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 darlegt[23] –, 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 Autonomie[25] 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) konfligiert 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 Charta[33] 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. 1ff.

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-Urteil[39] 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 Vergessen[41] 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 eingestufter Dokumente auf Wikileaks[42] 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 abzusprechen, 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.

In einem demokratischen Rechtsstaat darf es aber auch keine kontrollfreien Zonen, keine unbegrenzte ‚Macht im Schatten' geben.

5 DIE IDEEPOLIS-TAGUNG UND DIE BEITRÄGE DES BUCHES

An der Hochschule der Medien Stuttgart wurde 2013 das Institut für Digitale Ethik (IDE) gegründet. Seine offizielle Inauguration fand am 13. Januar 2014 mit der ersten Ausgabe der Fachtagungsreihe „IDEepolis" statt. Sie stand unter dem Titel „Anonymität und Transparenz in der digitalen Gesellschaft", der auch dem vorliegenden Buch voransteht. Ziel der Tagung war es, sich multiperspektivisch mit den Voraussetzungen und Funktionen von Anonymität in bestimmten Kontexten zu befassen. Sowohl mit Blick auf die Makroebene der Gesellschaft, die Mesoebene der organisationalen Akteure als auch die Mikroebene der handelnden Individuen sollten Argumentationen und Begründungen für den Geltungsbereich der Anonymität und Transparenz erörtert und für Diskussionen innerhalb einer fortzuschreibenden Digitalen Ethik erschlossen werden. Die eingegangen Vortragsvorschläge wurden in einem anonymisierten Peer-Review-Verfahren ausgewählt; der vorliegende Sammelband ist durch einige Beiträge ergänzt worden.

Der erste Abschnitt des Buches präsentiert Grundlagen von Anonymität, Transparenz und Ethik. Wolfgang Wunden führt in seinem Beitrag „Mehr Anonymität – bessere Kooperation?" grundlegend in die Ethik digitaler Kommunikation ein. Er führt deutlich vor Augen, dass die „informationelle Selbstbestimmung", das Recht auf das persönliche Geheimnis und Anonymität wie auch das „Recht, vergessen zu werden" (Right to Be Forgotten) „unaufgebbare Kulturgüter" sind. Karsten Weber und Sonja Haug weisen in ihrem Aufsatz „Vertrauen, Kontrolle und Privatsphäre in sozialen Beziehungen und die Wirkungen moderner Informations- und Kommunikationstechnologie" darauf hin, „dass es einen engen Zusammenhang zwischen Vertrauen, Kontrolle und Privatsphäre in engen sozialen Beziehungen gibt" und dass insbesondere die Nutzung von mobilen Informations- und Kommunikationstechnologien im Zusammenspiel mit Web-2.0-Angeboten „erhebliche negative Einflüsse auf diese Beziehungen haben kann." Patrick Kilian wirft bei Big Data und Transparenz einen Blick zurück auf die Wissenschaftsgeschichte der Radiologie und zu den Anfängen der modernen Geschichtsschreibung. Die „polarisierten Schattenbilder" der Röntgenschirme stehen bei ihm für die „Grenzen zwischen Sichtbarkeit und Unsichtbarkeit", die sich immer wieder aufs Neue verschieben. „Medien-Werden und Transparent-Werden sind dabei untrennbar aneinander gebunden", so Kilian. Inga Tappe bezieht sich bei ihren Ausführungen zu „Anonymität und Identität in sozialen Medien aus philosophischer Sicht" vor allem auf Hannah Arendts zentrales Werk „Vita Activa" („The Human Condition", 1958) und die Unterscheidung zwischen „Was einer ist" und „Wer einer ist". Sie kommt abschließend zu der Feststellung, „dass das Fehlen von Informationen zum ‚Was' die Identifikation des ‚Wer' maßgeblich erschweren" kann, „weil es die Zersplitterung zusammenhängender Lebensgeschichten in separate, nicht mehr eindeutig zu verknüpfende Teilgeschichten" zur Folge habe, so Tappe. Die eingangs noch hinter-

fragte Option, das Internet trotz der Möglichkeit zur anonymen, namenlosen Kommunikation „als einen Interaktionsraum zu deuten, in dem die eigentlichen Identitäten der Handelnden – ihr ‚Wer' – erfahrbar werden", wird von der Autorin letztlich negativ beschieden. Sarah Mönkeberg widmet sich den „Bildern und Reflexionen vom Ich" und damit der Frage nach dem Verhältnis von Anonymität und Transparenz in der digitalen Gesellschaft. Sie begreift die Veröffentlichungen des Selbst im Web 2.0 als „Formen der Bearbeitung und Versicherung von Identität". Mönkeberg legt dar, dass es sich bei den Selbstthematisierungen und -darstellungen im Internet „um Arbeit am Subjekt und Versicherungen desselben" vor dem Hintergrund gegenwärtiger Formen der Verunsicherung handelt. Verbindungen zu älteren Institutionen der Selbstthematisierung seien konzeptionell nicht zufällig: Die Autorin arbeitet Parallelen zur Beichte (mit einem Fokus auf Erlösung und Vergebung von Sünden) und zur Psychoanalyse (mit einem Fokus auf Gesundheit und Stärkung des Subjekts) heraus.

Der zweite Abschnitt des Buches versammelt Fallstudien zum menschlichen Handeln in der digitalen Welt. Unter der Überschrift „Medienverantwortung und journalistische Transparenz" stellen Tobias Eberwein, Huub Evers und Harmen Groenhart „Optionen für Redaktionen im digitalen Umbruch" vor. Grundlage ihrer Studie ist eine von ihnen 2011/12 durchgeführte, international vergleichende Befragung von mehr als 1.700 Journalisten in 14 Ländern. Die Daten verweisen auf eine „auffällige Diskrepanz zwischen journalistischen Ansprüchen an Transparenz und den tatsächlichen redaktionellen Initiativen in diesem Bereich. Ganz offensichtlich", so schlussfolgern die Autoren, „praktizieren Redaktionen etwas anderes, als sie predigen, wenn es um Transparenz und Publikumsinteraktion geht" – woraus sich aber einiges lernen lasse, wie die Autoren dann auch detailliert aufzeigen. Hektor Haarkötter gelangt zu durchaus analogen Befunden. Er widmet sich in seinem Beitrag der „Anonymität im partizipativen Journalismus", in dem er die Ergebnisse einer Inhaltsanalyse von mehr als 2.000 User-Kommentaren auf journalistischen Facebook-Seiten vorstellt. Die altbekannte netzeuphorische These, dass der Leser im Web 2.0 zum „Prosumenten" werde, kann die Studie nicht bestätigen: Es gelänge den Facebook-Kommentatoren kaum, Sachverhalte objektiv und argumentativ darzulegen. Vielmehr seien „hohe Selbstbezüglichkeit und Dialogverweigerung bis hin zum ‚Cyberbullying' zu konstatieren", so Haarkötter. Umgekehrt zeigten „auch die professionellen Journalisten nahezu kein Interesse an den kommentierenden Äußerungen ihrer Facebook-User. Hier liegt also einiges im Argen. Wie Facebook-Nutzer ihr unter dem schützenden Mantel der Anonymität erfolgendes Posting-Verhalten rechtfertigen, ist Aufhänger einer qualitativen, interviewbasierten Studie von Thomas Haas und Thomas Kilian („Jenseits der Anonymität"). Als theoretische Rahmung wählen die Autoren die soziologische Neutralisierungstheorie von Sykes und Matza (1957) mit ihren diversen Abwehr-, Leugnungs- und Rechtfertigungsstrategien. Als Kernergebnis scheint auf, „dass die meisten Nutzer das eigene Verhalten und das Verhalten anderer Benutzer als normal ansehen." Es scheint für die User also alles in Ordnung zu sein im Netz. In den Ergebnissen tritt aber deutlich zutage, „wie wenig Gedanken sich Nutzer über Anonymität machen" – und wie relativ sorglos sie etwa mit berechtigten diesbezüglichen Ansprü-

chen Dritter umgehen, etwa beim Hochladen von Fotos. Hier spielen laut Haas und Kilian wohl auch ausgeprägte Bedürfnisse nach Aufmerksamkeit und Selbstinszenierung eine Rolle. Der Mensch erscheint letztlich also unsicher und bedürftig. Christopher Koska untersucht, wie die beiden sich in der Praxis geradezu antagonistischen Gebiete „User- and Usagemining" (breit angelegte Auswertungen von Nutzer- und Nutzungsdaten) und „Privacy Preservation" (Privatheitsbewahrung) miteinander verzahnt werden können. Ziel des Beitrags ist es, die ethische Diskussion um den Schutz der Privatheit im Netz „anwendungsnah zu bereichern und weiterzuführen." Grundvoraussetzung hierfür, so Koska, sind möglichst gut strukturierte Informationen über Problemfälle, die dem Nutzer zur richtigen Zeit am richtigen Ort zur Verfügung gestellt werden müssten. Dies könne aber nicht darüber hinweg täuschen, dass der Mensch vor dem Hintergrund etwa von dynamischen Quellenverknüpfungen, proaktiven Empfehlungssystemen und dem aufkommenden Internet der Dinge „viel mehr als bisher von außen gesteuert" werde. Gesellschaftliche Handlungsperspektiven sieht der Autor u. a. in einer verbesserten Transparentmachung von Risiken und einer stärkeren Anregung von Diskursen hierüber. Martin Hennig analysiert in seinem Beitrag „‚Ich ist ein anderer'" die Anonymität in Massen-Mehrspieler-Online-Rollenspielen (MMORPGs). Anonymität besitze im Online-Rollenspiel sowohl auf das Individuum als auch auf die soziale Gemeinschaft beziehbare Funktionen. „Dabei ist Anonymität eng mit dem Konzept der Überwachung verknüpft", so Hennig: Aus dem anonymen Spiel könne man „ein Denkmodell ableiten, demzufolge Überwachung (wahrgenommen als Spiel) im anonymen Raum des Netzes lediglich zur Stimulation von noch vollständigerer Anonymität führt." Doch die Wirklichkeit werde zunehmend Teil des Spiels, meint Hennig: „Wenn nun allerdings tatsächlich Überwachungsdrohnen bis in die hintersten Winkel der Fantasie der Nutzenden dringen, zerbricht der dargestellte und gelebte alternative Systementwurf, denn damit nähert sich die virtuelle Welt den Kontrollcharakteristika der Realität." Inwieweit das interaktive Web 2.0, ein Hilfssystem des Alltags, bereits als Quasi-Religion wahrgenommen wird, untersuchen Natascha Zowislo-Grünewald, Julian Hajduk und Franz Beitzinger mit Rückgriff auf die Systemtheorie und das Kommunikationsmanagement von Organisationen. „Das Web 2.0 als System", so die Autoren, sei „weder Religion noch Massenmedium." Es stehe „zwischen den Extremen Wissen und Glauben" und löse das Problem der „praktischen Unüberprüfbarkeit von Anonymität" dadurch, dass das Netz „alle Operationen dem Code *Vertrauen/Nicht-Vertrauen* unterwirft. Somit transformiert es un-handhabbare in handhabbare Komplexität." Im Mittelpunkt dieser Sichtweise steht dabei immer das Vertrauen als unumgehbare Bedingung der ethisch angemessenen Nutzung des Internets, was die Netzkommunikation letztlich wieder auf den Menschen selbst zurückführt – und den Leser an den Anfang dieses Buches.

BIBLIOGRAFIE

Acquisti, Alessandro/Brandimarte, Laura/Loewenstein, George (2015): Privacy and Human Behavior in the Age of Information. In: Science, Vol. 347, No. 6221, S. 509–514. Online: http://www.sciencemag.org/content/347/6221/509.full.pdf (Abruf: 26.6.2015).

Ahlers, Conrad/Schmelz, Hans (1962): Bedingt abwehrbereit. In: Der Spiegel, 16. Jhg., Nr. 41 (10.10.), S. 32–53. Online: http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/25673830 (Abfrage: 10.8.2015).

Arendt, Hannah (1958): The Human Condition. Chicago: University of Chicago Press.

Au, Caspar von (2015): Wo bist du, was machst du? Der Musik-Streamingdienst Spotify möchte Zugriff auf Fotos, Kontakte und Ortsdaten seiner Nutzer haben. In: Süddeutsche Zeitung, 71. Jhg., Nr. 192 (22./23.8.), S. 25.

Bähr, Julia (2015): Das gläserne Kind. Neue Spielzeuge nehmen auf, was Kinder ihnen erzählen. Eltern können sich das anhören – und sparen sich echte Gespräche. Konzerne sammeln die Daten. In: Frankfurter Allgemeine Sonntagszeitung, 15. Jhg., Nr. 13 (29.3.), S. 5.

Bäumler, Helmut (2003): Das Recht auf Anonymität. In: Bäumler, Helmut/von Mutius, Albert (Hrsg.): Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts. Braunschweig/Wiesbaden: Vieweg, S. 1–11.

BBC News (2015): Netzpolitik: German treason inquiry dropped amid furore. Online: http://www.bbc.com/news/world-europe-33847249 (Abfrage: 10.08.2015).

Beckedahl, Markus (2015): Generalbundesanwalt stellt Ermittlungen wegen Landesverrat ein – Das reicht uns nicht! Online: https://netzpolitik.org/2015/generalbundesanwalt-stellt-ermittlungen-wegen-landesverrat-ein-das-reicht-uns-nicht/ (Abfrage: 10.08.2015).

Beckedahl, Markus/Meister, Andre (Hrsg.) (2013): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications/epubli.

Behrens, Christoph (2015): Identifikation aus dem Nichts. Nur wenige anonymisierte Bewegungsprofile reichen aus, um die Identität von Kreditkartennutzern zu erkennen. Je größer die gesammelten Datensätze werden, desto kleiner bleibt die Privatsphäre. In: Süddeutsche Zeitung, 71. Jhg., Nr. 24 (30.1.), S. 16.

Boie, Johannes (2015a): Ich will eure Stimmen hören. Der will doch nur spielen: Neue Produkte für Kinder sind mit Elektronik vollgestopft. Für den Nachwuchs mag das Spaß sein. Doch tatsächlich werden Daten abgegriffen. Denn das Spielzeug funkt aus dem Kinderzimmer in die Konzernzentrale. In: Süddeutsche Zeitung, 71. Jhg., Nr. 89 (18./19.04.), S. 23.

Boie, Johannes (2015b): A und O einer Weltmacht. Google baut um – und alle blinzeln nervös. Denn die neue Holding Alphabet trägt zwar Nostalgie im Namen, aber ihr Ziel ist die Zukunft. Schon heute entscheiden Programme über Leben und Tod, bringen Essen, fahren Auto, fliegen Drohnen und sammeln Daten zum Blutzucker. Über die Risiken, wenn ein Superkonzern Menschheitsfragen verhandeln will. In: Süddeutsche Zeitung, 71. Jhg., Nr. 186 (14./15./16.8.), S. 15.

Brynjolfsson, Erik/McAfee, Andrew (2014): The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York, London: Norton.

Bundesverfassungsgericht (1958): BVerfGE 7, 198, Urteil v. 15.1. (Lüth). Online: https://openjur.de/u/183740.html (Abfrage: 20.08.2015).

Bundesverfassungsgericht (1983): BVerfGE 65, 1, Urteil v. 15.12. (Volkszählungsurteil). Online: https://openjur.de/u/268440.html (Abfrage: 20.8.2015).

Bundesgerichtshof (2014): BGH, Urteil v. 23.9., VI ZR 358/13 (Jameda). Online: https://openjur.de/u/747038.html (Abfrage: 20.08.2015).

Couldry, Nick/Madianou, Mirca/Pinchevski, Amit (Hrsg.) (2013): Ethics of Media. Basingstoke/New York: Palgrave Macmillan.

Debatin, Bernhard/Funiok, Rüdiger (Hrsg.) (2003): Kommunikations- und Medienethik. Konstanz: UVK.

de Montjoye, Yves-Alexandre/Radaelli, Laura/Singh, Vivek Kumar/Pentland, Alex "Sandy" (2015):

Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. In: Science, Vol. 347, No. 6221, S. 536–539.
Eggers, Dave (2013): The Circle. A Novel. New York/Toronto/San Francisco: Knopf/McSweeney's Books.
Ellwein, Thomas/Liebel, Manfred/Negt, Inge (1966): Die Reaktion der Öffentlichkeit (=Die Spiegel-Affäre, Bd. 2). Olten/Freiburg i. Br.: Walter.
Ess, Charles (2012): Foreword. In: Heider, Don/Massanari, Adrienne L. (Hrsg.): Digital Ethics: Research and Practice. New York u. a.: Lang, S. IX–XIX.
Ess, Charles (2014): Digital Media Ethics. 2nd ed. Cambridge/Malden: Polity Press.
Europäischer Gerichtshof (2014a): EuGH, C-293/12 und C-594/12 (Digital Rights Ireland und Seitlinger u. a.), Entscheidung v. 8.4. Online: http://www.hrr-strafrecht.de/hrr/eugh/12/c-293-12.php (Abfrage: 20.08.2015).
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. Online: https://www.jurion.de/Urteile/EuGH/2014-05-13/C-131_12 (Abfrage: 20.08.2015).
Floridi, Luciano (ed.): The Onlife Manifesto: Being Human in a Hyperconnected Era. Cham/Heidelberg/New York/Dordrecht/London: Springer.
Foschepoth, Josef (2012): Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik. 3. Aufl. Göttingen: Vandenhoeck & Ruprecht.
Funiok, Rüdiger (2011): Medienethik. Verantwortung in der Mediengesellschaft (=Reihe KonTexte, Bd. 8). 2. Aufl. Stuttgart: Kohlhammer.
Generalbundesanwalt (2015): Pressemitteilung 29/2015 (2.8.): Pressemitteilung zum Verfahren aufgrund der Strafanzeigen des Bundesamtes für Verfassungsschutz. Karlsruhe.
Godefroid, Patrick/Keber, Tobias/Kühnle, Boris Alexander/Zöllner, Oliver (2013): Smart-TV – ein interdisziplinärer Überblick. In: MedienWirtschaft, 10. Jhg., Heft 3, S. 26–37.
Graff, Bernd (2015): Das Maß aller Dinge. Intelligente Systeme am Handgelenk sollen uns motivieren. Doch sie sorgen nur für den Frust des Müssens. In: Süddeutsche Zeitung, 71. Jhg., Nr. 1 (2.1.), S. 18.
Greenwald, Glenn (2014): No Place to Hide: Edward Snowden, the NSA and the Surveillance State. London, New York: Hamilton.
Grimm, Petra (2014): Ist Privatsphäre im digitalen Zeitalter noch ein Wert? Die Perspektive der Digitalen Ethik. In: Arns, Tobias et al. (Hrsg.): Zukunft der Wissensarbeit. Kongressband zur KnowTech 2014 – 16. Kongress zum Wissensmanagement und Social Media in Unternehmen und Organisationen. Berlin: Gito, S. 15–28.
Grimm, Petra/Krah, Hans (2014): Ende der Privatheit? Eine Sicht der Medien- und Kommunikationswissenschaft. Online: http://www.digitale-ethik.de//showcase//2014/11/Ende_der_Privatheit_Grimm_Krah.pdf (Abfrage: 25.08.2015).
Grimm, Petra/Zöllner, Oliver (Hrsg.) (2012): Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffentlichung des Privaten in Social Media und populären Medienformaten (=Reihe Medienethik, Bd. 11). Stuttgart: Steiner.
Grimm, Petra/Zöllner, Oliver (Hrsg.) (2015): Ökonomisierung der Wertesysteme. Der Geist der Effizienz im mediatisierten Alltag (=Reihe Medienethik, Bd. 14). Stuttgart: Steiner.
Grosser, Alfred/Seifert, Jürgen (1966): Die Staatsmacht und ihre Kontrolle (=Die Spiegel-Affäre, Bd. 1). Olten/Freiburg i. Br.: Walter.
Han, Byung-Chul (2012): Transparenzgesellschaft. Berlin: Matthes & Seitz.
Heins, Marjorie/Beckles, Tricia (2005): Will Fair Use Survive? Free Expression in the Age of Copyright Control. A Public Policy Report. New York: Brennan Center for Justice at New York University School of Law. Online: http://www.fepproject.org/policyreports/WillFairUseSurvive.pdf (Abfrage: 25.4.2014).
Heller, Christian (2011): Post-Privacy. Prima leben ohne Privatsphäre. München: Beck.
Hoffmann-Riem, Wolfgang (1998): Informationelle Selbstbestimmung in der Informationsgesellschaft. In: Archiv des öffentlichen Rechts (AöR), Bd. 123, S. 513–540.

Hoffmann-Riem, Wolfgang (2012): Die Spiegel-Affäre 1962 – ein Versagen der Justiz? In: Zeitschrift für Rechtspolitik (ZRP), 45. Jhg., Nr. 8, S. 225–256.

Kant, Immanuel (2013): Zum ewigen Frieden. Ein philosophischer Entwurf. Stuttgart: Reclam [zuerst 1795].

Keber, Tobias O. (2012): Secrecy, Privacy, Publicity, Transparency: A German Perspective on WikiLeaks. In: Dörr, Dieter/Weaver, Russell L. (Hrsg.): The Right to Privacy – Perspectives from Three Continents. Berlin/Boston: de Gruyter, S. 344–356.

Klicksafe (Hrsg) (2015): Ethik macht klick. Werte-Navi fürs digitale Leben. Arbeitsmaterialien für Schule und Jugendarbeit. Ludwigshafen: klicksafe.

Krotz, Friedrich (2007): Mediatisierung. Fallstudien zum Wandel von Kommunikation. Wiesbaden: VS.

Lanier, Jaron (2013): Who Owns the Future? New York/London/Toronto/Sydney/New Delhi: Simon & Schuster.

Lepsius, Oliver (2002): Besitz und Sachherrschaft im öffentlichen Recht. Tübingen: Mohr Siebeck.

Lever, Annabelle (2012): On Privacy. New York/London: Routledge.

Malik, Kenan (2014): The Quest for a Moral Compass: A Global History of Ethics. Brooklyn/London: Melville House.

Marx, Gary T. (1999): What's in a Name? Some Reflections on the Sociology of Anonymity. In: The Information Society, Vol. 15, No. 2, S. 99–112.

Mayer-Schönberger, Viktor/Cukier, Kenneth (2013): Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston/New York: Houghton Mifflin Harcourt.

Nassehi, Armin (Hrsg.) (2014): Privat 2.0 (=Kursbuch 177). Hamburg: Murmann.

Nienhaus, Lisa (2015): Los, bewegt euch! Die Krankenversicherungen honorieren, wenn ihre Mitglieder Sport treiben. Und überwachen bald jeden Schritt. Wer sich dem Fitnessdiktat widersetzt, zahlt drauf. In: Frankfurter Allgemeine Sonntagszeitung, 15. Jhg., Nr. 3 (18.1.), S. 24.

Nissenbaum, Helen (2010): Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

Rössler, Beate (2001): Der Wert des Privaten. Frankfurt am Main: Suhrkamp.

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

Sharman, Andy (2015): Tyred and wired: As the automobile turns into a smartphone on wheels, carmakers face a future where the real money is in technology and services – not the metal they have been engineering for decades. In: Financial Times, 4./5.4., S. 5.

Spehr, Michael/Tunze, Wolfgang (2015): Horchposten im Wohnzimmer. Internetfähige Fernsehgeräte hören in den Raum hinein. Die Technik ist umstritten. Was man wissen muss. In: Frankfurter Allgemeine Sonntagszeitung, 15. Jhg., Nr. 7 (15.2.), S. V9.

Sykes, Gresham M./Matza, David (1957): Techniques of Neutralization: A Theory of Delinquency. In: American Sociological Review, Vol. 22, No. 6, S. 664–670.

Taddicken, Monika/Jers, Cornelia (2011): The Uses of Privacy Online: Trading a Loss of Privacy for Social Web Gratification? In: Trepte, Sabine/Reinecke, Leonard (Hrsg.): Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Heidelberg/Dordrecht/London/New York: Springer, S. 143–156.

Taddicken, Monika (2014): The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. In: Journal of Computer-Mediated Communication, Vol. 19, No. 2, S. 248–273. Online: http://onlinelibrary.wiley.com/doi/10.1111/jcc4.12052/epdf (Abfrage: 14.05.2015).

Trepte, Sabine/Reinecke, Leonard (Hrsg.) (2011): Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Heidelberg/Dordrecht/London/New York: Springer.

Verbraucherschutzzentrale Rheinland-Pfalz (2015): Windows 10 – Überwachung bis zum letzten Klick. Online: http://www.verbraucherzentrale-rlp.de/windows-10---Ueberwachung-bis-zum-letzten-klick-1 (Abfrage: 10.8.2015).