

Petra Grimm / Tobias O. Keber / Oliver Zöllner (Hg.)



Medienethik

Franz Steiner Verlag

Schriftenreihe Medienethik – Band 15

Anonymität und Transparenz in der digitalen Gesellschaft

Petra Grimm / Tobias O. Keber / Oliver Zöllner (Hg.)
Anonymität und Transparenz in der digitalen Gesellschaft



Herausgegeben von

Rafael Capurro und Petra Grimm

Band 15

Petra Grimm / Tobias O. Keber / Oliver Zöllner (Hg.)

Anonymität und Transparenz in der digitalen Gesellschaft



Franz Steiner Verlag

Umschlagabbildung: Oliver Zöllner

Redaktion: Clarissa Henning

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist unzulässig und strafbar.

© Franz Steiner Verlag, Stuttgart 2015

Druck: Laupp & Göbel, Nehren

Gedruckt auf säurefreiem, alterungsbeständigem Papier.

Printed in Germany.

ISBN 978-3-515-11226-0 (Print)

ISBN 978-3-515-11227-7 (E-Book)

INHALTSVERZEICHNIS

<i>Petra Grimm, Tobias O. Keber, Oliver Zöllner</i> Anonymität und Transparenz in der digitalen Gesellschaft. Einleitende Bemerkungen zur Digitalen Ethik.....	7
--	---

I. Anonymität, Transparenz und Ethik: Grundlagen

<i>Wolfgang Wunden</i> Mehr ‚Anonymität‘ – bessere Kooperation? Zur Ethik digitaler Kommunikation.....	21
<i>Sonja Haug, Karsten Weber</i> Vertrauen, Kontrolle und Privatsphäre in sozialen Beziehungen und die Wirkungen moderner Informations- und Kommunikationstechnologie	37
<i>Patrick Kilian</i> Polarisierte Schattenbilder: Ein radiologisch-historischer Blick auf Transparenz und Big Data.....	57
<i>Inga Tappe</i> <i>Was einer ist und Wer einer ist: Anonymität und Identität in sozialen Medien aus philosophischer Sicht.....</i>	77
<i>Sarah Mönkeberg</i> Bilder und Reflexionen vom Ich: Das Web 2.0 als Institution der Selbstthematizierung?	97

II. Fallstudien zum menschlichen Handeln in der digitalen Welt

<i>Tobias Eberwein, Huub Evers, Harmen Groenhard</i> Medienverantwortung und journalistische Transparenz. Optionen für Redaktionen im digitalen Umbruch.....	117
<i>Hektor Haarkötter</i> Anonymität im partizipativen Journalismus. Empirische Untersuchung der User-Kommentare auf journalistischen Facebook-Seiten.....	133
<i>Thomas Haas, Thomas Kilian</i> Jenseits der Anonymität – Wie rechtfertigen Facebook-Nutzer ihr Verhalten? Eine empirische Studie auf Basis der Neutralisierungstheorie	151

Christopher Koska

User- and Usagemining | Privacy Preservation.

Schritte zur Integration beider Welten 163

Martin Hennig

„Ich ist ein anderer“: Anonymität in Online-Rollenspielen 185

Natascha Zowislo-Grünwald, Julian Hajduk, Franz Beitzinger

Web 2.0 als ‚Religion‘? Implikationen für das Kommunikations-

management von Organisationen 209

ANONYMITÄT UND TRANSPARENZ IN DER DIGITALEN GESELLSCHAFT

Einleitende Bemerkungen zur Digitalen Ethik

Petra Grimm, Tobias Keber, Oliver Zöllner

Es war fürwahr ein gesellschaftlicher und medienrechtlicher Paukenschlag, als im Juli 2015 an die Öffentlichkeit drang, dass der Generalbundesanwalt bereits einige Monate zuvor Ermittlungen gegen die Betreiber des Blogs *Netzpolitik.org* eingeleitet hatte. Der Verdacht lautete auf Landesverrat; Gegenstand der Ermittlungen waren Publikationen des Blogs von als Verschlusssache gekennzeichneten Dokumenten des Bundesamtes für Verfassungsschutz zum Thema *Internet-Überwachung*.¹ Das kritische Portal, bis dahin eher Fachleuten geläufig, war mit einem Schlag weit über Deutschland hinaus bekannt.² Der Fall schlug als politischer Skandal hohe Wellen und man darf prophezeihen, dass er – auch nach der relativ raschen Einstellung der Ermittlungen – in die deutsche Politik- und Rechtsgeschichte eingehen wird als eine Art SPIEGEL-Affäre Nummer zwei.³ Es war ein klarer Sieg für die Pressefreiheit und zumindest ein Dämpfer für die Verfechter von Online-Überwachung.

1 DIE DIGITALE DURCHDRINGUNG DES ALLTAGS UND IHRE FOLGEN

Die geschilderte Sommerposse aus dem Jahr 2015 hat insofern Relevanz für das vorliegende Buch, als sie einer großen Öffentlichkeit sehr eindringlich vor Augen führte, welches Ausmaß und welche weitreichenden Folgen die digitale Durchdringung des Alltags für den Einzelnen wie auch für die Gesellschaft längst hat. Zu diesem Zeitpunkt war die thematisch verwandte Whistleblower-Affäre um Edward Snowden und interne Dokumente der Geheimdienste National Security Agency (USA) und Government Communications Headquarters (Großbritannien) gerade erst zwei Jahre her.⁴ Die verheißungsvolle Vorstellung vom Internet als friedliche Spielwiese für Informationsrecherche, Online-Shopping und Kontaktmanagement

1 Vgl. Generalbundesanwalt 2015 sowie Beckedahl 2015.

2 Vgl. BBC News 2015.

3 Auslöser der ersten SPIEGEL-Affäre war ein nicht gezeichneter, Ahlers und Schmelz zuzuschreibender Artikel unter dem Titel „Bedingt abwehrbereit“ (Ahlers/Schmelz 1962). Den Ablauf und die Auswirkungen der Affäre dokumentieren zeitgenössisch Grosser/Seifert 1966 und Ellwein et al. 1966 sowie aktuell Hoffmann-Riem 2012; s. a. weiter unten.

4 Vgl. ausführlich hierzu Greenwald 2014 und die Beiträge in Beckedahl/Meister 2013.

konnte bereits zu jenem Zeitpunkt im Magazin der Utopien abgelegt werden. Der einzelne Nutzer muss sich im Klaren darüber sein, dass er oder sie im World Wide Web identifizierbar, adressierbar und nicht unbeobachtet ist. Das Internet ist ein Glaskasten – oder genauer: ein semi-transparenter Glaskasten, bei dem vor allem die User sichtbar sind. Für diese Deanonymisierung kann es auch durchaus sachlich und situativ zu rechtfertigende Gründe geben – das Internet ist kein rechtsfreier Raum.⁵ Weit weniger transparent und fassbar sind dagegen oft die Software- und Diensteanbieter und ihre Nutzungsbedingungen, Datenschutzregelungen oder algorithmischen Big-Data-Anwendungen. Gut in dieses Sinnbild passt, dass just am Tag der Beendigung der Ermittlungen gegen Netzpolitik.org die Verbraucherschutzzentrale Rheinland-Pfalz vor dem Computer-Betriebssystem Windows 10 der Firma Microsoft warnt, „das den PC in eine Art private Abhöranlage“ verwandele. „Nach Smartphones und Tablets erfolgt jetzt auch am heimischen Schreibtischrechner oder Notebook eine umfassende Beobachtung“.⁶ Organisationen der Privatwirtschaft – neben Microsoft allen voran Alphabet (Google), Amazon, Apple, Facebook und Vodafone, um nur die größten Global Players samt ihrer vielen Tochterfirmen und Joint Ventures zu nennen – sind also ebenso wie staatliche Einrichtungen Akteure der Überwachung von Internetnutzern. Sie prägen mit ihren Programmen, Dienstleistungen und Data-Mining-Auswertungen in erheblichem Maße den Alltag in der mediatisierten industrialisierten Welt.⁷ Auch Fernseher (Smart-TVs), Spielkonsolen und sogar neuere Barbiepuppen sind inzwischen mit dem Internet verbunden, sammeln und senden Daten,⁸ von Autos und Fitnessarmbändern ganz zu schweigen.⁹ Selbstverständlich ist die Nutzung dieser kommerziellen Angebote und Dienste freiwillig. Doch wer den meist sehr umfangreichen und für Laien oft kaum verständlichen Nutzungs- und Datenschutzbestimmungen nicht zustimmt, wird von der weiteren Nutzung eben ausgeschlossen: „Ein Nein akzeptiert das Unternehmen nicht“¹⁰, wofür der Musik-Streamingdienst Spotify, der neuerdings von seinen Usern auch Zugriff auf private Fotos, Adressbücher und Standortdaten verlangt, nur ein Beispiel ist.

2 DER IDENTIFIZIERBARE MENSCH

All das ist kaum wirklich neu und sicher erst der Anfang. Der Mensch in seiner digitalen Umwelt scheint sich allerdings daran zu gewöhnen, für Geheimdienste und datenhungrige Firmen weitgehend transparent und keineswegs anonym im Internet unterwegs zu sein.¹¹ Facebook etwa ist für viele längst ein Teil der Infrastruktur,

5 Vgl. hierzu die frühe Studie von Marx 1999.

6 Verbraucherschutzzentrale Rheinland-Pfalz 2015.

7 Zum Kontext dieser Entwicklung vgl. Brynjolfsson/McAfee 2014; Mayer-Schönberger/Cukier 2013.

8 Vgl. Godefroid et al. 2013; Bähr 2015; Boie 2015a; Spehr/Tunze 2015.

9 Vgl. Sharman 2015; Graff 2015; Nienhaus 2015.

10 von Au 2015, S. 25.

11 In einer interessanten Studie arbeitet Foschepoth (2012) die Post- und Telefonüberwachung in

Strom und Wasser nicht unähnlich.¹² Anonymität und Privatheit sind in solch einem Kontext folglich keine Selbstverständlichkeit mehr.¹³ Bereits vier spatiotemporale Datenpunkte reichen oft aus, um Individuen mit sehr hoher Wahrscheinlichkeit zu reidentifizieren, wie de Montjoye et al. (2015) anhand von Kreditkarten-Metadaten demonstriert haben.¹⁴ Selbst wo User um ihre Rückverfolgbarkeit im Netz wissen, ergreifen sie oftmals keine Gegenmaßnahmen (privacy paradox).¹⁵ Das Wissen um die eigene Überwachbarkeit kann individuell wie auch gesellschaftlich zu Verhaltensveränderungen führen wie etwa dem bewussten Vermeiden bestimmter Stichwörter oder Suchbegriffe, wodurch Diskurse eingeschränkt, geglättet oder unterdrückt werden können (streamlining, chilling effect).¹⁶ Und nicht zuletzt erscheint angesichts der Intransparenz vieler Anbieter und Angebote im digitalen Raum (oder auch ihrer marktbeherrschenden Stellung) die Vorstellung von der Selbstbestimmtheit und Freiwilligkeit der Auswahl auf Nutzerseite geradezu hinfällig, da leicht beeinfluss- und steuerbar (malleable choice).¹⁷ In einer längerfristigen Makroperspektive ist zudem von einer allmählichen Ökonomisierung der Wertesysteme auszugehen, die bis in den Alltag der Menschen dringt. Quasi alle Handlungen können quantifiziert, datafiziert und auf Märkten monetarisiert werden.¹⁸ Der Uber-Taxifahrer, den ich mit Punkten bewerte, wird auch mich bewerten. Und meine Krankenkasse oder Autoversicherung wird mir für risikoärmere Lebens- bzw. Fahrweisen Boni anbieten. Solche Vereinbarungen basieren auf den Prinzipien von Überwachung und Kontrolle und schaffen neue Verhaltensweisen und neue Abhängigkeiten.

Was also bleibt vom Ideal der Ermächtigung des Menschen, Herr seiner Werkzeuge zu sein? Ist in der Machtbeziehung zwischen Internetnutzern und Technologieanbietern im weiteren Sinne nicht längst eine Form von Unterwerfung zu konstatieren, wenn auch eine weitgehend freiwillige? Viele Nutzer verzichten auf Privatheit und Anonymität, zahlen mit ihren Daten für teils (scheinbar) kostenlose Dienstleistungen und bewegen sich fortan im Internet weitgehend datentransparent. „Der Insasse“ eines solchen „digitalen Panoptikums ist Opfer und Täter zugleich. Darin besteht die Dialektik der Freiheit. Die Freiheit erweist sich als Kontrolle“.¹⁹ In Abwandlung der bekannten Forderung nach Privacy by Design, also nach bereits in Endanwendungen eingebauten datenschutzfreundlichen Privatheitseinstellungen, könnte man hier auch von Surveillance by Design sprechen, bei der die Anonymität und Freiheit des Individuums-als-Netznutzer bestenfalls vorgegaukelt wer-

der Bundesrepublik Deutschland von 1949 bis 1989 auf, die als Vorgeschichte der Internetüberwachung gelten kann.

12 Vgl. Lanier 2013, S. 250.

13 Vgl. die Beiträge in Trepte/Reinecke 2011; Grimm/Zöllner 2012; Nassehi 2014 sowie Lever 2012; Nissenbaum 2010 und Rössler 2001.

14 Vgl. hierzu auch Behrens 2015.

15 Vgl. Taddicken/Jers 2011; Taddicken 2014.

16 Vgl. Heins/Beckles 2005.

17 Vgl. Acquisti et al. 2015.

18 Vgl. hierzu die Beiträge in Grimm/Zöllner 2015.

19 Han 2012, S. 82.

den. Dies dürfte Auswirkungen auch auf die Identität des Einzelnen haben. Es deuten sich neue Bilder des Menschen von sich selbst an.

3 ANONYMITÄT, MEDIENKOMPETENZ UND POLITIK

Notwendig erscheint vor diesem skizzierten Hintergrund eine umfassendere wissenschaftliche Perspektive auf Anonymität, Transparenz und Privatheit im digitalen Kontext, die individuelles Handeln, organisationale Interessen und gesellschaftliche Leitlinien kritisch analysiert und konkrete Handlungsoptionen aufzeigt, wie ein gedeihliches Leben gelingen kann.²⁰ Eine solche Sichtweise bietet die Digitale Ethik, eine Erweiterung der allgemeinen Medienethik.²¹ Die Digitale Ethik fokussiert in ihrem Kern auf die oben beschriebenen fundamentalen Transformationen, die die digitalen Medien der Gesellschaft wie auch dem Individuum auferlegen.²² Es sind die konzeptionellen Vorstellungen vom Selbst – und damit auch die Rahmenbedingungen der Ethik an sich, wie Ess darlegt²³ –, die sich durch die zunehmende Digitalisierung und weiter fortschreitende Mediatisierung verändern.²⁴

Ziel einer angewandten Digitalen Ethik ist es, den Erwerb einer wertebezogenen Medienkompetenz zu fördern. Damit ist die Befähigung verbunden, Medien bzw. mediales Handeln bewerten, Folgen abschätzen und verantwortungsbewusst handeln zu können. Nukleus einer so verstandenen wertebezogenen Medienkompetenz ist die Befähigung zu medienethischem Reflektieren und Handeln.

Die Bedeutung von Anonymität im Kontext von Medienkompetenz betrifft zwei unterschiedliche Konfliktfelder: zum einen den Schutz der Privatsphäre und zum anderen die im Schutze der Anonymität stattfindende Online-Gewalt wie z. B. Cybermobbing, Hass-Kommentare etc. Anonymität ist somit immer kontextgebunden zu bewerten. Im Kontext der Privatheit lässt sich Anonymität als instrumenteller Wert verstehen, der zum Schutz der Privatheit und Autonomie²⁵ dient. Anders verhält es sich, wenn Anonymität als Schutzmantel für verletzendes Kommunikationsverhalten genutzt wird. Dann ‚verliert‘ Anonymität ihren Status als ethischer Wert, da sie instrumentell dazu genutzt wird, die Integrität einer Person zu verletzen. Im Folgenden soll der Fokus auf Anonymität als Wert gelegt werden.

„Secrets are lies – Sharing is caring – Privacy is theft“ lautet das Credo des kalifornischen Internetkonzerns „The Circle“ in Dave Eggers’ gleichnamigem Roman.²⁶ Diese Dystopie erzählt am Beispiel der Protagonistin Mae, wie es der fiktiven Firma im Silicon Valley gelingt, eine digitale Welt zu kreieren, in der jeder Mensch online wie offline identifizierbar ist. Der totale Verzicht auf Anonymität soll dazu dienen, Kriminalität und unmoralisches Verhalten zu unterbinden. Wäh-

20 Zu Grundfragen der Ethik vgl. die hervorragende Einführung von Malik 2014.

21 Vgl. Debatin/Funiok 2003; Funiok 2011; Couldry et al. 2013.

22 Luciano Floridi nennt dies ganz passend das hypervernetzte „Onlife“. Vgl. Floridi 2014.

23 Vgl. Ess 2012, S. XVIII.

24 Vgl. näher hierzu Ess 2014; Krotz 2007.

25 Vgl. zum Verhältnis von Autonomie und Privatheit Rössler 2003, S. 32–36.

26 Eggers 2013, S. 303.

rend jedoch jeder Internetnutzer völlig transparent werden soll, bleiben die Konzerninhaber, genannt „Die drei Weisen“, intransparent. Ihre Macht resultiert genau aus diesem asymmetrischen Verhältnis von Verbergen und Wissen. Welche Folgen mit dem Verlust von Privatheit und Anonymität verbunden sind, veranschaulicht die Geschichte der Protagonistin: Indem Mae sukzessive die Transparenz-Regeln des Konzerns verinnerlicht, gibt sie ihre Identität und ihre Ideale auf. So verzichtet sie auf Solidarität, Freundschaft, Mitgefühl und persönliche Freiheit und macht sich damit zum Handlanger eines Konzerns, der vorgibt, ‚Gutes‘ zu wollen, aber Entgegengesetztes tut.

Warum sind Erzählungen, sowohl fiktive als auch reale, für den Erwerb von Privatheitskompetenz so wichtig? Narrationen sind in der Lage, das abstrakte Thema *Privatheit und Anonymität* konkret zu veranschaulichen und können damit einen medienethischen Reflexionsprozess in Gang setzen. Denn Erzählungen sind zentrale Bedeutungsvermittler und transportieren Werte; sie können abstrakte Sachverhalte und Prozesse veranschaulichen und Emotionen auslösen. Sie sind somit in der Lage, die möglichen Folgen von einer Datafizierung der Privatsphäre bildlich ‚greifbar‘ zu machen und eine digitale Privatheitskompetenz (privacy literacy) zu fördern. Um Erzählungen im didaktischen Kontext für eine medienethische Reflexion nutzbar zu machen, braucht es allerdings auch ein Instrumentarium, das dazu verhilft, die in Narrationen enthaltenen Wertesysteme und deren Semantik zu ‚entschlüsseln‘. Hier bietet sich die Narratologie bzw. Mediensemiotik an, die die empirische Grundlage für das Handlungsfeld der Medienethik bieten kann.²⁷

In summa gehören zur Privatheitskompetenz folgende Fähigkeiten:

- a) die Reflexionsfähigkeit, warum Privatheit und Anonymität als schützenswert einzustufen sind (ethische Kompetenz),
- b) das Wissen, wer private Daten zu welchem Zweck erhebt, verarbeitet und weitergibt (strukturelle Kompetenz),
- c) die Abschätzung der Folgen, die sich aus der Veröffentlichung privater Daten ergeben könnten (Risikokompetenz),
- d) das Wissen über mögliche (Selbst-)Schutzmaßnahmen und Privatheit schützende Kommunikationsmedien (Handlungskompetenz) sowie
- e) die Befähigung, über Machtaspekte der Digitalisierung – kurz Big Data, Big Power und Big Money – zu reflektieren (systemische Analyse und politisches Wissen).

Sich diese Fähigkeiten anzueignen ist allerdings kein leichtes Unterfangen. Wie in der medienpädagogischen Arbeit eine Sensibilisierung für die Folgen der Datafizierung der Privatsphäre und der Deanonymisierung aussehen könnte, wurde in einem vom Institut für Digitale Ethik und der EU-Initiative klicksafe gemeinsam entwickelten Projekt erprobt.²⁸ Grundlage für einen Reflexionsprozess ist die folgende „medienethische Roadmap“²⁹, die für eine Umsetzung in der medienpädagogischen Projektarbeit als Navigationsinstrument dient und folgende Stufen umfasst:

27 Vgl. Grimm/Krah 2014.

28 Vgl. klicksafe 2015.

29 Klicksafe 2015, S. 13ff.

- 1) *Verständnis für die Bedeutung von Privatheit schaffen*: Was verstehe ich unter „privat/öffentlich“? Was ist für mich „privat“ und was ist „öffentlich“? Welche Funktionen hat die Privatsphäre? Warum brauchen wir ein Recht auf Anonymität?
- 2) *Sensibilisierung für die Datenpreisgabe und die Datensammlung*: Wer erhebt und verarbeitet private Daten und gibt sie ggf. weiter?
- 3) *Auseinandersetzung mit den Risiken von Big Data*: Was kann mit freiwillig oder unfreiwillig preisgegebenen privaten Informationen geschehen? Was bedeutet es, wenn ich jederzeit und überall identifizierbar bin?
- 4) *Reflexion über die Folgen der Verletzung der Privatsphäre*: Welche Folgen können sich aus der gewollten oder ungewollten Preisgabe persönlicher Informationen bzw. personenbezogener Daten ergeben? Welche Folgen hat es, wenn Anonymität nicht mehr gewährleistet ist?
- 5) *Wertekonflikte thematisieren*: Wie verhalte ich mich, wenn der Wunsch nach Selbstschutz (des Privaten) kollidiert mit dem Bedürfnis a) sich selbst zu entfalten und darzustellen, b) soziale Anerkennung zu erhalten, c) es sich einfach und bequem zu machen, d) Incentives zu bekommen, e) Unterhaltungsangebote zu nutzen alten und/oder f) Dinge mit anderen zu teilen (Sharing)?
- 6) *Ethos der Privatheit entwickeln*: Warum ist Privatsphäre wünschens- oder schützenswert? Was hat das mit der Entwicklung eines autonomen und (handlungs-) freien Subjekts zu tun?
- 7) *Reflexion von Handlungsmöglichkeiten*: Wie könnte eine digitale Selbstverteidigung aussehen? Welche strukturellen Handlungsoptionen gibt es?

Um im Zuge der Digitalisierung unserer Lebenswirklichkeit eine Balance von Teilhabe an der (digitalen) Gemeinschaft und Schutz der Privatsphäre zu erlangen, bedarf es auch der Bereitschaft, auf politische Entscheidungsträger einzuwirken und sich der eigenen politischen Handlungsfähigkeit bewusst zu werden. Allerdings kann der Schutz der Privatsphäre nicht individuell ohne den dafür nötigen rechtlichen und politischen Rahmen gesichert werden. Dass Problem, wie persönliche Daten geschützt werden sollen, kann nicht auf den Schultern des Einzelnen gelastet werden. Die Förderung von Privatheitskompetenz ist zwar notwendige Voraussetzung für eine Sensibilisierung im Umgang mit den digitalen Medien, hinreichend für den Schutz der Privatsphäre ist sie nicht. Letztlich bedarf es regulatorischer Schritte und eines politischen Willens, um ein verantwortungsvolles Konzept der Privatheit und entsprechende technische Lösungen zu entwickeln. Zentrale Frage wären in diesem Zusammenhang: Wie lässt sich Privacy by Design bei der Entwicklung von neuen Technologien, Produkten und Vernetzungssystemen implementieren? Brauchen wir eine freiwillige Selbstverpflichtung der Wirtschaft und öffentlichen Organisationen – einen Code of Conduct –, um das Konzept der Privatheit als essentielle Säule unserer demokratischen Gesellschaft langfristig zu gewährleisten?³⁰

30 Grimm 2014.

4 ANONYMITÄT, TRANSPARENZ UND RECHT

Die neuen Möglichkeiten des digitalen Alltags bringen neuartige Herausforderungen mit sich. In der analogen Welt erfolgt der Einkauf im Supermarkt in aller Regel anonym. Das ist eine Selbstverständlichkeit und niemand käme auf die Idee, der Kassiererin beim Hinüberreichen des Bargelds den Namen, die Post- und E-Mailanschrift oder die Telefonnummer zu diktieren. Im Netz herrschen andere Gepflogenheiten. In der digitalen Welt ist der (rechtliche) Grundsatz der Datenvermeidung zum anachronistischen Fremdkörper verkümmert. Vertreter der so genannten Post-Privacy-Bewegung haben, das Argument der „normativen Kraft des Faktischen“³¹ ganz sicher überstrapazierend, bereits einen Abgesang auf die Privatheit angestimmt.³²

Öffentliche und private Sphäre drohen vollständig zu diffundieren. Dieser Entwicklung nichts entgegenzusetzen bedeutet, die Grundfesten einer freiheitlich demokratischen Gesellschaft insgesamt in Frage zu stellen. In der Magna Charta³³ des deutschen Datenschutzrechts, dem Volkszählungsurteil des Bundesverfassungsgerichts,³⁴ heben die Karlsruher Richter nicht nur das „Recht auf informationelle Selbstbestimmung“ aus der Taufe,³⁵ sondern unterstreichen auch sehr deutlich den objektiv-rechtlichen Gehalt dieses Rechts als „Funktionsbedingung eines freiheitlichen demokratischen Gemeinwesens“.³⁶

Teil des Rechts auf informationelle Selbstbestimmung ist das Recht auf Anonymität,³⁷ das auf einfachgesetzlicher Ebene in § 16 Absatz 6 TMG zum Ausdruck kommt. Dieses Recht wurde jüngst in einer Entscheidung des Bundesge-

31 Eingehend zu der von Georg Jellinek geprägten Begrifflichkeit Lepsius 2002.

32 Vgl. etwa Heller 2011.

33 Diese Parallele zieht erstmals Hoffmann-Riem 1998, S. 513.

34 Bundesverfassungsgericht 1983: BVerfGE 65, 1, Urteil v. 15.12. (Volkszählungsurteil).

35 Das Gericht begründet wie folgt: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ BVerfGE 65, 1 (155).

36 Im Volkszählungsurteil heißt es wörtlich: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ BVerfGE 65, 1 (154).

37 Zur Dogmatik vgl. Bäumler 2003, S. 1 ff.

richtshofs zu Einträgen auf einer Ärztebewertungsplattform bekräftigt.³⁸ Mit der Möglichkeit, anonym kommunizieren zu können, wird zugleich die Meinungsfreiheit flankiert, die ihrerseits für das Funktionieren einer freiheitlich-demokratischen Staatsordnung, wie das Bundesverfassungsgericht schon 1958 im Lüth-Urteil³⁹ herausgearbeitet hat, „schlechthin konstitutiv“ ist.

Einen engen Bezug zwischen idealerweise spurenfreier Kommunikation im Netz und der Meinungsfreiheit sieht auch der Europäische Gerichtshof in seiner Entscheidung zur Rechtswidrigkeit der EU-Richtlinie zur Vorratsdatenspeicherung.⁴⁰ Mit dieser und der Entscheidung zum so genannten Recht auf Vergessen⁴¹ haben die Richter in Luxemburg den Schutz der Privatheit in Europa erheblich gestärkt.

Ebenso wie das Recht auf informationelle Selbstbestimmung ist auch das Recht auf Anonymität nicht schrankenlos gewährleistet. Konfligierende Rechtspositionen, etwa die Rechte anderer, sind bei der Rechtsanwendung in Einzelfall gebührend zu berücksichtigen. Nicht nur individuelle Rechtspositionen können die Grundrechte einschränken, wie die Debatten um die Veröffentlichung als geheim eingestufte Dokumente auf Wikileaks⁴² und dem bereits angesprochenen Portal Netzpolitik.org zeigen.

Das Demokratieprinzip gebietet Transparenz. Für Kant war Publizität wesentlicher Bestandteil staatlicher Legitimation.⁴³ Andererseits lassen sich in wohl allen Rechtsordnungen der Welt Rechtsnormen finden, die das Offenbaren sensibler Informationen sanktionieren und die Sicherheit des Staates schützen. Wie geheim also darf ein demokratischer Rechtsstaat sein?

Im Fall Netzpolitik.org stellt sich konkret die Frage, ob Dokumente zum Personal- und Haushaltsplan des Verfassungsschutzes „Staatsgeheimnisse“ darstellen, deren Veröffentlichung im Netz als Landesverrat (§ 94 StGB) zu qualifizieren ist, oder ob Pressefreiheit und das öffentliche Informationsinteresse überwiegen.⁴⁴ Den Geheimdiensten ihre Daseinsberechtigung per se abzuspüren, geht sicher zu weit.

38 Bundesgerichtshof 2014: BGH, Urteil v. 23.09., VI ZR 358/13 (Jameda). In Rn. 50 des Urteils heißt es: Die Möglichkeit, Bewertungen auch anonym abgeben zu können, erlangt im Falle eines Ärztebewertungsportals im Übrigen ganz besonderes Gewicht. Denn häufig wird die Bewertung eines Arztes mit der Mitteilung sensibler Gesundheitsinformationen, etwa über den Grund der Behandlung oder die Art der Therapie, verbunden sein. Wäre die Abgabe einer Bewertung nur unter Offenlegung der Identität möglich, bestünde deshalb hier ganz besonders die Gefahr, dass eigentlich bewertungswillige Patienten im Hinblick darauf von der Abgabe einer Bewertung absehen.“

39 Bundesverfassungsgericht 1958: BVerfGE 7, 198, Urteil v. 15.01.

40 Europäischer Gerichtshof 2014a: EuGH, C-293/12 und C-594/12 (Digital Rights Ireland und Seitlinger u. a.), Entscheidung v. 08.04.

41 Europäischer Gerichtshof 2014b: EuGH, C-131/12 (Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos [AEPD] und Mario Costeja González), Urteil v. 13.5. Dieser Fall steht nach Meinung von Kommentatoren „exemplarisch dafür, wie weit die digitale Realität Justiz und Gesetzgebung voraus ist“ Boie 2015b, S. 15.

42 Dazu Keber 2012.

43 Vgl. Kant 2013 [1795], S. 65 ff. (Anhang II).

44 Das ist keine neue Fragestellung. Die Privilegierung des publizistischen Landesverrats wird seit der SPIEGEL-Affäre 1962 diskutiert. Zum Meinungsstand: Hoffmann-Riem 2012, S. 226.