befreit in diesem Fall von Konventionen, ermöglicht Freiheit und entwickelt so eine soziale Funktion: In einer Situation ›sozialer Anonymität‹ kann von Statusmerkmalen der Individuen abstrahiert werden und eine Gruppenidentität und -solidarität entstehen. Es wird möglich, den sozialen Status und mögliche soziale Machtbeziehungen des Gegenübers außen vor zu lassen. Anonymität wirkt dann als Mechanismus der ›Egalisierung‹.[15]

Wie bisher deutlich wurde, ist der Begriff der Anonymität komplex und erweitert durch den digitalen Strukturwandel seine Bedeutungen und Dimensionen: Sie ermöglicht das Gefühl, handeln zu können, ohne Konsequenzen fürchten zu müssen, also ohne Verantwortlichkeit. So entsteht eine Asymmetrie zwischen namenlosen KommunikationspartnerInnen und solchen, deren Identität offen liegt.

Perspektiven auf Anonymität und Privatheit im Kontext der Digitalisierung

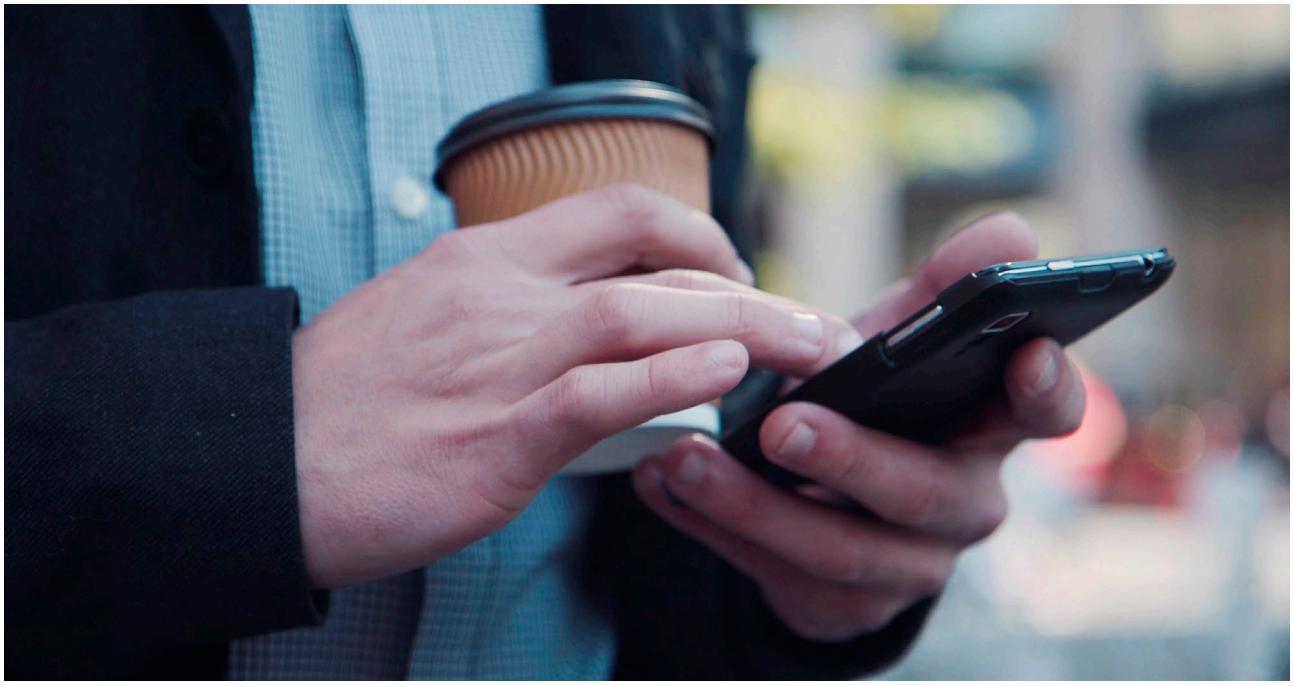
Findet eine Erörterung von Anonymität im Kontext der Privatheitsforschung statt, wird teilweise kritisiert, dass eine solche Perspektive die Spezifika von Anonymität unterschlage: Zum einen werde Anonymität lediglich als Bedingung für die Herstellung informationeller Privatheit verstanden,[16] zum anderen sei ihre Wirkung auf

13 Vgl. Thiel 2017, S. 156.

14 Vgl. Platon: *Politeia.* Buch 2, Rn. 358e–360d. Online: http://www.opera-platonis.de/Politeia2.pdf (17.11.2018).

15 Vgl. Helm 2017, S. 145.

16 Vgl. Ponesse, Julie: The Ties That Blind: Conceptualizing Anonymity. In: *Journal of Social Philosophy.* Bd. 45, Nr. 3, 2014, S. 305.



die Ebene des Individuums reduziert, weshalb die Besonderheiten des Anonymitätsbegriffes sowie dessen gesamtgesellschaftliche Relevanz nicht ausreichend gewürdigt würden.[17] Nachdem nun im folgenden Abschnitt verschiedene Aspekte aufgezeigt werden, wie Anonymität im Zusammenhang mit demokratietheoretischen Perspektiven im Kontext der Digitalisierung verstanden werden kann, wird die Schnittstelle von Privatheit und Anonymität näher diskutiert.

Im Kontext der Digitalisierung wird Anonymität schnell mit dem Internetphänomen ›Anonymous‹ in Verbindung gebracht, welches den Begriff ›anonym‹ im eigenen Namen für sich beansprucht. Das Pseudonym Anonymous wird in der Netzkultur von unterschiedlichen Personen und Gruppierungen verwendet. Demnach handelt es sich bei Anonymous um eine lose Verbindung von InternetnutzerInnen. Neben öffentlichen Demonstrationen wird eine neue Form des politischen Aktivismus genutzt, welche als ›Hacktivismus‹ bezeichnet wird, um verschiedene Ziele zu erreichen. Anonymous setzt sich z.B. für Redefreiheit, die Unabhängigkeit des Internets und gegen das Urheberrecht ein. Die Aktionen richteten sich bisher gegen diverse Organisationen, Behörden und Unternehmen.[18]

In Zusammenhang mit Diskursen zum Hacktivismus wird das ambivalente Anonymitätsverständnis innerhalb der Gesellschaft im digitalen Zeitalter in Bezug auf die liberale Demokratie erneut offensichtlich: Einerseits wird argumentiert, dass Anonymität, wie sie durch die Digitalisierung ermöglicht wird, eine Umverteilung des Rederechts fördere, da sich die Zugangsbedingungen zur Demokratie vereinfachten, indem die Idee aufgelöst werde, dass Politik die Handelnden etwas kosten müsse. Anonymität wird in diesem Zusammenhang zum Teil so verstanden, dass sie in einer Welt der Überwachung zu einem Gegenrecht wird, das es ermöglicht, eine neue demokratische Rechtsordnung von anonymen Weltbürgern ohne Staat zu konstituieren.[19]

Entgegen dieser These wird jedoch auch kritisiert, dass sich anonyme Personen ihrer individuellen und demokratischen Verantwortung entziehen könnten und Anonymität insgesamt zu einem Recht verklärt werde, dessen demokratische Legitimation angezweifelt werden müsse. Versuche von Anonymous, Legitimation in Verbindung mit einer Bezugnahme auf die Weltbevölkerung zu gewinnen,[20] blieben politisch resonanz- und folgenlos. Der Verweis auf eine schweigende Mehrheit ermögliche keine demokratische Legitimation und etliche offene Fragen[21], etwa danach wie eine Demokratie, die aus anonymen Weltbürgen besteht, aussehen könnte, blieben unbeantwortet. Deshalb führe Anonymität im Endeffekt zu einer politischen Selbstermächtigung, rechtliche Grenzen zu überschreiten, wodurch in die Rechte identifizierbarer BürgerInnen eingegriffen werde und demokratische Institutionen beschädigt würden. Eine Ansammlung anonymer Personen ermögliche somit keineswegs die Konstitution eines demokratischen Verfassungsstaates.[22]

Aus einer anderen Perspektive wird die Politisierung von Anonymität im Kontext des digitalen Strukturwandels durch einen demokratietheoretischen Ansatz wie bspw. den von Thorsten Thiel thematisiert, in dem die kommunikative Bedeutung von Anonymität

17 Vgl. Thiel 2017, S. 156 f.

18 Vgl. dazu vertiefend: Wiedemann, Carolin: *Kritische Kollektivität im Netz. Anonymous, Facebook und die Kraft der Affizierung in der Kontrollgesellschaft.* Bielefeld: Transcript Verlag 2016.

19 Vgl. de Lagasnerie, Geoffroy: *Die Kunst der Revolte. Snowden, Assange, Manning*. Berlin: Suhrkamp 2016, S. 98, 140–148. Vgl. dazu auch: Kersten, Jens: Anonymität in der liberalen Demokratie. In: *JuS.* Nr. 3, 2017, S. 193–203, hier S. 194.

20 Vgl. Bardeau, Frédéric/Danet, Nicolas: *Anonymous*. Münster: Unrast Verlag 2002, S. 68, 100, 156.

21 Vgl. Kersten 2017, S. 194.

22 Vgl. Kersten 2017, S. 194.

in der zweiten Hälfte des 20. Jahrhunderts mit dem Stellenwert von Anonymität in einer digital vernetzten Gesellschaft verglichen wird. Um die normative Wertigkeit von Anonymität zu ermitteln, wählt Thiel die moderne republikanische Theorie und stellt die Bedeutung von Anonymität für die demokratische Gesellschaft anhand der bereits erwähnten horizontalen und vertikalen Dimensionen heraus. Vor dem Hintergrund der Digitalisierung konstatiert er, dass sich Identifikationspflichten massiv ausgeweitet hätten und Identifizierungsmöglichkeiten enorm gewachsen seien. Anonymität müsse nun bewusst erzeugt und könne nicht mehr als selbstverständlich wahrgenommen werden.[23]

Von diesem Standpunkt wird die Bedeutung von Anonymität für die liberale Demokratie im Lichte des digitalen Strukturwandels insgesamt so gewertet, dass Anonymität trotz ihrer Ambivalenz ein wichtiges Strukturmerkmal demokratischer Öffentlichkeit sei.[24] Um Anonymität aus demokratietheoretischer Perspektive auch weiterhin in der digitalisierten Gesellschaft aufrecht zu erhalten, sei es notwendig, dass bei der Regulierung von Anonymität eine ausgewogene Berücksichtigung von Recht, Politik, Markt, sozialen Normen und Code-Architektur stattfinde.[25]

Anknüpfend an Thiel erörtert Jens Kersten aus juristischer Perspektive die Bedeutung von Anonymität in der liberalen Demokratie und geht dabei insbesondere auf die Steuerungsfähigkeit des Rechts in Zusammenhang mit der Politisierung von Anonymität ein. Es wird auch hier aufgezeigt, dass Anonymität als zentraler Baustein des liberalen Verfassungsstaates sowohl grundrechtliche Freiheiten wie z.B. Meinungs- und Versammlungsfreiheit gewährleiste als auch zugleich demokratische Legitimation, z.B. durch geheime Wahlen, sichere. Anonymität sei somit grundsätzlich von positiver Bedeutung für die Demokratie.[26]

Anonymität als informationelle Privatheit im öffentlichen Raum

Einige Ansätze sprechen sich aus den oben genannten Gründen gegen eine Verknüpfung von Anonymität und Privatheit aus, dennoch wird die Bedeutung von Anonymität für die Demokratie auch in der Privatheitsforschung diskutiert. Die Überschneidungen von Anonymität und Privatheit stellt Beate Rössler bereits in einem Beitrag aus dem Jahr 2003 heraus.[27] Aus ihrer Perspektive werden Zusammenhänge insbesondere bei der informationellen Ausprägung von Privatheit[28] deutlich. Der Schutz ›informationeller Privatheit‹ meint, die Kontrolle darüber zu haben, was andere über die eigene Person wissen können. Dieser Aspekt beschränkt sich nicht nur auf datenschutzrechtliche Informationskontrolle, sondern ist für das grundsätzliche Selbstverständnis von Personen als autonom konstitutiv, da nur so die Kontrolle über deren Selbstdarstellung gewahrt werden kann. Personen müssen wissen, was andere über die eigene Person wissen, damit sie ihr Handeln daran ausrichten oder sich dementsprechend verhalten können. Der Anonymitätsaspekt ist dabei nach Rössler wesentlich für die Kontrolle darüber, wie Personen sich wem gegenüber in welchen Kontexten präsentieren und inszenieren und somit auch substanziell für die Wahrung informationeller Privatheit. Somit kann

23 Vgl. Thiel 2017, S. 152–161.

24 Vgl. Thiel, Thorsten: Anonymität und der digitale Strukturwandel der Öffentlichkeit. In: *Zeitschrift für Menschenrechte.* Nr. 10 (1), 2016, S. 9–24.

25 Vgl. Thiel 2017, S. 159.

26 Vgl. Kersten 2017, S. 203.

27 Vgl. Rössler, Beate: Anonymität und Privatheit. In: Bäumler, Helmut/Mutius, Albert von (Hg.): *Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts.* Wiesbaden: Vieweg 2003, S. 27–40.

28 Vertiefend zum Begriff der informationellen Privatheit: Rössler, Beate: *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp 2001, S. 201–254.

Anonymität als Ausprägung informationeller Privatheit im öffentlichen Raum verstanden werden, die durch kognitive Asymmetrien, also die Verletzung von Erwartungen über das Wissen, welches Andere über die eigene Person haben, gefährdet wird. Die Gefahr von kognitiven Asymmetrien wird gesteigert, wenn üblicherweise freiheitssichernde Konventionen, z.B. das grundsätzliche Vorhandensein von Anonymität in der Offline-Gesellschaft, durch den Gebrauch neuer Technologien in Frage gestellt werden.[29]

Vor diesem Hintergrund lässt sich ein Zusammenhang zwischen Anonymität, Privatheit, individueller Freiheit und Autonomie generieren, der sich auf die liberale Demokratie insgesamt auswirkt, da diese auf autonome und sich ihrer Autonomie bewusste Subjekte angewiesen ist. Privatheit ist funktional auf Freiheit und Autonomie bezogen, weshalb sich auch Anonymität als informationelle Privatheit im öffentlichen Raum nach Rössler unmittelbar auf die Stabilität und das Gelingen liberaler Demokratie auswirkt.[30] Anonymität kann somit nicht nur als Faktor angesehen werden, der sich lediglich auf das Individuum erstreckt. Die individuelle und die kollektive Ebene sind in diesem Bezugsrahmen direkt miteinander verwoben.

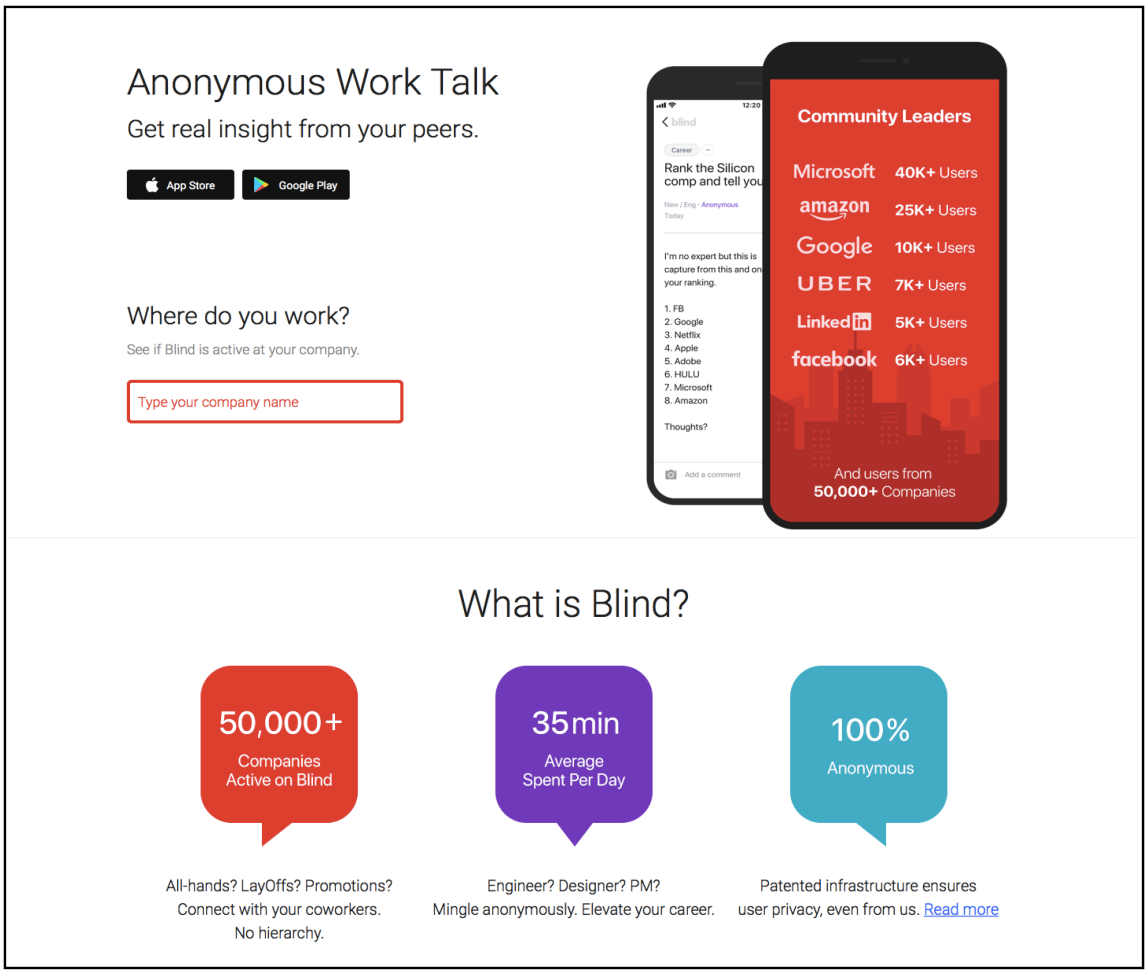
29 Vgl. Rössler 2003.

30 Vgl. Rössler 2003, S. 39.

Anonymität in ›Blind‹

Wie sich die Schnittstelle von Anonymität und Privatheit im digitalen Strukturwandel konkret von einer individuellen auf eine kollektive Ebene auswirken kann, wird aktuell anhand der App Blind deutlich, die anonyme Kommunikation innerhalb von Unternehmen ermöglicht und sich derzeit in den USA und in Südkorea großer Beliebtheit erfreut. Die Anonymität in Blind ermöglicht einen freieren Austausch der MitarbeiterInnen untereinander, sodass Fehlentwicklungen und Beschwerden eher thematisiert werden können. Negative Konsequenzen der Äußerungen müssen nicht befürchtet werden, da die Identität der jeweiligen Personen geheim bleibt. Die Relevanz wird insbesondere bei Tabuthemen, wie bspw. dem Gehalt oder sexueller Belästigung am Arbeitsplatz deutlich.[31]

31 Vgl. Rixecker, Kim: Blind: Diese anonyme App ist das Anti-Yammer. In: *t3n* 2018. Online: https://t3n.de/news/blind-diese-anpnyme-app-ist-das-anti-yammer-1102454/ (05.10.2018).



Ansicht der Blind-Homepage. Blind ermöglicht einen anonymen Austausch am Arbeitsplatz. Quelle: Teamblind.com (28.09.2018).

Bei der Anmeldung in Blind muss die berufliche E-Mail-Adresse angegeben werden, sodass NutzerInnen ihren jeweiligen Unternehmen zugeordnet werden können. Sobald mindestens 30 MitarbeiterInnen eines Unternehmens ein Blind-Konto besitzen, können sie sich anonym in einem Bereich über ihre Arbeit austauschen, der für die Öffentlichkeit nicht zugänglich ist. Ergänzend dazu existiert ein öffentlicher Bereich, in dem sich anonyme MitarbeiterInnen über generelle Karrierethemen, Bezahlung oder andere arbeitsrelevante Themen austauschen können.[32] Auch in diesem Bereich bleibt die Anonymität der NutzerInnen gewährleistet, da einzig deren Zuordnung zu einem bestimmten Unternehmen öffentlich einsehbar ist, nicht aber ihre Identität.[33]

Blind stärkt damit sowohl Aspekte horizontaler, als auch vertikaler Anonymität der Kommunikation. So bleiben MitarbeiterInnen auf horizontaler Ebene untereinander anonym, ebenso ist auch eine vertikale Anonymität in Bezug auf die Identifizierbarkeit durch die ArbeitgeberInnen bzw. die Vorgesetzten gewährleistet. Informationelle Privatheit im digitalen öffentlichen Raum wird somit sichergestellt, da sich MitarbeiterInnen anonym in der digitalen Öffentlichkeit bewegen und dennoch am Diskurs teilhaben können. Weiterhin zeigt sich hier, dass Anonymitäts- und Privatheitsaspekte über die individuelle Ebene hinaus Wirkung entfalten, da bspw. Tabuthemen auf diese Weise überhaupt erst öffentlich thematisiert werden und auch nur auf dieser Ebene lösbar sind. Die einzige Schwachstelle in Bezug auf die vollständige Gewährleistung vertikaler Anonymität ist die Registrierung, bei der die berufliche E-Mail-Adresse als Selektionskriterium benötigt wird, damit das Konzept der Plattform überhaupt funktioniert. Somit besteht die Möglichkeit kognitiver Asymmetrien, da einzelne Personen durch den Blind-Anbieter selbst identifiziert werden könnten.

Neue Chancen durch Anonymität?

Auch wenn Blind lediglich im beruflichen Kontext Verwendung findet, so wird hier auch exemplarisch der gesamtgesellschaftliche Wirkungsmechanismus an der Schnittstelle von Anonymität und Privatheit verdeutlicht. Obwohl die Möglichkeiten der Identifizierbarkeit durch digitale Technologien insgesamt gewachsen sind, eröffnen dieselben auch neue Wege für den Schutz von Anonymität und können so Partizipation und Demokratie stärken, sowohl in spezifischen Kontexten, als auch für die gesamte Gesellschaft. Weiterhin wird deutlich, dass die individuelle und kollektive gesellschaftliche Ebene bei der Analyse von Anonymität als informationelle Privatheit im öffentlichen Raum nicht losgelöst voneinander betrachtet werden sollten und sich Anonymität aus der Perspektive der Privatheitsforschung unmittelbar auf die Gesellschaft auswirken kann und in ihrer Wirkung keineswegs auf die Ebene des Individuums beschränkt sein muss.

Abschließend wird eine doppelte Ambivalenz von Anonymität im Kontext des digitalen Strukturwandels besonders deutlich. Erstens ist das Gefühl der horizontalen Anonymität im Internet stark. Vertikale Anonymität hingegen ist auflösbar, da bei computervermittelter Kommunikation stets direkt oder indirekt auf die anfallenden Daten zugegriffen werden kann. Zweitens oszillieren die Effekte der vermeintlich anonymen Kommunikation im Netz zwischen Troll und Teilhabe, zwischen Enthemmung und Aufrichtigkeit.

32 Vgl. Rixecker 2018.

33 Vgl. Teamblind: *Most Frequently Asked Questions.* Online: https://www.teamblind.com/faqs (11.10.2018).

Lea Watzinger

Wissenschaftliche Mitarbeiterin am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Patrick Herget

Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Soziale Funktionen von Anonymität

Warum nicht alles Fremde gleich eine Bedrohung darstellen muss

von Anne Deremetz

›Anonymous‹, WikiLeaks und ›Hatespeech‹ sind Beispiele heutiger sozialer Phänomene, die im Anonymen ihren Ausdruck finden und denen das Potenzial zugeschrieben wird, die bisherige soziale Ordnung grundlegend verändern oder sogar destabilisieren zu können.

Im Internet wird vor dem Hintergrund der Zunahme von Hasskommentaren und ›Shitstorms‹ die wachsende Gefahr von anonymen Posts diskutiert und deren staatliche Kontrolle eingefordert. Das sogenannte *Netzwerkdurchsetzungsgesetz* – NetzDG[1] stellt einen Versuch dar, die sozialen Netzwerke stärker in die Pflicht zu nehmen. Dem Anonymen werden damit gewisse Merkmale zugeschrieben wie beispielsweise, dass Anonymität TäterInnen schützt oder dass man Straftaten durch den Schutz der Anonymität schwieriger verfolgen kann. Der Grundgedanke ist, dass man sich im Anonymen sicher genug fühlt, Gesetze und soziale Regeln (z.B. die ›Netiquette‹) zu brechen.

Anonymität kann zunächst elementar mit drei Merkmalen beschrieben werden: Eine Person oder Sache ist anonym, wenn er, sie oder es Anderen nicht bekannt ist (Nichtbekanntsein), nicht erfahrbar in Erscheinung tritt (Nichtgenanntsein) oder ohne Erkennbarkeit und Zurechenbarkeit handelt (Namenlosigkeit).[2] Anonymität ist dabei nicht gleich Anonymität. Vielmehr manifestiert sie sich abhängig von der strukturellen Analyseebene. So kann man klassisch zwischen gesellschaftlicher (Makro-)Ebene, gemeinschaftlicher (Meso-)Ebene und individueller (Mikro-)Ebene unterscheiden. Anonymität nimmt in der jeweiligen betrachteten Ebene abhängig von den historischen Rahmenbedingungen je spezifische Funktionen und Rollen ein. Aus soziologischer Perspektive erinnert Anonymität dabei an das Konzept des Simmel'schen ›Fremden‹ und wird in diesem Beitrag zunächst in einem übertragenen Sinn gleichgesetzt.[3] In seinem *Exkurs über den Fremden* beschreibt Simmel dezidiert die Rollen und Funktionen, die der, die oder das Fremde gesellschaftlich, für Gemeinschaften und auf individueller Ebene einnehmen kann. So begegnet uns Fremdheit auf gesellschaftlicher Ebene tagtäglich in Form von Menschen, die uns unbekannt sind (Nichtbekanntsein) und Praktiken, die wir keiner Person unmittelbar zuordnen können (Namenlosigkeit). Das Fremde ist hier ›normaler‹ Bestandteil von Gesellschaft. Auf gemeinschaftlicher Ebene fungiert der, die oder das Fremde als das ›Andere‹, welches der Gemeinschaft nicht angehört. Dieses übernimmt vor allem Ventilfunktionen und fungiert als Projektionsfläche von (meist negativ konnotierten) Eigenschaften, wie bspw. sich manifestierenden Unsicherheiten und Ängsten der Gemeinschaft. Xenophobie kann in diesem Zusammenhang als die konkrete gemeinschaftliche Auseinandersetzung mit dem Fremden verstanden werden. Auf individueller Ebene begegnet uns der, die oder das Fremde vor allem in Form der ›dritten Person‹, wie etwa in der bekannten Redewendung ›Wenn zwei sich streiten, freut sich der Dritte‹. Der *tertius gaudens* ist hier der Simmel'sche Fremde in Reinform.

Es stellt sich die Frage, welche Funktionen Anonymität in Form des Fremden für heutige Gesellschaften übernimmt und ob sie unter Umständen dysfunktional für das gesellschaftliche Miteinander geworden ist. Um dieser Fragestellung nachzugehen, sollen die Funktionen von Anonymität auf den eingangs beschriebenen strukturellen Ebenen betrachtet werden.

Gesellschaft, Gemeinschaft und das postmoderne Individuum

Gesellschaft und soziales Zusammenleben zusammenzudenken ist unmittelbar mit dem Namen Ferdinand Tönnies verbunden, prägte dieser doch in seiner Habilitationsschrift *Gemeinschaft und Gesellschaft* von 1887 beide Begriffe und stellte sie als Oppositionspaar gegenüber.[4] Nach Tönnies beruht ›Gesellschaft‹ auf einem ›Kürwillen‹, also auf »den zweckrationalen Willensakten der Subjekte, auf einem Zusammenwollen des eigenen Vorteils wegen […]. ›Gemeinschaft‹ dagegen beruht darauf, dass die Betroffenen, der Idee nach, die umgreifende Lebensform gleichsam um ihrer selbst willen, als Selbstzweck auffassen […]«[5]. Tönnies spricht hier von einem ›Wesenswillen‹. Gesellschaft dagegen dient den Individuen zur systemischen Integration, also der Einpassung und Realisation gesellschaftlicher Prozesse in den Bereichen Politik, Wirtschaft usw. in Form von Institutionalisierung und Habitualisierung sozialer Praktiken. Für Tönnies bildet im klassischen Sinne die Stadt oder der urbane Raum das Konzept der Gesellschaft ab.

Gemeinschaft wird bei Tönnies noch als ein »Oppositionsbegriff gegen eine vom liberalen Fortschrittsgedanken getragene Auffassung der ›Gesellschaft‹«[6] gedacht. Mit Gemeinschaft ist im Tönnies'schen Sinne vor allem das Dorf gemeint – also eine soziale Gruppierung, in der sich die AkteurInnen meist persönlich kennen und ihr Zusammenleben gemeinsam gestalten. Die Funktion der Gemeinschaft ist vor allem die Sozialinklusion, also das Einbetten des Individuums in persönliche Verbundenheiten, das Einüben von sozialen Rollen (Sozialisation), Normen und Regeln. Zugespitzt könnte man es so formulieren: In der Gesellschaft bin ich eine von Vielen und als Kundin, Klientin oder Gast wahrnehmbar. In der Gemeinschaft erfahre ich Zuge-

1 Vgl. FAZ: *Bundestag verabschiedet Gesetz gegen Hasskommentare* 2017. Online: http://www.faz.net/aktuell/politik/inland/bundestag-verabschiedet-gesetz-gegen-hasskommentare-15084504.html (28.11.2018).

2 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): *Homepage* 2018. Online: https://www.bsi.bund.de/DE/Publikationen/Studien/Anonym/wasistanonymitaet.html (28.11.2018).

3 Vgl. Simmel, Georg: Exkurs über den Fremden. In: Ders.: *Soziologie*. Berlin: Duncker & Humblot 1983, S. 509–512.

4 Vgl. Tönnies, Ferdinand: *Gemeinschaft und Gesellschaft*. Darmstadt: Wissenschaftliche Buchgesellschaft 1963, S. 3.

5 Bickel, Cornelius: Ferdinand Tönnies. In: Kaesler, Dirk (Hg.): *Klassiker der Soziologie*. München: C.H. Beck 2006, S. 110.

6 Bickel 2006, S. 119.

hörigkeit, Geborgenheit, kann meine Identität herausbilden und werde dabei als Person wahrgenommen. Sowohl Gesellschafts- als auch Gemeinschaftsfähigkeit sind wesentliche Funktionen für soziales Miteinander und bedingen sich gegenseitig.

Im zunehmenden Modernisierungsprozess scheint die Gemeinschaft gegenüber der Gesellschaft jedoch nicht mehr diese komplementäre Rolle erfüllen zu können. Vielmehr scheint heutiges soziales Miteinander von einer zunehmenden Pluralisierung von Lebensformen, Werten und Normen beherrscht. Das gemeinschaftliche Prinzip weicht zugunsten der Individualisierung auf und erodiert – der Gesellschaft wird somit im Zuge der Modernisierung zunehmend der Begriff des ›Individuums‹ entgegengestellt. Man kann den Prozess der Individualisierung insofern definieren, als er »strukturell gesehen […] die Herauslösung aus den Strukturen der Industriegesellschaft, also aus ständisch geprägten Sozialmilieus und klassenkulturellen Lebensformen [bedeutet].«[7]. Das Individuum befreit sich von gemeinschaftlichen Strukturen und agiert mehr oder weniger autonom und herausgelöst. Die Stabilität, die gemeinschaftliche Institutionen der sich ständig verändernden Gesellschaft entgegenzubringen vermochten, weicht nun einer selbst geschaffenen Instabilität. Die Zugehörigkeiten zu gemeinschaftlichen Gruppen büßten nach Gerd Nollmann und Hermann Strasser zunehmend an Orientierungskraft ein.[8]

Dieses Herausfallen aus einer stabilen und lebenslangen Institution diagnostiziert auch Zygmunt Bauman als ein »Nicht-mehr-eingebettet-Sein«.[9] Der Einzelne erlebe sich nicht mehr in Gemeinschaft, sondern nur noch als losgelöstes Individuum. Dieser Umstand erscheint Bauman als postmoderne Pathologie und lasse das »Bedürfnis nach Kleingemeinschaften, […], die eine ganzheitliche Lebenswelt, Überschaubarkeit, ein personales Angenommensein versprechen«[10], wieder aufblühen. Der Begriff der Gemeinschaft erfährt demnach wieder zunehmende Bedeutung, was z.B. in Strömungen wie dem Kommunitarismus[11], wie auch in postmodernen Überlegungen Ausdruck erfährt. Die Postmoderne erzeugt ein gewisses Bedürfnis nach Ordnung und Struktur, welches heutigen Gesellschaften anzuhaften scheint. Nach Bauman hätten sich heutige Gesellschaften daher »zur Erschaffung von Ordnung verpflichtet, d.h. […] den Kampf gegen jedes Chaos, gegen jede Mehrdeutigkeit und jede Ambivalenz aufgenommen.«[12]

7 Kron, Thomas/Horácek, Martin: *Individualisierung*. Bielefeld: transcript Verlag 2009, S. 131 f.

8 Vgl. Nollmann, Gerd/Strasser, Hermann: *Das individualisierte Ich in der modernen Gesellschaft*. Frankfurt am Main: Campus Verlag 2004, S. 15.

9 Bauman, Zygmunt: *The individualized Society*. Cambridge: Polity Press 2001, S. 146.

10 Nave-Herz, Rosemarie: Die These über den »Zerfall der Familie«. In: *Kölner Zeitschrift für Soziologie und Sozialpsychologie*, Sonderheft 38, 1998, S. 307.

11 Dies meint die Betonung und Forderung eines stärkeren Gemeinschaftsgefühls.

12 Kron, Thomas: Die Unordnung aushalten – Zygmunt Baumans Plädoyer für eine postmoderne Moral. In: Volkmann, Ute/Schimank, Uwe (Hg.): *Soziologische Gegenwartsdiagnosen II*. Opladen: Leske + Budrich 2002, S. 217 f.

Anonymität in der Kontrollgesellschaft

Wenn wir heutzutage in einer Gesellschaft leben, in der das Ziel vor allem im Schaffen von Ordnung und Sicherheit besteht, so scheint der Anonymität in Gestalt des Fremden vermehrt ein dysfunktionaler Charakter zugewiesen zu werden. Anonymität und Transparenz können hierbei als Antagonismen betrachtet werden. Transparenz scheint sich als eine Art postmodernes Credo zu entwickeln, das Ordnung, Sicherheit und Schutz verspricht, nicht zuletzt aufgrund einer immer weiter um sich greifenden Bedrohung durch Unsicherheiten und Risiken, die sich im Schutz der Anonymität überhaupt erst formieren und dort gedeihen können. In der Sicherheitsgesellschaft[13] oder auch in Kontrollgesellschaften[14] – je nachdem, welche Zeitgeistdiagnostik man präferiert – wird Anonymität zunehmend als Bedrohung der etablierten Ordnung erfahren: »Folge der modernen Vorgehensweise ist Intoleranz gegenüber allem nicht der Ordnung Anpassbarem. An dieser Stelle muss man sich klar machen, dass es ›der Fremde‹ ist, durch den die Moderne sich in ihren Ordnungsbemühungen bedroht sieht […] Der Fremde bedroht die Vergesellschaftung.«[15]

Wie oben dargestellt, wird die soziale Funktion von Anonymität damit aber ebenso übersehen wie ihr essenzieller Einfluss auf soziokulturelle Prozesse: Gesellschaft, Gemeinschaft wie auch Individuen bedürfen der Anonymität. Sie beinhaltet immer auch Freiheitsgrade und fungiert geradezu als Stabilisierung der vorherrschenden Ordnung. Ihre Funktion ist dabei vor allem die des Ventils oder der Erleichterung zwischenmenschlicher Spannungen.

Anonymität auf gesellschaftlicher Ebene

Nach dem Tönnies'schen Denken zeigt sich das gesellschaftliche Prinzip vor allem in urbanen Strukturen: die Stadt als Sinnbild von Gesellschaft, in der unzählige Menschen tagtäglich miteinander interagieren und in der man sich dennoch fremd ist oder sein kann. Der Grad an Anonymität im urbanen Raum ist schon allein aufgrund der nicht mehr zu überblickenden Zahl an Menschen entsprechend hoch, die soziale Kontrolle durch Andere ist reduziert und wird durch systemische Kontrolle – bspw. durch die technische Überwachung des öffentlichen Raums – substituiert. Nicht mehr die Nachbarschaft, die man womöglich gar nicht kennt, lässt einen die Normen einhalten, vielmehr zählt die Hausordnung oder der Wunsch der EigentümerInnen.

Im urbanen Raum ist Anonymität allerdings nicht nur möglich, sondern auch gefordert. Erst im Anonymen können Individuen dem Einzelnen gegenüber gleichgültig und somit gleich gültig sein. Anonymität im urbanen Raum reduziert die Alltagskomplexität. Die Toleranz ist dementsprechend höher als im nicht-urbanen gemeinschaftlichen Raum. Erst im Gesellschaftlichen können sich Strukturen herausbilden, in denen sich Individuen unabhängig(er) von sozialen Sanktionen und sozialer Kontrolle entfalten können. Kreativität und Innovation können hier die Folge von Anonymität sein. Zwischenmenschliche Konflikte sind allein schon deshalb vermeidbar, da man auf andere Örtlichkeiten und Kontexte ausweichen kann. Man ist in der Gesellschaft nicht dazu gezwungen, sich auseinanderzusetzen. Folglich ist Anonymität im Gesellschaftlichen Garant für die individuelle Entfaltung. Dadurch entstehen Freiheitsgrade, die in der Gemeinschaft, in der jeder jeden kennt, meist vermisst werden.

Anonymität auf gemeinschaftlicher Ebene

Im Gemeinschaftlichen ist der Grad an Anonymität deutlich herabgesetzt, womöglich sogar überhaupt nicht gegeben. Dadurch, dass im Extremfall jeder jeden kennt, ist die Ordnung vor allem durch die Augen des Kollektivs garantiert. Soziale Kontrolle realisiert sich durch die Einbindung in die Gemeinschaft und durch die (be-)urteilenden Blicke meiner Mitmenschen, die mich mehr oder weniger gut, aber immerhin kennen. Lege ich ein der hier gesetzten Norm abweichendes Verhalten an den Tag, werde ich positiv oder negativ sanktioniert, da diese Tat unmittelbar Einfluss auf die Gemeinschaft hat.

Dennoch ist Anonymität auch für das Funktionieren von Gemeinschaften unabdingbar. Auch hier begegnet uns Anonymität vor allem in Form des Fremden. Der, die oder das Fremde als das der Gemeinschaft nicht angehörende Prinzip hat einen wesentlichen Einfluss auf die Sozialdynamik. Es kann eine neutrale oder mediatorische Funktion für die Gemeinschaft übernehmen und somit als Ventil für gemeinschaftlichen Unmut dienen. Dem Fremden werden die Missstände ausgeplaudert, es wird sich beschwert und Luft gemacht. Mit guter Gewissheit vertraut man den Fremden die Abgründe gemeinschaftlichen Zusammenlebens an, denn die Fremden befinden sich außerhalb der gemeinschaftlichen Strukturen und unterliegen daher weder ihren sozialen Normen noch ihrer sozialen Kontrolle. Das Anonyme und das Fremde sind für Gemeinschaften konstituierend, stabilisierend und stärken zugleich die interne Verbundenheit der Gemeinschaft.

13 Vgl. Singelnstein, Tobias/Stolle, Peer: *Die Sicherheitsgesellschaft*. Wiesbaden: Springer VS 2008.

14 Vgl. Deleuze, Gilles: *Postskriptum über die Kontrollgesellschaften. Kriminologische Grundlagentexte*. Wiesbaden: Springer VS 2016, S. 345–352.

15 Kron 2002, S. 219.

Anonymität auf interindividueller Ebene

Auch auf individueller Ebene ist Anonymität oder das Fremde durchaus ein wesentlicher Bestandteil sozialer Interaktionen. Das kann die Offenheit in einem Chat sein, das kann aber auch die katholische Beichte, der Anruf bei einem Hilfetelefon oder schlicht die Handlungsreisende sein, die der Barkeeperin ihr Herz ausschüttet, um am nächsten Tag – geradezu erleichtert – an einen neuen Ort aufzubrechen. Diese Beicht- oder Geständnisfunktion ähnelt dem, was Foucault unter dem Begriff ›Pastoralmacht‹ beschreibt.[16] Sie gleicht der Ventilfunktion des Fremden auf gemeinschaftlicher Ebene. Im interindividuellen Moment dieser Interaktion wird jedoch ein Grad an Intimität erreicht, der auf gemeinschaftlicher Ebene womöglich nur vereinzelt vorkommt. Hier erfährt das Individuum durch Anonymität die Möglichkeit, (ehrliche) Aussagen zu treffen, für die es in der Gemeinschaft sanktioniert werden würde. Im interindividuellen, anonymen Moment erfährt das Individuum den nötigen Schutz vor sozialer Kontrolle, den es benötigt, um Ehrlichkeit zu wagen. Das Geständnis entlastet das Individuum von sozialem Druck und ermöglicht Unkonventionalität. Im anonymen und sanktionsfrei(er)en Raum liegt das Potenzial für Kreativität und gesellschaftliche Innovation. Hier können Gedanken geäußert werden, die man im gemeinschaftlichen Kontext aus Angst vor sozialen Sanktionen womöglich nicht offenbart.

16 Foucault beschreibt die Pastoralmacht bzw. den Geständniszwang am Beispiel der Diskursivierung von Sexualität. Vgl. hierzu: Foucault, Michel: *Sexualität und Wahrheit. Der Wille zum Wissen*. Frankfurt am Main: Suhrkamp 1977, S. 38; Vgl. Hillebrandt, Frank: Die Disziplinargesellschaft. In: Kneer, Georg/Nassehi, Armin/Schroer, Markus (Hg.): *Soziologische Gesellschaftsbegriffe. Konzepte moderner Zeitdiagnosen*. München: Fink Verlag 1997, S. 121.

Das Anonyme aushalten können: Ein Plädoyer

In heutigen pluralistischen, liberalen Gesellschaften gehören Anonymität und das Fremde zum Alltag, sind sogar untrennbar mit sozialen Strukturen verknüpft. Anonymität bringt prinzipiell Freiheitsgrade für Gesellschaften und ist somit für gesellschaftlichen Wandel unabdingbar. In der Gemeinschaft kann die soziale Interaktion mit dem Anonymen in Form des Fremden das Wir-Gefühl stärken und zu mehr sozialer Verbundenheit und Solidarität führen. Auch in der interindividuellen Begegnung kann Anonymität wie ausgeführt als funktional betrachtet werden.

Doch was passiert, wenn sich im Zuge der sich zunehmend formierenden Sicherheits- oder Kontrollgesellschaften Ordnung und Sicherheit als wesentliche Prinzipien etablieren, die das Anonyme und das Fremde als potenzielle Bedrohung wahrnehmen? Vor allem Gemeinschaften sehen im Begriff der Anonymität ein Risiko für die bestehende Ordnung und fordern gleichwohl deren Kontrolle mittels Transparenz und Überwachung. Eine Überhöhung gemeinschaftlicher Prinzipien auf gesellschaftlicher Ebene bspw. durch die

Forderung nach mehr staatlicher Kontrolle oder mehr technischer Überwachung gesellschaftlicher Räume zur Reduzierung von Anonymität birgt jedoch systemische Gefahren.

In seiner Monografie *Grenzen der Gemeinschaft* weist Plessner 1930 bereits vor der ›Machtergreifung‹ der Nationalsozialisten und dem daraus entstehenden totalitären System in Deutschland auf die Gefahren hin, die sich aus einer übermächtigen Gemeinschaftsideologie und -bewegung ergeben können. Gemeinschaft deutet Plessner »verständlich als Ideologie der Ausgeschlossenen, Enttäuschten und Wartenden […], gerechtfertigt als Protest der unter Großstadt, Maschinentum und Entwurzelung Leidenden, entfaltet das Idol der Gemeinschaft seine Anziehungskraft auf die Schwachen dieser Welt«[17].

Sehnsucht und Überbetonung nach Gemeinschaft erweist sich als wiederkehrendes historisches Prinzip in vermeintlichen gesellschaftlichen Übergangsphasen, in denen dann die Forderungen nach Sicherheit, Kontrolle und Ordnung lauter werden. Es ist eine konservativ ausgerichtete Denkweise, die auch als Entschleunigung eines oft als zu schnell empfundenen sozialen Wandels fungiert. Eine Sehnsucht nach Gemeinschaft dient in heutigen Gesellschaften vor allem dazu, Ordnung und Sicherheit wiederherzustellen. Es ist zunächst der Versuch, mit Unsicherheit umzugehen. Oft wird dann das Fremde als Bedrohung identifiziert und übernimmt dabei die Rolle des ›Sündenbocks‹. An ihm laden sich die gemeinschaftlichen Spannungen ab. Der Ursprung gemeinschaftlicher Aufstände und Unruhen wird dann den Fremden zugeschrieben.[18]

Der, die oder das Fremde bleibt dabei reine Projektionsfläche für die Gemeinschaft. Heutzutage sind es bspw. Geflüchtete, die als Gruppe anonym und fremd wahrgenommen werden und somit eine vermeintlich ungeordnete Bedrohung darstellen. Auf individueller Ebene jedoch werden sie als zuordenbare, mir bekannte Personen identifizierbar und plötzlich nicht mehr als Bedrohung wahrgenommen. In ähnlicher Weise wie das Fremde als Bedrohung erscheint, wird auch Anonymität bspw. im Internet als Problem der Unordnung diskursiviert, wie etwa im Falle des sog. Darknets oder im Diskurs um das *Netzwerkdurchsetzungsgesetz*. Im Anonymen des Internets findet sich eine Projektionsfläche für die Funktion des ›Sündenbocks‹ heutiger Kontrollgesellschaften.

Insgesamt ist infrage zu stellen, ob Gesellschaften auf zunehmende Unsicherheit mit mehr Sicherheits- und Kontrollbestrebungen reagieren sollten, oder ob sich nicht gerade dadurch eine Dysfunktionalität im gesellschaftlichen Miteinander ergibt, denn die »Hoffnung auf Rückkehr zum entkomplizierten Urleben, auf Wiedergewinnung des Gemeinschaftsfriedens ist trügerisch, ein Symptom jener schlechten Zwiespältigkeit der neuen Welt.«[19]. So ist der Ruf nach mehr Transparenz, nach mehr Ordnung auf gemeinschaftlicher Ebene womöglich gerechtfertigt, deren Realisierung auf gesellschaftlicher Ebene jedoch kritisch zu betrachten. Es stellt sich doch eher die Frage, ob heutige Gesellschaften nicht lernen sollten, Unordnung auszuhalten.[20] Durch Anonymität, durch das Fremde können Unsicherheit, Unordnung, aber eben auch Kreativität entstehen. Nur im Zulassen des Anonymen und des Fremden besteht die Freiheit, sanktionsfrei zu denken und zu handeln. Anonymität muss daher als unabdingbare Errungenschaft freier Gesellschaften gelten – sowohl für gesellschaftliche als auch für gemeinschaftliche und interindividuelle Handlungen.

17 Plessner, Helmut: *Grenzen der Gemeinschaft*. Frankfurt am Main: Suhrkamp 2001, S. 28.

18 Vgl. Simmel 1983, S. 510 f.

19 Plessner 2001, S. 25.

20 Vgl. Kron 2002.

Anne Deremetz

Wissenschaftliche Mitarbeiterin am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

»Wir sind alle Exhibitionisten im digitalen Raum«

Interview mit Prof. Dr. Thomas Knieper von der Universität Passau über die anonyme Nutzung des Internets

von Lea Watzinger und Patrick Herget

Prof. Dr. Thomas Knieper hat an der Universität Passau den Lehrstuhl für Computervermittelte Kommunikation inne. Mit ihm sprachen Lea Watzinger und Patrick Herget vom Graduiertenkolleg über Anonymität im Netz, den Mythos des freien Internets und natürlich seinen viral gegangenen ›Schweinebraten-Tweet‹.

Patrick Herget: Im Herbst 2018 haben Sie selbst erfahren, wie unvorhersehbar und schnell sich eine Botschaft im Netz ausbreiten kann: Mit einem Tweet[1] über das Essen auf dem Oktoberfest sorgten Sie für Aufsehen. Wie lebt es sich im Twitter-Rampenlicht?

Thomas Knieper: Wahnsinn, wie mich das verfolgt. Wohin ich gehe, stets bin ich der ›Schweinebraten-Prof‹. Dabei macht man einmal ein Bild auf der Wiesn, postet das relativ unbedarft, und plötzlich nimmt das kaum kontrollierbare und überraschende Eigendynamiken auf...

Lea Watzinger: Welche?

Thomas Knieper: Der Tweet ging viral, entsprechend gab es Reaktionen von allen Seiten: positive, hämische, sarkastische, aber auch radikale, eben politische, die meinen harmlosen Tweet als Aufhänger für hetzerische Kommentare benutzt haben. Das hat mich erschreckt, weil für mich der Bezug zum rechten Rand nicht auf der Hand liegt. Bereits am nächsten Tag konnte ich das nicht mehr einfangen. So etwas ist dann in der Welt und man kann nur noch deeskalierend einwirken.

Patrick Herget: Sie sind auf Twitter mit Ihrem Klarnamen aktiv. Wie stehen Sie zur Debatte[2] um eine Klarnamenpflicht im Netz?

Thomas Knieper: Man muss kurz überlegen, warum eine Klarnamenpflicht gefordert wird: Auf der einen Seite leben wir in einer vergleichsweise enthemmten Gesellschaft und im Netz gibt es immer mehr strafrechtsrelevante Inhalte. Da möchte man die Leute zuordnen und zwar direkt. Auf der anderen Seite hat Anonymität natürlich auch Vorteile.

Patrick Herget: Welche?

Thomas Knieper: Zum Beispiel bei Befragungen zum Arbeitsklima. Für Kritik braucht man manchmal den Schutz der Anonymität. Das gilt auch für Themen, die einen selbst belasten könnten, wie etwa Drogenkonsum oder ähnliches. Klarnamen wären dann kontraproduktiv. Für solche sensiblen Bereiche ist daher eine gewisse Anonymität durchaus sinnvoll.

Lea Watzinger: Wie lässt sich mit der neuen Dimension anonymer computervermittelter Kommunikation umgehen?

Thomas Knieper: Da sind jetzt zwei Aspekte wichtig: Einerseits neigen wir alle zum ›digitalen Seelenstrip‹ – wir sind alle Exhibitionisten im digitalen Raum. Damit verbunden ist das Bedürfnis, mit Klarnamen aufzutreten, um die Lorbeeren des eigenen digitalen Tuns zu ernten. Andererseits weiß ich nicht, wer sich hinter meinem digitalen Gegenüber verbirgt, wenn dieser mit Pseudonym auftritt. Soziale Umweltreize sind herausgefiltert. Ich muss mir keine Gedanken machen, ob mein Gegenüber hierarchisch oberhalb oder unterhalb von mir steht oder welchen Gruppierungen es angehört. Ich kann losgelöst von sozialen Normen einfach frei und enthemmt meine Meinung äußern, was doch wunderbar ist. Wenn es jedoch strafrechtsrelevant wird, müssen wir damit umgehen lernen.

Prof. Dr. Knieper ist seit 7 Jahren auf Twitter aktiv. Quelle: Twitter.com/TomKnieper (01.11.2018).

Patrick Herget: Welche Rolle spielt Anonymität für die Meinungsfreiheit in digitalen Öffentlichkeiten?

Thomas Knieper: Man muss seine Meinung frei und ohne Sanktion äußern können. Dazu brauchen wir Räume, in denen Anonymität garantiert wird, zumindest die Anonymität der Teilnehmenden untereinander. Es sollte sichergestellt sein, dass man miteinander frei reden kann. Die Redebereitschaft ist erfahrungsgemäß dann am höchsten, wenn Themen eine hohe Relevanz haben und emotional aufgeladen sind. Auf der anderen Seite sollte man im Hinterkopf haben, dass das Auftreten mit dem Klarnamen den eigenen Argumenten unter Umständen ein höheres Gewicht geben kann. Man verleiht seinem Standpunkt damit quasi die Chance auf ein höheres Wirkpotenzial. Das Anonymbleiben sollten Userinnen und User im Einzelfall eigenständig entscheiden dürfen. In diesem Zusammenhang wäre es kurzsichtig, eine Klarnamenpflicht im Netz gesetzlich zu reglementieren.

Lea Watzinger: Zumindest der Provider weiß, wer die Person hinter dem jeweiligen Account ist.

1 Vgl. Knieper, Thomas: So sieht also ein Schweinebraten für € 19,80 auf der Wiesn aus. Auf: *Twitter* vom 22.09.2018. Online: https://twitter.com/TomKnieper/status/1043484907438264320 (20.11.2018).

2 Vgl. Mack, Daniel: Wird Zeit für eine gesetzliche Klarnamenpflicht auf Facebook, Twitter, Instagram und Co. Auf: *Twitter* vom 14.09.2018. Online: https://twitter.com/danielmack/status/1040520176691752961?lang=de (20.11.2018).

Thomas Knieper: Ja, das freie und unkontrollierte Internet ist ein Mythos; es ist kein freier Raum: Es ist einer der am besten kontrollierten Räume überhaupt. Das muss man sich immer vor Augen halten.

Lea Watzinger: Woher kommt dieser Mythos?

Thomas Knieper: Zum einen kann über das Internet jeder selbst Content in die Öffentlichkeit bringen. Früher konnten das nur die etablierten Medien. Das ist ein mächtiges Gefühl, selbst Themen setzen zu können. Jede Person kann teilnehmen und hat plötzlich eine Stimme im öffentlichen Diskurs. Zum anderen beobachte ich jedoch eine zunehmende Enthemmung. Es werden im Netz immer extremere Meinungen geäußert. Das mag an einer durchaus problematischen Vorbildfunktion liegen. Viele soziale Netzwerke haben ihren Ursprung in den USA und dort herrscht ein anderes Verständnis von Rede- und Meinungsfreiheit. Der Rahmen des Erlaubten ist dort weit weniger reglementiert und eingeschränkt.

Patrick Herget: Wozu hat dieses andere Verständnis von Rede- und Meinungsfreiheit geführt?

Thomas Knieper: Einzelne Userinnen und User in Deutschland haben über Jahre ethische und dann auch rechtliche Grenzen überschritten. Zugleich wurde dieses Fehlverhalten über lange Zeit nicht oder kaum sanktioniert und geahndet. Das hat auf Seiten der Nutzerinnen und Nutzern zu einer Art Wahrnehmungsillusion geführt, in einem rechtsfreien Raum zu agieren. In jüngster Zeit ist jedoch ein Umdenken auf der Seite der Betroffenen zu beobachten: Sie lassen sich nicht mehr länger gefallen, im Netz beleidigt, verleumdet oder bedroht zu werden. Dann schützt auch ein anonymes Auftreten nicht vor einer Strafverfolgung.

Lea Watzinger: Also bloß eine ›gefühlte Anonymität‹?

Thomas Knieper: Eher eine gefühlte und gelebte Freiheit. Ihre Anonymität war den Leuten bei der Überschreitung von ethischen und rechtlichen Grenzen im Zweifel eher egal, da sie allenfalls in seltenen Einzelfällen zur Rechenschaft gezogen wurden. Eine Sanktionierung von Taten erfolgte lange nicht. Das ändert sich gerade. Zukünftig sollte man sich genau überlegen, was man im Netz schreibt. Das unreflektierte Beleidigen Dritter mag zwar kurzfristig das Mütchen kühlen, führt aber langfristig zunehmend zu unangenehmen Konsequenzen. Um zu erkennen, ob eine Grenze überschritten wurde, empfehle ich einen Rollenwechsel: Wie würde es mir gefallen, mit so einem Kommentar angegangen zu werden? So erhält man schnell ein Gefühl für unangemessene Äußerungen. Prinzipiell sollte auch der Aspekt der ›Respekttoleranz‹ eine größere Rolle spielen: Selbst wenn eine Aussage legal ist, muss man sie nicht zwingend äußern. Wenn ein Inhalt eine dritte Partei ohne berechtigten Anlass vorsätzlich verletzt, dann war sie nicht legitim. Hier verlangt der Respekt, dass man freiwillig auf eine derartige Äußerung verzichtet.

Patrick Herget: Sie sagen also, dass die Userinnen und User zunehmend ein Bewusstsein dafür entwickeln, dass der Hass im Netz zukünftig Konsequenzen haben wird?

Thomas Knieper: Meine Prognose ist, dass das zunehmend in das Bewusstsein der Leute rücken wird. Viele Leute sind nicht mehr bereit, sich den Hass im Netz gefallen zu lassen. Es werden immer öfter rechtliche Schritte gegen die Delinquenten eingeleitet, sodass diese auch immer häufiger verurteilt werden. Daneben findet auch eine öffentlichkeitswirksame Thematisierung dieser Fälle statt, sodass dies langfristig – so jedenfalls meine Mutmaßung – zu einer Sensibilisierung und zu einem Umdenken führt. Regelungen wie das *Netzwerkdurchsetzungsgesetz* werden diesen Prozess sicherlich zusätzlich beschleunigen.

Patrick Herget: Wäre auch eine entgegengesetzte Entwicklung denkbar, dass Leute sich erst recht in der Anonymität verstecken?

Thomas Knieper: Schlussendlich bleibt man meist rückverfolgbar. Es ist eine Illusion, dass man sich hinter anonymen oder pseudonymisierten Accounts nachhaltig verstecken kann. Ein hasserfülltes, menschenfeindliches oder gar menschenverachtendes Auftreten im öffentlichen Raum und insbesondere in sozialen Netzwerken wird nicht mehr länger akzeptiert. Mit quasi forensischen Anstrengungen werden diese Personen zukünftig zunächst demaskiert beziehungsweise ›reidentifiziert‹ und dann zur Rechenschaft gezogen.

Lea Watzinger: Ein ermutigender Ausblick, dass es sich auch zum Besseren wandeln kann.

Thomas Knieper: Das Internet ist uns ans Herz gewachsen, aber es gibt dort eben auch Negativphänomene. Halten Sie sich vor Augen, seit wann es dieses Mitmachnetz, das Web 2.0, gibt. Erst seit Mitte der 2000er! Am Anfang gab es eine lange Phase des Ausprobierens. Jetzt befinden wir uns in einer Phase der Konsolidierung. Inzwischen ist zudem der Großteil der Gesellschaft online aktiv. Aus meiner Beobachtung würde ich sagen, dass es eine Sehnsucht nach einem Diskurs gibt, an dem sich jeder ohne Angst vor Sanktionen beteiligen kann und der einen gesellschaftlichen Mehrwert bringt. Das ist doch das Ziel.

Patrick Herget: Ein schönes Fazit. Wir bedanken uns für das Gespräch!

Anonymität und soziale Medien

von Franz X. Berger

Die fortschreitende Digitalisierung verlagert Alltagssituationen zunehmend ins Internet. Viele Dinge fallen leichter, gehen schneller oder sind effektiver, wenn man digitale Strukturen nutzt. Damit ist es nachvollziehbar, dass immer mehr Menschen auf das Medium Internet zurückgreifen und damit gleichzeitig diesen Verlagerungsprozess vorantreiben. Am Beispiel der Kommunikation lässt sich dies besonders gut veranschaulichen. Die Digitalisierung bietet dabei zahlreiche Vorteile: Eine globale Echtzeitkommunikation auf Knopfdruck, das Versenden riesiger Datenmengen in einer Datei und die Erreichbarkeit eines nahezu unbegrenzten Publikums vom eigenen Wohnzimmer aus, um nur einige Möglichkeiten zu nennen.

Gerade Letzteres ist ein Novum mit unglaublichem Potential. Wollte man früher, bzw. will man ohne Nutzung des Internets am demokratischen Meinungsbildungsprozess teilnehmen, bietet sich regelmäßig nur eine beschränkte Möglichkeit, ein größeres Publikum zu erreichen. In der Antike nutzte man das Forum um öffentlich zu sprechen und diese Tradition setzt sich vom Marktplatz im Mittelalter über die Speakers' Corner in London – als wohl prominentestes Beispiel – bis zur Gegenwart fort. Weitere Möglichkeiten sind einen Leserbrief zu verfassen, sich zusammenzuschließen und an einer Versammlung teilzunehmen oder sich politisch in einer Partei zu engagieren. Jedoch erfordern alle analogen Möglichkeiten zur Befriedigung des Bedürfnisses, am Meinungsaustausch teilzuhaben, ein Maß an Bereitschaft, Struktur und Organisation, welches das der digitalen Alternativen, insbesondere die Nutzung sozialer Netzwerke als Diskursplattformen[1], um ein Vielfaches übersteigt. Facebook als Marktführer, aber auch Twitter, YouTube, Instagram und Co. verzeichnen mittlerweile eine enorme Anzahl an NutzerInnen weltweit[2] und bieten damit eine potentielle Reichweite, mit der es so einfach und effektiv möglich ist wie noch nie, die eigene Überzeugung kundzutun und so am Meinungsbildungsprozess mitzuwirken.

Doch so verlockend die Reichweite und Zugänglichkeit sozialer Netzwerke erscheint, entstehen durch die genutzten Strukturen große Risiken für die NutzerInnen. Ein Post findet nicht immer nur Gefallen und die Resonanz kann teilweise harsch ausfallen. Im schlimmsten Fall potenziert sich das Echo auf einen Kommentar zu einem ›Shitstorm‹ oder die AutorInnen werden Opfer von ›Hatespeech‹[3] bzw. ›Cybermobbing‹. Diese Phänomene waren mitunter der Grund für den Gesetzgeber, regulierend tätig zu werden und er hat dazu das *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (*Netzwerkdurchsetzungsgesetz* – NetzDG) geschaffen, welches insbesondere durch die Einführung von Löschpflichten der schnellen und effektiven Bekämpfung etwa von Hasskriminalität dienen soll.[4]

Die Motive des Gesetzgebers waren dabei berechtigt, jedoch gab es hinsichtlich der konkreten Umsetzung viel Kritik[5] und die tatsächlichen Auswirkungen dieses Gesetzes sind auch derzeit noch nicht endgültig abschätzbar. Jedenfalls kann eine Löschung bereits veröffentlichter Hasskommentare deren negative Wirkung nicht vollends beseitigen, geschweige denn vorab verhindern. Das Spannungsfeld zwischen der Teilnahme am öffentlichen Meinungsbildungsprozess durch die Nutzung sozialer Medien auf der einen Seite und die eben dadurch steigende Gefahr, Opfer von Hassattacken im Internet zu werden auf der anderen Seite, bleibt konstant. Zudem besteht das Risiko, dass anfänglich im Internet begonnene Auseinandersetzungen sich in der realen Welt fortsetzen und damit auch negative Auswirkungen auf das Privatleben der Opfer haben. Um sich davor zu schützen, wäre es wiederum naheliegend, sich aus der aktiven Nutzung sozialer Medien zurückzuziehen und diese lediglich als einseitigen Informationskanal zu nutzen. Dabei gibt es eine Möglichkeit, am digitalen Meinungsaustausch mitzuwirken und gleichzeitig die eigene Privatheit bereits präventiv zu schützten: ›Anonymität‹[6] (von altgriech. ›anónymos‹ = ohne Namen).

Ohne Namen

Wer anonym handelt, agiert ohne bzw. unter falschem Namen, sodass es nicht möglich ist, eine bestimmte Handlung einem konkreten Akteur zuzurechnen.[7] Genau das bietet eine Möglichkeit, dem angesprochenen Spannungsfeld selbst aktiv etwas zu entgegnen. UserInnen sozialer Medien können ihre Meinung anonym kundtun, ohne Gefahr zu laufen, Opfer von Hassattacken zu werden, die sich negativ auf ihr Privatleben auswirken. Anonymität in sozialen Medien könnte somit als Konzept zur Ermöglichung der Mitwirkung am öffentlichen Meinungsaustausch bei gleichzeitiger Wahrung der persönlichen Privatheit dienen. Was so verlockend klingt, wirft jedoch viele Fragen auf und kann aus ebenso vielen Perspektiven betrachtet werden. Alleine aus rechtlicher Sicht bieten sich dabei zahlreiche Anknüpfungspunkte. Dieser Beitrag beansprucht daher nicht, dieses Thema auch nur annähernd erschöpfend zu behandeln, sondern soll lediglich als Zugang zum Konzept der anonymen Nutzung sozialer

1 Die Funktionen sozialer Netzwerke sind vielfältig. Sie dienen selbstverständlich nicht ausschließlich der Meinungskundgabe, bzw. dem Meinungsaustausch zwischen den NutzerInnen. Hinsichtlich dieses Beitrags ist jedoch besonders das von diesen Plattformen geschaffene Diskurspotential relevant, sodass andere Funktionen, z.B. die der Selbstpräsentation und das Verhältnis der Nutzungsmöglichkeiten zueinander, nicht berücksichtigt werden.

2 Vgl. We Are Social: *Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im Januar 2018 (in Millionen)* 2018. Online: https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/ (08.10.2018).

3 Es gibt keine prägnante Definition für den Begriff, jedenfalls bildet ›Hatespeech‹ keine juristische Kategorie. Vgl. Bundeszentrale für politische Bildung (bpb): *Was ist Hatespeech?* 2017. Online: https://www.bpb.de/252396/was-ist-hate-speech (09.10.2018).

4 Vgl. Regierungsentwurf zum NetzDG, S. 1 f. Online: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_NetzDG.pdf (08.10.2018).

5 Hierzu existieren zahlreiche Stellungnahmen, vgl. exemplarisch: Deutscher Anwaltverein (DAV): *SN 41/17: Netzwerkdurchsetzungsgesetz – NetzDG.* Online: https://anwaltverein.de/de/newsroom/sn-41-17-netzwerkdurchsetzungsgesetz-netzdg (08.10.2018).

6 Vgl. grundlegend Brunst, Phillip W.: *Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen.* Berlin: Duncker & Humblot 2009; Steinert, Philipp: *Die anonyme Internetnutzung als Herausforderung für den Ehrschutz im Internet.* Hamburg: Verlag Dr. Kovac 2016.

7 Vgl. Schmahl, Stefanie: Anonymität im Recht: Freiheitsverbürgung oder Freiheitsgefährdung? In: *Juristen Zeitung (JZ).* Bd. 73, Nr. 12, 2018, S. 581–632, hier S. 581.

Netzwerke dienen, indem eine Auswahl verschiedener Erscheinungsformen und deren rechtliche Einordnung aufgezeigt werden und die Ambivalenz anonymer Posts, einerseits zum Schutz der eigenen Privatheit, andererseits als Deckmantel zur Verbreitung von Hass, verdeutlicht wird.

Grundrecht auf Anonymität

Darf man sich überhaupt anonym im Internet bewegen, oder anders formuliert, gibt es ein Recht auf Anonymität? Die Verfassung äußert sich nicht ausdrücklich dazu, es ist jedoch unbestritten, dass es ein solches Grundrecht gibt.[8] Es leitet sich aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) ab und wird etwa durch das Recht auf informationelle Selbstbestimmung und die Meinungsfreiheit ergänzt.[9] Alle BürgerInnen dürfen damit grundsätzlich frei entscheiden, ob sie offen oder anonym auftreten und das selbstverständlich auch hinsichtlich der Internetnutzung. Wie alle Freiheitsrechte lässt sich allerdings auch das Grundrecht auf Anonymität in einer verhältnismäßigen Anwendung einschränken. Es wirkt unmittelbar nur gegen den Staat selbst und kann diesem entgegengehalten werden, sofern er durch Gesetze oder anderes hoheitliches Handeln darin eingreift. Auf Grund des Schutzpflichtcharakters ist zudem ein gewisser Mindeststandard zur Ermöglichung von Anonymität durch den Staat zu gewährleisten. Der Gesetzgeber wird dieser Funktion etwa mit dem § 13 Abs. 6 TMG gerecht. Dadurch regelt er das Verhältnis zwischen den Plattformbetreibern und den UserInnen, indem er Diensteanbieter im Rahmen einer technisch möglichen und zumutbaren Weise zur Schaffung einer anonymen Nutzungsmöglichkeit von Telemedien verpflichtet.[10] Darüber hinaus kommt der Staat dieser Schutzpflicht durch das Datenschutzrecht nach.[11]

Andere Konstellationen außerhalb des klassischen Grundrechtsverhältnisses zwischen Staat und BürgerInnen werden im Rahmen der mittelbaren Drittwirkung[12] beeinflusst. Dabei gilt es stets, die sich gegenüberstehenden Positionen der GrundrechtsträgerInnen in einem möglichst schonenden Ausgleich zueinander zu bringen.

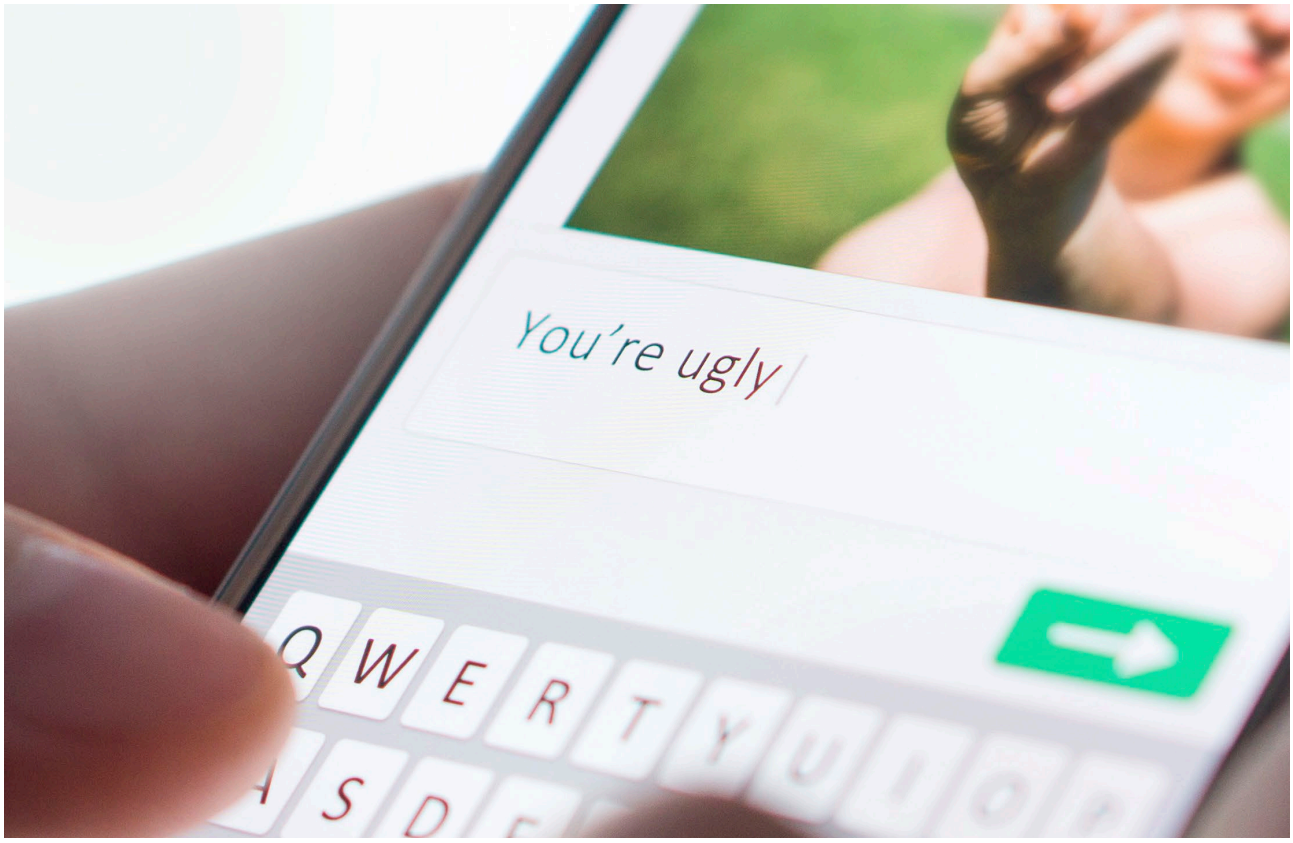
8 Vgl. Polenz, Sven: Teil 13: Datenschutz. In: Kilian, Wolfgang/Heussen, Benno (Hg.): *Computerrechts-Handbuch* 33. EL Februar 2018, 1. Abschnitt, Teil 13, Rn. 58 f.

9 Vgl. zur grundrechtlichen Dimension von Anonymität: Kersten, Jens: Anonymität in der liberalen Demokratie. In: *Juristische Schulung (JuS)*. Bd. 57, Nr. 3, 2017, S. 193–203, hier S. 195 ff.

10 Umfassend hierzu: Caspar, Johannes: Klarnamenpflicht versus Recht auf pseudonyme Nutzung. In: *Zeitschrift für Rechtspolitik (ZRP)*. Bd. 48, Nr. 8, 2015, S. 233–236.

11 Vgl. Härting, Niko: Anonymität und Pseudonymität im Datenschutzrecht. In: *Neue Juristische Wochenschrift (NJW)*. Bd. 66, Nr. 29, 2013, S. 2065–2071.

12 Zur mittelbaren Drittwirkung vgl. Guckelberger, Annette: Die Drittwirkung der Grundrechte. In: *Juristische Schulung (JuS)*. Bd. 43, Nr. 12, 2003, S. 1151–1157, hier S. 1154.



Anonymität im Konflikt zwischen freier Meinungsäußerung und dem Ehrschutz

Im Verhältnis zwischen den UserInnen von sozialen Netzwerken treffen regelmäßig das allgemeine Persönlichkeitsrecht und die Meinungsfreiheit aufeinander.

Ein einfaches Beispiel verdeutlicht einen Fall verhältnismäßiger Grundrechtseinschränkung: Wenn jemand in einem anonymen Post eine andere Person beleidigt, dann kann die Anonymität dieser Person nicht über das allgemeine Persönlichkeitsrecht der beleidigten Person gestellt werden. Die Anonymität der UserInnen tritt dabei hinter dem allgemeinen Persönlichkeitsrecht der Beleidigten zurück, sodass das Grundrecht auf Anonymität verfassungskonform eingeschränkt wird.

Im Verhältnis der UserInnen untereinander birgt die Anonymität weiter die Gefahr der Vereitelung etwaiger Rechtsdurchsetzung. Als entscheidende Grenze des Anonymitätsschutzes in sozialen Medien kann hierbei etwa die Rechtmäßigkeit des Posts herangezogen werden. Wird diese Grenze überschritten, bspw. bei einer Beleidigung, ist die Anonymität der rechtswidrig Handelnden nicht mehr schutzwürdig.

Der Zugriff auf anonyme NutzerInnen gestaltet sich dabei jedoch mitunter schwierig. Die Identifizierbarkeit durch Betroffene ist abhängig vom Grad der Anonymität.[13] Bei der anonymen Nutzung sozialer Medien gibt es derzeit verschiedene Varianten, abhängig von der genutzten Plattform.

Facebook etwa vertritt eine strikte Klarnamenpflicht[14], sodass weder die anonyme Anmeldung, noch die anonyme Nutzung zulässig sind. Die Kommunikationsplattform Twitter[15] fordert zwar eine Anmeldung mit Klarnamen, lässt eine pseudonyme Nutzung jedoch zu, wodurch eine Identifizierbarkeit durch den Anbieter möglich bleibt.[16] Als Beispiel für ein gänzlich anonymes Netzwerk lässt sich ›Jodel‹[17] anführen.

Hinsichtlich der Durchsetzbarkeit der Rechte der Beleidigten stellt sich die Anonymität als Hindernis in den Weg. Der unmittelbare Zugriff der Betroffenen auf die beleidigende Person ist bei anonymem Handeln nicht möglich. Eine Ermittlung der Identität gelingt dann ebenfalls oft nur mit Hilfe des Plattformbetreibers.[18] Damit ist es sinnvoll, den Plattformbetreiber in die Pflicht zu nehmen, rechtsverletzende Kommentare schnell zu löschen um die Rechte der Beleidigten effektiv zu wahren, wie es das NetzDG normiert.[19]

Es ist festzuhalten, dass die Anonymität in sozialen Medien sowohl zum eigenen Schutz vor Hass im Netz dienen aber auch dazu benutzt werden kann, sich drohenden Konsequenzen durch Fehlverhalten im Netz zu entziehen. Trotz dieser Ambivalenz ist sie aber ein verbürgtes Freiheitsrecht und nicht zuletzt wegen der Funktion als klassisches Abwehrrecht grundsätzlich aufrechtzuerhalten.[20] Eine vollkommene Abschaffung jeglicher Anonymität stellt damit keine Alternative dar. Dennoch stellt sich die Frage, inwieweit und in welchen Konstellationen die Verfassung diesbezüglich Einschränkungen zulässt.

Weitere Konstellationen

Wie aufgezeigt, genießen natürliche Personen ein Grundrecht auf Anonymität. Anders gestaltet sich die Situation, wenn juristische Personen, etwa Unternehmen, von Anonymität Gebrauch machen. Aus grundrechtlicher Perspektive ist dabei Art. 19 Abs. 3 GG entscheidend. Grundrechte gelten für juristische Personen nur dann, wenn sie dem Wesen nach auf diese anwendbar sind. Beim Grundrecht auf Anonymität ist dabei wegen dessen vielschichtiger Herleitung, insbesondere aus dem allgemeinen Persönlichkeitsrecht und der Meinungsfreiheit, eine differenzierte Betrachtung vorzunehmen. Hinsichtlich des allgemeinen Persönlichkeitsrechts wird vertreten, dass für juristische Per-

13 Zum Grad der Anonymität als rechtlicher Begriff vgl. Brunst 2009, S. 24.

14 Vgl. Facebook: *Nutzungsbedingungen* 2018. Online: https://www.facebook.com/legal/terms (08.10.2018); siehe auch LG Berlin: Urt. v. 16.1.2018 – 16 O 341/15. Die Einwilligung in die Klarnamenpflicht hielt der AGB-Prüfung nicht stand, das Urteil macht jedoch ausdrücklich keine Aussage in Bezug auf die Vereinbarkeit mit § 13 Abs. 6 TMG.

15 Vgl. Twitter: *Regeln* 2018. Online: https://about.twitter.com/de/safety/enforcing-our-rules.html (08.10.2018).

16 Die Klarnamenpflicht kann natürlich durch UserInnen schlicht umgangen werden, indem ein falscher Name bei der Registrierung angegeben wird, was dann zu einer Löschung des Accounts durch den Plattformbetreiber führen kann.

17 Vgl. Jodel: *Community Guidelines* 2018. Online: https://jodel.com/de/guidelines/ (08.10.2018).

18 Zu alternativen Ansätzen für einen effektiven Persönlichkeitsschutz trotz grundsätzlich gewährleisteter Anonymität: Heckmann, Dirk: Persönlichkeitsschutz im Internet – Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderung für Ehrschutz und Profilschutz. In: *Neue Juristische Wochenschrift (NJW).* Bd. 65, Nr. 36, 2012, S. 2631–2635, hier S. 2633 ff.

19 Vgl. § 3 Abs. 2 NetzDG; zur Kritik zum NetzDG, insbesondere hinsichtlich der Gefahr des ›Overblockings‹ auf Grund der Löschpflichten, statt vieler: Guggenberger, Nikolaus: Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht. In: *Zeitschrift für Rechtspolitik (ZRP).* Bd. 50, Nr. 4, 2017, S. 98–101, hier S. 99 f.; kritisch hinsichtlich des Overblocking-Arguments: Schiff, Alexander: Meinungsfreiheit in mediatisierten digitalen Räumen – Das NetzDG auf dem Prüfstand des Verfassungsrechts. In: *Multimedia und Recht (MMR).* Bd. 21, Nr. 6, 2018, S. 366–371, hier S. 369 f.; zu Hervorhebungen als Alternativvorschlag zu Löschungen: Heckmann, Dirk: Entwurf für ein Cybermobbing-Gesetz – Verbesserung des Persönlichkeitsrechtsschutzes im Internet. In: *Politische Studien.* Heft 479, Mai-Juni 2018, S. 30–39, hier S. 38.

20 Vgl. Kersten 2017, S. 195.

sonen lediglich ein abgesenktes Schutzniveau gilt, weil sie sich zumindest nicht auf dessen Menschenwürdegehalt berufen können.[21] Auf die Meinungsfreiheit etwa können sich nur inländische juristische Personen des Privatrechts berufen.[22] Das zeigt, dass der grundrechtliche Schutz der Anonymität sich nicht im gleichen Maße auf juristische Personen wie auf natürliche Personen erstreckt. Eine rechtliche Einschränkung der anonymen Nutzung von sozialen Medien durch juristische Personen scheint damit eine aus verfassungsrechtlicher Sicht mögliche Regulierungsoption zu sein.[23]

Auch die pseudonyme Nutzung[24] von Plattformen mittels ›Social Bots‹, also »Computerprogramme[n], die automatisiert bestimmte Aufgaben erfüllen«[25], wirft die Frage auf, ob dabei aus verfassungsrechtlicher Sicht eine Einschränkung zulässig ist, wenn bspw. durch künstlich generierte Posts, teilweise in Form von Fake News, versucht wird, den Meinungsbildungsprozess automatisiert und effizient zu beeinflussen. Dabei verstärkt sich die Wirkung durch den Anschein, die Kommentare stammten von einer Vielzahl realer UserInnen. Dies führt zu einer »Verstärkung der ›quantitativen Legitimität‹ einer Meinung«[26]. Um dieser Verwendung der anonymen bzw. pseudonymen Nutzung sozialer Medien entgegenzutreten, wird eine Kennzeichnungspflicht für Social Bots in Erwägung gezogen.[27] Social Bots sind als Computerprogramme selbst natürlich nicht grundrechtsfähig, jedoch lässt sich zumindest ein Grundrechtsschutz über die Meinungsfreiheit[28] der ProgrammiererInnen bzw. VerwenderInnen konstruieren, sodass im Falle einer Regulierung Art. 5 Abs. 2 GG zu beachten ist.[29] Die angesprochene Kennzeichnungspflicht für Social Bots entspricht dabei, anders als ein generelles Verbot der Nutzung von Social Bots, den Anforderungen an eine verfassungsgemäße Einschränkung der Meinungsfreiheit.

Fazit

Anonymität kann im Rahmen sozialer Medien eingesetzt werden, um die eigene Privatheit zu schützen. Sei es vor dem Zugriff des Staates bzw. der Plattformbetreiber auf die personenbezogenen Daten der NutzerInnen oder um Hasskommentaren anderer NutzerInnen eine Barriere in den Weg zu stellen, damit sie sich nicht in das reale Leben durchschlagen können. Anonymität zu gewähren ist erforderlich und von der Verfassung auch gefordert. Durch die anonyme Nutzung sozialer Medien zeigen sich jedoch auch Schattenseiten: Anonymität kann genutzt werden, sich möglicher Konsequenzen unzulässigen Verhaltens in sozialen Medien zu entziehen oder den Meinungsbildungsprozess missbräuchlich zu beeinflussen. Dennoch wäre es ein Freiheitsverlust sondergleichen, das Recht auf Anonymität aus diesem Grund gänzlich aufzugeben. Eine moderne und offene Gesellschaft muss Mittel und Wege finden, mit den dadurch entstehenden Herausforderungen schrittzuhalten. Hierfür scheint eine gesetzliche Einschränkung der Anonymität hinsichtlich juristischer Personen verfassungsrechtlich ebenso möglich wie eine Kennzeichnungspflicht für Social Bots. Die effektive Kontrolle der Umsetzung und die Durchsetzung solcher Regelungen stellen jedoch eine große Herausforderung dar, die nur mittels technischer Entwicklungsarbeit bewältigt werden kann.

21 Vgl. Di Fabio, Udo. In: Maunz, Theodor/Dürig, Günter (Begr.): *Grundgesetz-Kommentar* (83. EL April 2018), Art. 2 Abs. 1, Rn. 224, 225.

22 Vgl. Wendt, Rudolf. In: von Münch, Ingo/Kunig, Philip (Hg.): *Grundgesetz Kommentar*, Bd. 1, 6. Auflage 2012, Art. 5, Rn. 6, 7.

23 Vgl. hinsichtlich des allgemeinen Persönlichkeitsrechts auch Brunst 2009, S. 199.

24 Zu Pseudonymität als Unterform der Anonymität, vgl. Schmahl 2012, S. 881.

25 Bundeszentrale für politische Bildung (bpb): *Was sind Social Bots*? 2017. Online: http://www.bpb.de/252585/was-sind-social-bots (11.10.2018).

26 Brings-Wiesen, Tobias: Meinungskampf mit allen Mitteln und ohne Regeln? In: *JuWiss-Blog*, Beitrag vom 30.11.2016. Online: http://www.juwiss.de/93-2016/ (11.10.2018).

27 Vgl. Paal, Boris P./Hennemann, Moritz: Meinungsvielfalt im Internet – Regulierungsoptionen in Ansehung von Algorithmen, Fake News und Social Bots. In: *Zeitschrift für Rechtspolitik (ZRP)*. Bd. 50, Nr. 3, 2017, S. 76–79, hier S. 77 ff.

28 Die Frage, ob die Meinungsfreiheit auch beim Posten von Fake News durch Social Bots einschlägig ist – vertretbar, sofern man Fake News juristisch nicht ausschließlich als unwahre Tatsachenbehauptungen charakterisiert, welche nicht durch die Meinungsfreiheit geschützt sind (vgl. etwa Grabenwarter, Christoph. In: Maunz, Theodor/Dürig, Günter [Begr.]: *Grundgesetz-Kommentar* [83. EL April 2018], Art. 5 Abs. 1, Rn. 49) – ist für die Beurteilung der Verfassungsmäßigkeit einer generellen Kennzeichnungspflicht nicht relevant, sofern man davon ausgeht, dass Social Bots nicht ausschließlich zur Verbreitung von Fake News verwendet werden und wird deshalb nicht weiter erörtert.

29 Vgl. umfassend zu Social Bots: Schröder, Meinhard: Rahmenbedingungen der staatlichen Regulierung von Social Bots. In: *Deutsches Verwaltungsblatt (DVBl)*. Bd. 133, Nr. 8, 2018, S. 465–472; ebenso: Milker, Jens: »Social-Bots« im Meinungskampf. In: *Zeitschrift für Urheber- und Medienrecht (ZUM)*. Bd. 61, Nr. 3, 2017, S. 216–222; zusammenfassend: Metzl, Benedikt: Meinungsfreiheit für Maschinen? In: *for..net Blog*, Beitrag vom 21.06.2018. Online: https://www.for-net.info/2018/06/21/meinungsfreiheit-fuer-maschinen/ (09.10.2018).

Franz X. Berger

Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg »Privatheit und Digitalisierung« & am Lehrstuhl für Staats- und Verwaltungsrecht, Europarecht, Europäisches und Internationales Wirtschaftsrecht an der Universität Passau.

Kameras im Stadtgebiet

Der Eingriff in die Anonymität im öffentlichen Raum aus deutscher und russischer Sicht

von Hermann Jakobi

Der Beitrag widmet sich der praktischen Anwendung von öffentlicher Videoüberwachung in Russland im Vergleich zu Deutschland. Dazu soll ein Vergleich der russischen Stadt Krasnojarsk mit München zur Veranschaulichung dienen. Es soll aufgezeigt werden, welche rechtlichen Systematiken den Grundrechtsschutz in Bezug auf Videoüberwachung in den jeweiligen Rechtssystemen gewährleisten sollen. Zusammenfassend wird vorgeschlagen, Maßnahmen zum Schutz der bürgerlichen Grundrechte (informationelle Selbstbestimmung und Unverletzbarkeit des Privatlebens) in Russland zu etablieren, dennoch wird auch verdeutlicht, dass ein höheres Niveau des Grundrechtsschutzes (wie in Deutschland) nicht automatisch zu weniger Videoüberwachung führt.

Aufgrund der Veränderungen in der inneren und äußeren Sicherheitspolitik wurden auf europäischer sowie auf mitgliedstaatlicher Ebene viele Gesetzesänderungen entwickelt. Nicht zuletzt spielte dabei die Flüchtlingskrise eine wesentliche Rolle, wodurch einige polizeirechtliche Befugnisse erweitert und Grenzkontrollen verschärft wurden.

Ein Beispiel für eine solche Erweiterung der polizeilichen Befugnisse sind die präventiven Maßnahmen des Staates durch den Einsatz von Kameras im Stadtgebiet. Durch die Novellierung des bayerischen *Polizeiaufgabengesetzes* (PAG)[1] besteht auch in Deutschland die Gefahr, dass die Grundrechte einzelner Personen stark eingeschränkt werden.[2] In Bezug auf Videoüberwachung und die Anonymität einzelner Personen bedeutet das, dass die Möglichkeiten, im öffentlichen Raum anonym zu bleiben, weniger werden: Man nutzt regelmäßig öffentliche Verkehrsmittel, wartet an einer Haltestelle, durchquert Bahnhöfe oder verweilt auf dem Platz vor einem Einkaufszentrum. Dabei werden wir (v.a. in Großstädten) fast ununterbrochen durch Kameras gefilmt und die Aufnahmen gespeichert.

Ziel dieses Beitrages ist es, eine Analyse der gesetzlichen Lage zum Einsatz von Kameras auf öffentlichen Plätzen sowie generell im Stadtgebiet aus russischer und deutscher Sicht durchzuführen. Dabei soll aufgezeigt werden, welche Rechtsgrundlagen in en jeweiligen Ländern existieren, um die Überwachung im öffentlichen Raum aufzubauen und durchzuführen. Daran anknüpfend sollen allgemeine Vorschläge für die Entwicklung der gesamten Situation gegeben und ggfs. ein Prüfungsmodell in Bezug auf den Einsatz von Kameras in Russland entwickelt werden. Liegt ein solches Modell vor, kann man über die Rechtmäßigkeit der angewandten Maßnahmen diskutieren. Dieser Beitrag soll nicht Wege zur völligen Anonymität im öffentlichen Raum aufzeigen: Dies ist mittlerweile faktisch unmöglich. Stattdessen werden einige Ansätze dargestellt, die etwas mehr Anonymität gewährleisten könnten.

Der Einsatz von Kameras aus Sicht des russischen Gesetzgebers am Beispiel der Stadt Krasnojarsk

Zweifellos spielen polizeiliche Präventionsmaßnahmen in Form von Kameraeinsätzen im Stadtgebiet eine wichtige Rolle bei der Umsetzung der Sicherheitspolitik im öffentlichen Interesse. Außerdem können Aufnahmen auch als Beweismittel verwendet werden. Im Gegensatz zu Deutschland ist allerdings fraglich, ob der russische Gesetzgeber beim Einsatz von Kameras eine klare Grenze zwischen den Bereichen öffentlicher Platz, Personennahverkehr und Privatbereich zieht und ob er die Rechtsnatur der eingesetzten Kameras in ›privat‹ oder ›öffentlich‹ genau unterscheidet. Des Weiteren ist das Prüfungsschema der Rechtmäßigkeitsprüfung aus Sicht des russischen Gesetzgebers beim Einsatz der Kameras nicht klar.[3]

Es gibt im russischen Recht bzw. der russischen Rechtsliteratur kein Prüfungsmodell für den Einsatz von Überwachungskameras. In diesem Sinne wird versucht, das deutsche Modell anzuwenden, um eine Vergleichbarkeit der jeweiligen Sachverhalte herzustellen. Es ist jedoch zu beachten, dass dieses Modell nur theoretisch und nicht in der Rechtspraxis anwendbar ist, da die beiden Rechtssysteme unterschiedlich sind. So gilt im deutschen Recht das Prinzip der Verhältnismäßigkeit: Im Einzelfall ist stets darauf zu achten, dass eine Maßnahme, wie etwa die Videoüberwachung, geeignet, erforderlich und angemessen, also verhältnismäßig ist.[4]

Der Einsatz von Kameras zur Überwachung öffentlich zugänglicher Straßen und Plätze in Russland ist seit 2014 im Rahmen des staatlichen Programms *Die sichere Stadt* durch eine Verordnung der Russischen Föderation vorgesehen[5] und wird in den Regionen durch deren lokale Regierungen umgesetzt. Für die Region Krasnojarsk sind die ergriffenen juristisch-technischen Maßnahmen vor dem Hintergrund der *Verordnung der regionalen Regierung ›Über die Entwicklung der digitalen Gesellschaft‹* zu analysieren.[6]

Das bedeutendste Ziel des föderalen Programms *Die sichere Stadt* ist die Überwachung öffentlicher Plätze, insbesondere der Einsatz von Stadtkameras. Aus dem Programm ergibt sich, dass bislang weder vom Gesetzgeber noch von der Rechtspraxis Kriterien für den Einsatz von Kameras formuliert wurden. So ist das Programm *Die sichere Stadt* nur zielorientiert und um-

1 Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz – PAG) in der Fassung der Bekanntmachung vom 14. September 1990, das zuletzt durch § 1 des Gesetzes vom 18. Mai 2018 geändert worden ist. In: *Bayerisches Gesetz- und Verordnungsblatt* 2018, S. 301.

2 Vgl. Waechter, Kay: Polizeirecht in neuen Bahnen. In: *NVwZ*. Nr. 7, 2018, S. 458–462, hier S. 462.

3 Für die Vereinfachung des Inhaltes werden im Folgenden nur Aspekte der staatlichen Überwachung im öffentlichen Raum diskutiert. Es wird nicht um rein private Kameras wie z.B. sog. ›Dashcams‹ gehen, da dies den Umfang dieses Beitrags überschreiten würde.

4 Vgl. Brink, Stefan/Wilhelm, Maria. In: Wolff, Heinrich Amadeus/Brink, Stefan (Hg.): *BeckOK Datenschutzrecht*, 25. Ed., 01.08.2018, BDSG § 4 Rn. 3–6a.

5 Vgl. Verordnung der Regierung der Russischen Föderation vom 03. Dezember 2014, Nr. 2446-p. Online: http://www.pravo.gov.ru/ (15.10.2018).

6 Vgl. Verordnung der regionalen Regierung der Region Krasnojarsk: *Über die Entwicklung der digitalen Gesellschaft* (Übersetzung des Autors) vom 30. September 2013, Nr. 504-p. Online: http://docs.cntd.ru/document/422436883 (15.10.2018).

fasst inhaltlich lediglich die Anzahl der einzusetzenden Kameras. Bis zur *Winteruniversiade*, einem großen Sportevent in Krasnojarsk 2019, ist der Einsatz von ca. 400 bis 500 Kameras vorgesehen.[7] Dabei sind mehrere Kameras pro Standort, wie z.B. an der Promenade, geplant.

Für den Staat ist dabei das öffentliche Interesse bzw. die öffentliche Sicherheit relevant. Hauptsächlich spielt also die Anzahl der Straftaten, die mithilfe dieses Programms verhindert werden, eine Rolle. Das ergibt sich aus den Kommentaren der Polizei in den Medien über die Anwendung des Programms.[8] Für die BürgerInnen bedeutet das jedoch eine Reihe massiver Eingriffe in das Persönlichkeitsrecht und in ihre informationelle Selbstbestimmung. Der massive Kameraeinsatz führt somit zu einer Einschränkung der Anonymität der BürgerInnen im öffentlichen Raum.

Wie bereits erwähnt, werden für die folgende Prüfung Kriterien herangezogen, welche in der deutschen Rechtsliteratur angewendet werden. Bei dieser Prüfung geht es darum, dass der Eingriff in die informationelle Selbstbestimmung ein ›legitimes Ziel‹ verfolgen muss. Liegt ein legitimes Ziel vor, ist die Frage nach der Rechtfertigung relevant. Vor allem ist zu beachten, dass eine unkontrollierte und permanente Videoüberwachung auf keinen Fall mit dem Argument der öffentlichen Sicherheit gerechtfertigt werden kann, weil eine solche Videoüberwachung unverhältnismäßig ist. Zu betonen sind einige weitere Problemstellungen bei der Prüfung der Kriterien: Die erste Problemstellung beschäftigt sich mit der Frage nach der Geeignetheit, und zwar abhängig davon, welche Ziele die Polizei durch den Einsatz der Kameras verfolgt. Was filmen die Kameras? Welche Bereiche werden erfasst? Was wäre, wenn es sich nur um Attrappen handeln würde?

Fraglich ist zudem, ob die geplante Anzahl an Kameras erforderlich ist, oder ob Straftaten möglicherweise auch durch einen polizeilichen Streifgang verhindert werden könnten. Anhand des Beispiels der Kameras an der Promenade (vgl. Abb.) kann man sicher sagen, dass die vier gleichzeitig eingesetzten Kameras an einem Standort nicht erforderlich sind. Allerdings sind 400 Kameras nicht die größte Menge, die in einer Stadt mit einer vergleichbaren Bevölkerungszahl existieren kann; dies wird später am Beispiel von München aufgezeigt. Zuletzt stellt sich die Frage nach der Verhältnismäßigkeit. Laut der Berichterstattung und den Angaben der Polizei ist dabei zu beachten, dass eine Person mithilfe dieser Kameras identifiziert werden kann, wobei die Kameras ununterbrochen filmen.

Zusammenfassend ist festzustellen, dass bei der Umsetzung der Sicherheitspolitik in Russland die Systematik der Verhältnismäßigkeitsprüfung keine Anwendung

7 Vgl. Sobranie: *Die Entwicklung des Programms »Die sichere Stadt« in Krasnojarsk* (Übersetzung des Autors). Online: http://www.sobranie.info/newsinfo.php?UID=53486 (15.10.2018).

8 Vgl. Newslab.ru: *Über das Programm ›Die sichere Stadt‹* (Übersetzung des Autors) 2016. Online: http://newslab.ru/article/698799 (15.10.2018).

Die Kameras an der Jenissejpromenade in Krasnojarsk.
Fotos: Hanna Bauer

findet. Dies führt zu einem massiven Eingriff in die Grundrechte von Privatpersonen. Der russische Staat gewährleistet weder wirksamen Grundrechtsschutz noch eine effektive gerichtliche Kontrolle der polizeilichen Präventionsmaßnahmen. Vielmehr spricht diese Situation de facto für eine Verschärfung der Sicherheitspolitik in Bezug auf die Verhinderung von Straftaten. Ein unabhängiges Kontrollsystem der Polizei ist nach der Verordnung nicht vorgesehen.

Einsatz von Kameras im Stadtgebiet in Deutschland

Als Lösung wäre ein Modell vorstellbar, das sich in Bezug auf den Einsatz von Überwachungskameras beispielsweise an das bayerische *Polizeiaufgabengesetz* (Art. 11 PAG) sowie an die *Datenschutz-Grundverordnung* (Art. 6 DS-GVO) anlehnt. Nicht zuletzt spielt das deutsche *Bundesdatenschutzgesetz* (BDSG), welches die allgemeine Rechtsgrundlage für die Videoüberwachung öffentlich zugänglicher Räume in § 4 vorsieht, eine Rolle.

Aus Sicht des deutschen Gesetzgebers ist das dreistufige Modell der Verhältnismäßigkeitsprüfung für den Einsatz von Kameras im Stadtgebiet Standard: Die Diskussion über die Maßnahmen der Polizei bezüglich des Eingriffs in die Grundrechte ist daher nicht neu und wird in Deutschland und in der EU immer wieder geführt.[9] Zu bemerken ist, dass der deutsche Gesetzgeber einen klaren Unterschied zwischen den Überwachungsfeldern macht. Nach Wolfgang Kunz und Urs Kramer hat der deutsche bzw. europäische Gesetzgeber mit der Novellierung der gesetzlichen Lage versucht, eine spezifische rechtliche Grundlage bei der Prüfung von Maßnahmen im Einzelfall zu schaffen, damit man z.B. zwischen öffentlichen und nicht-öffentlichen Plätzen unterscheiden kann.[10] Dabei ist der öffentliche Raum als Bereich zu verstehen, innerhalb dessen nochmals zwischen spezifischen Bereichen unterschieden werden muss: Es ist bspw. zu differenzieren, ob Videoüberwachung in Läden, auf öffentlich zugänglichen Plätzen oder in Bahnhöfen stattfindet. Daneben muss auch beachtet werden, wer die Überwachung durchführt. Nach deutschem Recht ist Videoüberwachung z.B. auch durch private Sicherheitsdienste im Auftrag von staatlichen Behörden möglich.[11]

Ein Problem ergibt sich jedoch auch in Deutschland aus der ständigen Erhöhung der Anzahl von Kameras (sowohl von tatsächlich eingesetzten Kameras als auch Attrappen). Für die effektive Entwicklung der Sicherheitspolitik ist zudem die Zusammenarbeit der beteiligten Parteien, nämlich Polizei, BürgermeisterIn und Zivilbevölkerung notwendig. Die Polizei und andere zuständige Organe sowie die Zivilgesellschaft müssen kooperieren, um die Effektivität der Überwachungsmaßnahmen zu verbessern. Dieses Teamwork hilft der Polizei, Probleme effektiver zu lösen, falls eine reine Überwachungsaktivität nicht erfolgreich ist. Ein Beispiel dafür ist der Orleansplatz-Fall in München, bei dem die Überwachung durch Kameras allein nicht erfolgreich war.[12] Im Orleansplatz-Fall haben die Polizei und das Rote Kreuz zusammengearbeitet, um die Anzahl der Straftaten durch die dort verweilenden Personen zu reduzieren. Eine reine Überwachung durch die Kameras blieb dagegen ohne Erfolg.

Trotz eines systematischen Modells der Verhältnismäßigkeitsprüfung ist die derzeitige ›anonyme Situation‹ in München allerdings nicht besser als in Krasnojarsk. Laut der *Süddeutschen Zeitung* waren bereits vor einigen Jahren mehr als 9200 Kameras im Stadtgebiet installiert.[13] Die Einwohnerzahl in Krasnojarsk ist fast so hoch wie in München. Bei einer fast identischen Menge an potentiell zu überwachenden Individuen sind in München also mehr als zwanzig Mal soviele Kameras im Einsatz als in Krasnojarsk (etwa 400 bis 500). Zudem wird die Anzahl der Kameras stetig weiter erhöht.[14] Die Überwachungstätigkeit der Polizei wird also erweitert, sodass sich aus juristischer Perspektive insgesamt ein Vorrang des Sicherheitsbereichs gegenüber den Grundrechten von Privatpersonen feststellen lässt.

Fazit

Die aktuellen Herausforderungen der verhältnismäßigen Bekämpfung von Straftaten auf öffentlichen Plätzen können nur bewältigt werden, wenn die beteiligten Parteien, unter anderem exekutive Organe wie die Polizei und z.B. BürgermeisterIn sowie Zivilbevölkerung kooperieren. Denkbar wäre eine unabhängige Auf-

9 Vgl. Bausch, Stephan: *Videoüberwachung als präventives Mittel der Kriminalitätsbekämpfung in Deutschland und Frankreich.* Baden-Baden: Tectum Wissenschaftsverlag 2004, S. 184.

10 Vgl. Kunz, Wolfgang/Kramer, Urs: *Eisenbahnrecht*. Baden-Baden: Nomos 2018, S. 1916.

11 Vgl. Brink, Stefan/Wilhelm, Maria. In: Wolff, Heinrich Amadeus/Brink, Stefan (Hg.): *BeckOK Datenschutzrecht*, 25. Ed., 01.8.2018, BDSG § 4 Rn. 7–12.

12 Vgl. Bernstein, Martin: Da schau her, die Polizei. In: *Süddeutsche.de* vom 29.12.2016. Online: https://www.sueddeutsche.de/muenchen/videoueberwachung-da-schau-her-die-polizei-1.3313470 (15.10.2018).

13 Vgl. Fuchs, Florian/Staudinger, Melanie /Steinberg, Nicholas/Völklein, Marco: Stadt der 10000 Augen. In: *Süddeutsche.de* vom 23.01.2015. Online: https://www.sueddeutsche.de/muenchen/videoueberwachung-in-muenchen-stadt-der-augen-1.2316618 (15.10.2018).

14 Vgl. Bayerisches Staatsministerium des Innern, für Sport und Integration: *Mehr Videoüberwachung im öffentlichen Raum* 2017. Online: http://www.stmi.bayern.de/med/aktuell/archiv/2017/170822videoueberwachung/#link_1 (15.10.2018).

sichtskommission bestehend aus VertreterInnen der Zivilbevölkerung und ExpertInnen für die Kontrolle der polizeirechtlichen und allgemeinen verwaltungsrechtlichen Maßnahmen in Bezug auf die Videoüberwachung. Ein Beispiel für eine Aufgabe dieser Kommission könnte die Kontrolle der eingesetzten Kameras und die Prüfung ihrer Notwendigkeit sein. Der aktuelle Stand der technisch-organisatorischen Voraussetzungen wäre dabei zu berücksichtigen.

Ein wichtiger Punkt für den russischen Gesetzgeber wäre die Unterscheidung öffentlicher und privater Räume, wobei Überwachungsmaßnahmen mit Hilfe des deutschen Prüfungsmodells der Verhältnismäßigkeit kontrolliert werden könnten. Zudem sind die Eigenschaften der eingesetzten Kameras (Aufnahmen in Farbe oder schwarz-weiß, stationäre oder dynamische Kameras, mit Tonaufnahme oder ohne etc.) sowie die Dauer der Aufnahmen und deren Speicherung zu berücksichtigen. Bei der Entwicklung der Überwachungsmaßnahmen müssen die Unterschiede zwischen öffentlichen Plätzen und privaten bzw. intimen Bereichen detaillierter ausdifferenziert werden, damit eine gezielte Überwachung möglich ist und nicht allgemein alles und jeder gefilmt wird. Eine wichtige Voraussetzung für die Überwachungsaktivität der Polizei ist daneben auch eine ausreichende Anzahl an PolizeibeamtInnen, die das gesamte Überwachungsverfahren kontrollieren und auswerten können. Steht nicht genügend ausgebildetes Personal zur Verfügung, muss eine Alternative zum Einsatz der Kameras gefunden werden.

Für den deutschen Gesetzgeber wäre die Frage nach der allgemeinen Entwicklung der Sicherheitspolitik in Bezug auf die DS-GVO, das BDSG und die Novellierung der polizeilichen Befugnisse relevant. Besonders wichtig ist, dass die Aufsichtskommissionen die Tätigkeit der Polizei kontrollieren können, um Eingriffe in die Grundrechte möglichst zu verhindern. Dabei ist jedoch fraglich, ob die geplante Anzahl der Kameras in München erforderlich ist. Abgesehen davon, dass die russische Stadt Krasnojarsk viel weniger wirtschaftliche Bedeutung hat, sind dort bei ähnlicher Bevölkerungsanzahl nur 400 Kameras eingesetzt. Die Frage, ob es möglich wäre, Alternativmaßnahmen für die Münchener Polizei zu finden, ist derzeit noch offen, da die Rechtspraxis des neuen PAG noch unklar ist.

Letztendlich lässt sich sagen, dass weder das deutsche Modell der Verhältnismäßigkeitsprüfung in Bezug auf Kameraüberwachung im öffentlichen Raum bzw. dessen Implementierung in die Praxis noch die russische Situation des kaum juristisch eingeschränkten Kameraeinsatzes optimal sind. Vor allem zeigt die Rechtspraxis, dass sich die Anzahl der eingesetzten Kameras trotz der systematischen Prüfung auch in Deutschland ständig erhöhen wird. In Bezug auf Russland ist festzuhalten, dass das Fehlen eines systematischen Prüfungsmodells für den Einsatz von Videoüberwachung zu einem mangelnden Grundrechtsschutz führt. Da es kein russisches Prüfungsmodell gibt, kann man jedoch zumindest bei den theoretischen Auslegungen das deutsche Modell anwenden.

Hermann Jakobi

DAAD-Stipendiat am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Nationale Sicherheit zum Preis der Anonymität

Wie Russland versucht, ›Telegram‹ zu sperren

von Elizaveta Saponchik

Der Messenger ›Telegram‹ wurde vom russischen Internetunternehmer Pavel Durov im Jahr 2013 gegründet. Heute gehört Telegram zu den beliebtesten Messengern sowohl in Russland als auch in der gesamten Welt. Die Zahl der aktiven NutzerInnen beträgt etwa 200 Millionen Menschen weltweit (Stand März 2018).[1] Aktuell belegt Telegram den neunten Platz im Ranking der beliebtesten Messenger-Dienste.[2]

»Sie können Telegram sperren lassen, aber, wie ich früher gesagt habe, wird Ihnen das nicht wirklich helfen. Es ist offensichtlich, dass Freiheit und Datenschutz im Endeffekt alles andere besiegen werden. Diejenigen, die zurück ins Jahr 1930 möchten, werden verstehen, dass sie sich in einer anderen Realität befinden.«[3]

Pavel Durov.

Was ist an Telegram so besonders, dass diese Anwendung nicht nur derart an Popularität bei den NutzerInnen gewonnen hat, sondern auch zum Dorn im Auge des Föderalen Dienstes für Sicherheit der Russischen Föderation (des Inlandsgeheimdienstes FSB) wurde? Dies hat verschiedene Gründe. Wie in Telegrams FAQ steht, kann die App vollständige Sicherheit und Anonymität der Daten gewährleisten.[4] Telegram benutzt das eigens entwickelte Verschlüsselungsprotokoll ›MTProto‹. Allerdings wurde die Sicherheit von MTProto von manchen IT-ExpertInnen bezweifelt,[5] da MTProto noch nicht lange im Einsatz ist und dessen Zuverlässigkeit daher noch bestätigt werden muss.

Die hauptsächliche Besonderheit Telegrams im Vergleich zu anderen Diensten ist die Möglichkeit, sogenannte ›Kanäle‹ zu gründen. Diese Kanäle können sowohl öffentlich als auch privat und anonym sein. In einem öffentlichen Telegram-Kanal können die VerwalterInnen dieses Kanals Beiträge zu beliebigen Themen verfassen. Solche Kanäle erfreuen sich derzeit in Russland z.B. bei politischen AktivistInnen und JournalistInnen großer Beliebtheit. Darüber hinaus kann man als NutzerIn einen anonymen Kanal gründen. Ein anonymer Kanal ist ein geschützter Raum, in dem niemand überwacht und der Zensur unterworfen werden kann. Informationen darüber, wer den anonymen Kanal verwaltet und wer diesem Kanal folgt, sind geschützt. Nur die VerwalterInnen eines solchen Kanals haben Zugang zu diesen Informationen. Anonyme Telegram-Kanäle nutzen nicht nur Privatpersonen in Russland, sondern auch Medien und JournalistInnen. In manchen Telegram-Kanälen werden Informationen von ›InsiderInnen‹ veröffentlicht, die erst danach in die russischen Medien gelangen. Dank der Anonymität konnte man in Russland z.B. zum Amoklauf in Kertsch schnelle und auch glaubwürdige Information bekommen.[6]

Darüber hinaus bietet Telegram sogenannte *secret chats* an, die mit Ende-zu-Ende-Verschlüsselung geschützt sind und nicht als Backup gespeichert werden (anders als bei WhatsApp oder Viber, die Backups bei Google Drive oder iCloud speichern).[7] Diese Art der Ende-zu-Ende-Verschlüsselung soll Kommunikation in absoluter Anonymität gewährleisten. Die Verwaltung von Telegram hat keinen Zugang zu dieser Kommunikation. Übermittelte Daten werden nur auf den Smartphones der NutzerInnen entschlüsselt.

Alle anderen Arten von Telegram-Chats (inkl. Kanäle) sind *cloud chats* und werden nicht durch Ende-zu-Ende-Verschlüsselung geschützt. Allerdings werden die Daten in Datenzentren gespeichert, die sich in verschiedenen Jurisdiktionen befinden.[8] Das macht den Zugriff auf die Daten für Staatsorgane rechtlich schwierig, was im Weiteren geschildert wird.

Der Konflikt zwischen Telegram und dem Föderalen Dienst für Sicherheit der Russischen Föderation (FSB)

Der Konflikt zwischen Telegram und dem FSB begann 2017, als der FSB eine Anfrage an Telegram bezüglich der sechs mutmaßlichen StraftäterInnen des Terrorakts in Sankt Petersburg stellte.[9] Die Forderungen des FSB wurden mit Art. 10.1. Abs. 3.1. des *Föderalen Gesetzes ›Über Informationen, Informationstechnologien und Informationssicherheit‹* begründet.[10] Diese Norm verpflichtet Nachrichtenportale und

1 Vgl. Statista: *Number of monthly active Telegram users worldwide from March 2014 to March 2018 (in millions)* 2018. Online: https://www.statista.com/statistics/234038/telegram-messenger-mau-users/ (29.09.2018).

2 Vgl. Statista: *Most popular mobile messaging apps worldwide as of july 2018, based on number of monthly active users (in millions)* 2018. Online: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (29.09.2018).

3 Fontanka: *Beschuldigungen gegen Telegram sind sinnlos* (Übersetzung durch die Autorin) 2017. Online: https://www.fontanka.ru/2017/09/28/141/ (26.11.2018).

4 Vgl. Telegram: *What are your thoughts on internet privacy?* Online: https://telegram.org/faq#q-how-secure-is-telegram (29.09.2018).

5 Vgl. Turton, William: Cryptography expert casts doubt on encryption in ISIS' favorite messaging app. In: *The Daily Dot* vom 19.11.2015. Online: https://www.dailydot.com/layer8/telegram-isis-encryption-cryptography/ (29.10.2018).

6 Vgl. für einen Überblick deutscher Medien zu den Geschehnissen z.B.: Tagesschau: *Viele Tote bei Amoklauf auf der Krim* 2018. Online: https://www.tagesschau.de/ausland/explosion-krim-103.html (30.11.2018).

7 Vgl. Telegram: *How are secret chats different?* Online: https://telegram.org/faq#q-how-are-secret-chats-different (29.09.2018).

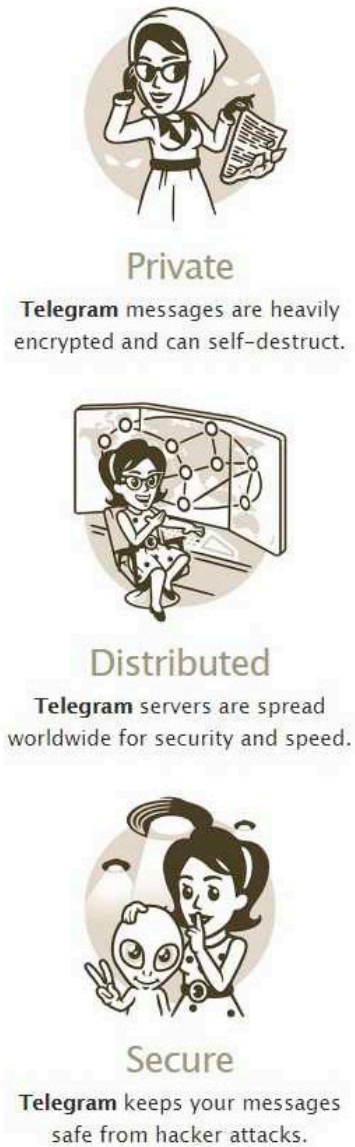
8 Vgl. Telegram: *Do you process data requests?* Online: https://telegram.org/faq#q-do-you-process-data-requests (01.11.2018).

9 Vgl. Vasilyev, Alexey: Terrorakte in Petersburg wurden mit Telegram geplant (Übersetzung durch die Autorin). In: *RG.RU* vom 15.12.2017. Online: https://rg.ru/2017/12/15/reg-szfo/fsb-predotvrashchennye-terakty-v-peterburge-splanirovali-cherez-telegram.html (01.11.2018). Vgl. dazu auch: Tass: *Ein Teil der Telefonnummer, die der FSB wegen des Terroraktes in Petersburg fordert, war nicht an Telegram gebunden* (Übersetzung durch die Autorin) 2017. Online: https://tass.ru/ekonomika/5162254 (01.11.2018).

10 Vgl. *Föderales Gesetz der Russischen Föderation über Informationen, Informationstechnologien und Informationssicherheit* (Übersetzung durch die Autorin). Online: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (29.09.2018).

Dienste wie Telegram, die Nachrichten verbreiten, zur Strafverfolgung erforderliche Daten (z.B. Textnachrichten, Sprachnachrichten, Bilder oder Metadaten) an staatliche Sicherheitsbehörden zu übermitteln. Die Rechtmäßigkeit dieser Normen sowie die Anforderungen des FSB rufen jedoch aus juristischer Perspektive einige Fragen hervor: Art. 23 der russischen Verfassung garantiert das Post- und Fernmeldegeheimnis, wobei dies jedoch kein absolut gewährleistetes Grundrecht ist. Laut Art. 23 Abs. 2 der russischen Verfassung ist der Zugang zu grundsätzlich geschützten Informationen dann zu gewähren, wenn ein Gerichtsurteil vorliegt.[11]

11 Vgl. *Verfassung der Russischen Föderation: Art. 23, Abs. 1, 2.* Online: http://pravo.gov.ru/konstituciya/ (29.09.2018).



Erläuterungen zur Kommunikations-App Telegram. Quelle: Telegram.org (06.12.2018).

Im Fall der Anfrage im Zuge des St. Petersburger Anschlags lag gleichwohl kein Gerichtsurteil vor. Die Nichtbeachtung dieser Verfassungsvorgabe durch den FSB hat für viel Kritik und Empörung in der russischen Gesellschaft gesorgt.[12]

Des Weiteren hat Telegram keinen Sitz in Russland, sondern ist in Großbritannien registriert. Dort befindet sich das Datenzentrum, in dem die Daten europäischer NutzerInnen verwaltet werden. Aus diesem Grund stellt sich die Frage, nach welcher rechtlichen Grundlage Telegram handeln muss, wenn es eine Anfrage von einer ausländischen Sicherheitsbehörde wie dem FSB erhält. Ist Telegram also überhaupt an russisches Recht gebunden? Klare Antworten auf diese Frage liegen noch nicht vor.

2018 wurde Telegram vom FSB aufgefordert, seinen universellen Verschlüsselungscode herauszugeben.[13] Die Herausgabe des Verschlüsselungscodes war jedoch technisch unmöglich, weil, wie oben erläutert, die *secret chats* mit Ende-zu-Ende Verschlüsselung geschützt sind und die cloud chats nie zentral an einem Ort gespeichert werden, sondern in verschiedenen Datenzentren. Da Telegram die Herausgabe des Codes auch aufgrund der technischen Unmöglichkeit verweigerte, wurde die App auf Klage der russischen Internetaufsicht ›Roskomnadzor‹ per Gerichtsbeschluss gesperrt. Bis zum heutigen Tag wird Telegram z.B. vom FSB-Chef öffentlich dafür kritisiert, dass seine Anonymität für viele StraftäterInnen attraktiv sei und die App somit der Kriminalität Vorschub leiste.[14]

Durch die Sperrung sollten russische BürgerInnen die Möglichkeit zur anonymen Kommunikation verlieren. Die Sperre ist allerdings relativ einfach mithilfe von ›VPN‹-Diensten und ›Proxyservern‹ zu umgehen, weshalb Telegram in Russland trotz allem weiterhin nutzbar ist. Nach aktuellen Medienangaben testen der FSB und die Aufsichtsbehörden allerdings neue Technologien, um Telegram endgültig zu blockieren.[15] Wenn den Behörden dies gelingt, könnte die anonyme Kommunikation im russischen Teil des Internets nahezu unmöglich werden.

12 Vgl. Tass: *Telegrams NutzerInnen verklagen FSB* (Übersetzung durch die Autorin) 2018. Online: https://tass.ru/obschestvo/5027250 (08.11.2018).

13 Vgl. *Anordnung des Föderalen Staatsdienstes zur Herausgabe von Daten durch Telegram* (Übersetzung durch die Autorin). Online: https://agora.legal/fs/a_delo2doc/54_file_Telegram_FSB_120717.pdf (26.11.2018).

14 Vgl. Bortnikov, Alexander: *Telegram versteht die Wichtigkeit der Terrorbekämpfung nicht* (Übersetzung durch die Autorin). In: Tass vom 08.11.2018. Online: https://tass.ru/obschestvo/5769905 (26.11.2018).

15 Vgl. Kolomytschenko, Maria: Russland testet neue Technologien für Telegram-Sperre aus (Übersetzung durch die Autorin). In: *Reuters* vom 30.08.2018. Online: https://ru.reuters.com/article/topNews/idRUKCN1LF201-ORUTP (29.09.2018).

Sind solche Maßnahmen wirklich erforderlich und verhältnismäßig, um die Sicherheit zu gewährleisten? Es ist offensichtlich, dass sich das Terrorismusproblem mit der Sperrung eines Dienstes nicht lösen lässt. StraftäterInnen können unterschiedlich miteinander kommunizieren, und Straftaten auf unterschiedliche Weise begehen. Terrorismus kann man nicht sperren oder verbieten. Man kann vermuten, dass auch nach einer faktischen Abschaltung Telegrams die Terrorgefahr in Russland auf einem ähnlichen Niveau bleiben wird, allerdings zum Preis einer massiven Einschränkung von Anonymität.

Russischer Staat gegen Anonymität

Zusammenfassend lässt sich also sagen, dass die Tendenz zu Verboten und restriktiven Regelungen in Russland steigt.[16] An dieser Stelle sei an den Vortrag der britischen Rechtsschutzorganisation ›Article 19‹ bei den Vereinten Nationen im Juni 2018 erinnert: »The Russian Federation is pursuing policies that are significantly and rapidly encroaching online freedoms affecting not only the rights of people living in Russia but Internet users everywhere.«[17]

Im Hinblick auf den Telegram-Fall könnte man dieser Meinung zustimmen. Die ergriffenen staatlichen Maßnahmen gewährleisten die öffentliche Sicherheit kaum, stattdessen werden in erster Linie russische BürgerInnen in ihren Grundrechten beeinträchtigt. Durch die Einschränkung der Anonymität im Netz durch den russischen Staat sind die Menschen in ihren Meinungsäußerungen weniger frei und die Zivilgesellschaft wird geschwächt. Die aktuelle russische Politik widerspricht daher sowohl verfassungsrechtlichen Vorgaben als auch demokratischen Grundwerten.

Es sind jedoch auch positive Entwicklungen zu beobachten: So sagte Alexey Volin, der stellvertretende Minister für digitale Entwicklungen der Russischen Föderation, im November 2018 während des sechsten russisch-chinesischen Mediaforums in Bezug auf Telegram: »Sperren sind eine veraltete Praktik, deren Effektivität heutzutage nicht nachweisbar ist. So etwas sollte der Vergangenheit angehören.«[18]

16 Vgl. *Föderales Änderungsgesetz zu Verwaltungsstraftaten* (Übersetzung durch die Autorin). Online: http://publication.pravo.gov.ru/Document/View/0001201806270048 (01.11.2018).

17 Article 19: *HRC38: Oral statement on internet freedoms in Russia 2018.* Online: https://www.article19.org/resources/hrc38-oral-statement-to-general-debate-on-item-4-on-internet-freedom-in-russia/ (29.09.2018).

18 RIA Novosti: *Die Situation um Telegram: Der stellvertretende Leiter des Ministeriums für Kommunikation sagte, dass die Sperrung im Internet unwirksam sei* (Übersetzung durch die Autorin). Online: https://ria.ru/society/20181101/1531904482.html (01.11.2018).

Elizaveta Saponchik

DAAD-Stipendiatin am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Erscheint im Sommer 2019

Datenschutz bleibt ein umkämpftes Thema im Kontext der voranschreitenden Digitalisierung. Die Beiträge des Bandes gehen der Frage nach, welche Formen Privatheit in einer digitalen Gesellschaft annehmen kann und welche Chancen und Risiken dabei entstehen. Dabei ergeben sich medienkulturelle Fragestellungen nach den Normierungsmustern hinter digitalen Anwendungen sowie die Notwendigkeit, digitale Nutzungsszenarien zu analysieren, einzuordnen und zu bewerten.

Weitere Publikationen

Aufsätze

Abold, Metawi/Riehm, Thomas: Mängelgewährleistungspflichten des Anbieters digitaler Inhalte. In: *Zeitschrift für Urheber- und Medienrecht*. Jahrgang 62, Heft 2, 2018, S. 82–91.

Hennig, Martin/Piegsa, Miriam: The Representation of Dataveillance in Visual Media. Subjectification and Spatialization of Digital Surveillance Practices. In: *On_Culture. The Open Journal für the Study of Culture*. Issue 6, 2018. Online: https://www.on-culture.org/journal/issue-6/hennig-piegsa-dataveillance/.

Hornung, Gerrit: Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch »Smart Everything«. In: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hg.): *Die Fortentwicklung des Datenschutzes.* Wiesbaden: Springer Vieweg 2018, S. 315–336.

Riehm, Thomas: Dateneigentum – Schutz nach allgemeinem Zivilrecht. In: Hornung, Gerrit (Hg.): *Rechtliche Herausforderungen der Industrie 4.0. Datenhoheit – Verantwortlichkeit – rechtliche Grenzen der Vernetzung.* Baden-Baden: Nomos Verlagsgesellschaft 2018, S. 73–96.

Riehm, Thomas: Smart Contracts und verbotene Eigenmacht. In: Paal, Boris/Fries, Martin (Hg.): *Smart Contracts* (im Erscheinen).

Riehm, Thomas: Vertragsrecht als Infrastruktur von Innovation. In: Grundmann, Stefan/Möslein, Florian (Hg.): *Innovation und Vertragsrecht* (im Erscheinen).

Sammelbände

Hornung, Gerrit (Hg.): *Rechtsfragen der Industrie 4.0. Datenhoheit – Verantwortlichkeit – rechtliche Grenzen der Vernetzung.* Baden-Baden: Nomos Verlagsgesellschaft 2018.

Monografien

Deremetz, Anne: *Die BDSM-Szene. Eine ethnografische Feldstudie.* Gießen: Psychosozialverlag 2018.

VERANSTALTUNGSHINWEISE

Januar – Februar 2019 | »Alles außer Kontrolle?«

Die aktuell laufende Passauer Ringvorlesung beschäftigt sich mit Herausforderungen der Digitalisierung für die Gesellschaft. Die Vorträge »Software als Institution? Eine ethisch-normative Perspektive auf Big Data« (08.01.2019), »Roboterpsychologie« (15.01.2019) oder »Die Gefährdung psychischer Gesundheit in Unternehmen der Industrie 4.0« (05.02.2019) finden dienstags ab 16.00 im HS8 WIWI statt und sind öffentlich.

Passau, DE | Eintritt frei

04.
Februar 2019

PRIVATHEIT & INFORMATIONELLE SELBSTBESTIMMUNG VON KINDERN IM DIGITALEN KONTEXT

Öffentlicher Gastvortrag
Dr. phil. Christoph Schickhardt

PHIL, HS4 | 18.00 Uhr c.t.

13.–15. Februar 2019 | »Wovon sprechen wir, wenn wir von Digitalisierung sprechen?«

Die vierte Veranstaltung der Bayreuther Symposienreihe widmet sich in begriffskritischer Arbeit der Erörterung und Revision wichtiger Grundbegriffe des Digitalen sowie zentraler Termini innerhalb der Digitalen Geisteswissenschaften. Die kritische Erörterung und Revision sowie der Entwurf und Ausarbeitung neuer Begriffe, die als angemessene Erkenntnismittel für das Verständnis digitaler Kulturen dienen können stehen im Zentrum.

Bayreuth, DE | Eintritt frei

11.
Februar 2019

ETHIK KÜNSTLICHER INTELLIGENZ

Öffentlicher Gastvortrag
Prof. Dr. Wolfgang Schröder

PHIL, HS4 | 16.00 Uhr c.t.

März – Juni 2019 | Veranstaltungsreihe Digitale Welten der Evangelischen Akademie Tutzing

Welche Auswirkungen hat das Internet auf unsere Gesellschaft? Wie verändert es unser Verständnis von Freiheit und Demokratie, Bildung und Kultur, Mensch und Welt? Und überhaupt – in was für einer Welt wollen wir in Zukunft leben? Und wie können wir diese aktiv mitgestalten? Um diese Fragen drehen sich die Tagungen im Bereich Digitale Welten. Weitere Informationen über die einzelnen Veranstaltungen unter https://www.ev-akademie-tutzing.de/themen/digitale-welten/.

Tutzing, DE | ab 100€

15.–17. Mai 2019 | »TILTing Perspectives 2019: Regulating a World in Transition«

Die TILTing Perspectives 2019 versammelt zum sechsten Mal ExpertInnen an der Schnittstelle von Recht, Technologie und Gesellschaft, um Erkenntnisse und Ideen auszutauschen und Antworten auf aktuelle Herausforderungen im Zusammenhang mit technologischen Innovationen zu formulieren und zu diskutieren. Die Konferenz umfasst Plenarsitzungen und Podiumsdiskussionen mit eingeladenen Referenten sowie Präsentationen von Teilnehmern eines Call for Papers.

Tilburg, NL | ab 50€

9.–11.
Mai 2019

VERANTWORTUNG IN DIGITALEN KULTUREN

Privatheit im Geflecht von Medien, Recht und Gesellschaft

Tagung des Kollegs

16.–17. Mai 2019 | »Privacy Online: What Have We Learned So Far?«

How can we understand human behavior online? Do we need new legal frameworks to better support people?
Is it possible to develop devices that offer both compelling features and effective privacy protection? For this conference scholars from all disciplines are invited to present an overview over the most relevant insights of both their own research and their respective fields.

Hohenheim, DE | ab 60€

DAS KOLLEG AUF REISEN

»Rethinking Privacy« in Frankfurt

von Lea Watzinger

Am 31. Mai 2018 war das Kolleg zu einer Kooperationsveranstaltung mit dem DFG-Forschungsprojekt »American Literature and the Transformation of Privacy« an der Goethe-Universität Frankfurt zu Gast, auch zwei Kollegiaten hielten Vorträge. Initiatoren der Kooperation waren die beiden Amerikanisten Prof. Dr. Karsten Fitz aus Passau und Prof. Dr. Johannes Völz aus Frankfurt. In sechs Vorträgen wurde versucht, Privatheit gemeinsam neu zu denken.

Sarah Igo von der Vanderbilt University (USA) machte mit einer Kulturgeschichte des Privaten in den USA den Anfang und zeichnete die Geschichte der amerikanischen Sozialversicherung nach. Die *social security number* wurde dabei zu dem zentralen Identifikationsdokument gegenüber staatlichen Stellen, was KritikerInnen vom ›Tod der Privatheit‹ und einer erzwungenen ›nackten Gesellschaft‹ sprechen ließ. Das Phänomen der Selbstentblößung hingegen und den unbesorgten Umgang mit persönlichen Informationen in der modernen digitalisierten Gesellschaft nahm Sandra Seubert (Universität Frankfurt a.M.) in den Blick. Sie reflektierte in der Tradition der Kritischen Theorie den Normenwandel und die Ökonomisierungstendenzen bezüglich des Privaten bis heute. Die sozialen Netzwerke und deren Privatsphäreeinstellungen seien überhaupt die großen praktischen wie wissenschaftlichen Herausforderungen für ein Neudenken von Privatheit. Martin Stempfhuber (Universität Würzburg) beschäftigte sich aus soziologischer Perspektive mit der Ablösung staatlicher Überwachung durch Selbstüberwachung und -entblößung in sozialen Netzwerken. Er konstatierte, dass konventionelle theoretische Einordnungen auf diese neue Art von Öffentlichkeiten und Privatheiten nicht mehr anwendbar seien. David Rosen (Trinity College, Hartford CT) und Aaron Santesso (Georgia Institute of Technology) fokussierten v.a. Überwachung als literarisches Narrativ und warfen dabei den Blick auf intergenerationelle Unterschiede und Gemeinsamkeiten. Sie machen eine generationelle Kluft am 11. September 2001 fest: AutorInnen, die nach dem 11. September schreiben, setzen demnach Privatsphäre kaum mehr voraus – der Status des Privaten als kultureller Normalfall habe sich grundlegend verändert. Lukas Edeler vom Passauer Graduiertenkolleg erforschte die Möglichkeiten zu Privatsphäre und Individualität in Auseinandersetzung mit dem Parteiwillen in der DDR. Die ideale sozialistische Persönlichkeit sollte sich nicht als privates Individuum verstehen, sondern als Teil der Gemeinschaft. Privatheit stellte daher in den Augen der Staatssicherheit eine Gefahr dar, was er am Beispiel des vorsichtigen Protests einer SchülerInnengruppe in der DDR verdeutlichte. Den Abschluss machte der Kollegiat Christian Aldenhoff: Er verstand Privatheit als normatives Konzept und daher als moralisches Recht, womit er sich vom geläufigen juristisches Diskurs absetzte. Mit Bezug auf Immanuel Kant leitete er das Konzept ›moralischer Rechte‹ her und wertete Privatheit als solches, welches die Grundlage für Autonomie sei. Das aktive Publikum diskutierte engagiert mit und auch beim abschließenden Biergartenbesuch riss der Gesprächsfaden nicht ab. Das Symposium stärkte den interdisziplinären Austausch und half, Brücken zwischen den Fachkulturen und Denkweisen zu schlagen. Der Umgang mit Privatheit und die Einschätzung, was privat ist, sind kulturell und historisch wandelbar. Gegenwärtig befinden wir uns – wieder einmal – in einer Phase des Aushandelns neuer Normen des Privaten. Durch die Digitalisierung, soziale Netzwerke und Terrorgefahr verändern sich Einstellungen zum und Formen des Privaten massiv. Narrative von Überwachung und Privatheit sind dabei stets eng miteinander verknüpft, sowohl in Literatur und Kultur wie auch in Politik und Gesellschaft.

Lea Watzinger

Wissenschaftliche Mitarbeiterin am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

DAS KOLLEG AUF REISEN

An der Hochschule der Medien in Stuttgart

von Lea Raabe

Vom 04. bis 06. Juni 2018 besuchte eine Delegation des DFG-Graduiertenkollegs 1681/2 »Privatheit und Digitalisierung« bestehend aus acht KollegiatInnen sowie dem Postdoc Dr. Martin Hennig und dem wissenschaftlichen Koordinator Kilian Hauptmann die Hochschule der Medien (HdM) in Stuttgart.

Hier sollte der Austausch mit dem dort ansässigen Institut für Digitale Ethik (IDE) unter der Leitung von Prof. Dr. Petra Grimm, Prof. Dr. Tobias Keber und Prof. Dr. Oliver Zöllner intensiviert werden. Im Rahmen des Aufenthalts übernahmen die KollegiatInnen vielfältige Aufgaben und hatten so die Möglichkeit, Erfahrungen in der Wissenschaftspraxis zu sammeln sowie den Dialog zwischen den beiden Forschungseinrichtungen mitzugestalten. Zentrale Arbeitsfelder des IDE sind unter anderem »Big Data und Privatsphäre«, »Manipulation und Informationsselektion« und »Gefährdungspotenziale durch Medieninhalte«[1] – alles Themen, zu denen Nachwuchswissenschaftler Innen des GRK forschen und somit einen wertvollen Beitrag zur Zusammenarbeit leisten können. Zum einen präsentierten die KollegiatInnen ihre jeweiligen Dissertationsprojekte vor einem Plenum aus ProfessorInnen sowie wissenschaftlichen MitarbeiterInnen der HdM und stellten sich dem fächerübergreifenden Dialog. Zum anderen hielten sie in Teams Lehrveranstaltungen ab. Kilian Hauptmann und Alix Michell übernahmen eine Sitzung im Bereich Empirische Medienforschung zu »Mediensemiotik & Ideologiekritik am Beispiel der Werbung von Dating-Apps«, um den StudentInnen der HdM anhand praktischer und aktueller Werbebeispiele zu Dating-Apps wie *Tinder* oder *LoveScout24* die empirisch-qualitative Methode der Mediensemiotik näherzubringen und zu untersuchen, welche normativen Vorstellungen von Gesellschaft den Werbungen zugrunde liegen. Christian Aldenhoff und Felix Sobala führten eine Veranstaltung im Medienrecht zum Thema »Cambridge Analytica – Der ›Skandal‹ und seine (rechtlichen) Perspektiven« durch und prüften dabei einerseits die datenschutzrechtlichen und medienrechtlichen Implikationen des Falls Cambridge Analytica und ordneten diesen gleichzeitig in allgemeine Privatheitskontexte ein. Anne Derametz, Lea Raabe und Marcel Schlegel hielten im Kurs Mediensoziologie eine Sitzung zu »Konstruktionen diskursiver und medialer Wirklichkeit(en)« und zeigten anhand der medialen Aufarbeitung der Geschehnisse in der Silvesternacht 2015/16 in Köln, wie unterschiedlich diese interpretiert wurden und welche Rolle dabei die mediale Konstruktion von Realität sowie mediale Verzerrungseffekte durch Intermediäre spielten.

Ergänzt wurde der fruchtbare Austausch von einem vielfältigen Rahmenprogramm, welches unter anderem eine Führung durch die HdM sowie einen Vortrag von Prof. Dr. Petra Grimm zu »Unser Leben im digitalen Zeitalter - Selbstbestimmt oder fremdbestimmt?« beinhaltete. Der gelungene Austausch zwischen den beiden Einrichtungen wird fortgeführt und soll im Mai 2019 um einen weiteren Forschungsaufenthalt an der HdM ergänzt werden.

1 Vgl. Grimm, Petra: Digitale Ethik – wozu brauchen wir sie? In: *Hochschule der Medien, Institut für Digitale Ethik* 2013. Online: https://www.digitale-ethik.de/institut/digitale-ethik/ (29.10.2018).

Lea Raabe

Wissenschaftliche Mitarbeiterin am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

DAS KOLLEG AUF REISEN

Privacy, Promis, Palantir

Die *Amsterdam Privacy Conference 2018*

Empfang auf der Amsterdam Privacy Conference 2018.
Foto: Marcel Schlegel

von Marcel Schlegel

Was im Fußball die Champions League, ist in der europäischen Privatheitsforschung die *Amsterdam Privacy Conference* (APC), die 2018 zum dritten Mal stattfand. Vom DFG-Graduiertenkolleg 1681/2 »Privatheit und Digitalisierung« trugen dort der stellvertrende Sprecher Prof. Dr. Kai von Lewinski sowie die Promovierenden Alix Michell, Christian Aldenhoff, Jakob Kelsch und Felix Sobala vor.

Eigentlich ist es nur eine Randnotiz, eine Alltagssituation, scheinbar nichts Besonderes: Zwei Frauen sitzen in der modernen Lobby der Amsterdamer Universität (UvA) auf dem ›Roeterseilandcampus‹. Sie schlürfen ihren Kaffee, unterhalten sich angeregt. Worüber? – Privatsache, natürlich. Doch wichtig ist dies ohnehin nicht. Denn der erneute Blick verrät: Die beiden, das sind Helen Nissenbaum[1] und Beate Rössler[2], zwei der ganz Großen der internationalen Privatheitsforschung.

1 Vgl. Rössler, Beate: *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp 2001.

2 Vgl. Nissenbaum, Helen: *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford University Press 2009.

DAS KOLLEG AUF REISEN

Kurz darauf stößt ein junger Mann dazu, erweitert die Gesprächsrunde, verändert wohl Thema und Kontext: Willkommen auf der *Amsterdam Privacy Conference 2018*.

Wenn man so will, steht diese scheinbar unbedeutende Szene synonym für den nahbaren und konstruktiven Charakter dieser viel beachteten Konferenz. In Amsterdam traf sich nicht nur die Elite der internationalen Privatheitsforschung, vielmehr tauschten sich dort WissenschaftlerInnen aus aller Welt und diversen Disziplinen aus. Die Doktorandin kam mit dem Privacy-Promi ins Gespräch, der Anthropologe mit dem Informatiker oder der Juristin, die Philosophin mit dem Unternehmer oder der Politikerin, der Facebook-Vertreter mit dem Medienethiker, oder eben Frau Nissenbaum mit Frau Rössler – und einem Nachwuchswissenschaftler.

Passauer Standpunkte in Amsterdam

Mittendrin aus Passau: Prof. Dr. Kai von Lewinski sowie die Promovierenden Alix Michell, Christian Aldenhoff, Jakob Kelsch und Felix Sobala vom DFG-Graduiertenkolleg »Privatheit und Digitalisierung«. Kai von Lewinski, Professor für Öffentliches Recht, Medien- und Informationsrecht und stellvertretender Sprecher des Graduiertenkollegs, gab einen Überblick darüber, welche rechtlichen Regulierungen von Algorithmen im Bereich der Human Resources schon existieren und vermittelte respektive gewichtete diese anschaulich anhand einer Matrix.

Die Kollegiatin Alix Michell und die Kollegiaten Christian Aldenhoff, Jakob Kelsch und Felix Sobala referierten in einem eigenständigen Panel ihre Dissertationsthemen – jeweils zugespitzt auf die Frage, ob die Digitalisierung als *game-changer* betrachtet werden könne. Als Moderator hatten sie den Juristen Prof. Dr. Tobias Keber gewinnen können, Professor für Medienrecht und Medienpolitik in der digitalen Gesellschaft an der Stuttgarter Hochschule der Medien. Im Anschluss an die vier Vorträge kam es zu intensiven Diskussionen – typisch für die APC.

In Keynotes, Panels und vor allem den Pausengesprächen wurde in Amsterdam interdisziplinärer Austausch gelebt. Das lässt sich auch an Zahlen festmachen: Über 50 Panels, meist fünf zeitgleich, mit gut 200 Vortragenden standen im Zeitplan der vier Konferenztage, dazu die hörenswerten Keynotes international beachteter MeinungsführerInnen wie Danielle Citron, Julie Cohen, Helen Nissenbaum, Michael Birnhack, Chris Hoofnagle und anderen – Champions League eben. Der Nachteil: Die schiere Masse an Vorträgen überforderte einen. Zuweilen wünschte man sich eine thematische Zuspitzung anstelle eines Überangebots. Denn auch auf wissenschaftlichen Konferenzen ist weniger oft mehr.

Khiara Bridges über Privatsphäre in den USA.
Foto: Marcel Schlegel

Besonders hervorzuheben ist der Vortrag der US-Amerikanerin Khiara Bridges[3]. Die Professorin für Jura und Anthropologie an der Boston University machte in ihrer kurzen und brillanten Rede auf Privatsphäre-Verletzungen aufmerksam, die US-Institutionen insbesondere an Müttern aus armen Bevölkerungsschichten verüben würden. Mehr noch: Sie konstatierte einen Zusammenhang zwischen statusbedingter Armut und einem graduellen Verlust individueller Privatsphäre sowie eine subtile Stigmatisierung armer US-amerikanischer Bevölkerungsteile durch staatliche Einrichtungen und deren Förderprogramme.

Ebenfalls inhaltlich wie rhetorisch großartig präsentierte sich Judith Sargentini dem großen Publikum im Audimax der UvA. Die niederländische EU-Parlamentarierin (GroenLinks) beschäftigte sich mit der Überwachung und Kontrolle von Flüchtlingen durch die Politik und zeigte auf, inwiefern derlei Maßnahmen die Privatsphäre der MigrantInnen zu einem – folgt man ihrer Argumentation – bedenklichen Ausmaß beschneiden können.

3 Vgl. Bridges, Khiara: *The Poverty of Privacy Rights.* Stanford: Stanford University Press 2017.

DAS KOLLEG AUF REISEN

Facebook & Google: Freund oder Feind?

Sargentinis und Bridges' Vorträge im Speziellen sowie die Keynotes im Allgemeinen stachen auf der APC 2018 heraus, weil sie das Thema Privatheit vornehmlich in einen analogen Blickwinkel rückten. Ansonsten dominierte auf der APC inhaltlich nämlich vor allem eines: das Digitale. ›Cloud-Computing‹, ›Big Data‹, ›Social Credit‹, Algorithmen und ›Bots‹, politische Zielgruppenansprache, Cambridge Analytica, der ökonomische Wert personenbezogener Daten, Datenschutzbestimmungen und weitere Themen aus der digitalen Sphäre – kaum ein Panel, das ohne Facebook, Google und Co. auskam; kaum ein Format, das diese großen Internetkonzerne nicht als Ausgangspunkt des eigenen Themas brauchte oder die amerikanischen Quasi-Monopolisten – mal subtil, mal explizit – als Gegenspieler darstellte.

Zuweilen vermittelten die Themen den Anschein, als sei Privatheit in der modernen Informations- und Kommunikationsumgebung kaum noch ohne die digitale Sphäre zu denken. Ist dem denn so? Ja, mitunter bekam man beim Blick auf das Veranstaltungsprogramm den Eindruck, als bedeute Privatsphäre im aktuellen interdisziplinären akademischen Diskurs vornehmlich, seine persönlichen Informationen im Netz gegen die datensammelnden Riesen aus dem Silicon Valley zu verteidigen. Die doppelte Ironie dabei: Manche der besagten Tech-Riesen sorgten auch abseits der Vorträge für Gesprächsstoff – als Geldgeber und Panelisten. Denn Google, Ziggo, Microsoft, Liberty Global und Palantir machten für die APC den Geldbeutel auf. Fast logisch, dass das finanzielle Engagement dieser Premium-Sponsoren nicht jedem schmeckte, zumal etwa Google, Microsoft und Palantir sogenannte *sponsored panels*, sprich eigene zweistündige Sitzungen, erhielten.

Überwachung oder Sponsoring?

Wie das Internet-Portal iTWire berichtete, zogen deshalb mindestens sechs WissenschaftlerInnen ihre Teilnahme an der APC zurück.[4] Ihr Boykott richtet sich in erster Linie gegen das ›Data-Mining‹-Unternehmen Palantir, das zuletzt zunehmend ins öffentliche Kreuz-

4 Vgl. Varghese, Sam: Six researchers boycott Dutch vonf due to Palantir's sponsorship. In: *iTWire* vom 20.09.2018. Online: https://www.itwire.com/security/84572-six-researchers-boycott-dutch-conf-due-to-palantir-s-sponsorship.html (29.10.2018).

v.l.n.r.: Marleen Stikker, Chris Hoofnagle, Khiara Bridges, Manuel Kohnstamm, Tracy Metz.
Foto: Marcel Schlegel

DAS KOLLEG AUF REISEN

feuer geriet. Zur Begründung führten sie an, dass Palantir bei der Entwicklung von Technologien zur Überwachung der eigenen Bevölkerung durch die US-Regierung eine essentielle Rolle spiele: Palantir habe der Trump-Regierung unter anderem beim Aufspüren illegaler EinwanderInnen geholfen und sei auf diese Weise zumindest indirekt an Menschenrechtsverletzungen beteiligt. Auch mit dem Cambridge-Analytica-Skandal um kommerzielle Facebook-Datenprofile stehe das Unternehmen in Verbindung. Weitere Bedenken der Ferngebliebenen: dem Event fehle es hinsichtlich der Finanzierung an Transparenz.

Kritik, die man teilen konnte, aber nicht musste. Immerhin waren die Veranstaltungen der besagten Geldgeber aus der Tech-Branche klar als gesponsert deklariert. Es handelt sich hierbei um eine Kritik, mit der sich die OrganisatorInnen um Chefkoordinator Bart van der Sloot und Geert ten Dam, Vorsitzende des Exekutivrates der UvA, nicht zum ersten Mal konfrontiert sahen. Schon auf der letzten *Amsterdam Privacy Conference 2015* war es zu ähnlichen Diskussionen gekommen, die damals primär mit dem Sponsor Facebook zusammenhingen. Und auch vor drei Jahren hatte Palantir die Tagung schon finanziell unterstützt, die VeranstalterInnen hielten indes an dem US-Konzern fest. Auch deshalb kam es – schon im Vorfeld der APC 2018 – erneut zu kontroversen Debatten. Diese spielten sich paradoxerweise ausgerechnet in den sozialen Netzwerken ab, bevorzugt in jenem für MeinungsführerInnen, versteht sich: auf Twitter.

Face-to-Face mit Palantir

Im Kurznachrichtendienst war schon seit Monaten eine teils heftige Diskussion darüber entbrannt, ob es verwerflich sei, für eine Konferenz zum Thema ›Privatsphäre‹ von eben jenen Unternehmen Geld zu nehmen, die wohl zu den prominentesten Datenschutzverletzern zählen. Zwei Lager formierten sich. Das eine rief unter dem Namen »Funding Matters«[5] speziell für die APC einen eigenen Kanal inklusive Blog und entsprechender Petition ins Leben, die von über 200 direkt oder indirekt an der APC beteiligten WissenschaftlerInnen unterschrieben wurde. Darunter auch die Keynote-Speaker Marleen Stikker, Frank Pasquale und Philip Pettit, welche unter anderem den Rauswurf Palantirs forderten. Die Gegenseite konterte mit eigenen Tweets und Posts, die zwar meistens die finanzielle Unterstützung durch Palantir nicht pauschal guthießen, aber die Kritik trotzdem zu einseitig adressiert fanden und stattdessen zum Austausch mit den Geldgebern aufriefen. Ihr Argument: Nur das Gespräch schaffe Transparenz.

Zu dieser Aussprache kam es letztendlich auch, in einer wohl im Vorfeld nicht geplanten und eigens für das Streitthema ›Sponsoring‹ einberufenen Gesprächsrunde. Zu dieser analogen Aussprache schickten auch Google und Co. ihre VertreterInnen, ganz nach dem Motto: ›Face-to-Face‹ statt ›Interface-to-Interface‹. Mit welchem Ergebnis? Das wird die nächste APC 2021 in drei Jahren zeigen. Und wer weiß, vielleicht war es genau das, worüber Beate Rössler und Helen Nissenbaum in der Lobby unter vier Augen sprachen? Wir werden es nicht erfahren. Denn das ist Privatsache, natürlich.

5 Vgl. Twitter: *Funding Matters.* Online: https://twitter.com/fundingmatters (28.10.2018).

Marcel Schlegel

Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

DAS KOLLEG AUF REISEN

Ist die Digitalisierung ein *game-changer?*

Die Passauer Beiträge auf der APC 2018 im Detail

v.l.n.r.: Prof. Dr. Tobias Keber, Felix Sobala, Christian Aldenhoff, Jakob Kelsch, Alix Michell.
Foto: Prof. Dr. Kai von Lewinski

von Marcel Schlegel

Auf der APC 2018 referierten außerdem vier Promovierende des Passauer Graduiertenkollegs. In ihrem Panel sprachen sie über Privatheit aus fächerübergreifenden Perspektiven mit dem besonderen Fokus auf die Veränderungsgewalt der Digitalisierung.

Alix Michell fragte sich in ihrem Vortrag, wie der Diskurs um Privatheit und Digitalisierung in der gegenwärtigen Medienkunst verhandelt wird. Welche Aussagen werden dort über aktuelle Privatheitskonzepte getroffen? Welche ästhetische Funktionalisierung von Privatheit lässt sich im Medienkunst-Diskurs nachweisen? Exemplarisch stellte die Passauer Kollegiatin ihre Untersuchungsergebnisse zu den Arbeiten *Slide to Expose* (2017)[1] des Künstlerkollektvivs um Nicole Ruggiero, Molly Soda und Refrakt sowie *Excellences & Perfections* (2014) von Amalia Ulman vor. An diesen ließe sich die virtuelle Welt als erweiterter Raum physischer Privatheit erkennen. Es bleibe hier allerdings bei traditionellen Semantiken von Privatheit, eine Veränderung

1 Vgl. Ruggerio, Nicole: *Slide to Expose* 2018. Online: https://www.nicoleruggiero.com/project/slide-to-expose/ (27.11.2018).

DAS KOLLEG AUF REISEN

von Privatheitskonzepten finde eher auf struktureller Ebene statt. Überdies fungieren private Codes im virtuellen Raum laut Michell als semiotische Marker gegenwartsästhetischer Kategorien wie ›Realness‹ oder ›Authenticity‹ und tragen so maßgeblich zur Bedeutungskonstitution bei.

Christian Aldenhoff stellte die Frage, ob auf der Grundlage des politischen Liberalismus ein moralisches Recht auf Privatheit entwickelt werden kann. Ein solches Recht könnte die normative Grundlage für ein staatliches Grundrecht auf Privatheit darstellen, argumentierte der Kollegiat. Unter Rückgriff auf die Arbeiten insbesondere von Beate Rössler und Ernst Tugendhat kam er zum Ergebnis, dass Privatheit – in ihrem funktionalen Zusammenhang zur Autonomie – ein grundlegendes Bedürfnis bedeute, das von einem unparteiischen Standpunkt anerkannt werden müsse. Seine These: Sofern man Autonomie als normatives Ideal akzeptiert, müssten Personen sich gegenseitig ein moralisches Recht auf Privatheit zugestehen.

Jakob Kelsch untersuchte die Bedeutung der Familie als elementaren Raum des Privaten im Kontext der zeitgenössischen Online-Serie und im Vergleich zu konventionellen TV-Produktionen. Schon allein, was die Rezeptions- und Produktionssituation, aber auch ihren Status als zentraler Impulsgeber der aktuellen Serienlandschaft betrifft, könne die Online-Serie als richtungsweisend angesehen werden. Er kam weiterhin zum Schluss, dass die Digitalisierung zunehmend experimentelle Formate ermöglicht, die kritisch die problematischen Aspekte des familiären Zusammenlebens hinterfragen und Alternativmodelle zur traditionellen Kernfamilie kreieren. Obgleich der Stellenwert des Privaten respektive der Familienthematik nach Kelsch als Trägerdiskurs also unberührt bleibt, ist die Digitalisierung somit ein *game-changer* auf dem Gebiet der Serie.

Felix Sobala setzte sich in seinem Vortrag mit dem datenschutzrechtlichen Prinzip der Datensparsamkeit auseinander. Er veranschaulichte mittels des historischen Beispiels des Amsterdamer Religionsregisters die ›Janusköpfigkeit‹ von Informationen in unterschiedlichen Kontexten. Daran anschließend stellte er neu hinzutretende Datenverarbeitungs- und -verwendungsmöglichkeiten durch die Digitalisierung anhand des Cambridge-Analytica-›Skandals‹ dar. Auf Grundlage dessen kam er zu der Ansicht, dass die Digitalisierung für den Datenschutz – und somit für den Schutz von Privatheit – ein *game-changer* sei, der wirksame regulatorische Antworten zur Folge haben müsse. Er betonte die über die rechtlich temporär präformierte Legitimität von Datenverarbeitungen hinausgehende Notwendigkeit faktischen Datenschutzes. Dieser müsse möglicherweise auch sich (grundlegend) wandelnde Kontexte als Risiken im Blick haben. Unter anderem arbeitete Sobala die Schwachstellen der derzeitigen Implementierung des Prinzips der Datensparsamkeit in der DS-GVO heraus und präsentierte im Anschluss daran die Idee einer technikrechtlichen Regulierung als marktbezogene Neuauflage.

Prof. Dr. Kai von Lewinski war derweil Teil eines Panels zum Thema »Detecting ways forward in regulation«. Sein Vortrag widmete sich unter anderem den Leitfragen: Welche rechtlichen Regulierungen von Algorithmen existieren im Bereich der ›Human Resources‹ (HR) bereits, wo gibt es noch Grauzonen, wo besteht noch Nachholbedarf? Von Lewinski, Lehrstuhlinhaber für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau, veranschaulichte die zunächst komplexe rechtliche Sachlage süffisant mithilfe eines Dreischritts, den er mit Film- und Bandnamen umschrieb: Bisher herrsche hinsichtlich der besagten Regulierung im juristischen Diskurs eine auf den ersten Blick recht unübersichtlichen Rechtslage, gewissermaßen ein ›Rage against the Machine‹. Diese Analogie fortführend, stellte von Lewinski dann – in Anlehnung an den gleichnamigen Film – eine ›Matrix‹ vor, mithilfe derer sich die rechtlichen Regulierungen von Algorithmen in den HR nachvollziehbar und vor allem übersichtlich darstellen und gewichten lassen. Das Resultat: ›The Circle‹, also ein rundes Ergebnis.

Narrative der Überwachung

Ein Bericht über die Ringvorlesung aus dem Sommersemester 2018 an der Universität Passau

von Patrick Herget

Getreu der im Ankündigungstext angesprochenen Bandbreite von Überwachungsnarrativen, »von Benthams *Panopticon*, über Orwells *1984* und Eggers *The Circle* bis hin zur *Weltraumtheorie* des BND«, kamen GastwissenschaftlerInnen aus den Bereichen Kultur-, Medien- und Sozialwissenschaften nach Passau, um die Grundzüge dieser Narrative aus ihren jeweiligen Fachperspektiven zu beleuchten. Denn, wie es weiter im Programm zur Ringvorlesung hieß: »Nicht erst seit den Enthüllungen Edward Snowdens gibt es eine Vielzahl von Motiven und Erzählungen der Überwachung, die kulturelle Verhandlungen und Vorstellungen von Sicherheit und Freiheit prägen«.

In die Vorlesungsreihe führte Prof. Dr. Hans Krah (Lehrstuhl für Neuere Deutsche Literaturwissenschaft) zusammen mit Dr. Martin Hennig ein. Beide erörterten »Typologie, Kategorien, Entwicklung von Überwachungsnarrativen« und legten so das Fundament für die folgenden Veranstaltungen. Auf die Auftaktvorlesung folgte ein abwechslungsreiches Programm, in dem Überwachungsnarrative aus verschiedenen Perspektiven und in unterschiedlichen Kontexten herausgestellt wurden: Von »Überwachungsnarrativen in filmischen Dystopien«, über »Überwachung in der Werbung«, bis hin zur »Kontrolle als Motiv und Prinzip des Computerspiels« wurde ein vielfältiges fachliches und thematisches Spektrum abgedeckt. Einen weiteren Höhepunkt bildete der praxisnahe Vortrag von Christian Flisek, Politiker und ehemaliger Obmann der SPD im NSA-Untersuchungsausschuss des Deutschen Bundestages. Flisek stellte in seinen Ausführungen zu »Der Fall Edward Snowden – politische Überwachungsnarrative auf dem Prüfstand« heraus, dass Narrative in der Politik insbesondere durch ›Framing‹, also der sprachlichen Rahmung von politischen Problemen, eine zentrale Rolle spielen, da komplexe Sachverhalte so vereinfacht dargestellt werden. Frames können allerdings dazu führen, dass die politische Deutungshoheit in Debatten dadurch gewonnen wird, dass Gefühle der BürgerInnen adressiert und sachliche Argumente sowie Fakten vernachlässigt werden. In Bezug auf seine Tätigkeit im NSA-Untersuchungsausschuss gab Flisek spannende Einblicke in die Ausschussarbeit und be-

leuchtete den Fall Snowden anhand von zwei Narrativen, die gegensätzlicher nicht sein könnten: »Snowden der Held« vs. »Snowden der Verräter«.

Auch Miriam Piegsa und Lukas Edeler vom Graduiertenkolleg trugen mit Vorträgen aus ihrer jeweiligen Fachperspektive zur Ringvorlesung bei. Miriam Piegsa referierte über »Untergangsstimmung im ›Bildungsfernsehen‹ – Überwachung in der deutschen Dokumentation«. Die Kollegiatin stellte Gemeinsamkeiten der Überwachungsnarrative bezogen auf die Digitalisierung in Dokumentarfilmen, Dokumentationen und TV-Wissenssendungen heraus. Neben Narrativen zum Menschen als Datensubjekt und dem digitalen Raum als ›datafizierte‹ Welt, waren auch Narrative zur ›Countersurveillance‹, also solche rund um den Überwachungswiderstand bzw. zur Gegenüberwachung, Thema der Vorlesung. Unter anderem wurde in diesem Zusammenhang das Narrativ des »Whistleblowers als Heldenfigur« erneut aufgegriffen.

Lukas Edeler zeigte »Dimensionen von Privatheit und Persönlichkeit im sozialistischen Leipziger Raum der 1980er Jahre« auf. Der Kollegiat stellte ›Überwachung‹ als zentrales Narrativ für die Deutung des Geschichtsbildes der DDR heraus und machte deutlich, dass Dimensionen von Privatheit und Persönlichkeit hierzu interessante Perspektivenerweiterungen darstellen können. Er legte dar, dass Geschichtsbilder Vehikel kollektiver Realität bzw. Weltanschauung sind und Geschichte als Narration wahrgenommen wird. Der Kollegiat führte weiterhin aus, dass eine Bearbeitung der Frage nach Privatheit in der DDR zu einem differenzierten Verständnis von staatssozialistischen Diktaturen und für die darin lebenden Menschen führen kann. Texte und Quellen der Überwachenden wie der Überwachten können in diesem Zusammenhang als wertvolle Zugänge zu Interaktionen zwischen Regime und Gesellschaft dienen. Insgesamt wurde veranschaulicht, dass Geschichtsbilder durch unterschiedliche und teils kontroverse Narrative geformt werden.

Zusammenfassend hielt Dr. Martin Hennig fest, dass Narrative in vielen verschiedenen gesellschaftlichen Bereichen wirksam sind. Auch in Bereichen, in denen man dies zunächst nicht erwartet, wie bspw. in der Kriminalitätsbekämpfung, der Politik, der Geschichtsschreibung oder der Technologieentwicklung, spielen Überwachungsnarrative eine bedeutende Rolle. Narrative sind somit nahezu allgegenwärtig und zentral dafür, wie wir uns als Kultur über uns selbst verständigen und deshalb auch essentiell für die Gewährleistung gesellschaftlicher Kommunikation. Dennoch verstellen sie auch den Blick auf tatsächliche Gegebenheiten, sodass die stetige Wiederholung von Narrativen in einzelnen gesellschaftlichen Bereichen die Gefahr birgt, dass Ideologien hinter Narrativen verschleiert werden, bspw. wenn Aussagen zur ›Allmacht‹ von Big Data mit scheinbar erstrebenswerten Werten – im Sinne der Wahrheit und Objektivität von Datenerhebungen – verknüpft werden und dabei wirtschaftliche und politische Interessen maskieren. Insbesondere im Bereich der Digitalisierung, der die Gesellschaft als Ganzes betrifft und ein hohes Maß an Komplexität mit sich bringt, ist die fast ausschließliche Verständigung über Narrative, wie sie in der gesellschaftlichen Debatte praktiziert wird, den vielschichtigen Problematiken nicht angemessen.[1]

1 Vgl. Fazit zur Ringvorlesung »Narrative der Überwachung«. In: *ZIM Mediathek der Universität Passau.* Online: https://univideo.uni-passau.de/2018/07/fazit-zur-ringvorlesung-narrative-der-ueberwachung/ (20.11.2018).

Patrick Herget

Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

DIE NÄCHSTE AUSGABE ERSCHEINT IM SOMMER 2019

DFG Graduiertenkolleg Privatheit und Digitalisierung
UNIVERSITÄT PASSAU
DFG Deutsche Forschungsgemeinschaft
Projektnummer 164644301

Die Finanzierung dieses Magazins erfolgt aus Mitteln der Deutschen Forschungsgemeinschaft.

Das Magazin hat Ihnen gefallen?

Sie möchten das Magazin online abrufen oder sich zum regelmäßigen Empfang in den Verteiler eintragen? Besuchen Sie uns auf unserer Website: www.privatheit.uni-passau.de/magazin-des-graduiertenkollegs/

Für Hinweise, Anregungen, Lob und Kritik sind wir Ihnen sehr dankbar. Schreiben Sie einfach an privatheit@uni-passau.de

IMPRESSUM

Anschrift
Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Vertretung
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.

Organisation
Gemäß Art. 4 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Redaktion
Patrick Herget, Lea Watzinger

Layout & Satz
Jonas Gerbsch, Miriam Becker, Franziska Schönhöfer

Chefredaktion
Dr. Martin Hennig, Kilian Hauptmann