Der Überwachung entgegenkommen

Paradoxien der Privatheit im Internet

Rössler, B.

DOI
10.12907/978-3-593-44695-0

Publication date
2022

Document Version
Final published version

Published in
Normative Paradoxien

Der Überwachung entgegenkommen. Paradoxien der Privatheit im Internet

Beate Rössler

Personen, die in den sozialen Netzwerken großzügig und freigebig über ihr privates Leben erzählen, behaupten doch auf der anderen Seite, dass sie insbesondere informationelle Privatheit als ein hohes Gut ansehen und es als eine wichtige Aufgabe des Gesetzgebers und des Staates betrachten, diese informationelle Privatheit zu schützen. Solcherlei Beobachtungen beim Internetverhalten von vor allem jungen Menschen, haben Theoretiker_innen in den letzten Jahren zur Verwendung des Begriffs »*privacy-paradox*« oder Privatheitsparadox geführt.

Es ist dieses Paradox, das im Folgenden mein Thema sein wird. Das Paradox drückt sich im Verhalten und in den Überzeugungen von Personen aus, die gegensätzliche und unvereinbare Dinge denken und wollen. Es ist ein Paradox, das sich auf der Ebene der individuellen Nutzer_innen feststellen und beschreiben lässt: doch es sind noch andere Paradoxien, die man bei der Analyse des Gebrauchs von Daten im Internet untersuchen muss. Denn es scheint zumindest prima facie paradoxal, wenn die großen Internetbetriebe (und auch der Staat selbst, in der Form von Datenschutzbehörden) sich dafür einsetzen, die persönlichen Daten der Nutzer_innen zu schützen, während sie auf der anderen Seite diese Nutzer_innen dazu motivieren, möglichst viele Daten zu produzieren und im Netz zu hinterlassen. Das Geschäftsmodell der Internetbetriebe ist als solches darauf angewiesen, möglichst viele Daten zu sammeln und zu bearbeiten: deshalb haben sie keinerlei Interesse daran, Daten erst gar nicht zu produzieren und auch der Staat ermutigt sie keineswegs dazu. Im Gegenteil unterstützt er das Geschäftsmodell und verabschiedet dann Datenschutzgesetze, die die weitere Verwendung der gesammelten und benutzten Daten beschränken sollen.

Es scheint nicht unberechtigt, hier von einer normativen Paradoxie zu sprechen: wenn es geradezu den Kern des Geschäftsmodells nicht nur der sogenannten *Big Five* (Amazon, Microsoft, Google, Facebook, Apple) ausmacht, soviel Daten wir irgend möglich zu sammeln, zu verarbeiten, zu ver-

kaufen, dann ist jeder Verweis eben dieser Betriebe auf den Schutz der Privatheit dieser Daten deshalb schon widersinnig, weil der Anlass für den Schutz ausschließlich darin liegt, dass die Sammelwut immer stärker, ungehemmter, brutaler wird. Analysieren lässt sich dies am besten auf dem Hintergrund der *surveillance society*. Denn in den letzten Jahren setzt sich zunehmend die Einsicht durch, dass die Analyse der Überwachungs- oder Beobachtungsgesellschaft als der notwendige Gegenpart zu den genannten Verletzungen von Privatheit begriffen werden muss. Erst im Zusammensehen dieser beiden Diskurse findet man eine Interpretationsthese der Paradoxie, die komplexer und dem sozialen Phänomen gegenüber angemessener erscheint: dann handelt es sich nicht einfach mehr um ein subjektives Paradox, das den Irrationalitäten der Nutzer_innen geschuldet ist, sondern um eine angemessene Reaktion auf die Struktur der Überwachungsgesellschaft, nämlich um digitale Resignation, Apathie, oder Frustration (vgl. Draper und Turow 2019). Diese Haltungen stellen sich ein, wenn Subjekte Kontrolle über die eigenen Daten verlangen, aber begreifen müssen, dass dies in der Überwachungsgesellschaft unmöglich ist.

Resignation würde dann keine irrationale, sondern eine gewissermaßen vernünftige Einstellung als Erklärung des Paradoxes beschreiben angesichts der Tatsache, dass individuelle Nutzer_innen gegenüber den großen Technologieunternehmen nichts ausrichten können, der Schutz des Privaten ohnehin nicht möglich sei und man deshalb ruhig prätendieren könne, nichts zu verbergen zu haben. Diese Resignation kann sich im übrigen auch als Zynismus, Frustration, oder Apathie äußern – und sie kann bestenfalls umschlagen in berechtigten Aktivismus.

Ich möchte in meinem Beitrag diskutieren, ob diese Interpretationshypothese des sozial-politischen Phänomens auch auf dem Hintergrund überzeugend ist, dass eben dieselben resignierten Gebraucher_innen die sozialen Netzwerke doch weiterhin als ausgezeichnetes Medium der Selbstdarstellung – des Mitteilungsdrangs – begreifen. Dabei werde ich in folgenden Schritten vorgehen: Ich werde zunächst genauer beschreiben, worin das Privatheitsparadox eigentlich besteht, um dann einen ersten kurzen Blick auf die verschiedenen möglichen Erklärungen des Paradoxes zu werfen. In einem nächsten Schritt will ich den notwendigen Hintergrund der Entstehung des Paradoxes erläutern, nämlich die Überwachungsgesellschaft, die unser Alltagsleben bis in seine Poren hinein prägt.

Erst im Anschluss hieran wird es möglich sein, die verschiedenen Erklärungen des Paradoxes und ihre Rationalität zu prüfen. Dabei werde ich zu

zeigen versuchen, dass das Paradox auf der subjektiven Ebene nicht einfach irrational ist, sondern eine durchaus rationale Antwort auf die Überwachungsgesellschaft darstellt. Sieht man auf die Entstehung des Paradoxes in dieser Überwachungsgesellschaft, dann kann man nämlich erkennen, dass es die manipulativen Machtverhältnisse sind, die immer mehr Daten zu produzieren suchen und ohne deren Kritik auch das Privatheitsparadox nicht kritisiert werden kann.

Das Paradox genauer besehen

Seit mittlerweile beinahe zwei Jahrzehnten wird in der Literatur das Phänomen des Privatheitsparadoxes beschrieben und diskutiert. So schreiben etwa Hargittai und Marwick: »The ›privacy paradox‹ suggests that young people claim to care about privacy while simultaneously providing a great deal of personal information through social media.« (Hargittai und Marwick 2016: 3737) Bei Norberg, Horne und Horne heißt es: das Paradox betreffe die »discrepancy between individuals' intentions to protect their own privacy and how they behave in the marketplace.« (Norberg, Horne und Horne 2007: 100) Und um noch einen letzten zu zitieren: »Although survey results show that the privacy of their personal data is an important issue for online users worldwide, most users rarely make an effort to protect this data actively and often even give it away voluntarily.« (Gerber, Gerber und Volkamer 2018: 226)

Paradoxal ist dies deshalb, weil den eigenen Überzeugungen – dass Privatheit wichtig sei – mit dem eigenen Verhalten widersprochen wird: freiwillig wird viel Privates auf den sozialen Medien geposted. Eine der ersten, die dies feststellt, ist Helen Nissenbaum in ihrem 2010 erschienenen Buch. Hier verweist sie auf Forschungen, die deutlich machen, dass Benutzer_innen häufig in keiner Weise klar ist, was eigentlich mit ihren Daten passiert und was der Schutz von Privatheit bedeutet:[1] »Another survey, published in 2005, indicated persistent ignorance: a significant majority of the respondents believed that the presence of a privacy policy on a Website means that the company cannot sell customers' information (75 percent).« (Nissenbaum

1 Vgl. Nissenbaum (2010: 103 ff.) zum Problem des Paradoxes im Zusammenhang mit dem was sie »media exhibitionism« nennt; vgl. auch die hilfreiche Übersicht über verschiedene Positionen bei (Kokolakis 2017).

2010: 106) Schon Nissenbaum weist darauf hin, dass man hier deshalb von einem absichtlich produzierten Paradox reden müsse, weil die *privacy policies*, die die Unternehmen auf ihren Webseiten veröffentlichen, wissentlich so komplex und umständlich formuliert werden, um geradezu zu vermeiden, dass die Benutzer_innen verstehen, was tatsächlich mit ihren Daten passieren kann. Dies hat sich zwar seit 2018 mit der neuen Datenschutzgrundverordnung jedenfalls in Europa geändert, aber ein Problem bleibt es dennoch (vgl. Sloot, Hoofnagle und Zuiderveen Borgesius 2019).

Bleiben wir erst einmal bei diesem Blick auf das Paradox als eines, das im je individuellen Verhalten zu verorten ist, und schauen auf Erklärungsversuche dieses Paradoxes.[2] Nissenbaum nannte schon eine erste Erklärung mit dem Verweis auf die mangelnde Kenntnis der Bedeutung der Informationen über die Privatheitspolitik eines Unternehmens und generell einem *Informationsdefizit*, das zum Teil zu abwegigen Einschätzungen auf Seiten der Nutzer_innen führen kann (vgl. auch Acquisti und Gross 2006). Ein weiterer und zugleich der häufigste Erklärungsversuch ist der, den Gebraucher_innen zumindest eine gewisse Kenntnis zu unterstellen, was mit den Daten passiert und dann das entsprechende paradoxale Verhalten als schlicht widersprüchlich, *irrational* zu beschreiben. Behauptet eine Person einerseits, ihre Privatheit zu schätzen und auch zu wissen, was mit gegebenenfalls im Internet veröffentlichten Daten passiert, dann ist es, so diese Erklärung, schlicht irrational, dennoch private Daten – unnötig und großzügig – freizugeben. Hat demgegenüber eine Gebraucherin kein Bewusstsein von den Gefahren für ihre Privatheit und ist sich auch nicht im Klaren darüber, was es heißt, den jeweiligen *privacy policies* zuzustimmen, wie im ersten Fall, kann ihr Verhalten jedenfalls subjektiv nicht als irrational beschrieben werden.[3]

Eine weitere Erklärung bietet der sogenannte *privacy calculus*: Streng genommen ist es keine wirkliche Erklärung des Paradoxes, sondern eine Analyse des Verhaltens von Nutzer_innen, die ihnen rationale Berechnung beim Gebrauch des Internets unterstellt. Die Nutzer_innen verrechnen den Nutzen, den sie vom Gebrauch des Internets haben, gegen die Kosten, die sie mit

2 Übrigens will ich doch wenigstens kurz auf eine vordigitale Form des Paradoxes hinweisen: feministische Autorinnen haben schon in den 1960er und 1970er Jahren des letzten Jahrhunderts darauf verwiesen, dass im privaten Bereich häufig Gewaltverhältnisse herrschen, die durch den Ruf nach dem Schutz des Privaten gerade aufrechterhalten werden, obgleich dieser Ruf im Namen eines Privaten erfolgt, das sich als Rückzug und Schutz beschreibt. Vgl. hierzu die Übersicht in Rössler (2001).

3 Vgl. Kokolakis (2017) sehr hilfreich als Überblick über die verschiedenen Positionen, außerdem Dienlin und Trepte (2015); Barnes (2006); Nissenbaum (2010).

der möglichen Verletzung ihrer Privatheit bezahlen und nehmen deshalb in Kauf, dass sie gegebenenfalls Aspekte, Teile ihrer Privatheit abgeben müssen (vgl. Gerber, Gerber und Volkamer 2018; Barth und de Jong 2017).

Nun gibt es demgegenüber jedoch Ansätze, die nicht nur den kognitiven Zustand der Benutzer_innen erklären wollen, sondern eine solche Erklärung auf dem Hintergrund von allgemeineren sozialpsychologischen und gesellschaftskritischen Theorien verorten wollen. Das *framing* spielt dann die entscheidende Rolle: Der sozialtheoretische Hintergrund, mit Hilfe dessen das Internetverhalten analysiert wird, kann zu je unterschiedlichen Bewertungen oder Einschätzungen dieses Verhaltens führen. Ich werde diesen Hintergrund gleich noch genauer beschreiben, will für den Augenblick nur festhalten, dass Kategorien wie die der Frustration, Apathie, Resignation oder auch des Zynismus bei der Interpretation des Verhaltens von Internetgebraucher_innen sozialpsychologische und gesellschaftskritische Analysen voraussetzen, die diesen Einstellungen einen plausiblen Platz geben. Warum ist dies so? Weil die anderen Interpretationen (Informationsmangel, schlichte Inkonsistenz, Gewinnkalkül) plausibilisiert werden können durch einfache Verweise auf basale Logik (man kann nicht zugleich a und non-a glauben) und auf andere epistemische Probleme, wie etwa den Mangel an notwendigen Informationen. Interpretationshypothesen wie Resignation als sozialpsychologische Reaktion setzen jedoch komplexere Ursachen voraus, die als solche nur sichtbar werden, wenn die soziale Welt der Benutzer_innen genauer in den Blick rückt.[4]

Hier wird im Übrigen noch ein weiterer Aspekt der normativen Paradoxie deutlich: Denn das Paradox entsteht deshalb, weil etwa *privacy policies*, die eigentlich gerade eine Ermächtigung der Nutzer_innen bedeuten sollen, zu deutlich mehr resignativen Einstellungen führen. Gerade diese *policies* werden nämlich als zu überwältigend erfahren und erst durch sie wird allererst (jedenfalls ansatzweise) deutlich, wie viele und welche Daten gesammelt werden. So kann man leicht sehen, warum Nutzer_innen resignieren. Die Tatsache, dass mehr und mehr Daten gesammelt werden, auf die man letzt-

4 Vgl. wiederum Kokolakis (2017), zum Zynismus vgl. Hoffmann, Lutz und Ranzini (2016); Norberg, Horne und Horne (2007); zur *online apathy* vgl. Hargittai und Marwick (2016: 3751): »Our data suggest that the existence of fatigue surrounding online privacy and the simultaneous presence of concern over privacy and widespread self-disclosure is not necessarily paradoxical, but rather a pragmatic response to the contemporary networked social environment.«

lich keinen Zugriff hat, lässt den Schutz dieser Daten immer unwahrscheinlicher erscheinen.

Was bedeutet Überwachung?

Es ist die vollkommene Überwachung aller Lebensbereiche, die beschrieben und analysiert werden muss, will man das Privatheitsparadox selbst ebenso wie die verschiedenen Erklärungsversuche verstehen. Dabei halte ich es für sinnvoll, hier mit David Lyons von »Überwachungskulturen« zu sprechen, weil die Überwachung mittlerweile tatsächlich Teil unserer normalen Alltagskultur geworden ist. Überwachung kann dabei auch als Beobachtung verstanden werden, denn es sind keine im eigentlichen Sinn »strafenden« Instanzen, die hinter der Überwachung stehen, sondern vor allem Unternehmen, die am Sammeln der Daten interessiert sind – obwohl sie faktisch natürlich sehr wohl einen solchen Schaden zufügen.[5]

Ich will kurz auf drei Merkmale dieser Überwachungskulturen genauer eingehen: auf die exponentielle Zunahme von Datensammlungen, das Phänomen der *Big Data*; auf die Entgrenzung des gewohnten »offline«-Lebens gegenüber dem »online«-Leben, also auf die völlige Durchdringung von Digitalität und Alltagsleben; und schließlich auf den vollkommenen Kontrollverlust über unsere Daten und darüber, was uns eigentlich im Netz gezeigt wird.

In unserer Überwachungsgesellschaft wird alles, was wir tun, beobachtet und verfolgt. Das wissen wir mittlerweile alle und leben damit, niemand ist in Gesprächen über die Sammlung, Weitergabe oder den Verkauf von Daten noch überrascht. Meinungen gehen nur darüber auseinander, wie gefährlich diese Datensammlungen und ihre Verwendung sind. Bekanntlich ist es die Theorie von Michel Foucault und deren Tradition, die die moderne Gesellschaft als Überwachungsgesellschaft beschrieben und analysiert hat, und damit das theoretische Instrumentarium bereitstellt, auch die digitale Überwachung zu beschreiben. Es ist nicht mehr länger (nur) der Staat oder einzelne genau festmachbare Institutionen, die die Überwachung ausführen, die Überwachung hat sich vielmehr vervielfältigt, pluralisiert und quantifiziert:

5 *Wie* ihnen geschadet wird, ist nicht Thema dieses Artikels, vgl. zur Manipulation und Ausbeutung etwa Susser, Rössler und Nissenbaum (2019); auch Zuboff (2018).

In einem unvorstellbaren Ausmaß werden Nutzer_innen von den großen Internetbetrieben kontrolliert und verfolgt (vgl. Paul 2020; Haggerty and Ericson 2000). Häufig stützen sich deshalb Analysen der Überwachungsgesellschaft in den sogenannten *surveillance studies* auf das Werk von Gilles Deleuzes Konzeptionen von Kontrolle mit dem Begriff der *assemblage*, um die Vervielfältigung der Mechanismen der Überwachung zu beschreiben (vgl. Haggerty und Ericson 2000). Interessant für die Überwachungstheorie und -kultur ist, dass diese »Assemblagen« Bestandteile eines allgemeinen Ganzen sind, in diesem Fall: der Überwachungskultur, und dass die Beziehungen zwischen diesen Teilen nicht stabil und fest sind, sondern innerhalb und zwischen anderen Instanzen verschoben und ersetzt werden können. So können die verschiedenen Unternehmen, staatlichen Institutionen oder selbst Personen, die uns auf sehr unterschiedliche Weise überwachen, addiert und zusammengestellt werden, um die Überwachung zu intensivieren, obwohl sie nicht in institutionalisierten (geschweige denn transparenten) Beziehungen zueinanderstehen.[6]

Mit der Produktion dieser überwältigenden Masse an Daten geht einher, dass Nutzer_innen nicht mehr in der Lage sind, eine klare Grenze zwischen dem Alltag mit und dem ohne Digitalität zu ziehen. Auch bei scheinbar nicht-digitalen Aktivitäten – wie einem Spaziergang, einem Gespräch im Café – ist die Digitalisierung präsent (das Handy zählt die Schritte und lokalisiert uns; während des Gespräches werden kurz die sozialen Medien gecheckt). Diese Entgrenzung des digitalen Alltags, in dem wir nicht nur kein Interesse mehr an einer Grenzziehung haben, sondern uns diese auch strukturell schwergemacht, oder verunmöglicht wird, ist mittlerweile selbstverständlicher Teil unserer Überwachungskultur. Das Sozialleben, das vor allem bei jungen Erwachsenen zu einem großen Teil in den sozialen Medien stattfindet, verändert sich ebenso wie der Arbeitsplatz (vgl. Dijck, Poell und de Waal 2018); das zeigt sich während der COVID-19-Epidemie ganz besonders deutlich. Hier wurden rasend schnell Arbeitsplätze digitalisiert, bei denen man das vorher nie für möglich gehalten hätte, wie zum Beispiel praktisch alle Arbeitsplätze im Unterrichtswesen. Welche Unmengen von Daten hier Betriebe wie Zoom, Teams und andere sammeln, ist kaum mehr vorstellbar, trotz aufrichtiger Versuche, gerade Student_innen und Schüler_innen vor Eingriffen ins Private zu schützen. Doch es geht nicht allein um den Schutz

6 Vgl. Lyon (2018: 57 ff.). Der letzte Schritt in diesen Überwachungsanalysen wird von Shoshana Zuboffs Projekt des Überwachungskapitalismus unternommen, in ihrem monumentalen Werk Zuboff (2018).

des Privaten, sondern darum, dass in der Überwachungsgesellschaft nach und nach alle täglichen Praktiken digitalisiert und damit beobachtbar, kontrollierbar, messbar werden.

Warum diese Entgrenzung problematisch ist, zeigt sich auch anhand des dritten Aspekts, auf den ich eingehen möchte: Es ist nicht nur ein Gefühl, dass uns die Kontrolle über die Daten mehr und mehr entgleitet, sondern es ist die Realität. Das betrifft die gerade beschriebenen Praktiken, es betrifft auch die rechtliche Kontrolle und die Eingriffe in und Verwendung von Daten durch andere ohne demokratisch legitimierte Prozeduren. Der Schutz persönlicher Daten ist zwar in der europäischen Gesetzgebung recht weitgehend gewährleistet, doch dieser Datenschutz reicht nicht oder nur sehr begrenzt bis zu den Firmen, die ihren Sitz in den USA haben (vgl. Sloot, Hoofnagle und Zuiderveen Borgesius 2019). Als Beispiel für diesen Kontrollverlust kann man etwa die weitestgehend personalisierte Kommunikation (sogenannte *filter bubbles*, vgl. mittlerweile klassisch Pariser 2011) nennen, die etwa dafür sorgt, dass wir nur vorsortierte Nachrichten empfangen; ein weiteres Beispiel ist die gezielte personalisierte Werbung, mit der Nutzer_innen in den sozialen Medien konfrontiert werden (vgl. Pasquale 2015; Zuiderveen Borgesius 2015; Calo 2014).

Doch die genannten Beispiele für den Kontrollverlust über Daten in der Überwachungsgesellschaft müssen ergänzt werden mit solchen aus der Erste-Person-Perspektive: mit Beispielen der *Selbst-Überwachung*. Denn in den sozialen Medien geben Personen enorme Datenberge, Informationen preis, »teilen« ihre Daten mit endlos vielen anderen Personen, aber – und das ist viel problematischer – nicht nur mit Personen, sondern mit den großen Technologieunternehmen. Das betrifft nicht nur jedes »like«, das Nutzer_innen vergeben und das selbstverständlich registriert wird, es betrifft auch beispielsweise die gerade genannten Health apps, vor allem Fitness apps. Verwendet man diese apps so wie es empfohlen wird, dann werden die gespeicherten Daten – in Echtzeit – nicht nur gegebenenfalls mit anderen Personen geteilt, sondern mit den Unternehmen und direkt wiederverwendet, um die Person zu motivieren, weiter an ihrem Programm zu arbeiten und dabei vor allem dazu zu motivieren, in der app zu bleiben und weitere Daten zu produzieren.[7] Dieser Form der Datensammlung und Manipulation setzen Nutzer_innen sich zumeist unwissentlich aus, so wie auch das Sammeln von Daten auf Instagram, Facebook usf. häufig geschieht, ohne

7 Vgl. Yeung (2017) und ihre Analyse des »Hypernudging«; Marijn Sax analysiert diesen Mechanismus anhand der sogenannten Health apps (vgl. Sax 2020).

dass den Nutzer_innen bewusst ist, dass ihre Daten gesammelt und wiederverwendet werden.[8] Die sozialen Medien tragen ganz entscheidend zur Überwachungskultur bei.

Es gibt keine natürliche Grenze zwischen dem Privaten und dem Öffentlichen

Das Teilen von privaten und intimen Details aus dem eigenen Leben in den sozialen Medien, ebenso wie das gesamte Internetverhalten (was wird angeklickt usf.), ist konstitutiv für die Überwachungskultur; doch ebenso konstitutiv ist ein Aspekt, der in diesem Kontext häufig übersehen wird. Denn es ist Teil dieser Kultur, dass der Grenzverlauf zwischen privat und öffentlich ganz unklar ist.

Eine wichtige Rolle spielt bei der Erklärung des Paradoxes nämlich die Tatsache, dass die Grenzen des Privaten – und damit auch die Grenzen der Datenproduktion – gar nicht einzuhalten sind, weil und wenn es keine wirkliche Grenze gibt, die uns immer wieder sagen würde, was gesagt oder nicht gesagt, geteilt oder nicht geteilt werden kann. Wenn also junge Erwachsene in den sozialen Netzwerken Erlebnisse oder Meinungen veröffentlichen, Webseiten besuchen oder »liken«, die anderen als zu privat oder intim erscheinen, und wenn sie doch am Wert des Privaten festhalten wollen, dann ist dies nicht einfach nur paradoxal, sondern auch Ausdruck der prekären Grenze zwischen dem Privaten und dem Öffentlichen.

Dass diese Grenze prekär ist, wird jedoch beispielsweise von Thomas Nagel bestritten; und neuerdings auch wieder von Eric Barendt, wenn er argumentiert: »Some topics are just off-limits for general discussion in any mature society.« (Barendt 2020: 17) Oder auch wenn er schreibt: »A society in which privacy is valued, necessarily excludes from general discussion a range of personal reflections, feelings, and experiences – individuals' sexual fantasies and desires, their judgments of their friends and (to some extent) colleagues, their medical history and appointments, and intimate relationships.« (Ba-

8 Vgl. zum Kontrollverlust auch Hargattai und Marwick (2016: 3737): »However, they feel that once information is shared, it is ultimately out of their control. They attribute this to the opaque practices of institutions, the technological affordances of social media, and the concept of networked privacy, which acknowledges that individuals exist in social contexts where others can and do violate their privacy.«

rendt 2020: 8) Man kann hier Barendt sicherlich zustimmen, wenn es um die Privatheit *anderer* geht, also um die Forderung nach Respekt vor den privaten Angelegenheiten anderer Personen. Doch Barendt geht, im Anschluss an Nagel, viel weiter: es geht ihm nämlich um den *prinzipiellen Ausschluss* bestimmter Themen aus der öffentlichen Diskussion (vgl. Nagel 1998). Eine »reife« oder »erwachsene« Gesellschaft muss wissen, wo die Grenze liegt – eine solche Position kann gerade nicht verstehen oder konzeptualisieren, warum bestimmte Thematisierungen privater Angelegenheiten durchaus emanzipatorisch und befreiend sein können. Hier kann man zum Beispiel auf die enttabuisierenden Filme verweisen, die die jungen feministischen Publizistinnen Hannah Witton oder Ashley Mardell ins Netz stellen und die endlos kommentiert werden. Sie führen die zahllosen Möglichkeiten vor Augen, solche Internetforen für befreiende kulturelle, soziale, politische Ziele zu benutzen. Menstruation, sexuelle Phantasien und Bedürfnisse, oder auch Homosexualität bei jungen Menschen – all dies sind Tabuthemen, die für junge Erwachsene sehr wichtig und problematisch sein können und die deshalb gerade eine öffentliche Arena brauchen, um freier diskutiert werden zu können. danah boyd zitiert in ihren Interviews mit jungen Erwachsenen eine junge Frau, die erklärt: »I just think that [technology is] redefining what's acceptable for people to put out about themselves. I've grown up with technology, so I don't know how it was before this boom of social networking.« (boyd 2015: 61)

Dies ist eine andere Version der Begründung des Paradoxes: Personen wollen auf der einen Seite an der eigenen Privatheit festhalten, und finden dies auch außerordentlich wichtig für ihr eigenes Leben, zugleich jedoch ist unklar, individuell *und* sozial, wo eigentlich genau Privatheit missachtet, eine Grenze überschritten wird.[9]

Zurück zum Privatheitsparadox: Wie erklärt man es am besten?

Kommen wir auf diesem Hintergrund nun zurück zum Privatheitsparadox: Man muss, so denke ich, eingestehen, dass die Praktiken der großen Techno-

9 Vgl. Rusty (2019): »For many teenagers and adults, not actively using these big tech platforms would create the eerie sensation that you don't exist. And that's a real problem. We invest so much of our identities in platforms that see us as data points to be studied & marketed. The crux here is the user's lack of control.«

logieunternehmen es ziemlich unwahrscheinlich – praktisch unmöglich – machen, dass die rationale Abwägung gemäß dem *privacy calculus* tatsächlich effektiv sein kann. Es scheint sehr zweifelhaft, dass man *rationalerweise* der Sammlung und Auswertung extrem vieler persönlicher Daten zustimmen könne, um die Freuden des Konsums und der Sozialität auf den sozialen Platforms genießen zu können, schon weil man gar nicht absehen kann, welche Daten genau gesammelt werden (vgl. hierzu vor allem Zuboff 2018). Eine angemessenere Erklärung des Privatheitsparadoxes ist dann eher, dass Personen tatsächlich aus mangelnder Kenntnis heraus handeln und ihnen nicht klar ist, was mit ihren Daten passiert und was »privacy policies« eigentlich bedeuten. Solche »privacy policies« führen, das ist empirisch durchaus nachweisbar, zu mehr Unsicherheit und zu mehr Missverständnissen darüber, was mit den eigenen Daten passiert.[10] Es ist sicherlich verständlich, dass Personen sich häufig der Gefahren nicht bewusst sind, die mit dem »Posten« privater Mitteilungen, generell mit dem Verhalten im Internet, hinsichtlich der Sammlung von Daten und deren nicht kontrollierbarer Weitergabe verbunden sind.

Wenn sie sich jedoch der Gefahren bewusst sind, dann sehen die Nutzer_innen es als aussichtslos an, sich tatsächlich gegen die Überwachung schützen zu können. Deshalb scheint es plausibel, Resignation oder auch Frustration, Zynismus, Apathie als Reaktionen auf die *Big Data* und den damit einhergehenden Kontrollverlust zu beschreiben. Ich werde im Folgenden vor allem den Begriff der Resignation verwenden, denke aber, dass die Differenzen zwischen Apathie, Frustration, Zynismus und Resignation als psychische und mentale Haltung gegenüber dem Kontrollverlust beim Schutz der eigenen Daten vernachlässigbar sind.[11]

Resignation als Haltung gründet sich auf die Einschätzung der eigenen Handlungsmöglichkeiten im Blick auf das Erreichen eines möglichen Ziels. Man akzeptiert eine bestimmte Situation ausschließlich deshalb, weil man denkt, diese Situation nicht ändern zu können, selbst wenn man mit dieser Situation außerordentlich unzufrieden ist. Hier schließt sich der Begriff der *digitalen* Resignation an, wie Draper und Turow schreiben: »Mit digitaler Re-

10 Vgl. Nissenbaum (2010); Martin und Nissenbaum (2016).

11 Vgl. zum Zynismus etwa Hoffmann, Lutz und Ranzini (2016: 1): »Complementing these perspectives, we propose that some users faced with seemingly overwhelming privacy threats develop an attitude of ›privacy cynicism‹, leading to a resigned neglect of protection behavior. Privacy cynicism serves as a cognitive coping mechanism, allowing users to rationalize taking advantage of online services despite serious privacy concerns.« Vgl. auch Gerber, Gerber und Volkamer (2018); Hargittai und Marwick (2016).

signation meinen wir den Zustand, in dem Personen Kontrolle darüber haben wollen, was ›digitale Entitäten‹ über sie wissen, aber fühlen, dass sie unfähig sind, solche Kontrolle zu erlangen. [...] [Es handelt sich um eine] häufig unbemerkte Beschreibung dessen, wie Amerikaner im 21. Jahrhundert ihre sozialen Einflussmöglichkeiten einschätzen.« (Draper und Turow 2019: 1)

Wenn Resignation als Haltung gegenüber den eigenen Handlungsmöglichkeiten verstanden wird, dann bedeutet dies im Blick auf das Internet, dass es sinnlos scheint, sich gegen das Sammeln und Verwerten von Daten, gegen die Strukturen der Überwachungskultur wehren zu wollen. Schon Draper und Turow verwiesen darauf, dass die Überwachung der Nutzer_innen dann unübersehbar und unentrinnbar wird, wenn es nicht mehr um inzidentelles Sammeln von Daten geht, sondern um die ökonomische Struktur der Datensammlung und -verwertung selbst. Wie stark die Überwachungskultur in das alltägliche Leben der Nutzer_innen eingreift, haben wir oben schon gesehen. Jetzt wird deutlich, wie das Privatheitsparadox mit Hilfe der Analyse der Überwachungskultur und der Haltung der Resignation erklärt werden kann: denn es scheint nicht unvernünftig, sondern vielleicht gerade die angemessene realistische Haltung, angesichts der Unmöglichkeit der Kontrolle der eigenen Daten zu resignieren.[12]

Resignation als Haltung entsteht, wenn man den zutreffenden Eindruck hat, bestehende Machtverhältnisse nicht beeinflussen, nicht ändern zu können: Die Genese dieser Haltung liegt folglich in den gänzlich asymmetrischen und intransparenten Machtverhältnissen der Technologiebetriebe und ihrer Praktiken. Strukturen der Ungleichheit können nämlich genau dann zu resignativen, auch *politisch*-resignativen Haltungen führen, wenn ungleiche Machtverhältnisse so eindeutig sind, dass man sich ihrer mühelos bewusst werden kann.[13] Auch dies gehört zur Genese der Resignation: die Einsicht in die Existenz der Machtasymmetrie. Deshalb ist die Kontextualisierung

12 Hier muss man natürlich auf Adorno verweisen: »Uns älteren Repräsentanten dessen, wofür der Name Frankfurter Schule sich eingebürgert hat, wird neuerdings gern der Vorwurf der Resignation gemacht. Wir hätten zwar Elemente einer kritischen Theorie der Gesellschaft entwickelt, wären aber nicht bereit, daraus die praktischen Konsequenzen zu ziehen. Weder hätten wir Aktionsprogramme gegeben noch gar Aktionen solcher, die durch die kritische Theorie angeregt sich fühlen, unterstützt.« (Adorno 1971: 145) Resignation hat hier bei Adorno einen leicht anderen Ton: Denn der Vorwurf ist, dass keine Aktion erfolgt, obgleich klar ist, was Aktion bedeuten würde. Bekanntlich wehrt sich Adorno hiergegen mit dem Verweis auf die intellektuelle Arbeitsteilung. Digitale Resignation ist demgegenüber noch fundamentaler, weil noch nicht einmal klar ist, was Aktion hier genau bedeuten würde.

13 Vgl. in diesem Sinn Draper und Turow (2019: 1829 ff.); vgl. auch Benson und Kirsch (2010).

des Privatheitsparadoxes in der Überwachungsgesellschaft auch so wichtig für seine Erklärung: Die asymmetrischen Machtstrukturen der Überwachungsgesellschaft machen die digitale Resignation ebenso möglich wie plausibel.

In einer großen Studie zur amerikanischen Tabak- und Bergbauindustrie haben Benson und Kirsch darauf hingewiesen, dass kapitalistische Systeme davon profitieren, Resignation als eine Strategie zu produzieren und zu benutzen, eine Strategie, die Protest und politische Aktion neutralisieren kann. Man kann in diesem Sinn auch die digitale Resignation begreifen; ähnlich jedoch wie bei der kritischen Analyse von gezielter Manipulation von Benutzer_innen durch die Technologiefirmen, könnte man auch in diesem Fall einwenden, dass unklar ist, ob man eine solche intentionale, bewusste Strategie dann ausmachen und prüfen kann, wenn es sich schlicht um das legale Geschäftsmodell der Betriebe handelt.[14]

Was kann man aus diesen kurzen Bemerkungen folgern? Wenn man die Auflösung des Privatheitsparadoxes in dem radikalen Sinn anstrebt, dass sich Nutzer_innen letztlich nicht mehr zu entscheiden bräuchten, ob sie entweder das Internet benutzen und damit ihre Privatheit aufgeben oder ihr Leben offline verbringen wollen, dann muss es darum gehen, die Machtverhältnisse und den immensen Einfluss der Internetbetriebe zu kritisieren und zu begrenzen. In genau diese Richtung gehen auch die Überlegungen sowohl in der EU wie in den Vereinigten Staaten im Blick auf die Frage, wie digitale Märkte begrenzt und reguliert werden können.[15]

Zum Schluss

Es ist nicht völlig unverständlich, so haben wir gesehen, sich im Blick auf den Schutz und den Wert der eigenen Privatheit paradoxal zu verhalten – die Überwachungsgesellschaft und -kultur ist überwältigend und die je individuellen Möglichkeiten, sich dieser zu entziehen, praktisch so gut wie gar

14 Vgl. wiederum Susser, Rössler und Nissenbaum (2019); auch bei der Analyse der Strategien der Internetunternehmen halte ich Zuboff (2018) für besonders hilfreich, wenn auch ihre Theorie des Überwachungskapitalismus umstritten ist.

15 Benson und Kirsch (2010: 475) beispielsweise sind optimistischer: »Amidst a politics of resignation, we need a new starting point. How do we unlock the folded arms of cynicism? […] Widespread dissatisfaction with corporate practices represents an important starting point for social change.«

nicht gegeben. Politisch und ökonomisch begriffen scheinen individuelle Fluchtversuche jedenfalls prima facie sinnlos im Blick auf die Änderung des Systems als solchem; und sie sind insbesondere mit enormen persönlichen Einschränkungen im Blick auf Sozialität, Informationen und Unterhaltung mit Hilfe des Internets verbunden.

Sozialkritisch betrachtet sind diese Formen von Paradoxien auch aus anderen Kontexten bekannt: etwa im Blick auf den Klimaschutz. Vergleichbar ist dies deshalb, weil wir auch hier Inkonsistenzen zwischen Überzeugungen und Verhalten begegnen, die häufig mit denselben Äußerungen von Resignation einhergehen wie die, die ich oben beschrieben habe. Man könnte einwenden, dass es in anderen Hinsichten nicht vergleichbar sei: denn beim Klimaschutz nützt jede kleinste Verhaltensänderung auch auf individuellem Niveau, während dies beim Internetgebrauch nicht der Fall sei.

Aber stimmt das? Denn man kann natürlich auf der einen Seite an die Politik und Gesetzgeber_innen appellieren, die Machtverhältnisse zu ändern, die Macht der *Big Five* zu begrenzen und das Internet jedenfalls in seinen grundlegenden Hinsichten zu einem *public good* zu machen. Das heißt aber nicht, dass andererseits nicht auch individuelles kritisches Verhalten gegebenenfalls – überraschend – zum Erfolg führen kann. Erinnert sich noch jemand an das Projekt »google glasses«? Im Jahr 2013 war es der große Hit, doch google hatte die Nutzer_innen überschätzt:[16] Diese Brillen waren in ihrer potentiellen Verletzung der Privatsphäre zu gefährlich und wurden nicht akzeptiert, weder gesellschaftlich und politisch noch von den Nutzer_innen. Die Macht und die Einflussmöglichkeiten der Konzerne hat folglich offenbar noch Grenzen – und auch die Datenschutzgrundverordnung der EU aus dem Jahre 2018 kann zur Ermächtigung der Bürger_innen jedenfalls beitragen. Die genaue Kritik der Machtverhältnisse, verbunden mit der Forderung nach Transparenz, bleibt der erste Schritt.

Literatur

Acquisti, Alessandro und Ralph Gross 2006: Imagined Communities. Awareness, Information Sharing, and Privacy on the Facebook, in: Lecture Notes in Computer Science 4258, 36–58.

16 Vgl. etwa ‹https://medium.com/nyc-design/the-assumptions-that-led-to-failures-of-google-glass-8b40a07cfa1e›; vgl. auch Kudina und Verbeek (2019).

Adorno, Theodor, W. 1971: Resignation, in: Kritik. Kleine Schriften zur Gesellschaft. Frankfurt a. M.: Suhrkamp, 145–150.

Barendt, Eric, 2013: Privacy, Anonymity and Public Discourse. Faculty of Laws, University College London (unveröffentlichtes Manuskript).

Barnes, Susan B. 2006: A Privacy Paradox. Social Networking in the United States, in: First Monday 11. 9.

Barth, Susanne und Menno D. T. de Jong 2017: The Privacy Paradox. Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior. A Systematic Literature Review, in: Telematics and Informatics 34, 1038–1058.

Benson, Peter und Stuart Kirsch 2010: Capitalism and the Politics of Resignation, in: Current Anthropology 51. 4, 459–486.

boyd, danah 2015: It's Complicated. The Social Lives of Networked Teens. London: Yale University Press.

Calo, Ryan 2014: Digital Market Manipulation, in: The George Washington Law Review 82. 4, 995–1051.

Dienlin, Tobias und Sabine Trepte 2015: Is the Privacy Paradox a Relic of the Past? An In-Depth Analysis of Privacy Attitudes and Privacy Behaviors, in: European Journal of Social Psychology 45, 285–297.

Dijck, José van, Thomas Poell und Martijn de Waal 2018: The Platform Society. Oxford: Oxford University Press.

Dommeyer, Curt und Barbara Gross 2003: What Consumers Know and What They Do. An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies, in: Journal of Interactive Marketing 17. 2, 34–51.

Draper, Nora A. und Joseph Turow 2019: The Corporate Cultivation of Digital Resignation, in: New Media & Society 21. 8, 1824–1839.

Gerber, Nina, Paul Gerber und Melanie Volkamer 2018: Explaining the Privacy Paradox. A Systematic Review of Literature Investigating Privacy Attitude and Behavior, in: Computers & Security 77, 226–261.

Haggerty, Kevin D. und Richard V. Ericson 2000: The Surveillant Assemblage, in: British Journal of Sociology 51. 4, 605–622.

Hargittai, Eszter und Alice Marwick 2016: »What Can I Really Do?« Explaining the Privacy Paradox with Online Apathy, in: International Journal of Communication 10, 3737–3757.

Hoffmann, Christian P., Christoph Lutz und Giulia Ranzini 2016: Privacy Cynicism. A New Approach to the Privacy Paradox, in: Cyberpsychology. Journal of Psychosocial Research on Cyberspace 10. 4, article 7.

Kokolakis, Spyros 2017: Privacy Attitudes and Privacy Behaviour. A Review of Current Research on the Privacy Paradox Phenomenon, in: Computers & Security 64, 122–134.

Kudina, Olya und Peter-Paul Verbeek 2019: Ethics from Within. Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy, in: Science, Technology & Human Values 44. 2, 291–314.

Lyon, David 2018: The Culture of Surveillance. Watching as a Way of Life. Cambridge: PolityPress.

Martin, Kirsten E. und Helen Nissenbaum 2016: Measuring Privacy. An Empirical Test Using Context to Expose Confounding Variables, in: Columbia Science and Technology Law Review 18. 1, 176–218.

Nagel, Thomas 1998: Concealment and Exposure, in: Philosophy & Public Affairs 27. 1, 3–30.

Nissenbaum, Helen 2010: Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books.

Norberg, Patricia A., Daniel R. Horne und David A. Horne 2007: The Privacy Paradox. Personal Information Disclosure Intentions versus Behaviors, in: The Journal of Consumer Affairs 41. 1, 100–126.

Pariser, Eli 2011: The Filter Bubble. What the Internet is Hiding from you. London: Verso.

Pasquale, Frank 2015: The Black Box Society. The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press.

Paul, Kali 2020: Congress Should Rein in Top US Tech Companies, Lawmakers' Inquiry Finds, in: The Guardian. ‹https://www.theguardian.com/technology/2020/oct/06/amazon-google-facebook-apple-antitrust-hearing›.

Rössler, Beate 2001: Der Wert des Privaten. Frankfurt a. M.: Suhrkamp.

Rusty 2019: Ride the Mastodon Out of the Walled Garden, in: S-Map the Social Media Alternatives Project. ‹https://www.socialmediaalternatives.org/?p=172›.

Sax, Marijn 2020: Between Empowerment and Manipulation. The Ethics and Regulation of For Profit Health Apps. Faculteit der Rechtsgeleerdheid, Universiteit van Amsterdam (unveröffenlichtes Manuskript).

Susser, Daniel, Beate Rössler und Helen Nissenbaum 2019: Technology, Autonomy, and Manipulation, in: Internet Policy Review 8. 2, 1–22.

Sloot, Bart van der, Chris Jay Hoofnagle und Frederik J. Zuiderveen Borgesius 2019: The European Union General Data Protection Regulation. What It Is and What It Means, in: Information & Communications Technology Law 28. 1, 65–98.

Yeung, Karen 2017: »Hypernudge«. Big Data as a Mode of Regulation by Design, in: Information, Communication & Society 20. 1, 118–136.

Yoon, Clara 2018: Assumptions That Led to the Failure of Google Glass ‹https://medium.com/nyc-design/the-assumptions-that-led-to-failures-of-google-glass-8b40a07cfa1e›.

Zuboff, Shoshana 2018: Das Zeitalter des Überwachungskapitalismus. Frankfurt a. M. und New York: Campus.

Zuiderveen Borgesius, Frederik 2015: Improving Privacy Protection in the Area of Behavioural Targeting. Alphen aan den Rijn: Kluwer Law International.